Zes uitdagingen voor artificiële intelligentie binnen Defensie

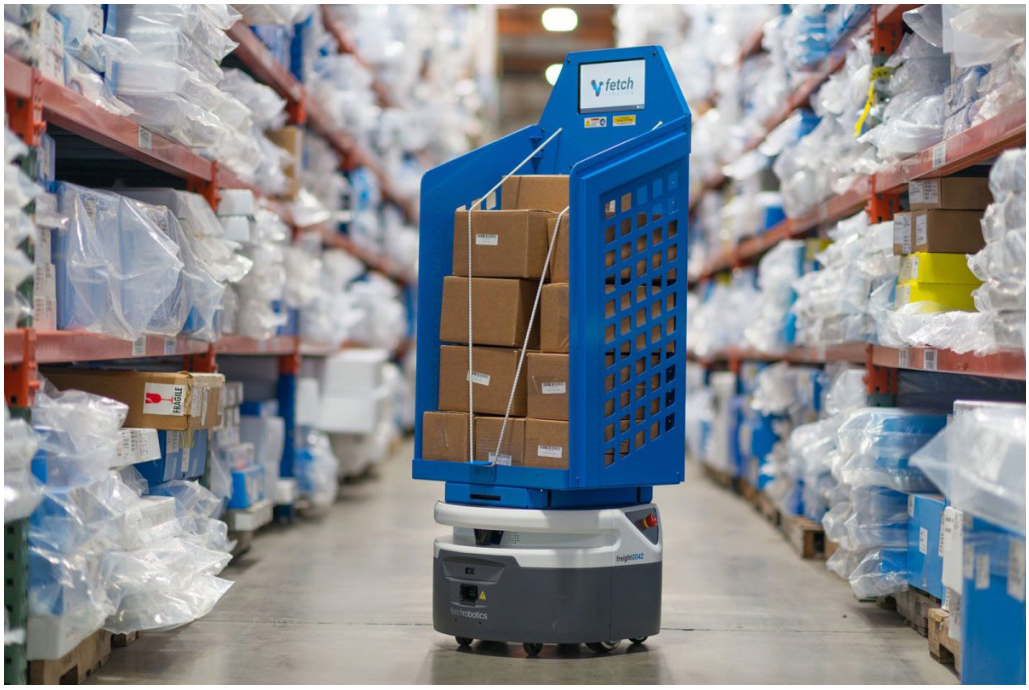
Gunther GODEFRIDIS

Na het volbrengen van zijn Hogere Stafopleiding met de 132ste promotie werd luitenant kolonel stafbrevethouder Godefridis, ir. tewerkgesteld in de Belgische *National Armament Directorate*. Vanuit zijn functie volgt hij de huidige trends van de technologische en industriële markten nauw op en neemt hij deel aan meerdere regionale, nationale en internationale inspanningen in het domein van innovatie en artificiële intelligentie.

L'intelligence artificielle (IA) n'est pas une nouveauté. L'histoire de l'IA se compose d'une succession d'attentes et de déceptions. L'émergence des nouvelles technologies accentue l'essor de l'intelligence artificielle. Les développements actuels apportent de nouvelles opportunités et de nouveaux défis. Les nombreux développements préliminaires, conditions de mise en œuvre et défis à relever rendent l'introduction optimale de cette technologie extrêmement complexe : chaque étape nécessite sa propre expertise spécifique. Alors, comment s'assurer d'une IA fiable et quels sont les défis pour une introduction réussie au sein de la Défense ? Le présent article donne un aperçu général de certains défis auxquels la Défense sera confrontée.

Artificiële of kunstmatige intelligentie (AI) is niet nieuw. De eerste dromen over AI worden aangehaald in het epos de Ilias van Homerus en dateren van de 9de - 8ste eeuw v.Chr. De geboorte van AI als vakgebied dateert echter van 1956 wanneer John McCarthy, Marvin Minsky, Allen Newell en Herbert Simon er de basis voor legden. De vierenzestigjarige geschiedenis van AI is er een van hooggespannen verwachtingen die telkens weer leiden tot tegenvallers en teleurstellingen. De laatste tien jaar is opnieuw een periode van enthousiasme en hoop daar diverse doorbraken elkaar in snel tempo opvolgen. Er bestaat echter geen officiële definitie van AI. Er kan wel gesteld worden dat AI een benaming is van een technologische evolutie in het domein van

de ontwikkeling van algoritmes waarbij de huidige en toekomstige technologische toepassingen een vorm van intelligentie krijgen. Hiermee kunnen deze toepassingen autonoom analyseren, begrijpen en interageren teneinde de capaciteiten van mens en organisatie te vergroten. De opkomst van *Learning Systems* en de introductie van AI-toepassingen in de bestaande technologiegebieden bieden nieuwe mogelijkheden maar ook bedreigingen, zowel binnen een breed maatschappelijk kader als binnen het veiligheidsdomein. Het introduceren van toonaangevende AI wordt aanzien als een strategisch instrument om superioriteit te behouden of te behalen.



