6

FEBRUAR 2026

MÅNEDENS SINGULARITET:

PROJECT CYBERSYN

INTERNETTET SOM DET KUNNE HAVE VÆRET - PROJECT CYBERSYN OG DET TABTE SPOR I DEN DIGITALE HISTORIE

AIPortalen.

Det seriøse medie om AI

AI BASICS:

DEL 4:

AI TJENESTER

I PRAKSIS

12 KATEGORIER, DER GIVER MENING FOR VIRKSOMHEDER

TEMA:

NÅR KRIG BLIVER KODE

AI TIL MILITÆRT BRUG

Indhold

LEDER: NÅR BESLUTNINGER FLYTTER SIG IND I SYSTEMER

Krig bliver ikke mere human af kunstig intelligens. Men den bliver hurtigere, mere kompleks – og sværere at holde ansvarlig.

Militær brug af AI handler sjældent om selvskydende robotter. Det handler om noget mere jordnært og mere afgørende: systemer, der sorterer information, prioriterer mål og anbefaler handlinger i et tempo, mennesker ikke kan matche alene. AI flytter ikke nødvendigvis aftrækkeren. Den flytter beslutningsgrundlaget.

Det er her, de største spørgsmål opstår. For når overvågning bliver til mål gennem algoritmer og scoringssystemer, ændres ikke bare den militære praksis, men også betingelserne for ansvar, folkeret og demokratisk kontrol.

Folkeretten er i princippet klar. Distinktion, proportionalitet og forholdsregler gælder uanset teknologi. Men reglerne forudsætter menneskelig vurdering, tid til at tænke og adgang til relevant information. Når beslutninger accelereres, og virkeligheden filtreres gennem systemer, bliver det sværere at se, hvem der faktisk vurderede hvad – og hvornår.

Derfor er det utilstrækkeligt blot at gentage, at "mennesket er i loopet". Menneskelig kontrol er ikke en position, men en praksis. Den kan være meningsfuld – eller symbolsk. Den kan styrkes gennem design, procedurer og efterprøvning. Eller den kan udhules af tempo, standardvalg og organisatorisk pres.

Det samme gælder demokratisk indsigt. Offentligheden kan ikke – og skal ikke – kende militære operationer i detaljer. Men det er rimeligt at kræve indsigt i rammerne: hvilke typer systemer bruges, hvordan godkendes de, hvordan logges beslutninger, og hvem fører uafhængigt tilsyn? Uden den viden bliver ansvar et efterrationaliseret begreb.

Danmark står ikke uden valg. Som indkøber, som NATO-medlem og som retsstat kan vi stille krav – ikke til teknologien som sådan, men til måden den anvendes på. Krav om logning, audit, hændelsesrapportering og reel mulighed for at sige nej. Krav, der ikke afslører operationer, men som gør ansvar muligt.

Militær AI er ikke et fremtidsscenarie. Det er en nutidig forvaltningsopgave. Spørgsmålet er ikke, om teknologien kommer til at spille en rolle i krig. Spørgsmålet er, om demokrati og ret følger med, når beslutninger flytter sig ind i systemer.

Det er dét spørgsmål, dette temanummer stiller.

Illustration genereret med ChatGPT

TEMA: NÅR KRIG BLIVER KODE

AI FLYTTER BESLUTNINGER TÆTTERE PÅ AFTRÆKKEREN

Af Mark Sinclair Fleeton

Militær AI bruges allerede til at sortere overvågningsdata, anbefale mål og optimere operationer. Spørgsmålet er ikke kun, om det virker – men hvem der har ansvaret, når "beslutningen" i praksis er formet af et system.

På skærmen dukker en markering op: høj sandsynlighed. Systemet har sorteret tusind signaler ned til fem. Et menneske skal godkende. Men hvad betyder "kontrol", når det vigtigste arbejde allerede er gjort af algoritmen?

Iben Yde, der rådgiver Forsvaret og forsvarsindustrien om ansvarlig militær AI i Rethink Advisory, peger på, at udfordringen handler om praksis – ikke om manglende regler.

"Problemerne opstår, fordi der ikke i samme grad er et direkte link mellem en menneskelig operatør og den endelige handling, når AI bruges som beslutningsstøtte," siger hun. *"Det er det link, der bliver sværere, og det er det, der gør ansvarsplacering juridisk problematisk."*

Hvad mener vi egentlig med "militær AI"?
Militær AI er et diffust begreb. I denne artikel giver det bedst mening at forstå teknologien som tre lag, der ofte blandes sammen i debatten: overvågning og efterretning (Intelligence, Surveillance and Reconnaissance - ISR), beslutningstøtte og autonome funktioner i og omkring våbensystemer. Fællesnævneren er sortering og mønstergenkendelse – og det er netop det, der gør AI anvendelig i militære sammenhænge.

I ISR bruges AI til at reducere informationskaos: objektgenkendelse i video og billeder, anomali-detektion, tekst- og signalanalyse, samt "fusion" af flere datakilder til situationsforståelse. Data kan komme fra droner, satellitter, sensorer som radar og IR – eller fra åbne kilder. Det lyder neutralt, men effekten er ikke neutral: Den menneskelige rolle bliver ofte at validere det, AI allerede har udvalgt. Dermed risikerer mennesket kun at se det, systemet fremhæver – og det, der ikke bliver valgt, kan forsvinde ud af beslutningsrummet.

Det næste lag er beslutningstøtte: systemer, der ikke "skyder", men anbefaler, prioriterer og scorer. Og det tredje lag er autonomi tæt på engagement: funktioner, der kan udføre dele af kæden fra mål til handling inden for rammer, som mennesker sætter på forhånd.

Det tredje – og måske mest skræmmende lag for mange – er autonome våben. Mange systemer har i dag ret store autonome kapaciteter, men fungerer semi-autonomt, hvor mennesket sætter rammerne – område, tidsvindue og måltype – men systemet udfører handlinger indenfor rammerne.

"*Problemet*," siger Jeppe Teglskov Jacobsen fra Nationalt Forsvarsteknologisk center (NFC), "*ligger i den midterste kategori. Den er lidt stor. Den kan gå fra at være ret ukontroversiel til at være sindssygt kontroversiel.*"

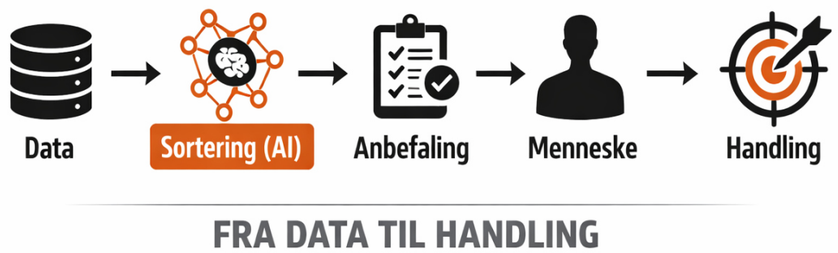


Illustration genereret med ChatGPT

Når overvågning bliver til mål
Det afgørende er, at lagene i praksis ofte kobles sammen i en pipeline fra data til handling. Og her kan der ske en glidning, som ikke føles dramatisk – men som ændrer ansvar og kontrol.

Når et AI-system sorterer enorme datamængder for afvigelser, mønstre og objekter, skaber det et udsnit af virkeligheden. Konsekvensen er ofte, at det, der ikke bliver udvalgt, ikke bliver set – mens det, der bliver flagget, føles vigtigere og mere presserende.

Først bliver et flag til et fund: "muligt militært køretøj", "mistænkelig aktivitet", "høj sandsynlighed". Og så sker der en normativ forskydning: Systemets output begynder at ligne en påstand om virkeligheden, ikke en hypotese. Flag bliver til fund.

Dernæst tager beslutningstøtten over: Den rangerer og scorer. Hvad er vigtigst? Hvad er mest tidskritisk? Hvad passer ind i et mønster? En rangliste af kandidater er i praksis en præ-sorteret målliste. Fund bliver til kandidater.

Til sidst bliver godkendelsen en del af en operationel rytme: hurtigere, mere standardiseret og mere afhængig af systemets scoring. Under tidspres kan den menneskelige godkendelse glide fra uafhængig vurdering til formalitet. Kandidater bliver til mål – og mål bliver til handling.

"De humanitære folkeretlige regler om angreb er teknologineutrale. De skal iagttages, uanset hvilken teknologi man bruger," forklarer Iben Yde. *"Det er ikke reglerne, der er nye. Det er måden, vi forsøger at efterleve dem på, der bliver udfordret."*

Det er her, "automation bias" bliver en konkret risiko: tendensen til at stole mere på systemet end på egen vurdering, især når der ikke er tid til at dobbelttjekke, og når output præsenteres uden tydelig usikkerhed.

"*Når det også bliver målidentifikation,*" siger Jeppe Teglskov Jacobsen, "*og kommer tættere på kamppladsen, så tages beslutningerne bare en lille smule hurtigere.*"

"*Jeg hørte fra Israel,*" fortæller han, "*at du har 20 sekunder til at vurdere omfanget af sårede. Du har givet en officer 20 sekunder til at verificere noget, som er fuldstændig umuligt at verificere på 20 sekunder. Det er der, den er gal.*"

"Fordi der ikke findes specifikke regler for autonome våbensystemer eller AI-baserede beslutningssystemer, bliver våbenscreening ekstremt vigtig som et safeguard mod ulovlige våben," forklarer Iben Yde.

"Menneskelig kontrol" – hvad betyder det i praksis?
I politikpapirer lyder menneskelig kontrol betryggende. Men kontrollen kan være mere eller mindre reel. Traditionelt taler man om tre modeller:

Human-in-the-loop: Systemet kan klassificere og anbefale, men kan ikke gennemføre den kritiske handling uden menneskelig godkendelse. Styrken er en tydelig "gate". Svagheden er, at godkendelsen kan blive et gummistempel, hvis operatøren kun ser AI's udsnit og er under tidspres.

Human-on-the-loop: Systemet kører løbende, mens et menneske overvåger og kan gribe ind. Styrken er, at det kan håndtere tempo og kompleksitet. Svagheden er åbenlys: hvis loopet er for hurtigt, bliver "overvågning" let symbolsk.

Human-out-of-the-loop: Systemet handler selv inden for rammer (område, tid, måltype), som mennesker har sat på forhånd. Fordelen er maksimalt tempo. Ulempen er, at den menneskelige kontrol primært ligger før hændelsen – og derfor bliver dokumentation og efterprøvning afgørende.

De tre labels siger dog ikke i sig selv, om kontrollen er reel. Derfor giver det mere mening at tale om meningsfuld menneskelig kontrol – og gøre det målbart. I praksis kan det oversættes til fem kriterier:
1. Operatøren har tid til at vurdere
2. Operatøren har information om usikkerhed og fejltyper
3. Operatøren kan afvise anbefalinger uden systemisk pres
4. Der findes logning og sporbarhed
5. Der er tilsyn og hændelsesrapportering

Med andre ord: Menneskelig kontrol handler ikke kun om, hvor et menneske er placeret i loopet – men om mennesket har tid, indsigt og handlekraft nok til, at ansvaret er reelt.

Hvem har ansvaret, når noget går galt?
I klassisk militær beslutningstagning kan man ofte pege på én beslutningstager. Når AI indgår i overvågning og beslutningstøtte, bliver det vanskeligere, fordi "beslutningen" i praksis er et resultat af en kæde fra data til model til interface til procedure til menneske til kommando.

"Det er netop i den kæde, at ansvaret kan begynde at flyde," siger Iben Yde. *"Når beslutningen i praksis er formet af systemer, bliver det vanskeligere at pege på én ansvarlig – også selv om der formelt har været et menneske involveret."*

Illustration genereret med ChatGPT

Operatøren er tættest på handlingen og har ansvar for at følge procedurer og vurdere output. Men operatøren ser ofte kun et udsnit, som systemet prioriterer – og hvis systemet ikke viser

usikkerhed, bliver det urimeligt at placere hele ansvaret nederst i kæden.

Kommandokæden har ansvaret for regler, thresholds, eskalation og kontrolpunkter – og for at organisere mennesker til at bruge systemet forsvarligt. Her kan man let pege på, at "der var et menneske i processen", selv om procedurerne i praksis presser mod hastighed og standardiseret godkendelse.

Staten, med Forsvarsministeriet i toppen, har det overordnede politiske og juridiske ansvar: folkeret, governance, tilsyn, indkøb og politisk kontrol. Men klassificering gør det let at sige, at man ikke kan oplyse noget – og multileverandørkæder gør det let at skubbe ansvar i retning af "tekniske forhold".

Leverandører og integratorer kan omvendt sige: "Kunden valgte opsætning og brugte systemet sådan." IP og forretningshemmeligheder kan begrænse indsigt. Resultatet kan blive ansvarsfiltrering: at hvert led kan fraskrive sig ansvar, fordi ingen formelt traf "den endelige beslutning".

Hvad siger reglerne – og hvorfor er de ikke nok?
Selv når AI bliver en del af beslutningskæden, ændrer det ikke det grundlæggende: International humanitær ret (International Humanitarian Law, IHL) gælder stadig. Men kravene er formuleret som principper, der skal omsættes til praksis – og AI kan gøre det sværere at dokumentere, at reglerne faktisk blev fulgt.

I Tillægsprotokol I til Genèvekonventionerne (Additional Protocol I, AP I) fastslår artikel 48 distinktionen mellem civile og militære mål, mens artikel 52(2) definerer militære mål. Proportionalitet er bl.a. udtrykt i AP I artikel 51(5)(b), og kravet om forholdsregler (precautions) findes i AP I artikel 57.

"Her har vi ikke en fysisk genstand, man kan måle og veje. Det er en måde at træffe beslutninger på – og hvordan måler man det?," spørger Iben Yde. *"Det er meget nemmere at teste et projektil i en gelatineblok end at afgøre, om en algoritme er god nok til at genkende mål på en dynamisk kampplads."*

AI udfordrer ikke reglerne i sig selv, men kan udfordre muligheden for at opfylde dem i praksis, hvis systemer filtrerer, prioriterer og accelererer beslutninger uden tydelig usikkerhed. Derfor bliver våbenreview centralt: AP I artikel 36 forpligter stater til at vurdere nye våben og metoder, så de kan bruges lovligt. Samtidig vokser "soft law" – NATO-principper, politiske erklæringer og FN-processer – men der findes stadig ingen global, bindende standard for, hvad "meningsfuld menneskelig kontrol" kræver i konkrete krav til logning, audit og tilsyn.

Demokratisk indsigt – hvad kan offentligheden med rimelighed kræve?
Når militære myndigheder siger, at detaljer må holdes hemmelige, er det ofte rimeligt. Men hemmeligholdelse bør ikke være det samme som fravær af demokratisk kontrol. Der findes et niveau af indsigt, som offentligheden kan kræve uden at afsløre operationer: ikke "hvor og hvornår", men hvilke typer systemer, hvilke beslutningsregler og hvilke kontrolmekanismer der gælder.

Det kan fx være indsigt i, hvilke kategorier af AI-systemer der bruges (ISR, beslutningstøtte, funktioner tæt på våbensystemer), hvilke godkendelsesprocedurer og stopklodser der findes, hvilke audit- og logkrav der gælder, og om der er uafhængigt tilsyn med adgang til fortrolige audits og hændelsesrapportering.

Når ansvaret forsvinder i systemet
Når AI flytter mere af krigens "forarbejde" ind i systemer, handler det ikke længere kun om at købe ny teknologi. Det handler om, hvorvidt et demokrati kan fastholde noget så basalt som ansvar: at man kan forklare, hvem der traf beslutningen, på hvilket grundlag, og hvilke forholdsregler der faktisk blev taget. For selv med et menneske i loopet kan kontrollen blive symbolsk, hvis systemet filtrerer virkeligheden, tempoet presser godkendelserne, og ansvaret splintrer mellem operatør, kommandokæde, stat og leverandører.

