AI voor een veilig Nederland: adviezen voor verantwoorde inzet

Position paper TNO voor het rondetafelgesprek over Informatiegestuurd optreden, Multi Domain Operations, en Defensie Strategie Data Science en AI 20 maart 2024

Inleiding

De input van TNO voor het rondetafelgesprek is gericht op operationaliseren van verantwoorde AI in het militaire domein, zoals verwoord in de Defensie Strategie Data Science en AI 2023-2027. TNO doet al decennia onderzoek naar (toekomstige) vormen van optreden van Defensie en de technologieontwikkelingen die hierbij ingezet kunnen worden. TNO is Nederlands grootste (onderzoeks)organisatie op het gebied van AI en Data Science (DS). Naast breed onderzoek naar AI in het programma Appl.Ai loopt er veel onderzoek naar specifieke toepassingen van AI voor Defensie, waarbij nauw wordt samengewerkt met industrie en NAVO partners.

Oproep aan de politiek

AI heeft de potentie om Defensie een voorsprong te geven op tegenstanders door verhoging van de effectiviteit en snelheid van het optreden. Defensie loopt momenteel achter in het gebruik van AI t.o.v. peer partners en tegenstanders. De huidige sterke media-aandacht voor risico's werkt verlammend op de besluitvorming en doorzetting. Hierdoor dreigt Defensie de aansluiting op partners en slagkracht tegen tegenstanders te verliezen. AI vraagt door een aantal intrinsieke eigenschappen en kenmerken van de Defensieomgeving extra aandacht. TNO roept daarom op om:

- Juridische, ethische en beleidsmatige kaders aan te passen aan AI-mogelijkheden en dreigingsbeeld;
- Keuzes te maken welke AI-capaciteiten soeverein ontwikkeld moeten worden;
- Door te pakken met verantwoord operationaliseren van AI.

Achtergrond

Defensie verwacht dat AI tot een grote verbetering van effectiviteit en snelheid van optreden kan leiden op gebieden van onbemande systemen, (militaire) besluitvorming ondersteuning & inlichtingen, logistiek & predictive maintenance, bedrijfsvoering en (bedrijfs)veiligheid. Huidige en toekomstige tegenstanders voelen zich minder gehinderd door potentiële risico's bij de inzet van AI en zetten hier vol op in. Hierdoor dreigt Defensie op (informatie)achterstand te komen, hetgeen grote gevolgen zal hebben voor de effectiviteit en snelheid op het slagveld. AI heeft een aantal intrinsieke eigenschappen en specifieke uitdagingen daar waar ingezet voor defensietoepassingen die verantwoorde en effectieve operationalisering van AI complex maken. Tegelijk lijkt er een schisma te zijn tussen de taakstelling van Defensie in combinatie met het huidige en toekomstig dreigingsbeeld en de juridische en beleidsmatige kaders met effect op de inzet van AI in het militaire domein. Hierdoor kan Defensie zich niet optimaal voorbereiden op oorlogvoering.

Visie en voorstellen

De ambitie en noodzaak voor Defensie om AI verantwoord en effectief in te zetten, maken dat op korte termijn een aantal keuzes gemaakt moet worden om het operationaliseren van verantwoorde AI te versnellen.

1. Juridische, ethische en beleidsmatige kaders aanpassen aan AI-mogelijkheden en dreigingsbeeld

Veel regelgeving is ofwel niet van toepassing op militaire applicaties (Europese AI Act), blijft vaag, of richt zich nog te weinig op de nieuwste AI-ontwikkelingen. Het rapport van de onderzoekscommissie LIMC[1]

1 Rapport "grondslag gezocht" van de Onderzoekscommissie Land Information Manoeuvre Centre (LIMC), o.l.v. dhr H. Brouwer

laat duidelijk zien dat de huidige juridische en beleidsmatige kaders niet in lijn zijn met het huidige dreigingsbeeld. Vanuit het adagium: "*train as you fight, fight as you train"*, moet Defensie in staat zijn om ook in vredestijd veilig en gecontroleerd te oefenen met AI in het informatie/cyber domein en robotica in het fysieke domein. Hiervoor is het noodzakelijk om data te verzamelen, data te analyseren en ervaring op te doen met het gebruik van algoritmes. Dit is in oorlogstijd en tijdens missies toegestaan, maar in vredestijd zijn er diverse restricties die dit onmogelijk maken. Als gevolg kan Defensie zich niet effectief voorbereiden op de inzet en het gebruik van AI in verschillende operaties, waar tegenstanders zoals Rusland dit wel doen.

