De digitale uitdaging voor Defensie

Filip GILLET

Brigadegeneraal Filip GILLET werd in 2023 in plaats gesteld als de eerste *chief information officer* (CIO) van Defensie. Voordien bekleedde hij onder meer functies als ondersectiechef van de corporate IT-systemen, hoofd van de militaire cybercapaciteit en veiligheidsadviseur bij de eerste minister.

La nature de la guerre a changé : nos forces armées opèrent désormais dans des milieux opérationnels imprévisibles, souvent en partie civils et de plus en plus complexes, où tous les domaines opérationnels sont contestés simultanément à tous les niveaux d'opération. Des nouveaux concepts militaires tels que les opérations multidomaines doivent pouvoir s'appuyer sur des mécanismes performants de synchronisation, de coordination et de communication et obligent les organisations militaires à s'adapter fondamentalement. En parallèle, la technologie évolue de plus en plus vite. L'intégration des nouvelles technologies numériques dans les opérations militaires promet des capacités améliorées et une plus grande efficacité, mais entraîne également une multitude de défis et une complexité accrue. La Défense devra moderniser ses structures et ses processus afin de faire face de manière contrôlée à cette nouvelle réalité opérationnelle.

De gewijzigde operationele omgeving

De grootste uitdaging voor militaire organisaties blijft ongewijzigd: strategisch, operationeel en tactisch overwicht behouden in diverse operationele omgevingen. De erkenning van cyberspace en, meer recent, ruimte als nieuwe operationele domeinen heeft echter nieuwe arena's voor conflicten en confrontaties gecreëerd. Tegelijkertijd is de VUCA[1]-omgeving het nieuwe normaal geworden. Onze strijdkrachten opereren

[1] De term VUCA (*volatile, uncertain, complex, ambiguous*) wordt gebruikt om de complexiteit en dynamiek van een snel veranderende operationele omgeving te beschrijven.

tegenwoordig in onvoorspelbare, vaak gedeeltelijk civiele en steeds complexere operationele omgevingen, waarin alle operationele domeinen op alle niveaus simultaan worden betwist.

Daarnaast worden we geconfronteerd met een steeds sneller tempo van technologische ontwikkelingen en hun toepassingen in het militaire domein. Digitalisering is alomtegenwoordig en transformeert fundamenteel de wijze waarop strijdkrachten communiceren, beslissingen nemen en opereren. Het hoge tempo van technologische vooruitgang vereist dat militaire organisaties voortdurend nieuwe technologieën integreren in hun operaties. De uitdaging ligt in het naadloos samenvoegen van geavanceerde technologieën met traditionele militaire infrastructuren en processen, zonder de operationele capaciteit te verstoren. Nieuwe technologieën zijn vaak ook onmiddellijk toegankelijk voor alle betrokken partijen, wat betekent dat strategisch voordeel alleen kan worden behaald door te anticiperen op technologische ontwikkelingen en vroegtijdig inzicht te verwerven in de mogelijke strategische en operationele implicaties ervan.

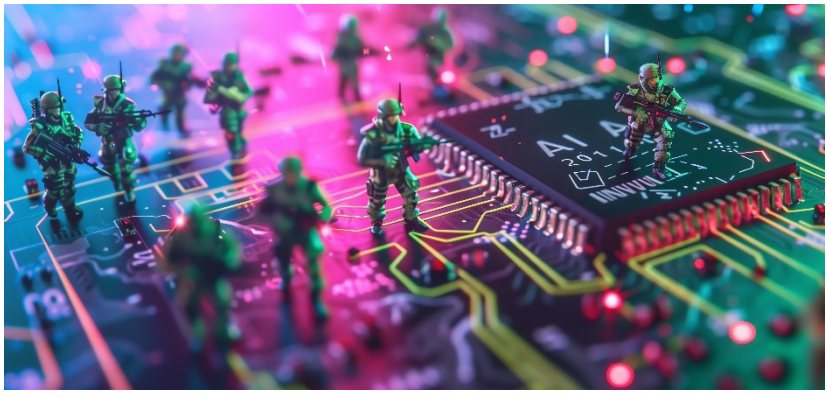
Als reactie op de VUCA-omgeving heeft de NAVO *multi-domain operations* (MDO) gedefinieerd als het nieuwe beslissende concept voor toekomstige militaire operaties, wat een rechtstreekse impact heeft op het niveau van samenwerking, communicatie en synchronisatie dat we nodig hebben om operationeel succes te behalen. Interoperabiliteit en informatiedominantie worden cruciaal in toekomstige operaties en om dit te ondersteunen is het noodzakelijk dat onze militaire organisaties datacentrisch worden. Digitale connectiviteit, data-uitwisseling en data-exploitatie worden nu nog meer dan vroeger essentiële *enablers* om MDO mogelijk te maken.