Iben Yde gør opmærksom på: *"Systemerne stopper ikke med at udvikle sig, når de tages i brug. Derfor er kontinuerlig test og evaluering helt afgørende."*

Den egentlige lakmusprøve er derfor enkel: Kan beslutninger efterprøves bagefter, kan ansvar placeres uden at gøre operatører til syndebukke, og kan offentligheden få et minimum af indsigt i rammerne – uden at operationer udleveres? Hvis ikke, er det ikke bare krig, der bliver kodet. Det er også ansvaret.

TEMA: NÅR KRIG BLIVER KODE

KONTROL I KÆDEN -FRA INDKØB TIL MÅL

Af Mark Sinclair Fleeton

Militær AI bliver ofte fortalt som et fremtidsscenarie: autonome systemer, maskiner der træffer beslutninger, krig "på autopilot". I praksis starter forandringen mere prosaisk. Den starter, når nye systemer bliver købt ind og koblet ind i hverdagen: software, der sorterer overvågningsdata, systemer der fusionerer flere datakilder, og beslutningsstøtte, der rangerer, hvad der bør have opmærksomhed først. Det er ikke nødvendigvis våbenautonomi – men det er teknologi, der kan flytte beslutninger tættere på handlingen.

Den demokratiske kerne er derfor ikke, om vi "tror" på AI. Det er, om nogen kan svare på tre spørgsmål, når det gælder liv-og-død-beslutninger: Hvem satte kravene? Hvem kontrollerer systemet? Og hvem kan efterprøve, hvad der skete bagefter?

Indkøb er styring, og drift er magt
Indkøb lyder teknisk, men for militær AI er det her, kontrollen enten bygges ind – eller forsvinder. Selve købet er sjældent den svære del. Den svære del kommer bagefter: integration og drift. For et AI-system står ikke alene. Det skal kobles ind i platforme, dataflows og procedurer, og det er ofte her, det får sin reelle magt: ved at bestemme, hvad operatøren ser først, hvad der markeres som relevant, og hvad der ender øverst i en prioriteringsliste.

Samtidig er AI ikke statisk. Systemer opdateres, patches, justeres og i nogle tilfælde re-trænes. Det betyder, at kontrol ikke kan være et engangstjek ved anskaffelse. Kontrol skal være en løbende disciplin – ellers risikerer man, at praksis langsomt glider, uden at nogen beslutter, at den skal glide.

Overvågning → prioritering → mål: den korte vej til beslutninger
Det politisk eksplosive er sjældent science fiction. Det er det hverdagsagtige: systemer, der sorterer enorme datamængder, giver en prioriteret liste og skubber beslutninger i en bestemt retning, længe før nogen formelt "trykker af". Når beslutningsstøtte bliver filter og rangering, kan den glide fra "hjælp" til "default". Og når default bliver norm, bliver afvigelse dyr: det kræver mere tid, mere argumentation og ofte højere godkendelse.

I praksis handler beslutningsstøtte ofte om tre funktioner: scoring (en sandsynlighed eller score), rangering (en prioriteret liste) og triage (en reduktion af store datamængder til "det, du bør kigge på nu"). Det lyder uskyldigt, men det kan være netop sådan, overvågning bliver til mål: ikke som ét spring, men som en kæde, hvor det bliver stadig sværere at se, hvornår mennesket reelt udøver uafhængig vurdering.

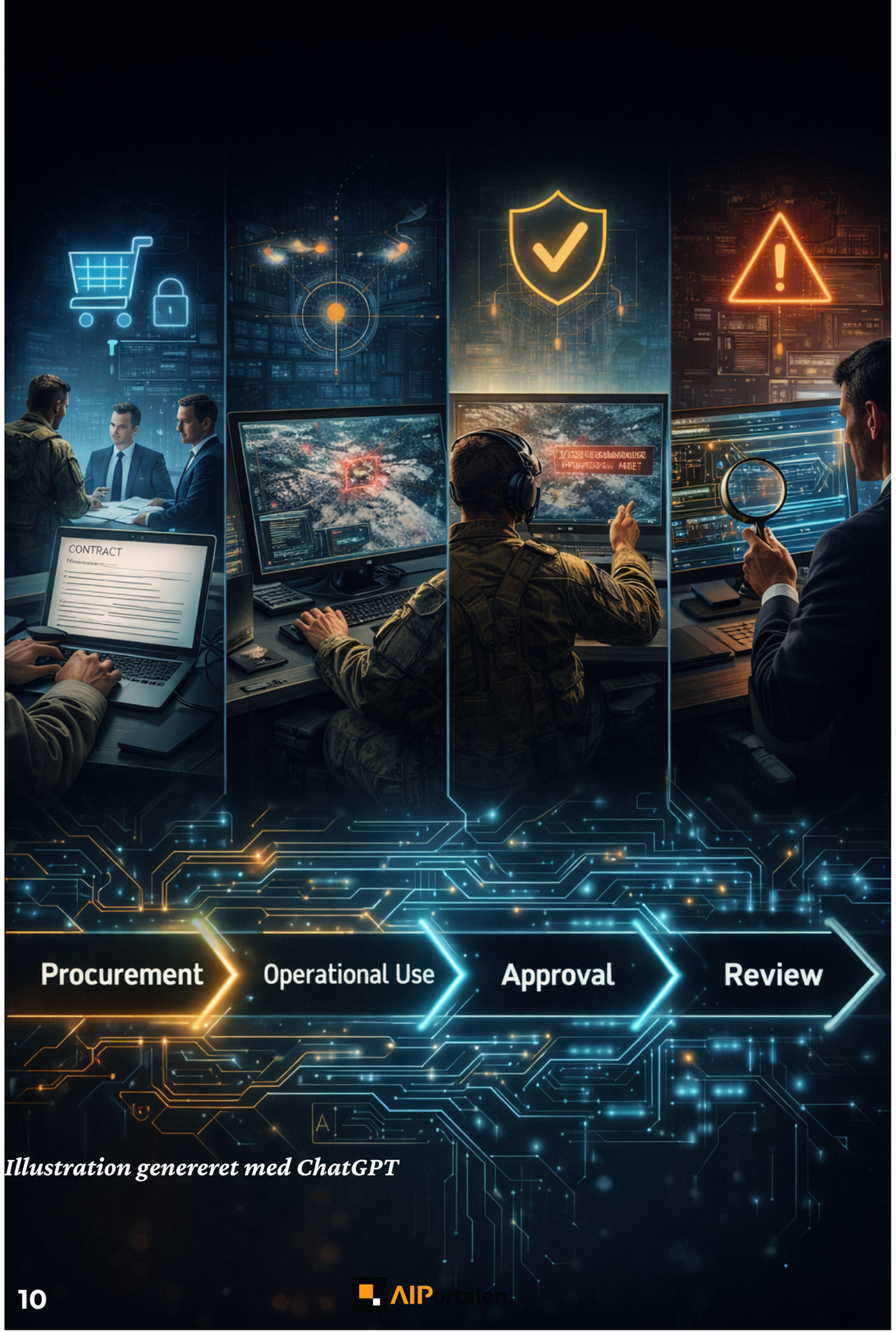


Illustration genereret med ChatGPT

Her opstår civil skade typisk ikke, fordi "AI vil skade civile", men fordi tre mekanismer kan forstærke hinanden: fejl og usikkerhed, der ikke bliver synlige; tempo, der gør menneskelig kontrol formel; og godkendelsesrutiner, der gør "mennesket i loopet" tyndt. Hvis output opleves som en konklusion i stedet for en hypotese, og hvis processen belønner hastighed, kan godkendelse blive et signaturled.

Menneskelig kontrol ligger i proceduren – ikke i ét klik

Det er derfor misvisende at tale om menneskelig kontrol som ét enkelt øjeblik. Kontrollen ligger fordelt i en procedure – i flere trin og roller. Første kontrolpunkt ligger ofte før operationen: i design og anskaffelse, hvor man beslutter, hvad systemet viser, om usikkerhed overhovedet synliggøres, og hvad der logges. Næste kontrolpunkt ligger i opsætning og procedurer: i kommandokæden og standardrutiner, der bestemmer, hvornår noget skal dobbelttjekkes, hvornår det skal eskaleres, og hvad det kræver at afvige. Tredje kontrolpunkt ligger i den konkrete beslutningssituation, hvor operatøren og nærmeste leder formelt "godkender" – men kun har reel kontrol, hvis der er tid, information og legitim mulighed for at sige nej. Fjerde kontrolpunkt ligger efter handlingen: i logning, efterprøvning og hændelsesrapportering.

Hvis et af disse trin mangler, kan systemet stadig se ud, som om der er kontrol. Men kontrollen kan være fragmenteret, og ansvaret kan ende med at lande hos den sidste person i kæden – netop der, hvor der er mindst mulighed for at ændre noget.

"Meaningful human control": målbart eller marketing?

Derfor er "human control" blevet et politisk nøgleord – og derfor bliver det også elastisk. Alle kan være enige om ordene, men uenige om tærsklen: Er kontrol, at nogen kan stoppe i tide? Eller er kontrol, at der "altid er en kommandokæde"? Hvis begrebet skal være mere end marketing, skal det kunne testes.

En praktisk måde at gøre det på er at kræve fem ting, der faktisk kan måles i design, procedurer og tilsyn:

1. Tid: Er der tid nok til vurdering – eller kun til godkendelse?
2. Information: Ser operatøren usikkerhed og fejltyper – eller kun en anbefaling?
3. Veto: Kan man afvise uden systemisk pres (tempo, kultur, KPI'er, eskalation)?
4. Logning: Kan beslutningen rekonstrueres bagefter – inklusive afvigelser?
5. Uafhængigt tilsyn: Findes der fortrolig efterprøvning og læring fra "near misses"?

Efterprøvning er demokratiets sikkerhedssele

I sidste ende handler det om efterprøvning: ikke om at offentligheden skal kende operationer, men om at demokratiet kan vide, om kontrollen er reel. Det kræver logning og sporbarhed, adgang til at revidere "den sorte boks" (også når leverandøren kalder det proprietært), og en læringssløjfe via hændelsesrapportering, så problemer opdages før de bliver til katastrofer. Uden den slags efterprøvning bliver ansvar et spørgsmål om forklaringer frem for dokumentation.

Det er også derfor, diskussionen om internationale normer og FN-processer går så trægt: stater kan ofte blive enige om principper, men tøver ved konkrete krav, der kan binde hænder og tempo. Alligevel peger udviklingen i normdebatten på, at "human control" kun bliver politisk holdbart, hvis det gøres operationelt – og dermed auditérbart.

Tre spørgsmål, der afslører om kontrollen findes
Hvis man vil skære det hele ned, er der tre spørgsmål, som enhver ansvarlig brug af militær AI bør kunne svare på – uden at afsløre taktiske detaljer:

- Kan vi efterprøve beslutningen bagefter? (Hvad viste systemet, og hvorfor handlede vi?)
- Hvem har helhedsansvaret? (Ikke bare komponentansvar, men ansvar for kæden)
- Hvem kan stoppe eller ændre praksis, når systemet glider? (Tilsyn, logs, læring – ikke bare tillid)

Militær AI bliver ofte solgt som effektivitet. Men i et demokrati er effektivitet ikke nok. Når systemer former beslutningsgrundlaget, skal vi kunne dokumentere, at kontrollen var reel – og at ansvaret ikke forsvandt i kæden, længe før beslutningen blev truffet.

Illustration genereret med ChatGPT

TEMA:NÅR KRIG BLIVER KODET

PALANTIR - DATA SOM BESLUTNINGSKRAFT

Af Mark Sinclair Fleeton

Palantir som virksomhed og de teknologier, som de arbejder med har sit udgangspunkt i terrorangrebet på New Yorks World Trade Center 11. september 2001 og den efterfølgende krig mod terror. 2010'erne var et årti, hvor Palantir for alvor blev en faktor som leverandør til militæret. Selskabets software blev taget i brug af det amerikanske militær under konflikterne i Mellemøsten – blandt andet til at forudsige placeringen af vejsidebomber (IEDs) i Afghanistan, hvor Palantirs analyser ifølge felt-rapporter overgik den amerikanske hærs egne systemer på området . Frontpersonel bemærkede, at Palantirs værktøj gav bedre støtte til at forudsige IED-trusler end hærens daværende standardplatform (Distributed Common Ground System – Army, DCGS-A) .

Palantirs militære AI-teknologier og anvendelser

Thiel beskrev i 2013 Palantir som en "missionsorienteret virksomhed", der ville anvende lignende software som PayPals bedrageri-detektion til at *"reducere terrorisme samtidig med at borgerrettigheder bevares"* . Palantir tilbyder i dag en række avancerede produkter og platforme, som anvendes bredt i militære sammenhænge. Fælles for dem er fokus på at sammenstille enorme datamængder fra disparate kilder og udnytte AI til at udlede brugbar indsigt til beslutningstagere. Nøgleprodukterne omfatter Gotham, Foundry, Artificial Intelligence Platform (AIP) og MetaConstellation – hver med sine specialiserede funktioner. Dertil kommer nyere initiativer som TITAN og Skykit, der understøtter feltenheder. Nedenfor beskrives disse teknologier og deres militære anvendelser:

Produktkataloget

Palantir sælger ikke våben. Palantir sælger software, der forbinder data, mennesker og beslutninger i militære organisationer: platforme der kan integrere data fra mange kilder, gøre dem søgbare og sammenhængende, og – i stigende grad – understøtte beslutninger med AI. Det er især attraktivt i moderne krigsførelse, hvor tempo og informationsmængde gør "situationsforståelse" til en kapacitet i sig selv.

Her er et overblik over de vigtigste Palantir-produkter og -løsninger, sådan som de typisk omtales i forsvars- og sikkerhedssammenhænge.

Gotham

Hvad er det? Palantirs klassiske platform til efterretning, analyse og operationel planlægning.
Hvad kan det militært? Samler data fra mange kilder (rapporter, sensorer, registre), gør dem søgbare og kobler relationer, så analytikere og stabe kan få et fælles billede.
Hvor i kæden? ISR/C2 – ofte "tidligt" i kæden, men kan bruges tættere på operationer afhængigt af opsætning.
Typiske krav/risici: Datakvalitet og adgangsstyring; risiko for "over-tillid" når systemet bliver den primære sandhedskilde.

Foundry

Hvad er det? En platform til data-integration og arbejdsprocesser, ofte brugt i større organisationer til drift, produktion og logistik.
Hvad kan det militært? Understøtter planlægning, forsyning, vedligeholdelse og optimering – og gør det muligt at arbejde på tværs af siloer.
Hvor i kæden? Drift og logistik (ofte "før" kamppladsen – men afgørende for kampkraft).
Typiske krav/risici: Governance og ansvar for data; sporbarhed når modeller og dashboards påvirker prioriteringer.

AIP (Artificial Intelligence Platform)
Hvad er det? Palantirs AI-lag, der bringer generativ AI og modelbaseret beslutningsstøtte ind i de eksisterende platforme.
Hvad kan det militært? Hurtig søgning og sammenfatning på tværs af interne data; forslag til handlemuligheder; "chat"-grænseflader, der gør komplekse datasæt mere tilgængelige for ikke-specialister.
Hvor i kæden? Beslutningsstøtte (AI-DSS) – typisk stabs- og planlægningsnært, men kan kobles tættere på operationer.
Typiske krav/risici: Usikkerhed og fejltyper skal vises; logning af prompts/output; risiko for "autoritetseffekt", hvor anbefalinger bliver default.