© Fetch Robotics

Voorbeeld van hedendaagse AI-toepassingen: logistiek

Inzake militaire toepassingen werd er reeds vele malen met doorgedreven autonomie geëxperimenteerd en steeds met wisselend succes. De technologie was nog niet voldoende geëvolueerd om een 'onvoorwaardelijk' vertrouwen te genieten van de menselijke gebruiker. De huidige vooruitzichten creëren echter de verwachtingen dat de actuele ontwikkelingen inzake AI niet alleen revolutionair zullen zijn voor C4ISR[1]-

[1] *Acroniem voor Command, Control, Communication, Computer, Intelligence, Surveillance & Reconnaissance*

toepassingen maar voor de volledige werking van Defensie, in al zijn facetten. De meerdere voorafgaandelijke ontwikkelingen, uitvoeringsvoorwaarden en uitdagingen maken de optimale introductie van deze technologie uiterst complex: elke facet vereist een eigen specifieke expertise. De volgende paragrafen geven een algemeen overzicht van een aantal uitdagingen die Defensie te wachten staan.

De drie essentiële uitdagingen voor Defensie omtrent betrouwbare AI

Wegsturend van de stigmatiserende discussies toegespitst op *Lethal Autonomous Weapon Systems* (LAWS) is het evident dat de centrale eis omtrent AI-algoritmen, zoals voor alle software, betrouwbaarheid is. Betrouwbare AI voldoet aan drie voorwaarden: wettig, ethisch en robuust.

Wettig – **AI voldoet aan wet- en regelgeving** – De snelle opkomst van AI vraagt om regulering van verantwoordelijkheid, maar ook om juridische context en een samenhangend regelgevingskader. De vraag wie er verantwoordelijkheid draagt bij aansprakelijkheid van AI is een van de belangrijke juridische kwesties die nog niet geheel uitgeklaard zijn. Vaak bestaan er slechts enkele voorschriften maar nog geen eenduidige, dwingende wettelijke regelgeving. Binnen het breed maatschappelijk kader is de wetgeving er dus nog niet volledig klaar voor, laat staan binnen het veiligheidsdomein. Ondanks het feit dat men vanuit juridisch-technisch perspectief een onderscheid kan maken tussen de fysieke machine zelf en het algoritme dat de machine bestuurt, kan het ontbreken van de menselijke factor echter problematisch zijn bij schuld- en risicoaansprakelijkheid.

Op 21 november 2019 publiceerde de Europese *Expert Group on Liability and New Technologies* haar verslag waarin ze de brede principes formuleert over hoe om te gaan met schade en aansprakelijkheid bij technologische innovaties zoals AI in de EU. Haar studie buigt zich over bestaande juridische mechanismes en stelt zich de vraag of deze wel voldoende in staat zijn om zich aan te passen aan de in hoog tempo veranderende technologieën. Er wordt verwacht dat dit verslag nieuwe initiatieven zal voeden die uiteindelijk dienen uit te monden in een aanpassing van Europese richtlijnen en in de noodzakelijk concrete aanbevelingen voor de aanpassing van nationale wetgevingen.

Teneinde deze resultaten niet passief af te wachten en constructief deel te kunnen nemen aan het debat, is het uitermate belangrijk voor Defensie om te (blijven) investeren in gespecialiseerde juristen en raadgevers inzake de toegepaste en toekomstige rechtsleer in het domein van (militaire) AI-systemen.