TNO adviseert de politiek niet dat de regels overboord gegooid moeten worden, maar wel dat de mogelijkheid gecreëerd moet worden om binnen de regels, door specifieke ontheffing (op o.a. AVG), of met een specifieke Defensiewet te trainen, effectief algoritmes te ontwikkelen en tegelijk mogelijke risico's te mitigeren.

2. Keuzes maken voor capaciteiten die soeverein ontwikkeld moeten worden

Nederland (en Europa) heeft niet de capaciteit om voor alle toepassingen zelf AI-capaciteiten te ontwikkelen. Tegelijk kan en wil Nederland voor een aantal toepassingen niet afhankelijk zijn van derden. Dit impliceert dat voor toepassingen van strategisch belang, Nederland zelf (of met vertrouwde partners) in staat moet zijn om deze capaciteiten te ontwikkelen. Dit geldt vooral voor:

- Toepassingen waarbij de betrouwbaarheid van het model (en het vaststellen daarvan) cruciaal is;
- Toepassingen waarbij de data en/of het model vertrouwelijk is;
- AI-modellen waarmee een strategische voorsprong op de tegenstander verkregen kan worden;
- AI-modellen voor sturing van kritieke infrastructuur en logistiek.

TNO roept de politiek op keuzes te maken, dan wel kaders vast te stellen voor welke capaciteiten soevereiniteit noodzakelijk is en dus eigen ontwikkeling rechtvaardigen en daar vervolgens op sturen. Daartoe dient nationaal of Europees een innovatie-ecosysteem, bestaande uit academia, kennisinstituten, industrie en defensie ingericht en versterkt te worden en aanbestedingstechnisch mogelijk gemaakt.

3. Doorpakken met verantwoord operationaliseren van AI

Voor het verantwoord operationaliseren van AI bestaan geen generieke oplossingen; er moet altijd gekeken worden naar een concrete invulling, van een concreet systeem, te gebruiken in een concrete context. Verantwoorde inzet van AI voor Defensie vraagt daarom om een integrale multidisciplinaire aanpak, en een veilige en betrouwbare ontwikkel/ experimenteer/ trainingsomgeving (sandbox) voor AI-systemen, waar ervaring over de effectiviteit en risico's gedurende de gehele levenscyclus (beleid, ontwerp, ontwikkeling, ontplooiing, inzet en afstoting) vastgesteld kan worden[2]. Hierin ligt een belangrijke rol voor de politiek om samen met experts (wetenschappers, ontwerpers, militaire eindgebruikers, juristen, maatschappelijke organisaties, etc.) de governance in te richten voor het verantwoord operationaliseren van AI. Waaronder het invullen van en creëren van kaders voor de belangrijke randvoorwaarden van verantwoorde en effectieve inzet, zoals:

- Data governance, -kwaliteit en -beschikbaarheid, essentieel voor het trainen van goede AI-modellen, extra uitdagend bij vertrouwelijke informatie;
- Verificatie en validatie van ontwikkelde, aangeschafte of door derden beschikbaar gestelde AI-systemen inclusief de tijdens de levensduur bijlerende systemen;
- Robuustheid en resilience van AI-systemen: het vermogen om bestand te zijn tegen natuurlijke en gerichte (Counter AI) verstoringen en daarvan te herstellen;

TNO roept de politiek op om haar verantwoordelijkheid te nemen in de governance van AI, Defensie in staat te stellen deze randvoorwaarden in te vullen door in te stemmen met de Defensiestrategie AI en Data Science, en tenslotte toe te zien op de naleving ervan.

Contactpersoon: Tim Kreuk, manager Public Affairs (tim.kreuk@tno.nl)

[2] Voor een mogelijke aanpak zie TNO REAIM white paper "Operationalization of Meaningfull Human Control for Military AI, P. Elands, .e.a.