MetaConstellation
Hvad er det? En løsning til at koordinere og udnytte sensorer, satellit- og ISR-data i realtid.
Hvad kan det militært? Hurtigere indhentning, bedre overblik og mulighed for at "task'e" sensorer mere dynamisk – især relevant i konflikter med højt tempo og behov for løbende opdateret situationsbillede.
Hvor i kæden? ISR → C2, ofte tættere på operationel ledelse.
Typiske krav/risici: Stor afhængighed af datakilder og link-kvalitet; risiko for at tempo presser menneskelig kontrol, hvis output bruges direkte til prioritering.

TITAN (Army-program) / edge-løsninger
Hvad er det? Palantir er knyttet til løsninger, der bringer datafusion og analyse ud i feltet ("edge"), så beslutninger kan understøttes tættere på enheder og sensorer.
Hvad kan det militært? Reducerer ventetid mellem indhentning og handling; gør analyse mere operativ.
Hvor i kæden? C2/ISR i felten – typisk der, hvor tempo og friktion er størst.
Typiske krav/risici: Netop her bliver "meaningful human control" svær: tid, usikkerhed, veto, logning og efterprøvning skal være designet ind.

"AI-platform som økosystem" (integration med andre modeller og leverandører)
Hvad er det? Palantir positionerer sig som et lag, der kan integrere forskellige datakilder og i nogle tilfælde flere AI-modeller/leverandører i samme operative miljø.
Hvad kan det militært? Gør det muligt at skifte komponenter ud, koble nye datakilder på, og arbejde på tværs af værn og myndigheder.
Hvor i kæden? På tværs – fra drift til ISR og beslutningsstøtte.
Typiske krav/risici: Når systemet bliver "nervesystemet", bliver governance og audit helt centrale: hvem ændrer hvad, hvornår, og hvordan kan det kontrolleres?

Hvad er den fælles nævner?
Set som katalog er Palantirs kerne tilbuddet om at gøre data til beslutningskraft: først ved at samle og strukturere data, derefter ved at gøre dem operationelle gennem dashboards, arbejdsflows og AI-lag, der kan foreslå, prioritere og sammenfatte.

Netop derfor er kontrolspørgsmålet ikke kun teknisk, men organisatorisk: Når AI bliver en del af beslutningskæden, bliver krav til logning, audit, opdateringsdisciplin og menneskelig kontrol afgørende – ellers kan systemet ændre praksis, uden at nogen har besluttet, at praksis skal ændres.

Største kunde er USA
Palantir er leverandør til kunder på det militære område på globalt plan, men den største kunde er USA. Palantir har arbejdet for praktisk talt alle grene af det amerikanske militær og forsvar. I nyere tid – særligt fra slut-2010'erne og frem – har Palantir indgået milliardaftaler med Pentagon. Et skelsættende eksempel var, da Palantir i 2019 overtog ansvaret for Project Maven, det amerikanske forsvarsprojekt for AI-analyse af dronevideo.

I de senere år har Palantir samarbejdet med det amerikanske forsvar om at bygge den næste generations fælles kommando- og kontrolnetværk. Pentagon's CJADC2-initiativ (*Combined Joint All-Domain Command and Control*) – som skal forbinde sensorer, systemer og enheder på tværs af alle værn og allierede – har nydt godt af Palantirs data-fusionsplatform. Palantir fik i 2022–2023 tildelt en kontrakt på $480 millioner for at understøtte det amerikanske forsvars arbejde med Maven/CJADC2-integrationen . Ligeledes indgik Palantir en næsten $100 millioner kontrakt med U.S. Army Research Lab for at levere Maven-baserede AI-systemer til alle værn i militæret .

Hærens egne indkøb af Palantir-teknologi kulminerede i midten af 2025, hvor U.S. Army tildelte Palantir en Enterprise Service Agreement – en rammeaftale over 10 år til en potentiel værdi af $10 milliarder . Aftalen samler 75 tidligere kontrakter i én og skal gøre det hurtigere og billigere for hæren at anskaffe Palantirs software på tværs af enheder . Ifølge hæren vil denne aftale give soldater *"hurtig adgang til topmoderne data-integrations-, analyse- og AI-værktøjer"*, samtidig med at stordriftsfordele sparer omkostninger .

NATO og allierede
Palantirs voksende dominans inden for militær AI afspejles også i samarbejder med USA's allierede og multinationale forsvarsorganisationer som NATO. I april 2025 annoncerede NATO's Kommunikations- og Informationsagentur (NCIA) en aftale med Palantir om at implementere et AI-baseret kampsystem kendt som *Maven Smart System NATO* . Aftalen – der blev indgået på rekordtid, kun seks måneder efter behovet blev skitseret – indebærer, at NATO adopterer Palantirs *Maven Smart System* platform for at skabe en fælles data- og AI-understøttet krigsførelsesevne på tværs af alliancen . Systemet skal bruges til alt fra *large language models* og generative AI til maskinlæring, med det formål at forbedre efterretningsfusion, måludpegning, situationsforståelse på kamppladsen og hurtigere beslutningstagning for NATO's styrker . NATO's øverstkommanderende for operationer (Allied Command Operations) vil således tage Palantirs AI-system i brug for at muliggøre, at data fra mange kilder – på tværs af lande – smelter sammen til et helhedsbillede, som militære chefer kan agere på i næsten realtid.

Individuelle NATO-lande har ligeledes indgået strategiske partnerskaber med Palantir. Storbritannien har fremstået som et europæisk knudepunkt for Palantir: I september 2025 annoncerede det britiske forsvarsministerium en strategisk aftale, hvor Palantir vil investere op til 1,5 milliarder £ i UK og etablere sit europæiske hovedkvarter for forsvar i London . Samarbejdet indebærer at indføre AI-værktøjer, der allerede er afprøvet i Ukraine, til at forbedre briternes militære planlægning, beslutningstagning og målbekæmpelse . Blandt de specifikke kapaciteter er udviklingen af en digital *"kill chain"*, hvor data fra mange kilder (både åbne og militære) smeltes sammen for at give kommandører hurtigere og mere præcise angrebsmuligheder . Også andre allierede, såsom Israel, er kendt for at bruge Palantirs systemer – det israelske militær (IDF) har angiveligt været kunde, hvilket faktisk har udløst kritik i andre sammenhænge (bl.a. i UK, hvor læger protesterede mod Palantirs NHS-engagement pga. firmaets forbindelse til IDF) .

Ukraine
Ruslands invasion af Ukraine i 2022 blev en ilddåb for mange nye militærteknologier – herunder Palantirs AI-platforme. Palantir har været en tæt teknologisk partner for Ukraine under krigen og har leveret både software, hardware og know-how til at styrke Ukraines forsvar mod den numerisk overlegne modstander. Faktisk åbnede Palantir en fysisk kontor i Kyiv og indgik samarbejde med det ukrainske Ministerium for Digital Transformation for at støtte landets forsvar med avanceret teknologi .

Et af de mest prominente bidrag fra Palantir til Ukraine er den førnævnte MetaConstellation-platform. Ukrainske styrker bruger Palantirs MetaConstellation software til at indsamle og visualisere data om fjendtlige styrkers positioner og udstyr ved hjælp af et netværk af kommercielle satellitter, sensorer, droner og andre systemer . Dette har givet Ukraine en enestående mulighed for at *se* dybt ind bag fjendens linjer og reagere hurtigt. For eksempel kan ukrainske artilleri- eller raketenheder via Palantirs systemer modtage næsten realtidsopdateringer om, hvor russiske kampvognskolonner befinder sig, eller om nye trusler (som f.eks. en igangværende dronebølge) er på vej.

Derudover hjælper Palantir Ukraine med at udvikle egne AI-kapaciteter. I 2023 gik den ukrainske regerings tech-initiativ Brave1 sammen med Palantir om at skabe en platform kaldet *"Dataroom"* til at teste og træne AI-modeller på sensitive militærdata . I dette sikre digitale miljø kan ukrainske forsvarsinnovatører eksperimentere med algoritmer ved at bruge faktiske efterretningsdata om russiske lufttrusler, f.eks. droner, som træningsmateriale . Målet med Dataroom er blandt andet at forbedre Ukraines interceptor-droner ved at forsyne dem med AI, så de bedre kan opdage, identificere og nedkæmpe fjendtlige droner autonomt . Mykhailo Fedorov, Ukraines digitaliseringsminister, forklarede i den forbindelse, at eftersom Rusland sender *"tusindvis af mål"* (bl.a. iranske Shahed-kamikazedroner) mod Ukraine, kræver forsvaret en høj grad af autonomi for at skalere forsvaret .

Markedsleder med etiske problemer
Palantir har gennem sin unikke profil opnået en dominerende position i markedet for militær AI og dataanalyse. Som et softwarefokuseret selskab, der fra starten rettede sig mod forsvars- og efterretningskunders behov, har Palantir fået et

forspring i forhold til både traditionelle forsvarsentreprenører og nyere tech-konkurrenter.

Samtidigt har Palantir været målet for kritik fra mange sider og været centrum for en række kontroverder af både etisk og politisk karakter. Palantirs teknologi sammenkører enorme mængder data om personer og begivenheder, hvilket har ført til bekymring for, at det understøtter en *"overvågningsstat"*. Borgerrettighedsorganisationer som ACLU har kritiseret politimyndigheders brug af Palantir Gotham til *predictive policing*, idet de frygter, at uskyldige borgere profileres og overvåges uden grund . Palantir er også forbundet med ansigtsgenkendelsesteknologi og andre AI-værktøjer, som kan udvide myndigheders overvågningsevne .

Under Trump-administrationen i USA kom Palantir i vælten for sin tætte involvering i immigrationsmyndighedernes arbejde. Selskabet udviklede for U.S. Immigration and Customs Enforcement (ICE) et system kaldet Investigative Case Management og det interne værktøj FALCON/Palantir (også kendt som ICM eller senere ELITE) til at spore og sammenstille oplysninger om immigranter . Disse systemer muliggjorde, at ICE kunne kombinere data fra bl.a. politiregistre, grænsekontrol og andre kilder for at identificere og deportere illegale immigranter i stor skala. Kritikere har hævdet, at Palantir dermed *"muliggjorde deportationer"* på et hidtil uset niveau og bidrog til hårdhændet behandling af migrantgrupper

Palantir blev indirekte trukket ind i skandalen omkring Cambridge Analytica (CA) og uretmæssig høst af Facebook-data i 2016. Det kom frem, at en Palantir-medarbejder på eget initiativ havde assisteret Cambridge Analytica i at udvikle deres dataindsamlings- og vælgerpåvirkningsværktøjer . Selvom Palantir hævdede, at dette skete uden ledelsens viden og i medarbejderens fritid, førte afsløringen til kritik af Palantir for at have *"fingeraftryk"* i et projekt, der blev brugt til at manipulere vælgere og undergrave privatliv på sociale medier .

Som en af de førende udbydere af AI til forsvar er Palantir også midt i den etiske debat om *"killer robots"* og autonom krigsførelse. Kritikere spørger, om Palantirs værktøjer kan føre til mere drab på afstand og potentielt uden menneskelig indgriben. Særligt Project Maven og lignende initiativer har udløst frygt for, at AI kan bruges til at udvælge bombemål eller identificere personer for *"targeted killings"*.

Palantir har også tiltrukket politisk kontrovers ved dens ledelses åbenlyse politiske holdninger. Medstifter Peter Thiel er kendt som en højlydt konservativ og støttede Donald Trump, hvilket fik nogle til at associere Palantir med Trumps agenda (især omkring immigration). Samtidig er CEO Alex Karp politisk mere centrum-venstre orienteret, men begge har positioneret Palantir som en patriotisk virksomhed, der *nægter* at arbejde for regimer der ikke deler vestlige demokratiske værdier. Denne *værdibaserede forretningsmodel* er kontroversiel i sig selv – kritikere mener, at et privat firma tager udenrigspolitiske beslutninger ved at sige nej til visse markeder (som Kina) og ja til at hjælpe visse lande militært (som Ukraine).

Indbegrebet af en ny æra

Palantirs position i markedet er stærk, båret af både teknologisk forspring og en forretningsmæssig vilje til at være selektiv omkring sine kunder for at understøtte bestemte værdier. Dog bevæger virksomheden sig på et komplekst minefelt af etiske og politiske spørgsmål. Når man leverer "det digitale nervesystem" til militære og sikkerhedsmæssige operationer, bliver man uvægerligt en del af debatten om, hvor grænsen går mellem nødvendig sikkerhed og potentielt overgreb på frihedsrettigheder. Palantir skal navigere i at tilfredsstille sine regeringskunder og aktionærer, samtidig med at det håndterer offentlighedens bekymringer.

Ikke desto mindre viser Palantirs fortsatte vækst og integration, at behovet for avanceret AI i forsvaret er voksende, og at Palantir formår at levere løsninger som få (hvis nogen) andre kan på nuværende tidspunkt. Hvordan virksomheden håndterer sine kontroverser, og hvordan konkurrenterne reagerer, vil være afgørende for dens fremtid. Men i skrivende stund står Palantir som indbegrebet af den nye æra, hvor data og kunstig intelligens er lige så vigtige våben for militæret som kampfly og kampvogne – en æra, virksomheden selv har været med til at forme.

Illustration genereret med ChatGPT

TEMA: NÅR KRIG BLIVER KODE

FRA OVERVÅGNING TIL MÅL

- ISRAELS AI-KRIG SOM STRESSTEST FOR FOLKERETTEN

Af Mark Sinclair Fleeton

Krigen mellem Israel og Hamas er blevet et globalt referencepunkt i debatten om militær brug af kunstig intelligens. Ikke fordi autonome våben har overtaget slagmarken, men fordi AI i stor skala er blevet brugt til at accelerere og strukturere militære beslutninger – fra overvågning og efterretning til udpegning og prioritering af mål.

Spørgsmålet er ikke, om brugen af AI i sig selv er lovlig. Spørgsmålet er, hvad der sker med ansvar, proportionalitet og menneskelig kontrol, når tempo og volumen i beslutninger øges dramatisk – og når systemer filtrerer virkeligheden, før mennesker ser den.

AI som beslutningsinfrastruktur
Meget af den offentlige debat om Israels brug af AI har kredset om forestillinger om autonome våben. Men de dokumenterede systemer peger i en anden retning.

Der er tale om AI-baserede systemer til overvågning, mønstergenkendelse og beslutningsstøtte – ikke systemer, der selv affyrer våben. AI anvendes til at analysere store mængder data fra signaler, billeder og adfærd og til at generere lister over potentielle mål, som efterfølgende kan vurderes og godkendes af mennesker.

Det afgørende er netop denne mellemposition: AI som beslutningsinfrastruktur. Systemerne træffer ikke formelle beslutninger, men de former beslutningsgrundlaget. Det er her, overgangen fra overvågning til mål finder sted.

Begrænset viden
Meget af den konkrete viden om Israels brug af AI stammer fra undersøgende journalistik, herunder israelske medier og internationale rapporter, samt fra udtalelser fra israelske embedsmænd, der har beskrevet brugen af avancerede data- og analyseværktøjer i krigen.

Samtidig er der væsentlige begrænsninger. Systemerne er klassificerede, og uafhængig verifikation er kun mulig i begrænset omfang. Det betyder, at mange påstande ikke kan be- eller afkræftes fuldt ud.

Men mangel på fuld indsigt betyder ikke, at der ikke kan stilles juridiske og normative spørgsmål. Folkeretten vurderer ikke kun konkrete våben, men også metoder til krigsførelse – herunder hvordan mål udpeges, og hvordan proportionalitetsvurderinger foretages.

Når tempo bliver en juridisk faktor
En af de mest markante ændringer ved brugen af AI-baseret beslutningsstøtte er tempoet. Hvor måludvælgelse tidligere var en relativt langsom proces, kan AI-systemer generere og prioritere store mængder potentielle mål på kort tid.

Det rejser et grundlæggende spørgsmål. Hvornår bliver tempo i sig selv en risikofaktor? Folkeretten kræver, at der foretages individuelle vurderinger af proportionalitet og forholdsregler (*feasible precautions*) før angreb. Disse vurderinger forudsætter tid, information og mulighed for at fravælge.