Ethisch – **AI respecteert waarden en normen** – Indien we niet oppassen kan AI belangrijke grondrechten en publieke waarden onder druk zetten, zoals verbod van discriminatie, menselijke waardigheid en autonomie. Een voorbeeld hiervan is de Chinese sociale scorekaart AI-toepassing waarbij alle inwoners 24/7 in het oog worden gehouden en gerangschikt worden volgens hun gedrag. Hierbij wordt rekening gehouden met actuele gedragingen maar ook met individuele informatie zoals medisch, academisch, financieel en internet gebruik. Onder slechte gedragingen wordt verstaan: te laat rekening betalen, inbreuk tegen verkeersregels, anti-gouvernementele mening uitspreken, te veel alcohol kopen, geld spenderen aan frivole aankopen, te veel tijd spenderen aan videospelletjes, enz. De score kan stijgen en dalen in reële tijd in functie van het gedrag van de specifieke persoon maar ook van de mensen waarmee hij/zij geassocieerd wordt (familie, vrienden, enz.). Bij een te lage score worden er straffen opgelegd die gaan van het ontzeggen van toegang tot sociale media, het ontzeggen van gebruik van trein en vliegtuig, en het ontzeggen van jobs bij de overheid tot en met boetes en gevangenisstraffen.

België onderschrijft de richtlijnen die de Europese Commissie heeft gedeeld in haar mededeling over ethische richtsnoeren voor vertrouwen in mensgerichte AI. Uitdagingen van AI in relatie tot mensenrechten en publieke waarden en normen moeten in samenwerking met nationale en internationale partners (inclusief bedrijfsleven, wetenschap en maatschappelijke instellingen) worden opgepakt.

Het is aan Defensie om met zijn internationale partners een gedragscode te ontwikkelen die ondernemers helpt bij het ontwikkelen van verantwoorde AI-toepassingen. Deze gedragscode is samengesteld op basis van ethische principes zoals onder andere deze van de Europese Commissie omtrent transparantie in de gebruikte technologie.

Robuust – **AI moet veilig en accuraat zijn**

Veiligheid ligt in vertrouwen & vertrouwen in ervaring – De huidige AI-algoritmen kunnen gekenmerkt worden als een recent en vaak (nog) niet mature technologie die

een output kan genereren die door de gebruiker gepercipieerd kan worden als fout of afwijkend. Vanuit de positieve en negatieve ervaringen zullen de experten en de gebruikers beter in staat zijn om de risico's, die verbonden zijn met het gebruik van bepaalde AI-systemen, in te schatten. Naarmate men beter wordt in het inschatten van de risico's, zal het vertrouwen in het gebruik van AI-systemen groeien. Naast de groei in vertrouwen zal men ook steeds beter in staat zijn om specifieke behoeftes te formuleren die een toename van de veiligheid in de hand werkt. Defensie dient over voldoende mensen te beschikken die dergelijke AI-systemen naar waarde kunnen schatten en de gebruikers bijstaan in het opbouwen van vaardigheden en ervaringen.

Connectiviteit – Op het gebied van connectiviteit liggen de klemtonen op beschikbaarheid, stabiliteit en snelheid. Voor vele AI-toepassingen die ultrasnelle en betrouwbare connectiviteit vereisen om de toegang tot gegevensbanken te garanderen of de interconnectiviteit tussen diverse sensoren te faciliteren, stuiten de huidige telecommunicatienetwerken immers op hun beperkingen. Met de komst van de 5G-technologie worden er mogelijkheden geboden variërend van supersnel mobiel internet tot het *Internet of Things* (IoT) die een nieuwe basis zullen vormen voor een verdere ontwikkeling van AI-toepassingen. De komst van deze nieuwe technologie komt niet alleen met nieuwe opportuniteiten maar ook met nieuwe uitdagingen. We merken op dat de ontwikkeling van dergelijke technologie moeilijk bruikbaar is in buitenlandse operaties. Vele landen worden voorzien van de benodigde hardware ondersteuning terwijl de militairen opereren in gebieden waarin deze ontwikkeling niet gekend zijn of deze technologie slechts beperkt beschikbaar is. Het gebruik van satellieten kan hier een oplossing bieden. Maar met het identificeren van ruimte als een 'nieuw' militair actiedomein, onderkennen we echter dat het gebruik ervan betwist zal worden in de toekomst. Tegenstanders, die over de nodige middelen beschikken, zullen niet twijfelen om het conflict naar de ruimte uit te breiden indien dit de strategische superioriteit van het gebruik van AI-toepassingen en -systemen degradeert of ontzegt.

Databeheer en -kwaliteit – Data is de basis van AI. Daarom zijn de kwaliteit, betrouwbaarheid en beschikbaarheid van data van het allergrootste belang. Defensie moet over hoogwaardige data beschikken om betrouwbare AI-algoritmen te ontwikkelen en te voeden, en moet deze data goed beheren teneinde de continue beschikbaarheid ervan te garanderen. De manier waarop men de data genereert, organiseert, beheert, beveiligt en inzet kan het verschil betekenen tussen succes en mislukking.