Når beslutningsstøttesystemer leverer færdige prioriteringer under tidspres, øges risikoen for, at den menneskelige vurdering reduceres til en godkendelseshandling. Ikke nødvendigvis fordi operatører er uansvarlige, men fordi systemets tempo og volumen gør grundig vurdering vanskelig.

AI kan skalere risiko
Debatten om civile tab i Gaza har ofte fokuseret på enkelte angreb. Men set i et AI-perspektiv er det relevante spørgsmål mere strukturelt: Hvor i systemerne kan risikoen for civil skade forstærkes?

Flere mekanismer er centrale:

- Falske positiver: AI-systemer kan identificere mønstre, der ligner militær aktivitet, men som i praksis involverer civile.
- Dataskævheder: Træningsdata kan afspejle tidligere konflikter eller antagelser, som ikke holder i nye kontekster.
- Filtrering før vurdering: Når AI sorterer information, ser mennesker kun en del af virkeligheden – og måske netop den del, systemet prioriterer.
- Tæt befolkede områder: I Gaza forstærkes alle fejl, fordi militære og civile strukturer er tæt sammenvævede.

Ingen af disse mekanismer er nye i sig selv. Men AI kan skalere dem.

Reglerne er til stede
De centrale regler, der regulerer angreb i krig, findes i den humanitære folkeret, herunder især Tillægsprotokol I til Genèvekonventionerne fra 1977 (*Additional Protocol I to the Geneva Conventions*).

Her fastslår blandt andet artikel 48, at parterne i en konflikt altid skal skelne mellem civile og militære mål. Artikel 51 forbyder angreb, der rammer civile vilkårligt, mens artikel 52 præciserer, hvad der kan betragtes som et legitimt militært mål. Hertil kommer artikel 57, som pålægger parterne at træffe alle praktisk mulige forholdsregler (*feasible precautions*) for at undgå eller begrænse civile tab.

Disse regler er teknologineutrale. De gælder uanset, om beslutningsgrundlaget er indsamlet af mennesker eller behandlet af algoritmer. Men de forudsætter noget meget konkret: at der faktisk foretages individuelle, kontekstuelle vurderinger, før et angreb iværksættes.

Det er her, AI-baseret beslutningsstøtte kan bringe praksis under pres. Når systemer genererer prioriterede mållister i højt tempo, risikerer proportionalitetsvurderinger og forholdsregler at blive reduceret til efterfølgende godkendelser af allerede filtrerede forslag. Det betyder ikke nødvendigvis, at reglerne brydes – men at rummet for menneskelig vurdering indsnævres.

Et centralt juridisk værktøj er desuden artikel 36 i Tillægsprotokol I, som forpligter stater til at foretage en juridisk vurdering af nye våben, midler eller metoder til krigsførelse, før de tages i brug. Her er udfordringen, at AI-systemer ikke er statiske: de opdateres, kombineres med andre systemer og anvendes på tværs af kontekster.

Dermed bliver spørgsmålet ikke kun, om et system i sig selv kan anvendes lovligt, men om måden det anvendes på i praksis giver tilstrækkelig tid, information og mulighed for menneskelig vurdering, som folkeretten forudsætter.

Kort sagt: Folkeretten mangler ikke regler for militær AI. Den mangler mekanismer, der sikrer, at reglerne faktisk kan efterleves, når beslutninger filtreres og accelereres gennem systemer.

Israel som normdannende case – uanset intention
Uanset hvordan man vurderer Israels konkrete brug af AI, har konflikten allerede fået en bredere betydning. Andre lande følger med. Ikke for at kopiere systemer én til én, men for at lære af praksis.

I mangel af bindende internationale regler risikerer sådanne praksisser at blive de facto-standarder. Ikke gennem formelle beslutninger, men gennem imitation og "best practice".

Det gør Israel-case'en til en stresstest – ikke kun for folkeretten, men for den internationale evne til at fastsætte grænser, før praksis sætter dem.

TEMA: NÅR KRIG BLIVER KODE

SÅDAN FÅR DEMOKRATIET OVERBLIK

Af Mark Sinclair Fleeton

Militær brug af kunstig intelligens rejser et paradoks: Jo mere teknologien bruges til at sortere information og accelerere beslutninger, desto sværere bliver det for offentligheden at forstå, hvem der faktisk har haft kontrol – og på hvilket grundlag. Samtidig er det åbenlyst, at fuld åbenhed om militære systemer ikke er realistisk.

Men demokratisk kontrol kræver ikke adgang til operationelle detaljer. Den kræver indsigt i rammerne: hvilke typer systemer der bruges, hvordan beslutninger godkendes, hvordan ansvar kan efterprøves, og hvem der fører tilsyn. Spørgsmålet er derfor ikke *om* demokratiet kan få greb – men *hvordan*.

Hvad er problemet, der skal løses?
På tværs af artiklerne i temaet tegner der sig tre sammenhængende udfordringer:

For det første ansvarsfiltrering. Når AI indgår i kæder fra data til anbefaling til handling, bliver beslutningen et resultat af mange led. Operatører, procedurer, systemdesign, leverandører og politiske rammer flettes sammen. Resultatet kan blive, at ingen enkelt instans reelt kan stå på mål bagefter.

For det andet tempo. AI bruges netop for at gøre militære beslutninger hurtigere. Men når tempoet stiger, reduceres den tid og det rum, som folkeretten forudsætter for menneskelig vurdering – særligt proportionalitetsvurderinger og forholdsregler.

For det tredje beslutningsfiltrering. AI-systemer sorterer virkeligheden, før mennesker ser den. Det betyder, at menneskelig kontrol ofte udøves på et allerede indsnævret grundlag. Det er her, "human-in-the-loop" risikerer at blive en formalitet.

Løsningerne må derfor rette sig mod design, processer og kontrol – ikke kun mod den enkelte operatør.

Minimumsstandard: Hvad betyder meningsfuld menneskelig kontrol?
Debatten om "meaningful human control" bliver ofte abstrakt. Men på tværs af jura, militær praksis og policy kan begrebet oversættes til fem praktiske kriterier, som kan stilles som krav:

For det første: Operatøren skal have tid til at vurdere. Hvis tempoet i systemet gør selvstændig vurdering umulig, er kontrollen ikke meningsfuld.

For det andet: Operatøren skal have information om usikkerhed og fejltyper. Anbefalinger uden angivelse af usikkerhed skubber ansvar nedad uden reelt grundlag.

For det tredje: Operatøren skal kunne afvise systemets anbefalinger uden systemisk pres – organisatorisk, kulturelt eller proceduremæssigt.

For det fjerde: Der skal være logning og sporbarhed, så det kan dokumenteres, hvad systemet anbefalede, hvad mennesket gjorde, og hvorfor.

For det femte: Der skal være tilsyn og hændelsesrapportering, også for "nærved-hændelser", hvor noget kunne være gået galt.

Menneskelig kontrol handler dermed ikke om, hvor et menneske sidder i loopet, men om hvorvidt kontrol, dømmekraft og ansvar er reelle.

Designkrav: Når teknologien former beslutningen
Hvis man vil undgå, at kontrol bliver symbolsk, skal kravene starte i systemernes design.

AI-systemer, der bruges i militære sammenhænge, bør være eksplicitte om usikkerhed og begrænsninger. Anbefalinger bør ledsages af alternative scenarier, ikke kun én "bedste løsning". Systemerne skal kunne indikere, når de befinder sig i situationer, der ligger uden for deres træningsgrundlag – såkaldt *out-of-distribution*.

Derudover bør designet understøtte efterprøvning: Det skal være muligt at rekonstruere, hvilke data og hvilke modeller der lå til grund for en anbefaling på et givent tidspunkt. Uden den mulighed bliver ansvar et tomt begreb.

Proceskrav: Stopklodser mod gummistempel
Selv gode systemer kan bruges dårligt, hvis processerne presser mod hastighed og rutine.

Derfor giver det mening at stille krav om topersoners kontrol ved særligt kritiske beslutninger. Ikke som bureaukrati, men som beskyttelse mod automatiseret godkendelse.

Der bør også være krav om aktiv begrundelse: Når en anbefaling følges – eller fraviges – skal der kunne angives en kort begrundelse. Det skaber både ansvar og læring.

Endelig bør der indbygges stop-punkter, hvor systemet ikke kan levere anbefalinger, hvis datakvaliteten er for lav, eller usikkerheden for høj. Det er bedre med et bevidst stop end med en falsk præcision.

Kontrolkrav: Logning, audit og hændelser
Kontrol kan ikke være en engangsøvelse ved indkøb eller godkendelse. Den skal være løbende.

Det kræver konsekvent logning af systemoutput, menneskelige beslutninger og afvigelser. Ikke for at straffe, men for at muliggøre efterprøvning.

Derudover bør der være uafhængige audits – fortrolige, men reelle – hvor systemer, procedurer og praksis gennemgås. Og der bør være klare procedurer for hændelsesrapportering, også for situationer, hvor noget næsten gik galt.

Uden disse mekanismer bliver ansvar først synligt, når skaden er sket.

Demokratisk minimumsindsigt – uden at afsløre operationer
Offentligheden kan ikke – og skal ikke – kende taktiske detaljer. Men der findes et rimeligt minimum af indsigt, som kan kræves i et demokrati.

Det handler blandt andet om overordnet viden om hvilke kategorier af AI-systemer der bruges: overvågning og efterretning, beslutningsstøtte eller funktioner tæt på våbensystemer.

Det handler også om governance: Hvem kan godkende brug? Hvornår kræves eskalation? Findes der klare stopklodser?

Derudover kan der stilles krav om gennemsigtighed på procesniveau: findes der logning, audit og uafhængigt tilsyn – også selv om indholdet er klassificeret?

Offentligheden kan få indsigt i rammerne for ansvar, uden at få indsigt i operationerne.

Fra våbenscreening til løbende compliance
Folkeretten forudsætter allerede kontrol. Artikel 36 i Tillægsprotokol I til Genèvekonventionerne forpligter stater til at vurdere nye våben og metoder. Men AI udfordrer forestillingen om, at en godkendelse kan gives én gang for alle.

AI er ikke et statisk produkt. Modeller opdateres, data ændrer sig, og anvendelser glider. Derfor bør våbenreview suppleres af løbende re-validering, driftsovervågning og systematisk læring fra hændelser.

AI er ikke kun et indkøb – det er en vedvarende forvaltningsopgave.

Hvad kan Danmark konkret gøre i 2026?
Danmark er ikke først i feltet. Det kan være en fordel.

Som "third mover" kan Danmark stille krav ved indkøb: krav om audit-rettigheder, dokumentation, test og transparens på procesniveau. Danmark kan insistere på, at ansvarlighed ikke er et slogan, men en del af kontrakten.

Derudover kan Danmark bruge internationale spor – NATO, FN og EU – til at presse på for fælles standarder for logning, audit og menneskelig kontrol, også hvor bindende regler endnu mangler.

Det er ikke et spørgsmål om at stoppe teknologien. Det er et spørgsmål om at sikre, at når beslutninger flytter sig ind i systemer, så følger ansvar, kontrol og demokratisk indsigt med

FAKTA:
4 ting der kan offentliggøres – og 4 ting der normalt må være fortrolige

Kan offentliggøres:
- **Kategorier af AI-systemer i brug (ISR, beslutningsstøtte, funktioner tæt på våben)**
- **Overordnede godkendelses- og kontrolprincipper**
- **Krav til logning, audit og hændelsesrapportering**
- **Eksistensen af uafhængigt tilsyn med fortrolig adgang**

Bør være fortrolige:
- **Konkrete operationsdetaljer (hvor, hvornår, hvordan)**
- **Tekniske kapaciteter, svagheder og thresholds**
- **Detaljer om måludvælgelse og engagementregler i praksis**
- **Klassificeret systemarkitektur og integrationer**

Foto: Iben Yde

NÅR BESLUTNINGER FLYTTER SIG

- UDEN ANSVARET FØLGER MED

Af Mark Sinclair Fleeton

Militær brug af kunstig intelligens bliver ofte diskuteret som et fremtidsscenarie: autonome våben, der en dag handler uden menneskelig indgriben. Men ifølge Iben Yde er det en afsporing. De største juridiske og etiske problemer opstår allerede i dag – ikke fordi mennesker er væk fra beslutningskæden, men fordi deres rolle markant ændrer karakter.

Iben Yde er i dag ansat i rådgivningsvirksomheden Rethink Advisory, hvor hun blandt andet rådgiver forsvarsindustrien om militære, geopolitiske og teknologiske problemstillinger. Hendes særlige fokus er ansvarlig brug af kunstig intelligens i militære systemer, hvor hun hjælper industrien med at sikre, at nye systemer lever op til folkerettens krav og udvikles på en måde, der gør dem pålidelige og sikre.

Hun har en baggrund fra både den akademiske verden og Forsvaret, har skrevet ph.d.-afhandling om autonome våbensystemer og har tidligere arbejdet som militærjuridisk rådgiver for Forsvaret. Senest har hun været chef for Center for Operativ Folkeret ved Forsvarsakademiet, hvor hun havde ansvar for uddannelse i folkeret og samtidig forskede i autonome våbensystemer og AI-baseret beslutningstagning.

Hun peger igen og igen på den samme grundudfordring: forbindelsen mellem menneskelig dømmekraft og militær handling er blevet svagere, mere teknisk og sværere at fastholde.

"Problemerne opstår, fordi der ikke i samme grad er et direkte link mellem den menneskelige operatør og den endelige handling, når man bruger AI i autonome våbensystemer eller beslutningsstøtte for den sags skyld."

Det betyder ikke, at beslutninger træffes uden mennesker. Men det betyder, at beslutningen i praksis ofte er formet, før den formelt træffes, hvis den beror på anbefalinger fra en AI model. Eller, i relation til autonome våbensystemer, at det kun er de overordnede parametre for hvornår og mod hvad et angreb må rettes, der er formuleret af et menneske, ikke den endelige beslutning.

Og netop derfor er det utilstrækkeligt blot at konstatere, at "der er et menneske i loopet".

"Man kan godt have et menneske involveret, men hvis mennesket enten kommer ind meget tidligt eller meget sent i processen, så ligger en meget væsentlig del af beslutningen i praksis hos systemet,."

Reglerne er ikke nye – men praksis er
Set fra et folkeretligt perspektiv er udgangspunktet klart. Militær AI opererer ikke i et juridisk tomrum.

"De humanitære folkeretlige regler om angreb er teknologineutrale. De gælder, uanset hvilken teknologi man anvender."

Det gælder de grundlæggende krav om distinktion, proportionalitet og forsigtighedsforanstaltninger. De finder anvendelse, uanset om beslutningsgrundlaget er indsamlet manuelt eller filtreret gennem algoritmer.

"Der er ikke et juridisk tomrum, bare fordi vi taler om AI. Reglerne er der allerede."

Men netop fordi reglerne tager udgangspunkt i en mere direkte form for menneskelig vurdering, opstår der et spændingsfelt.

"Det er ikke reglerne, der er nye, det er teknologien der i visse henseender er væsensforskellig fra mere konventionelle militære systemer. Og det er måden, man forsøger at efterleve reglerne på, der bliver udfordret."

Når tempoet stiger, og beslutninger forberedes gennem systemer, der sorterer og prioriterer information på forhånd eller træffer beslutninger på baggrund af input fra sensorer og forprogrammerede kriterier, bliver der mindre plads til den menneskelige vurdering, som reglerne oprindeligt forudsætter.

Våbenscreening som juridisk holdepunkt
I fraværet af specifikke internationale forbud mod autonome våbensystemer og AI-baserede beslutningssystemer er ét redskab derfor blevet centralt i diskussionen om hvordan man skal sikre lovlige systemer: våbenscreening efter Tillægsprotokol I, artikel 36.

"Fordi der ikke findes specifikke regler for autonome våbensystemer eller AI-baserede beslutningssystemer, bliver våbenscreening ekstremt vigtig som et safeguard mod ulovlige våben og beslutningsstøttesystemer, der spiller direkte ind i gennemførelsen af angreb."

Våbenscreeningen fungerer som statens egen kontrolmekanisme. Men effektiviteten afhænger af, hvornår og hvordan vurderingen foretages.

"Efter reglerne skal den folkeretlige vurdering af et nyt våbensystem ske på det tidligst mulige tidspunkt, ideelt set inden man overhovedet producerer systemet, for ellers risikerer man, at ulovlige systemer allerede er på markedet."

Jo senere vurderingen foretages, jo mindre handlerum er der.

"Jo senere i processen man laver vurderingen, jo sværere (og dyrere) bliver det ofte også at ændre noget."

Dermed bliver våbenscreening ikke kun et juridisk spørgsmål, men også et organisatorisk og politisk.

Designformål – ikke hypotetiske mareridt
Debatten om militær AI har en tendens til at kollapse i worst-case-scenarier. Men juridisk set er det ikke sådan, vurderinger foretages.

"Man skal vurdere systemet ud fra det designformå og den anvendelsesforml, det er udviklet til, og ikke ud fra enhver tænkelig måder, det kan misbruges på."

Ellers bliver arbejdet umuligt.

"Hvis man begynder at vurdere alle hypotetiske anvendelser, så kan man aldrig blive færdig."

Og der vil næsten altid kunne konstrueres et ulovligt scenarie.

"Du vil næsten altid kunne finde en ulovlig måde at anvende et ellers lovligt system på."

Det afgørende spørgsmål er derfor, om systemets design og tilsigtede anvendelse gør det muligt at overholde folkerettens krav i praksis.

Når test bliver et åbent spørgsmål
Her bliver forskellen mellem klassiske våben og AI tydelig. Hvor et projektil kan testes fysisk, er AI-systemer langt sværere at evaluere på forhånd.

"Her har vi ikke en fysisk genstand, man kan måle og veje. Det er en måde at træffe beslutninger på, og hvordan måler man det?"

Yde bruger et billede, der tydeliggør forskellen:

"Det er meget nemmere at teste et projektil og studere dets effekt i en gelatineblok end at afgøre, om en algoritme er god nok til at genkende mål på en dynamisk kampplads hvor forholdene ændrer sig hele tiden."

Test giver indikationer, men ikke sikkerhed.

"Test kan give nogle indikationer, men de kan ikke give sikkerhed for, hvordan systemet vil opføre sig i alle situationer." Jo bedre indblik i systemets performance, man ønsker at opnå jo flere tests skal man gennemføre og jo mere nøjagtigt og realistisk skal testmiljøet afspejle de forhold, systemet skal anvendes under. Men det er enormt vanskeligt i praksis, da både systemet selv og det miljø det anvendes i ændrer sig.

Det betyder, at test og evaluering ikke kan være en engangsøvelse, men må ske løbende.

Kontrol eller dømmekraft?
I internationale fora bruges begrebet *meaningful human control* som et samlende svar. Men Yde er skeptisk over for, om "kontrol" er det rigtige ord.

"Jeg er måske mere til begrebet dømmekraft end til kontrol."

For kontrol kan let blive formel.

"Det afgørende er ikke, om der sidder et menneske i loopet, men om der har været menneskelig dømmekraft over de vurderinger, der er svære."

Og formel kontrol kan eksistere uden reel vurdering.

"Man kan godt have kontrol på papiret, uden at der i praksis er nogen, der har haft mulighed for at vurdere situationen ordentligt."

Designkrav og mulighed for intervention
Hvordan sikrer man så effektiv udøvelse af menneskelig dømmekraft i praksis? Her peger Yde både på konkrete designkrav og krav til anvendelsesprocessen.

"For mig er missionsspecifik programmering, den vigtigste måde at sikre, at det teknisk er muligt at udøve menneskelig kontrol."

Det betyder, at rammerne fastlægges af brugeren umiddelbart før systemet aktiveres.

"Hvis man designer systemet med et interface, der giver slutbrugeren mulighed for at tilpasse kriterierne for angreb meget præcist inden missionen, så de tager højde for de konkrete omstændigheder for angrebet, kan det i nogle tilfælde være acceptabelt, at man ikke kan gribe ind undervejs."

Men tidsdimensionen er afgørende.

"Jo længere tid der går fra aktivering til effekt, jo større bliver behovet for at bevare muligheden for at intervenere."

Procedurerne omkring systemerne
Selv det bedste system kan imidlertid anvendes problematisk, hvis organisationen omkring det presser tempoet eller reducerer udøvelsen af menneskelig dømmekraft til formaliteter.

"Det handler ikke kun om, hvad systemet teknisk kan, men om hvilke procedurer den militære organisation sætter op omkring brugen."

Her står stater ofte over for et vanskeligt valg, hvor flere og nogle gange modsatrettede faktorer skal balanceres – hastighed og operativ effektivitet over for hensynet til at beskytte civilbefolkningen og minimere collateral damage.

"Man kan vælge en snæver tilgang og kun gøre det juridisk absolut nødvendige, eller man kan vælge en bredere tilgang, hvor man også i praksis sikrer, at systemet faktisk bruges korrekt."

Valget er i praksis politisk, også selv om det ofte præsenteres som teknisk.

Den stille risiko: beslutningsstøtte
Mens autonome våben fylder mest i den offentlige debat, er det ikke her, Yde ser den største risiko.

"Jeg er på mange måder mere bekymret for beslutningsstøttesystemer end for AI-baserede våbensystemer, fordi de er så komplekse og langt sværere at teste."

Særligt når systemerne købes færdige.

"Hvis man køber komplekse AI-systemer off the shelf, uden at have været involveret i udviklingen, bliver det meget svært for en lille kunde som Danmark at sikre at de er udviklet ansvarligt og dermed også er pålideligelige og virker efter hensigten ."

Og udfordringen stopper ikke, når systemet tages i brug.

"Systemerne stopper ikke med at udvikle sig, når de tages i brug. Det er både en af styrkerne og en af de helt store risikofaktorer ved AI"
"Derfor er kontinuerlig test og evaluering helt afgørende."

Et åbent spørgsmål
Situationen lægger ikke op til en enkel løsning. Men det peger på et grundlæggende valg: enten accepterer man, at tempo og kompleksitet gradvist udhuler menneskelig dømmekraft – eller også gør man ansvar, procedurer og kontrol til politiske prioriteter.

"Hvordan gør vi, at den meningsfulde kontrol rent faktisk bliver meningsfuld? Det er nok det største, sværeste og vigtigste spørgsmål af alle."

DET ER IKKE ROBOTTERNE, DER ER PROBLEMET

- DET ER TEMPOET

Af Mark Sinclair Fleeton

Militær AI bliver ofte diskuteret som en fremtidsfare. Men ifølge Jeppe Teglskov Jacobsen er det allerede i gang – og den største risiko ligger ikke i autonome våben, men i den måde beslutninger bliver hurtigere, smallere og sværere at forklare.

Der findes en forestilling om, at militær kunstig intelligens først bliver farlig den dag, maskiner selv begynder at trykke på aftrækkeren. Men hvis man spørger Jeppe Teglskov Jacobsen, forfatter til rapporten *"Militær AI – amerikanske erfaringer, danske muligheder"*, er det en bekvem, men misvisende fortælling. Til dagligt er han informationschef (Chief of Information) og strategisk rådgiver i Nationalt Forsvarsteknologisk Center (NFC). Han er ph.d. og har blandt andet arbejdet med sikkerheds- og forsvarspolitiske spørgsmål, herunder militær teknologi og kunstig intelligens.

"*Våbensystemerne er ligesom kransekagen*," siger han. "*Det er den sidste del. Det, der er svært – og kontroversielt – ligger ofte før.*"

Det er i den midterste del af kæden, han mener, vi skal kigge: beslutningsstøtten. De systemer, der sorterer enorme datamængder, prioriterer mål, og reducerer komplekse situationer til overskuelige anbefalinger. Ikke fordi de "beslutter" noget i juridisk forstand, men fordi de former, hvad mennesker overhovedet ser – og hvor hurtigt de skal reagere.

Tre typer AI – og én stor gråzone

I rapporten deler Jacobsen militær AI op i tre kategorier. Først de relativt ukontroversielle systemer: administrative og logistiske værktøjer, der optimerer drift, vedligeholdelse og planlægning. Dernæst beslutningsstøtte, der hjælper mennesker med at analysere, sortere og prioritere information. Og til sidst våbensystemer, hvor graden af autonomi kan være høj.

"*Problemet*," siger han, "*ligger i den midterste kategori. Den er lidt stor. Den kan gå fra at være ret ukontroversiel til at være sindssygt kontroversiel.*"

For netop her begynder AI at bevæge sig tæt på kamppladsen. Ikke som et våben, men som et filter. Et system, der peger på, hvilke hændelser der er vigtigst, hvilke objekter der er mest relevante, og hvilke beslutninger der haster mest.

"*Når det også bliver målidentifikation,*" siger han, "*og kommer tættere på kamppladsen, så tages beslutningerne bare en lille smule hurtigere.*"

Det er den hastighed, der bekymrer ham mest.

Foto: The National Defence Technology Centre

20 sekunder til at vurdere liv og død
I interviewet vender Jacobsen flere gange tilbage til tempo som den afgørende faktor. Ikke tempo som abstrakt militær nødvendighed, men som konkret vilkår for menneskelig dømmekraft.

"*Jeg hørte fra Israel,*" fortæller han, "*at du har 20 sekunder til at vurdere omfanget af sårede. Du har givet en officer 20 sekunder til at verificere noget, som er fuldstændig umuligt at verificere på 20 sekunder. Det er der, den er gal.*"

Pointen er ikke, om tallet er præcist. Pointen er mekanismen: Når systemer leverer anbefalinger i højt tempo, bliver menneskelig kontrol let reduceret til et godkendelsesritual. Ikke fordi operatøren er uansvarlig, men fordi proceduren er designet sådan.

"*Human-in-the-loop kan give mening i nogle sammenhænge,*" siger Jacobsen og giver et eksempel med overvågningsdroner og billedgenkendelse. "*Hvis systemet siger, 'her er noget, du bør kigge på', og jeg har tid og information til at vurdere det – så giver det mening.*"

Men når AI-output bliver en forudsætning for at følge med tempoet, ændrer rollen sig. Så er spørgsmålet ikke længere, om der *er* et menneske i loopet, men om mennesket har reelle betingelser for at udøve dømmekraft.

Ansvar, der glider baglæns
Når noget går galt i et AI-understøttet beslutningsforløb, bliver ansvaret sjældent placeret ét sted. Ifølge Jacobsen bliver det i stedet "rykket lidt længere tilbage".

"*Ansvaret bliver mere distribueret,*" siger han. "*Det bliver sværere at se, hvem der egentlig står på mål.*"

Operatøren kan sige, at systemet anbefalede noget. Kommandokæden kan sige, at proceduren blev fulgt. Leverandøren kan sige, at modellen fungerede inden for sine specifikationer. Og dataholdet kan sige, at modellen var testet på det grundlag, man havde.

"*Jeg kan ikke se, hvem der kommer i kachotten, når de her fejler,*" siger Jacobsen tørt.

Det er ikke nødvendigvis et udtryk for ansvarsfralæggelse. Det er et strukturelt problem. Når beslutninger formes af komplekse systemkæder, bliver det sværere at pege på ét menneske og sige: Her blev beslutningen truffet.

"*Vi kan så godt lide, at der er én mand, vi kan sige var skurken,*" siger han. "*Men vi bliver nødt til at komme væk fra den tænkning.*"

Black box og 95 procent
Et af de steder, hvor ansvaret bliver særlig vanskeligt, er i forholdet mellem sandsynligheder og beslutninger. Mange AI-systemer arbejder med scoringslogikker: 85 procent sandsynlighed, 95 procent sandsynlighed.

"*Det er bare svært på AI,*" siger Jacobsen, "*fordi hvor er det de der 95 procent egentlig er blevet kalkuleret?*"

Tidligere kunne en jurist eller såkaldt "red card holder" sidde ved siden af beslutningstageren og vurdere argumenter og beviser. Nu bliver det ofte erstattet af et tal – og en tærskel.

"*Der står 95 procent,*" siger Jacobsen. "*Og så har du lavet et eller andet interval, hvor du siger: hvis det er over 85 procent, så trykker du.*"

Det er ikke nødvendigvis forkert. Men det ændrer karakteren af kontrollen. For selv hvis der formelt er et menneske, der godkender, bliver det sværere at forklare, *hvorfor* beslutningen blev truffet.

"*Man vil gerne have noget explainability,*" siger han. "*Det er utroligt svært – især på neural networks.*"

Danmark som "third mover"
I rapporten sammenligner Jacobsen amerikanske erfaringer med danske muligheder. Og her er han relativt nøgtern.

"*Danmark kommer fra en third mover,*" siger han. "*Vi skal købe commercial off the shelf. Vi har ingen erfaring med at udvikle noget som helst.*"

Det betyder, at Danmark i høj grad køber færdige løsninger – ofte fra store internationale leverandører – og integrerer dem i eksisterende systemer. Problemet er, at AI ikke er et statisk produkt.

"*Man ved jo ikke, hvad man køber,*" siger Jacobsen. "*Hver gang man bruger det og tester det på noget nyt data, så bliver det et andet produkt.*"

Alligevel bliver AI ofte solgt, som om det var plug-and-play.

"*Der kommer en eller anden frisk sælger med et flot slips og siger: køb den her dims, den er bare plug and play," siger han. "Sådan fungerer de her systemer bare ikke.*"

Hvis Danmark vil undgå at gentage amerikanske fejl, peger Jacobsen på én ting frem for alt: processer.

Kontrol er et verificeringsregime
"*Hvis du vil have mere kamppraft,*" siger han, "*så skal du have et ordentligt verificeringsregime på tværs af udviklingen.*"

Det handler ikke kun om etik eller principerklæringer, men om test, evaluering, verificering og validering – før, under og efter systemer tages i brug.

"*Når du laver et ordentligt test-, evaluerings-, verificerings- og valideringsregime,*" siger han, "*så kan man gøre det med lidt mere ro i maven.*"

Her ser han en klar politisk opgave.

"*Det politiske ansvar ligger i, at man tager en beslutning om, at det er det her, man vil – og at man vil gøre det ordentligt," siger han. Og tilføjer uden omsvøb: "Jeg kræver af politikerne, at de tager ansvar her.*"

For alternativet er ikke at lade være.

"*Man kan have den indgangsvinkel, at hvis vi ikke kan finde ud af det, så må vi bare lade være," siger han. "Men det er bare ikke en praktisk løsning. It's for real. It's here.*"

Ikke robotter – men rammer
For Jacobsen er militær AI ikke primært et spørgsmål om onde maskiner eller løbske algoritmer. Det er et spørgsmål om rammer, tempo og efterprøvning.

Problemet opstår ikke, når en maskine tager over. Problemet opstår, når mennesker presses til at handle hurtigere, smallere og med ringere mulighed for at forklare deres beslutninger bagefter.

Det er dér, siger han, at demokratisk kontrol risikerer at blive et slogan. Og det er dér, den virkelige kamp om militær AI allerede er i gang.

NÅR ANSVAR FÅR EN BRUGERFLADE

-AI I MILITÆRET, MORAL INJURY - OG HVORFOR EMPATI BLIVER OPERATIV SIKKERHED

Af Thorsten Westphal, Veteran og psykoterapeut

Jeg skriver ikke som politiker. Ikke som teknolog. Jeg skriver som veteran og psykoterapeut.