Om over te kunnen gaan tot een succesvolle AI-implementatie, moet er eerst begonnen worden met een eerlijke beoordeling van de data beschikbaar binnen Defensie om te bepalen of ze geschikt zijn om als input te dienen voor AI-algoritmen. Daarom moet Defensie een uitgebreide datastrategie ontwikkelen en zijn zwakke punten op het gebied van databeheer, kwaliteit, catalogisering en beveiliging aanpakken. Ervaringen vanuit de bedrijfswereld leren ons dat het organiseren en logisch combineren van grote hoeveelheden data een zeer lastige taak is en dus ook Defensie veel inspanning zal kosten.

Voorbeeld van AI-toepassing: AEGIS, het US Navy Weapon Command, Control & Decision system

AI in cybersecurity of cybersecurity in AI? – Het beveiligen van algoritmen, data, connectiviteit en energievoorziening impliceert zonder enige twijfel het in plaats stellen van een performante cybersecurity. Met de komst van nieuwe AI-toepassingen zal deze nood niet alleen groter maar ook veel complexer worden. De onvolledige inhoudelijke kennis van AI algoritmes (*black box*) en de plaatsing ervan in een IoT met een groot aantal sensoren, creëert een exponentiële toename aan nieuwe mogelijkheden voor cybercriminelen. Maar de relatie tussen AI en cybersecurity is ook wederkerig. Actueel maken de ontwikkelaars van cybersecurity-software gebruik van *machine learning*-technieken om hun producten performant te maken en te houden. Alsook de cybercriminelen… AI-ondersteunde cybersecurity is simpelweg een vereiste geworden. Daarom moet Defensie in staat zijn om vanuit zijn specifieke behoeftes cybersecurity-software ontwikkelaars aan te sturen in het ontwikkelen en onderhouden van een aangepaste performante oplossing.

Drie bijkomende uitdagingen voor Defensie omtrent AI

Naast de betrouwbaarheid van AI zijn er ook een aantal uitdagingen waarop Defensie eveneens dient een antwoord te vinden alvorens te komen tot een succesvolle implementatie van AI: vorming, bestaand materieel en interoperabiliteit.

Vorming – AI is een vlag dat een zeer grote lading dekt. Een vorming 'AI' zal nooit verder kunnen gaan dan het niveau van sensibilisering over de grote onderdelen en uitdagingen van AI. Een verdere verdieping in dit onderwerp is al zeer snel gespecialiseerde materie, weinig toegankelijk voor het 'brede' publiek, en verliest de betrokkene snel het holistisch perspectief. Het is echter wel zo dat elk onderdeel (algoritme, connectiviteit, datamanagement, cyber, legaliteit, enz.) zijn eigen specialisten vereist. Het introduceren van AI zal dus een grote behoefte aan gespecialiseerd personeel met zich meebrengen. Deze behoefte zal gezien de huidige schaarste op de arbeidsmarkt eerder via interne vormingen moeten ingevuld worden. Deze vormingen bestaan echter nog niet en gevormd personeel zal zeer aantrekkelijk zijn op de arbeidsmarkt. Opgelet: het zou verkeerd zijn indien de focus enkel gelegd wordt op gebruikers en 'ontwikkelaars'. Teneinde al deze inspanningen correct te omkaderen en te begeleiden dient er eveneens een sterk bestuursmodel uitgebouwd te worden in dit domein. Daarom dient het (hoger) management ook opgeleid te worden of versterkt met experten. Naast de inspanning om de interne vormingen op te lijnen aan deze nieuwe technologische ontwikkeling zal er dus intens moeten samengewerkt worden met externen om de vereiste interne kennisopbouw te faciliteren.

Bestaand materieel – Als we Defensie wensen te 'AI'-moderniseren zonder hierbij in te boeten bij inzetbaarheid, dan dient er rekening gehouden te worden met belangrijke investeringen in het opwaarderen van huidige capaciteiten en technologieën. Veel van deze capaciteiten en technologieën actueel in gebruik binnen Defensie beschikken echter over een gesloten architectuur. Vanuit hun industriële design zijn ze niet geschikt om te opereren in een digitale omgeving of bieden ze niet de benodigde connectiviteit. Nieuw materieel zoals de F 35, de A400M, de mijnenjagers en voertuigen in het CAMO-project bevatten een open architectuur en zijn dus beter geschikt voor een doorontwikkeling langsheen de introductie van nieuwe AI-technologieën.