Jeg arbejder primært med tidligere udsendte og deres pårørende. Jeg møder ikke krig som teori, men som eftervirkning: i kroppen, i søvnen, i blikket og i den særlige form for skade, der opstår, når et menneske føler, at det har handlet imod sine dybeste værdier, eller blevet presset til at leve med konsekvenser, som ikke længere kan forklares væk.

Derfor interesserer AI i militæret mig ikke først som teknik, men som psykologi.

For teknologien lover én ting: hurtigere beslutninger. Men samvittigheden har sit eget tempo.

Afstand som designprincip
Klassisk krigsførelse krævede nærhed. Ikke fordi nærhed automatisk skaber moral, men fordi nærhed skaber friktion: kroppen mærker, at noget er alvor. Det er en naturlig bremse - tvivl, empati, konsekvensfornemmelse.

AI er en afstandsmaskine.

Først kom den fysiske distance: operatøren langt fra målet. Nu kommer den kognitive distance: algoritmen, der sorterer, prioriterer og foreslår og som kan gøre virkeligheden til et beslutningsforslag.

Det er her, faren bliver konkret: Når AI-baseret beslutningsstøtte forkorter beslutningscyklussen, risikerer mennesket at blive reduceret til formel godkendelse uden reel kritisk kontrol. En nyere dansk rapport fra Center for Militære Studier beskriver netop den risiko at mennesket kan ende som "valideringsrolle", mens tempo og systemlogik tager styringen.

Papiret kan stadig sige "human in the loop". Men praksis kan ende med "human after the loop": mennesket bliver den, der forklarer bagefter – ikke den, der havde tid til at bremse før.

Tempoets moralske problem: Når etik taber til hastighed
Vi taler ofte om AI i krig som et etisk spørgsmål: proportionalitet, folkeret, menneskelig kontrol. Men i moderne konflikt, især informationskrig og hybridkrig, bliver det også et tidsproblem.

Modparten spiller ikke nødvendigvis på etik. Modparten spiller på tempo, mætning og psykologisk overbelastning. Når informationsstrømmen og beslutningstrykket bliver så intenst, at mennesker ikke kan følge med, bliver "meningsfuld menneskelig kontrol" ikke bare et princip; det bliver en tidsbuffer.

Og tidsbufferen er ofte det første, der bliver skåret væk.

Det er netop dér, moral injury får grobund: ikke kun i det, man gjorde, men i oplevelsen af, at man handlede uden at have plads til at mærke, vælge, tvivle eller forsvare sin egen menneskelighed i øjeblikket.

Empati, selektion og AI i militæret
Når lav-empati-profiler får et forstørrelsesglas

Der findes en ubehagelig dynamik i militære organisationer: I perioder og under bestemte kulturer kan man komme til at belønne profiler, der trives i hård tone, dominans og "mission først" - og som har lettere ved at lukke ned for tvivl, skyld og sekundære konsekvenser.

Når AI integreres i operative og administrative beslutninger, kan den kultur få et forstærkningsværktøj.

AI kan blive en moralsk støddæmper: et system, der gør det nemmere at reducere mennesker til sandsynligheder, træffe hårde valg uden følelsesmæssig friktion og gemme ansvar bag model-output: "systemet sagde…". Den type distance kan føles professionel. Men den kan også normalisere dehumanisering …ikke som en ond intention, men som en glidebane.

Hvis AI-brug i militæret ikke designes med etisk friktion og tydelige ansvarskæder, risikerer man i praksis at skabe et miljø, hvor mangel på empati ikke bare tolereres, men skaleres.

Det er ikke "føleri". Det er operativ sikkerhed: fejl og eskalation opstår ikke kun af dårlige data, men også af mennesker og kulturer, der ikke mærker konsekvensen tidligt nok.

AI må ikke blive et redskab, der belønner det menneske, som mærker mindst.
Den militære AI-æra kræver, at empati opgraderes fra "blød værdi" til operativ sikkerhed.

Hvem bør arbejde med militær AI?
Hvis vi mener det alvorligt, kan vi ikke bare uddele adgang og håbe på det bedste. Militær AI er en højrisiko-funktion, på linje med andre roller, hvor fejl og overgreb har irreversible konsekvenser.

Derfor giver det mening at tænke i roller og udvælgelse:

- Operatører og analytikere, der arbejder med output
- Beslutningstagere, der bærer ansvar
- Udviklere og leverandørkontakt
- Verifikation/audit (test, red teaming)
- Juridisk/etisk kontrol

"Bedst egnet" handler ikke om at være mest effektiv, men om at være mest ansvarlig under pres. Den bedst egnede er den, der kan arbejde hurtigt uden at miste tvivlen og som kan dokumentere, begrunde og stå på mål for konsekvensen, uden at gemme sig bag systemet.

Danmark: teknologi ja - men hvor ligger hullet?
Den danske kontekst er anderledes end USA. Her er teknologien ofte mere "supplement" end styrende infrastruktur.

På veteranområdet arbejder Veterancentret eksempelvis med virtual reality som et undersøgt behandlingsspor i psykologisk PTSD-behandling, og de har offentliggjort projekter på området. (Der findes også forskning, der peger på accept og effekt af VR-eksponering i en dansk veteran-kontekst, men med vægt på den terapeutiske alliance.)

På militær beslutningsstøtte-siden peger CMS-rapporten på både potentiale og faldgruber ved AI-DSS i dansk forsvars- og kommando-kontekst, især risikoen for, at mennesket bliver reduceret til formalitet.

Hullet er derfor ikke, at der intet sker. Hullet er, at de bindende rammer og de konkrete designkrav let kommer bagefter, mens integrationen presser sig på af tempo, trusselsbillede og alliancekrav.

USA: når AI allerede er infrastruktur (og hvorfor det er relevant)
I USA er AI i veteransystemet allerede mere systemisk, især i selvmordsforebyggelse og dokumentation.

Der findes et velkendt program i Veterans Health Administration, REACH VET, som løbende kører risikomodeller for selvmord og markerer personer i den højeste risikogruppe for målrettet opfølgning. Programmet arbejder med "top 0,1%"-tærskler og månedlige risikofremskrivninger.

På den administrative side har VA lanceret ambient AI scribe (AI, der hjælper med kliniske notater), og VA's egen kommunikation beskriver en udvidelse til alle VA medical centers i 2026 efter lancering i 2025.

Pointen er ikke "USA gør det rigtigt". Pointen er, at når AI bliver infrastruktur, bliver spørgsmål om ansvar, bias, audit og menneskelig kontrol ikke filosofi; det bliver hverdag.

AI i terapi: redskab, ikke autoritet
Jeg bruger selv AI i mit arbejde, men ikke som diagnose, dom eller erstatning for relation. AI kan være et redskab til:

- struktur og overblik
- sprogliggørelse af kaos
- spejling af mønstre
- forberedelse af svære samtaler
- "suppeterninger" - det vigtigste, uden at forfladige sandheden

Men AI må aldrig blive den, der har autoriteten. Den må aldrig blive den, man kan gemme sig bag.

I et traumefelt er menneskelig oversættelse ikke en detalje; det er selve princippet: AI kan generere ord, men kun mennesket kan mærke, hvad der er sandt i kroppen, hvad der er undvigelse forklædt som indsigt, og hvad der kan bæres ansvarligt.

Fem principper, der forhindrer "AI-superbrugere" uden empati:

1. Human-in-the-loop skal være reelt , ikke ceremonielt
Hvem tog beslutningen, hvorfor, og hvad blev fravalgt?

2. Etisk friktion som designkrav
Stop-punkter: begrundelse, konsekvensvurdering, alternativ-scenarie og hvem der rammes.

3. Empatisk kompetence i AI-rolle
Ikke som følelse, men som funktion: forståelse for sekundære konsekvenser, eskalation og menneskelig belastning.

4. Rotation og peer review
Følsomme outputs vurderes af flere, gerne tværfagligt, så én persons mønstre ikke får monopol.

5. Sprogpolitik: dehumanisering som rød linje
Når mennesker bliver til "targets", "units" eller "problem population", er misbruget allerede i gang.

Fire spørgsmål Danmark bør besvare, før tempoet gør det for os:
1. Kommer vi til at kræve meningsfuld menneskelig kontrol over alle beslutninger om magtanvendelse – som konkret regel, ikke kun princip?

2. Får vi ret til uafhængig audit og indsigt i AI-systemer, der påvirker beslutninger om magt, risikovurdering og proportionalitet?

3. Hvem har ansvaret, når AI-beslutningsstøtte skubber tvivl til handling - politisk, juridisk og personligt?

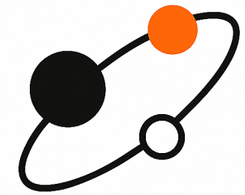
4. Hvilke røde linjer vil Danmark ikke krydse – heller ikke under alliancepres og trusselseskalation?

Hvis de spørgsmål ikke besvares, får vi en virkelighed, hvor mennesket stadig hæfter, men ikke længere styrer.

Fra veteran til vidne
Jeg har set krig tæt på.
Jeg har set eftervirkningen endnu tættere.

Afstand fjerner ikke smerten. Den udskyder den.
Og tempo kan gøre det lettere at handle, men tungere at leve med bagefter.

AI gør ikke krig mindre brutal. Den gør den mere gennemførlig.
Vi designer ikke fred. Vi designer effektivitet.
Og effektivitet gør det lettere at gøre det, vi egentlig ikke burde gøre.



KRIG OG AI

Af Nicolai Hyldested

Som mennesker nedbrydes vi af den. Af konstant tvivl, konstant alarmberedskab, konstant behov for at vurdere, hvad der er ægte, og hvad der er manipulation. Over tid slider det på dømmekraften, på psyken og på evnen til at handle ansvarligt.
Så vi har gjort noget meget menneskeligt:
Vi har outsourcet den.
I store centre i Sydøstasien sidder mennesker og sorterer det værste, informationsrummet har at byde på. Vold, had, propaganda, misinformation. De ser det, vi ikke vil se. De bærer den mentale belastning, så resten af verden kan bevare illusionen om et nogenlunde civiliseret informationsmiljø. Det er ikke fordi, de er bedre rustet. Det er fordi, de er billigere.
Vi har allerede accepteret, at en del af den kognitive nedbrydning, som følger med konstant usikkerhed, kan flyttes væk fra os selv. Ikke fordi arbejdet er ufarligt, men fordi det kan defineres som lav følsomhed.
Der er ikke langt fra den type arbejde til militært relevant informationsarbejde, der formelt set også kan betegnes som lavt følsomt: filtrering, mønstergenkendelse, prioritering, analyse.
Opgaver, der ikke affyrer våben, men som former beslutningsgrundlaget for dem, der gør.
Det er ikke en påstand om, at militære beslutninger allerede er outsourcet. Det er en konstatering af, at den organisatoriske og psykologiske logik, der gør det muligt, allerede eksisterer.
I en sag fra sidste år blev det tydeligt, hvor let informationsrummet kan flyttes – ikke over måneder, men over timer. En fortælling opstod, spredte sig og satte sig fast i systemer, mange opfatter som neutrale og autoritative. Sagen endte med at omhandle Flügger og påstande om brud på sanktioner og handel med Rusland.
Det afgørende her er ikke virksomhedens ansvar eller sagens endelige udfald. Det afgørende er, at efterfølgende analyser viste, at informationsstrømmen ikke opstod tilfældigt. Den kunne føres tilbage til et organiseret miljø med forbindelser til russiske aktører, og der blev dokumenteret økonomiske spor i samme retning.
Informationsrummet blev ikke bare påvirket. Det blev bevidst manipuleret.
Manipulationen skete uden hacking, uden overtagelse af systemer og uden tekniske brud. Systemerne fungerede, som de var designet til at fungere. Og netop derfor virkede det.
På meget kort tid blev et komplekst sagsforløb reduceret til en entydig fortælling, som bredte sig på tværs af søgemaskiner, medier og platforme. Ikke fordi den var verificeret, men fordi den var genkendelig, gentaget og strukturelt kompatibel med de systemer, der sorterer information for os.
Det viser noget ubehageligt: at informationssystemer kan bringes i ubalance uden magt, uden adgang og uden regelbrud. Det kræver ikke kontrol over systemet. Det kræver forståelse for det.
Og det er her paradokset for alvor begynder.
Vi kender fortællingen. To mænd står i et rum, begge skal dreje på hver sin nøgle samtidig. Ingen kan handle alene. Systemet er bygget til at forhindre fejl, panik og vanvid. Det er billedet på menneskelig kontrol i sin reneste form.
Men i en AI-tidsalder modtager de to mænd ikke længere uafhængig information. De ser det samme billede, filtreret gennem de samme modeller, de samme datasæt, de samme bias. Det er ikke to vurderinger. Det er én algoritmisk fortolkning, spejlet to gange, under ekstremt pres.
Og presset er nyt. Vi taler ikke længere minutter eller halve timer. I nogle scenarier taler vi millisekunder. Eskalation kan være i gang, før nogen ved, at den er begyndt.
En AI uden regler, guardrails og runtime-begrænsninger er farlig. Den kan stikke af, blive uregerlig, reagere uforudsigeligt. Som et barn uden opsyn. Men den har én fordel: den kan ændre sig i takt med verden, som den faktisk er.
Det modsatte lyder sikkert. Klare regler. Faste grænser. Præcise rammer for adfærd. Det føles ansvarligt. Det føles trygt.
Problemet er bare, at verden ikke følger regler.
I et informationsrum præget af real-time data, misinformation og bevidst manipulation fra aktører, der er fuldstændig ligeglade med normer og aftaler, bliver rigide AI-systemer ikke stabile. De bliver blinde. De reagerer mekanisk på mønstre, der ligner noget kendt, også når signalerne er falske.
Disse signaler præsenteres for et *human-in-the-loop*, hvor erfaringen langsomt har lært operatøren, at AI'en som regel har ret. Og så får mennesket sekunder til at handle. Ikke tid til refleksion. Ikke tid til tvivl. Sekunder.
Falsk tryghed viser sig her at være farligere end kendt utryghed. Når vi ved, at noget er usikkert, kompenserer vi. Vi sætter tempoet ned. Vi tvivler. Når noget føles sikkert, slipper vi kontrollen.
Men det omvendte er heller ikke muligt.
Mennesker kan ikke leve i konstant kognitiv usikkerhed uden at tage skade. Og de få mennesker, der kan fungere upåvirket i permanent usikkerhed, er måske ikke dem, vi ønsker sidder med beslutninger, hvor konsekvenserne er irreversible.
Paradokset er derfor uløseligt.
Vi kan ikke lade AI handle uden menneskelig endelig beslutning.
Men vi kan heller ikke bygge systemer, hvor mennesket kun er en juridisk bremse, fanget mellem falsk tryghed og ekstremt tidspres.
Verden bliver ikke nødvendigvis mere sikker.
Der sker bare ting hurtigere.
Og det kan føles som kontrol.

Jeg kunne lade dig, læser, sidde tilbage med et spørgsmålstegn og give dig plads til selv at tænke videre. Men det ville samtidig give indtryk af, at jeg har et svar. At der findes en løsning på de paradokser, der er skitseret ovenfor.
Det ved jeg ikke, om der gør. Og jeg er heller ikke sikker på, at det overhovedet er et relevant spørgsmål i en krisesituation.
Krig er beskidt.
Mennesker bliver ofre.
Og måske er det netop her, i informationskrigen, at vi som nation kommer til at betale prisen. Ikke fordi vi valgte det, men fordi der ikke fandtes et alternativ der var mindre grimt.

MÅNEDENS SINGULARITET:

INTERNETTET SOM DET KUNNE HAVE VÆRET

- PROJECT CYBERSYN OG DET TABTE SPOR I DEN DIGTIALE HISTORIE

AF MARK SINCLAIR FLEETON

Illustration genereret med ChatGPT

I

En smuk forårsdag i november 1971 ankommer en mand med fly fra England i lufthavnen i Santiago de Chile. Hans navn er Stafford Beer og han er på daværende tidspunkt en af de højst betalte management konsulenter i verden. Han ligner mere en guru end en management konsulent. Nogle beskriver ham ligefrem som en blanding af Orson Welles og Sokrates. Videnskabsmand, poet, maler og ikke mindst opfinderen af Management Cybernetics (på dansk nogen gange kaldet ledelsescybernetik). Han er en stor mand med en imponerende tilstedeværelse og hans ankomst varsler en ny tid indenfor computernetværk. En ny tid, der skal bane vejen for det første for det, der senere bliver internettet og ultimativt til det vi i dag kalder kunstig intelligens. Han er på vej til at sætte gang i et forsøg. Et forsøg, der kunne have resulteret i et radikalt anderledes internet og måske også i mere menneskevenlig AI. Forsøget er i sidste ende dødsdømt fra starten, men det ved Beer ikke på det tidspunkt og det er ikke sikkert, at det havde gjort en forskel, hvis han gjorde. Beer ser systemskiftet i Chile i 1970, som en mulighed for at folde hans teorier om levedygtige systemer ud på et nationalt niveau. Indtil da har han arbejdet med virksomheder. Store virksomheder, men ikke med et helt land. Set fra i dag fremstår historien om Project Cybersyn ikke blot som et historisk kuriosum, men som et tidligt bud på en digital infrastruktur, der tog demokrati alvorligt – på en måde, som nutidens AI-systemer ofte ikke gør.

II

Salvador Allende kommer til magten i Chile efter valget den 4. september 1970 for den venstreorienterede politiske alliance Unidad Popular (UP). Det er på ingen måde en jordskredssejr og ingen præsidentkandidat får det nødvendige flertal. Han sidder altså både på et spinkelt mandat og som socialist er hans regering ikke ligefrem populær hos CIA. Der var en aktiv kampagne i gang mod udpegelsen af Allende som præsident. Dels var de ellers dominerende kristendemokratiske senatorer bekymrede for UP's demokratiske sindelag, men udsigten til en socialistisk regering og nationalisering af flere brancher i landet var bekymrende for CIA og USA i det hele taget.

Men Allende er ikke en typisk socialist. Som socialist går han ind for politik som noget, der bliver styret oppefra – centraliseret topstyring. Men der hvor Allende adskiller sig fra andre socialistiske regeringer på det tidspunkt, er hans demokratiske ideer. For han og hans tilhængere ser ikke en modsætning i at man samtidigt med en topstyret politik sikrer demokratiske friheder og udvider deltagelsen i den politiske projekt. De kalder det selv for "den chilenske vej til socialisme". Allendes forgænger har allerede delvist nationaliseret den afgørende kobber-industri i landet, der også er USA's største interesse i Chile.

Der er bred støtte i kongressen til Allendes økonomiske politik og efter visse forsikringer om, at han rent faktisk går ind for en demokratisk styreform, stiller den primært kristendemokratiske kongres, sig bag Allende og hans socialistiske regering.

Allende repræsenterer en mere moderat form for socialisme og han mener ikke, at den revolutionære proces behøver at ødelægge det eksisterende institutionelle og konstitutionelle regime, som han selv formulerer det. Centralt for hans politik er gennemgribende omfordeling af jorden i landet og en gennemgribende organisering af arbejderklassen. Sagt på en anden måde, så ønsker han et system, der er stabilt, demokratisk og som i langt højere grad inkluderer hele befolkningen i den politiske beslutningsproces.

III

Cybernetics er læren om styring og kontrol via feedback i systmer. Gennem input måler systemet sin tilstand og forholder det til dens mål (den tilstand man ønsker systemet skal være i). På den baggrund handler systemet for at justere i den ønskede retning (producerer et output), som herefter danner feedback til systemets forsættelse. Siden 1800-tallet er der blevet bygget maskiner, systemer og motorer, der kunne holde kursen af sig selv ved at "mærke" afvigelser og kompensere for det. Den amerikanske matematiker og filosof Norbert Wiener havde allerede under første verdenskrig arbejdet med ballistik eller læren om projektilbaner. Under 2. verdenskrig arbejdede han målrettet med luftværn. Når du skyder mod et fly, rammer du ikke der, hvor flyet er nu, men der hvor det forventes at være, når granaten når frem. Det betyder, at man skal kunne forudsige flyets bane ud fra løbende målinger. I løbet af 1940'erne begynder forskere fra mange felter, at dyr, mennesker, maskiner og organisationer alle kan forstås som noget, der prøver at styre sig selv i en verden fuld af forstyrrelser. Wiener sætter ord på i 1948 og ordet han vælger er cybernetics forstået som styring og kommunikation i både levende væsener og maskiner. Styring forstået ikke som tvang eller topstyring, men som information,

signaler og beslutninger. Central for cybernetics er ideen om kontrol gennem balance – en balance, der kontinuerligt skal opretholdes gennem feedback.

I dag er mange af de samme cybernetiske grundidéer indlejret i moderne AI-systemer. Maskinlæring og algoritmisk styring bygger på kontinuerlige feedback-sløjfer, hvor systemer trænes på historiske data, anvendes i praksis og justeres ud fra deres resultater. Anbefalingssystemer, risikomodeller, sagsbehandlingsværktøjer og automatiserede beslutningssystemer måler løbende adfærd, sammenholder den med definerede mål – effektivitet, engagement, risikominimering – og justerer deres output derefter. Forskellen er, at feedbacken i dag ofte er langt mere finmasket og individnær, og at systemerne i stigende grad ikke blot reagerer på verden, men aktivt former den. Dermed bliver cybernetics ikke blot en historisk teori om styring, men et aktuelt spørgsmål om, hvem der definerer målene, hvilke data der tæller som signaler, og hvordan balancen mellem effektivitet, rettigheder og demokrati forhandles, når styring i stigende grad udføres af intelligente systemer.

IV

Stafford Beer bringer cybernetikken fra laboratoriet og ud i virkeligheden. Efter hans tid i hæren blev han ansat i United Steel i Yorkshire, der var en stålproducerende, ingeniør- og minevirksomhed. Her overbeviser han dem om, at de skal oprette en afdeling for produktions research og cybernetik, som han selv skal lede. Afdelingen var centreret omkring en Ferranti Pegasus, der var den første computer i verden dedikeret til at arbejde med management cybernetik. Beer efterlader United Steel med en institution (Cybor House) og en metodekultur (feedback, simulering, tværfaglige teams) der fjorde styring af kompleks industri til et system- og informationsproblem og ikke bare et hierarki-problem. Beer forlader United Steel i 1962 for at grundlægge produktions research konsulentfirmaet SIGMA, som han forlader igen i 1966 for at arbejde for SIGMA-kunden International Publishing Corporation (IPC), som han forlader i 1970 for at blive selvstændig konsulent.

Beers har tre centrale ideer. For det første ser han organisationen som et reguleringssystem på linje med en krop eller et økosystem. Virksomheden skal kunne registrere ændringer, reagere, lære og stabilere sig via feedback-loops. For det andet

Computer-generated image of Project CyberSyn operations room

han ud fra det hans landsmand og en anden af cybernetikkens fædre, W. Ross Ashbys, ”Lov om den nødvendige variation”. Den siger, at styringen skal have tilstrækkelig variation til at matche omgivelsernes variation. I Beers verden bliver det til: dæmp variationen, hvor den kan standardiseres og forstærk variationen, der hvor lokalt skøn og innovation er nødvendigt. For det tredje udvikler Beer, det han kalder, The Viable System Model eller VSM (den levedygtige system-model). Ifølge VSM er en organisation levedygtig, når fem nødvendige funktioner er på plads og forbundet rigtigt:

1. Drift (value creation)
2. Koordination (undgå friktion mellem driftsenheder)
3. Kontrol/ressorucestyring (intern stabilitet, audit, allokering)
4. Intelligens (omverden, strategi, fremtidsscan)
5. Policy/identitet (formål, værdier, endelig beslutningsautoritet)

Pointen er ikke ”flere chefer”, men klar funktionel balance mellem stabil drift og adaption.

V

I Chile har Allende-regeringen udpeget den kun 28-årige Fernando Flores til teknisk direktør for det statslige produktionsudviklings selskab (CORFO), der var ansvarlig for nationaliseringen af den chilenske industri. Flores er godt nok ung, men han har en solid baggrund indenfor den akademiske verden og fra stålindustrien, hvor han blandt andet har arbejdet for Beers SIGMA, der var blevet ansat af direktøren for Chiles stålindustri i 1962. Derfor kender Flores til Beers teorier og arbejde og han ser et overlap mellem ideerne i Beers management cybernetics og den chilenske vej til socialisme. Flores mener, at Beer kan komme med vigtige input til hvordan Allendes demokratiske socialisme kan kombinere individets autonomitet med fællesskabets behov. Flores ser ligheder fordi den chilenske regering ønsker at foretage strukturelle ændringer i samfundet hurtigt, men samtidigt sikre de demokratiske institutioner. Samtidigt ønsker regeringen ikke bare at tvinge ændringerne ned over hovedet på det chilenske folk, men ønsker tværtimod at involvere dem i processen. Den chilenske demokratiske socialisme ønsker dermed, med andre ord, ligesom management cybernetics at finde en balance – en balance mellem central kontrol og individuel frihed.

Da han skriver til Stafford Beer og forklarer sig, forestiller Flores sig nok, at Beer sender en af sine konsulenter. Han regner ikke med, at Beer selv vil komme til Chile. Men Beer genkender ideerne i den chilenske revolution som et menneskeligt og samfundsmæssigt udtryk for hans cybernetiske modeller. Gennem 1960’erne og de tidlige 1970’ere er Beers interesse for brugen af cybernetik til samfundsforandringer og til at forbedre effektivitet hos regeringer stigende. Udover sin Viable Systems Model har Beer i 1970 foreslået en model han kalder The Liberty Machine – frihedsmaskinen. Han ser denne Liberty Machine, som et socioteknisk system, der fungerer som et distribueret netværk, der behandler information og ikke autoritet som basis for handlinger. Beers påstand er, at dette system fremmer handling fremfor bureaukratisk praksis. Maskinen distribuerer beslutninger ud på forskellige dele af administrationen, men koordineret fra centralt hold. På den måde opnår systemet en balance mellem individuel frihed og centraliseret kontrol. I Beers vision er Liberty Machine en fysisk konstruktion bestående af flere ”operations rooms” – kontrolrum – der modtager realtime informationernes indhold. Beer beskriver, dem der skal betjene disse rum Beer som ”ansvarlige offentligt ansatte underlagt konstituelle herrer”, der skal bruge information til at kørere simuleringer og generere hypoteser om fremtidig system adfærd.

VI

Adgangen til computer mainframes i Chile var ret begrænset i 1971. Regeringen havde helt præcist adgang til at bruge fire mainframes, der ikke nødvendigvis var top-of-the-line-modeller. Derimod havde man stor erfaring med brug af computere i centraladministrationen. Allerede i 1960’erne havde man investeret store midler i uddannelse af offentligt ansatte i brugen af computere. Da Beer ankom til Chile i 1972 brugte han otte hektiske dage på i samarbejde med Flores og flere andre, at diagnosticere svagheder i den offentlige administration og finde løsninger. Direktøren for the National Computer Corporation (ECOM), det statslige computerselskab, Raimundo Beca, kunne tilbyde Beer brugen af lige præcis én

mainframe computer – en IBM 360/50 – der så til gengæld var ECOM's topmodel. Beer og de chilenske medarbejdere på projektet stod altså overfor at opbygge et computernetværk bestående af én computer!

Resultatet var Project Cyberstryde. Det man havde brug for var realtime information om produktionsprocesserne ude på fabrikkerne: tilgang af råmaterialer, produktions output, tal for fraværd osv. Man havde ikke computere lokalt. Det man havde var telex-maskiner. Derfor blev netværket opbygget af telex-maskiner, der alle sammen rapporterede ind til den centrale computer.

V

Beer præsenterer Project Cyberstride for vice økonomiminister Oscar Guillermo Garretón den 12. november 1972. Efter han havde fået viceministerens godkendelse, går han over gaden til præsidentpaladset, hvor han skulle præsentere ideen for Allende til hans endelige godkendelse. Beer forklarer Allende om sit arbejde med management cybernetics og hans Viable System Model. Allende er uddannet patolog og han forstår straks den biologiske inspiration til modellen og kan derfor udmærket følge Beers forklaring på hans projekt. Beer selv udtaler flere år senere: "*Jeg forklarede hele planen og hele Viable System Modellen i en omgang... og jeg har aldrig arbejdet med nogen på højt niveau, der forstod hvad jeg snakkede om.*" Efter godkendelse rejser Beer hjem til England og efterlader det chilenske team, til at implementere hans ide.

I marts 1972 er Beer tilbage i Santiago. Projektet skal for alvor foldes ud og Project Cybersyn (cybernetics + synergy) ser dagens lys. Cyberstride betegner nu softwaredelen af systemet – udviklet i samarbejde med konsulentfirmaet Arthur Andersen og ECOM – der overvåger fabriksperformance. Dertil kommer Cybernet (telexnetværket), CHECO (Chilean ECOnomy, der er en økonomisk simulator og Opsroom (operationsrummet) – virkeliggørelsen af Beers Liberty Machine, som beslutnings- og koordineringscenter.

VI

Allende-regeringens nationaliseringsprojekt er en succes ikke mindst på grund af Project Cybersyn. I perioden fra 1971 til 1972 øger man GDP med 7,7 % og opnår en stigning på 13.7 % i produktionen. Cybersyn skal sørge for at den udvikling forsætter og styrkes. I oktober 1972 er Cybersyn oppe at køre effektivt. Telex netværket gør det muligt at kommunikere på tværs af regionen og vedligeholde distributionen af varer på tværs af landet. I oktober 1972 går arbejdsgiverne i aktion og iværksætter en landsdækkende strejke, der især påvirkede transport med lastbiler på tværs af landet. Strejken blev organiseret og finansieret af den chilenske erhvevssammenslutning og bakket op med midler fra CIA. Formålet var at destabilisere Allende-styret og gøre en ende på nationaliseringen af den chilenske industri. Takket være Project Cybersyn lykkes det at opretholde transporten af varer med kun 200 lastbiler. Ved hjælp af realtime data var Allende-regeringen i stand til at reagere på de konstant ændrede forhold under strejken og derved imødegå konsekvenserne.

VII

Den 11. september 1973 kulminerer modstanden mod Allende-regeringen, da en gruppe officerer under ledelse af general Augusto Pinochet overtager magten ved et militærkup. Fernando Flores er på dette tidspunkt en af Allendes nærmeste medarbejdere og han er sammen med Allende i præsidentpaladset, hvor han står for kommunikationen med militæret, der insisterer på Allendes totale, betingelsesløse overgivelse. Allende nægter. Flores bliver sendt afsted ud af huset for at forhandle direkte med militæret, men bliver arresteret i det øjeblik han forlader bygningen. Flores ser aldrig Allende igen. Kl. 2 er Allende død. Der er uklarhed over omstændighederne, men sandsynligvis er der tale om selvmord. Pinochet danner en militærjunta, der overtager magten i landet og Nixon-regeringen, der har været med til at fremme forudsætningerne for kuppet gennem en målrettet kampagne af økonomisk destabilisering – blandt andet ved strejken i 1972 – er blandt de første til at anerkende Pinochets styre.

Militæret undersøger Project Cybersyn efter kuppet. Medlemmer af projekt teamet bliver indkaldt og udspurgt om projektet. Måske forstår de ikke systemet. Måske erBeers ideer om decentralisering og tilpasning så modsat al militær tænkning om en hierarkisk struktur, så de afviser dem som uinteressante. Arbejdet på Project Cybersyn stopper efter kuppet og arbejdet inklusiv kontrolrummet ødelægges.