De verhoogde digitalisatie en connectiviteit laten ons toe om een militaire IoT uit te bouwen waarin we al onze AI-algoritmen met elkaar kunnen verbinden. Het samenbrengen van AI technologieën en (aangepast) bestaand materieel in dit militair IoT levert nieuwe uitdagingen op. Door de industriële beperkingen in het aanpassen van de gesloten architectuur van het bestaand materieel bekomt men niet optimale AI-constructies die de integriteit en veiligheid van het militaire IoT extra zullen belasten. Door de connectie van nieuwe en bestaande systemen verkrijgen we uiteindelijk een delicaat systeem van systemen, waarvan de 'bestaande' aan AI aangepast, maar ervoor

niet geoptimaliseerd zijn. In dit metasysteem met een continue *feedback loop*, zal het gedrag van ieder het andere beïnvloeden op een manier waarvan we niet altijd de 'waarom' begrijpen en dus de aansprakelijkheid nog moeilijker te bepalen valt. En laten we niet vergeten dat de 'tegenstander' hierin ook een rol te spelen heeft.

Tot slot dient er ook vermeld te worden dat veel van onze capaciteiten en technologieën reeds (de mogelijkheid bieden tot) data genereren zonder dat deze correct worden gecapteerd en gestockeerd. Het betreft hier een rijkdom dat verloren gaat en niet meer gerecupereerd kan worden voor de introductie en ontwikkeling van toekomstige AI-algoritmen.

Interoperabiliteit[2] – In het kader van interoperabiliteit wordt er vaak gedacht aan syntactische interoperabiliteit waarbij twee of meer systemen met elkaar kunnen interageren en data uitwisselen. Vanuit technologisch standpunt is dit reeds een moeilijke oefening op zich. Daarom vinden er enorme standaardisatie-inspanningen plaats binnen NATO en EU.

De kracht van AI ligt in het aanbieden van data van verschillende sensoren die al dan niet bewerkt doorgestuurd worden naar een dataopslag. Hoe groter het netwerk, des te groter de mogelijkheden van de AI, en des te groter het aantal sensoren. Hoe groter het aantal sensoren, des te groter de hoeveelheid en soorten van gegenereerde data. De gegenereerde data is pas waardevol als al deze data zinvol is voor de verschillende AI-algoritmes die gebruik maken van dit netwerk. Ervaring heeft reeds uitgewezen dat al de data in dezelfde formaat plaatsen, niet volstaat voor succes. Een recent voorbeeld hiervan is de data omtrent de Covid-19 crisis waarbij de gegevens van de landen niet altijd te vergelijken waren.

Indien men wenst over te gaan tot een succesvolle implementatie van AI, moet men naar een semantische interoperabiliteit streven waarbij de informatie dat gedeeld wordt tussen twee (of meerdere) machines door alle andere toestellen in het netwerk verstaan wordt. Het probleem van interoperabiliteit wordt er dus alleen maar complexer op.

[2] Entiteiten (producten, systemen of organisaties) zijn interoperabel als ze zonder beperkingen samen kunnen werken. Voor de interoperabiliteit van deze entiteiten zijn standaarden, protocollen en procedures nodig voor een wederzijdse afstemming van de entiteiten.

Besluit

Binnen Defensie zijn er reeds meerdere initiatieven lopend om bovenstaande punten aan te pakken maar de af te leggen weg is nog ver en vol met hindernissen. Laat staan dat het beloofde AI-potentieel ook daadwerkelijk zal worden ingevuld door de wetenschappers en industrieën. Doorheen de militaire geschiedenis heeft de technologie (te) vaak gefaald om de verwachtingen correct in te vullen.

De huidige technologische trends dwingen Defensie ertoe om zich dringend en diepgaand te bezinnen over het verwerven van AI-ondersteunde capaciteiten, het in plaats stellen van een effectief AI-beheer, het creëren van een personeelsbestand geschoold in AI, het deelnemen aan de creatie van een legaal kader omtrent de integratie en gebruik van AI-toepassingen en het uitbouwen van partnerschappen met industrie en internationale partners. Op korte termijn moet Defensie kunnen beschikken over een moderne adaptieve organisatie, die leerstellig rekening houdt met AI-aangestuurde evoluties, die voor een betere interoperabiliteit zorgen, en waarin de beschikbare AI-algoritmen benut worden.

Trefwoorden: Kunstmatige intelligentie, artificial intelligence, introductie, defensie-organisatie