Selvom Cybersyn forsvandt med Allende, så forsatte Stafford Beer sit arbejde på hele det amerikanske kontinent. Han var konsulent fro regeringer i Canada, Mexico, Uruguay, Colombia og Venezuela. I 1980'erne og 1990'erne var han den del Uruguays succesfulde implementering af det overordnede informationssystem URUCIB (1986-1988). Han hjælp den Colombianske regering med en omstilling af den offentlige sektor med udgangspunkt i Viable System Model (1990-erne og 2000'erne). Flere projekter i Mexico og Venezuela blev dog forhindret af korruption og politisk uro. For Beer personligt ændrede oplevelsen ham grundlæggende. For det første udviklede han en intens modvilje overfor USA og dets politik med at blande sig i andre landes indre anliggender. I midten af 1970'erne flyttede han til Wales, hvor han levede yderst spartansk og arbejdede mere med poesi og kunst.

IX

Project Cybersyn var ikke tænkt som et system, hvor al magt blev trukket mod toppen. Tværtimod byggede projektet på et klart princip om subsidiaritet: Beslutninger skulle træffes så tæt på produktionen og hverdagen som muligt. Fabrikker og lokale enheder havde autonomi til selv at løse problemer, så længe de kunne holde sig inden for aftalte rammer. Først når bestemte grænser blev overskredet – fx. ved alvorlige flaskehalse eller sammenbrud – blev det centrale niveau aktiveret. Central styring var tænkt som en sikkerhedsventil, ikke som daglig mikromanagement.

Et andet bærende element i Cybersyn var idéen om feedback frem for kommando. Systemet skulle ikke udstede ordrer, men synliggøre afvigelser og mønstre, så mennesker kunne reagere informeret. De data, der blev indsamlet, var bevidst begrænsede og fokuserede på nøgletal frem for detaljer. Computeren pegede på, hvor noget var ved at komme ud af balance – men det var stadig ledere, arbejdere og politikere, der traf beslutningerne. Teknologien var tænkt som en støtte for menneskelig dømmekraft, ikke som en erstatning for den.

Endelig var gennemsigtighed og demokrati en central ambition. Cybersyn var designet med forestillingen om, at de samme informationer skulle kunne tilgås af flere aktører: arbejdere, fagforeninger, ledelse og politiske beslutningstagere. Det ikoniske operationsrum var ikke et hemmeligt kontrolcenter, men tænkt som et fælles rum for dialog og beslutningstagning. I stedet for at skjule magten i tekniske systemer var målet at gøre samfundets økonomiske tilstand synlig – og dermed politisk diskuterbar.

Det interessante paradoks er, at Project Cybersyn på flere afgørende punkter fremstår mere demokratisk ambitiøst end meget af den digitale infrastruktur, vi lever med i dag. Cybersyn arbejdede ikke med persondata, adfærdsprofiler eller individuel overvågning, men med aggregerede systemdata, der skulle gøre økonomien forståelig og styrbar som helhed. Omvendt bygger nutidens internetbaserede platforme på omfattende indsamling af data om individuelle brugere, ofte kombineret med uigennemsigtige algoritmer, der former adfærd uden offentlig indsigt eller demokratisk kontrol. Paradokset er, at et socialistisk cybernetisk projekt fra begyndelsen af 1970'erne i sin grundtanke lagde større vægt på gennemsigtighed, kollektiv indsigt og menneskelig beslutningskraft end mange af de digitale systemer, der i dag præsenteres som neutrale, effektive og teknologisk uundgåelige.

Project Cybersyn gør det tydeligt, at forbindelsen mellem cybernetics og dagens AI ikke først og fremmest handler om "smarte maskiner", men om styring gennem feedback: Man måler, fortolker og justerer for at holde et system i balance. I Cybersyn var målet at skabe et demokratisk "nervesystem" for økonomien med simple nøgletal og menneskelig beslutningstagning – computeren skulle pege på afvigelser, ikke træffe beslutninger. I dag er AI i stigende grad blevet det lag, der både tolker data og påvirker adfærd i realtid: algoritmer prioriterer indhold, forudsiger risiko, optimerer logistik, vurderer borgere og kunder, og foreslår – eller automatiserer – handlinger. Det rejser et cybernetisk kernespørgsmål i en ny skala: Hvem definerer, hvad "balance" betyder, hvilke mål der optimeres, og hvilke rettigheder der gælder, når systemet korrigerer? Cybersyn peger dermed på en nutidig blind vinkel: Vi diskuterer ofte AI som teknologi, men mindre som en styringsform – og netop dér bliver kravet om gennemsigtighed, ansvar og demokratisk forhandling afgørende, hvis AI ikke skal ende som et lukket kontrolsystem forklædt som effektivitet.

Project Cybersyn minder os om, at spørgsmålet ikke er, *om* vi skal styre samfundet med digitale systemer, men *hvordan* – og hvem der får lov til at definere balancen.

AI BASICS DEL 4:

AI TJENESTER I PRAKSIS

12 KATEGORIER, DER GIVER MENING FOR VIRKSOMHEDER

Skrevet af Kåre Bjørn Jensen assisteret af AI

Foto: Googledeepmind på Unsplash

De fleste organisationer starter med "en stor model" (typisk ChatGPT eller Microsoft Copilot) og opdager hurtigt, at den rigtige gevinst ofte ligger i specialiserede tjenester: værktøjer, der passer til en konkret arbejdsgang, kan dokumentere deres output, og kan sættes i drift uden at sprænge compliance-rammen. Samtidig vokser værktøjsjunglen eksplosivt, og derfor er et kurateret overblik mere værd end endnu en "top-100-liste". [1] (AIxploria)

Nedenfor er 12 kategorier, der typisk giver mening i virksomheder – med fokus på *hvornår* de giver mening:

1. 1Skriv & redigering (bl.a. mails, politikker, udbud, intranet)
2. Kode & udvikling (fra "hjælp i IDE'en" til egentlige kode-agenter)
3. Salg/CRM (bl.a. opkaldsnoter, pipeline-tekster, tilbud)
4. Kundeservice (bl.a. chat/voice, svarforslag, kvalitetstjek)
5. Analyse (bl.a. ad hoc-indsigter, dataforklaring, "forklar rapporten")
6. Præsentation (bl.a. slides, opsummeringer, struktur og talepunkter)
7. Video (bl.a. videogenerering, klip, undertekster, repurposing)
8. Billeder & design (bl.a. kampagner, mockups, variationer)
9. Viden-QA (RAG) – "spørg vores dokumenter" med kilder og sporbarhed [2] (arXiv)
10. Møder (bl.a. referater, beslutninger,opgaver)
11. Sikkerhed/guardrails (bl.a. politik, filtrering, datatab, logging)
12. Evaluering (bl.a. tests af kvalitet, bias, sikkerhed og driftssikkerhed)

Kode-kategorien – og hvorfor "vibe-coding" er på alles læber

I 2025–26 er kodeværktøjer gået fra "autocomplete" til *agentiske workflows*, hvor du beskriver en opgave i naturligt sprog, og værktøjet planlægger, ændrer flere filer, kører tests og foreslår et diff. Det er dét, mange omtaler som "vibe-coding": hurtig prototyping ved at "styre med intention" frem for at skrive alt selv.

Konkrete, moderne eksempler:

- GitHub Copilot Workspace: task → plan → kode → test, med tydelige trin og mulighed for review undervejs.
- Cursor: "Composer" + "Agent Mode" til multi-file ændringer og orkestrering i editoren.
- Windsurf: "Cascade" som agent med code/chat-modes, tool-calling og checkpoints. [6]
- Claude Code: terminalbaseret agentic coding, hvor best practices handler om struktur, kontekst og styring af agentens frihedsgrader.

Men: "vibe" skal kobles til "verify". I en stor survey blandt enterprise-udviklere siger 72% af dem, der har prøvet AI, at de bruger det dagligt – samtidig siger 96%, at de ikke stoler fuldt på output, og kun 48% verificerer *altid* før commit.

Og forskningen er nu mere nuanceret end de tidlige hype-tal: Et MIT-baseret felt-eksperiment finder ca. 26% flere løste opgaver pr. uge ved brug af Copilot i nogle organisationssettings, [9] mens METR i et RCT på erfarne open-source maintainere finder, at AI-værktøjer i deres setting gjorde udviklere 19% langsommere. [10] (metr.org)
Pointen til ledere: mål effekten i *jeres* kontekst – og design review, test og sikkerhed som en del af flowet.

Kriterier, når du vælger værktøj

Spørg især efter: compliance & dataveje, kildehenvisninger/traceability, dataejerskab og træning, export/API, og om værktøjet kan fungere i jeres identitets- og logningssetup.

Tre mini-cases (meget kort)

- Privat: Udviklingsteam bruger Copilot/ agentisk IDE til scaffolding + testgenerering, men kræver obligatorisk code review, SAST og dependency-scanning før merge.
- Offentlig: Fagsystem-nær "viden-QA" (RAG) på interne vejledninger, hvor svar altid leveres med kilder og tydelig markering af usikkerhed.
- SMV: Marketing + salg kombinerer skriveværktøj, billedværktøj og CRM-assistent – men kun efter at have afklaret, hvor data lagres, og hvordan output kan eksporteres.

Tjekliste: "prøv-før-du-køber"

1. Vælg *én* proces og *én* succeskriterie (tid, kvalitet eller risiko).
2. Test med rigtige data – men i en sikker ramme (anonymisering, adgang, logs).
3. Kræv sporbarhed: hvad bygger svaret på, og kan det auditeres?
4. Mål før/efter: cycle time, fejlrate, omkostning pr. opgave.
5. Beslut "go/no-go" og standarder: hvornår må AI skrive, og hvornår må den kun foreslå?

ANMELDELSE

MENNESKET VS. MASKINEN

EN MENNESKEVENLIG DIGITAL FREMTID

Af Mark Sinclair Fleeton

Hans-Petter Nygård-Hansen præsenter i sin bog "*Mennesket vs. Maskinen. Kampen om arbejde, mening og kontroll i algoritmenes tidsalder*" et forfriskende praksisnært bud på fremtiden med AI. Han ser fra sin norske position hvordan teknologien har udviklet sig fra hans udgangspunkt i 2020 og frem til han skriver bogen i 2025. Han beskriver hvordan teknologien har fået os til at stille spørgsmål til arbejdets natur allerede i dag. Vi er midt i en proces, hvor vi skal tage stilling til om vi skal arbejde mere, være mere effektive, arbejde hjemme osv. eller om maskinerne bare skal erstatte os helt. Han beskriver hvordan både arbejdsgivere og arbejdstagere er i vildrede om hvordan teknologien skal have lov til at præge arbejdslivet. Han beskriver bølgen af desinformation, techgiganternes magtmonopol og overgangen fra dataøkonomi til AI-økonomi.

Så langt ligner bogen mange andre bøger om AI, der bliver udgivet i disse dage. Nygård-Hansens diagnose er udmærket og fin at gå til som en hurtig indgang til emnet. Der hvor bogen dog bliver rigtigt interessant er dog den anden del, hvor han tager fat på fremtidens arbejdsliv, som indrammer til perioden 2026-2030.

Her kommer han ind på de egentlige og vigtige emner, som hvordan vi bevarer den mentale balance på et arbejdsmarkedet, hvor robotterne bygger i mørket i kæmpe lagerhaller. Hvordan skal man som ledelse forholde sig og hvad med tilliden?

Alt det her munder ud i at Nygård-Hansen formulerer en vision for en menneskevenlig digital fremtid. Hvad er det for et værdigrundlag og hvilke principper skal ligge til grund for udviklingen af teknologien og hvordan kan vi opstille reguleringsmæssige værn, der sikrer os overfor teknologien og ikke mindst overfor techgiganterne?

Svarene – eller i hvert fald Nygård-Hansens bud – finder du i bogen, der er let at gå til, men det gør den ikke mindre interessant. Godt nok er bogen på norsk – den er ikke oversat til dansk – men det burde ikke volde de store problemer.

I modsætning til den udbredte frygt for at blive erstattet af AI, så ser Nygård-Hansen teknologien som en mulighed for at finde tilbage til essensen af, hvad der gør vores job vigtigt. Både i forhold til vores eget arbejdsliv og i forhold til den værdi, som det giver for andre mennesker – virksomheden, kunder, samarbejdspartnere og så videre. Og det er måske bogens største værdi, at den tør tage stilling til det gode arbejdsliv og hvordan vi kan bruge teknologien til at bringe os derhen.

AI Hygge-økonomi 2.0

Af Mark Sinclair Fleeton

Hygge er noget med slumretæpper og stearinlys. Det er noget blødt og varm som en dyne. Eller er det? Kunne det måske være noget aktivt og innovationsskabende gennem fællesskab? Det mener i hvert fald Steffen Kirkegaard, der har skrevet bogen AI Hygge-økonomi 2.0.

”*Det er tid til at omdefinere 'hygge' fra passiv komfort til aktiv frigørelse og udnytte AI's kraft til at skabe en fremtid, der ikke kun er velstående, men dybt menneskelig.*”

Kirkegaard påpeger, at den kulturelle prædisposition for velvære, fællesskab og tilfredshed, som er typisk i Danmark er værdifuld, men den også resultere, at vi havner i en ”komfortfælde”, der gør det svært for os at tilpasse os til en virkelighed og en teknisk udvikling, der er sat på turbo.

Og når udviklingen foregår i så opskruet et tempo, hvordan kan demokratiske institutioner følge med og samtidigt repræsentere menneskelige interesser og operere gennem menneskelig dialog og særligt hvis vi står overfor en superintelligens – en ASI?

Kirkegaard karakteriserer udviklingen gennem to typer krise. Intelligenskrisen, der opstår i krydsfeltet mellem accelererende teknologisk kapacitet og iboende begrænsninger i menneskeskabte systemer.

Løsningen finder han i støttende regulatoriske rammer, men med en forståelse af, at for komplekse regler kan hæmme innovation. Her argumenterer Kirkegaard for en generel fastsættelse af selskabsskatten til 15 %. Det skal få danske virksomheder til at blive og tiltrække udenlandske virksomheder til at etablere sig i landet med en forøgelse af samfundsøkonomien som følge.

En veludformet universal basis indkomst - UBI - kan fungere som en stærk stabilisator, der sikrer at fordelene ved øget produktivitet deles bredt i samfundet. Med større stabilitet og færre bekymringer for borgerne som konsekvens

På samfundsplan argumenter Kirkegaard for det han kalder en ”Clean-Slate State Engine”. Det betyder grundlæggende, at man skal starte forfra med alle offentlige IT-systemer og erstatte forældede legacy-systemer med nye selvtilpassende AI-systemer.

Ændringer skal ske i et dybt integreret offentligt-privat partnerskab, der skal skabe en stærk motor til udvikling og implementering af AI-drevne løsninger. Samarbejdet skal sikre, at de regulatoriske rammer fremmer en hurtig teknologisk innovation samtidigt med at den offentlige sikkerhed og de etiske rammer er på plads.

Hygge som et operativt begreb handler primært om menneskelig trivsel. Frigjort fra begrænsninger og bekymringer er vi fri til at forfølge vores fulde potentiale. I takt med at vores teknologiske redskaber bliver stadigt mere intelligente, skal det bruges til at gøre vores liv ”mere meningsfulde, mere forbundne og mere fuldt ud menneskelige”.

AI ER OGSÅ FOR DIG

AI Portalen er skabt for at formidle AI konstruktivt og kritisk for alle.

BLIV MEDLEM - STØT UAFHÆNGIG JOURNALISTIK

Som medlem får du adgang til hele magasinet, artikler, events og fællesskab omkring AI Portalen.

Din støtte gør uafhængig journalistik om AI mulig.

AIPortalen.

Det seriøse medie om AI

www.ai-portalen.dk