Technologische (r)evolutie

Artificiële intelligentie bestaat inmiddels al meer dan 50 jaar, maar de vooruitgang op het gebied van rekenkracht, de beschikbaarheid van enorme hoeveelheden data, de schaalbaarheid van *cloud*-platformen en de ontwikkeling van nieuwe algoritmen hebben de afgelopen jaren tot grote doorbraken geleid. Artificiële intelligentie is geen op zichzelf staande technologie, maar eerder een verzameling van faciliterende en transformerende technologieën die uiteindelijk geïntegreerd zullen worden in alle

toekomstige technologische innovaties. De toepassingen van artificiële intelligentie binnen de militaire sector zijn talrijk en divers. Voorbeelden hiervan zijn te vinden in het domein van operationele paraatheid, voor het voorspellen van storingen van (wapen)systemen of toekomstige onderhoudsbehoeften; in het inlichtingendomein, voor de automatisering van data- en beeldanalyse; in het cyberspacedomein, voor het identificeren van cyberdreigingen en het ontwikkelen van op maat gemaakte reacties; of in het domein van vorming en training, voor het creëren van ultrarealistische simulaties waarmee strijdkrachten kunnen trainen in virtuele omgevingen.

De vooruitgang op het gebied van ruimtevaarttechnologie heeft het ruimtesegment gecommercialiseerd en ook toegankelijker gemaakt voor kleinere staten. Satellietconstellaties in een lage baan om de aarde bieden interessante opportuniteiten voor strategische communicaties, gekenmerkt door hogere bandbreedtes en kleinere tijdsvertragingen. Het toenemende operationele belang van orbitale systemen heeft sommige landen geïnspireerd om technologieën te ontwikkelen die gericht zijn op het verstoren of vernietigen van in de ruimte gestationeerde capaciteiten, terwijl andere landen juist extra beschermingsmaatregelen nemen om zich te verdedigen tegen dergelijke acties.



© T. Hansen on Pixabay

Autonome systemen beloven onder meer een grotere efficiëntie en een verminderd risico voor militair personeel. Naarmate de technologie zich verder ontwikkelt en de ontwikkelingskosten dalen, breidt ook het aantal militaire toepassingen uit.

Veelbelovend onderzoek wordt gevoerd naar autonome systemen voor logistieke ondersteuning aan gevechtseenheden, wat zou kunnen betekenen dat de noodzaak voor honderden logistieke functies wordt vervangen door een kleiner, meer gespecialiseerd personeelskader dat toezicht houdt op deze autonome systemen.

De implicaties van kwantumtechnologieën voor defensieorganisaties zijn eveneens omvangrijk en beloven onder meer enorme rekenkracht voor data-exploitatie en pre-kwantumdecryptie, uiterst veilige digitale communicatie-infrastructuren en ultragevoelige sensoren voor navigatie en detectie. De verwachting is dat de technologie de komende vijf tot tien jaar militair relevant zal worden. Het is daarom van cruciaal belang om markttrends nauwlettend te volgen om capaciteitsontwikkeling en investeringsbeslissingen te kunnen sturen.

In 2019 identificeerde de NAVO voor het eerst de technologiedomeinen die potentieel disruptief konden zijn voor militaire operaties. Ondertussen werd die lijst al twee keer bijgewerkt, wat op zichzelf aangeeft in welk tempo de technologische uitdagingen zich ontwikkelen. Wat al deze technologieën gemeen hebben, is dat ze een enorm potentieel bieden om de operationele efficiëntie te vergroten en dat ze sterk afhankelijk zijn van digitale expertise en infrastructuren.

Het belang van data

De proliferatie van digitale technologieën heeft geleid tot een exponentiële toename van datavolumes. De huidige datavolumes zijn zo omvangrijk en complex, en de snelheid waarmee dataparameters wijzigen is zo hoog, dat traditionele methoden voor het verzamelen van gegevens en eenvoudige statistische analyses niet langer toereikend zijn. Nieuwe, geavanceerde algoritmen en moderne analytische technologieën bieden de mogelijkheid om enorme hoeveelheden gegevens te verzamelen, analyseren en interpreteren.

Het effectief benutten van gegevens uit alle beschikbare (interne en externe) informatiebronnen is essentieel om operationele commandanten en beleidsmakers tijdig te voorzien van de benodigde informatie. De efficiëntie en effectiviteit van deze data-exploitatie dienen ervoor te zorgen dat onze strijdkrachten het plannings- en beslissingsproces[2] sneller en doelmatiger dan onze tegenstanders kunnen doorlopen.

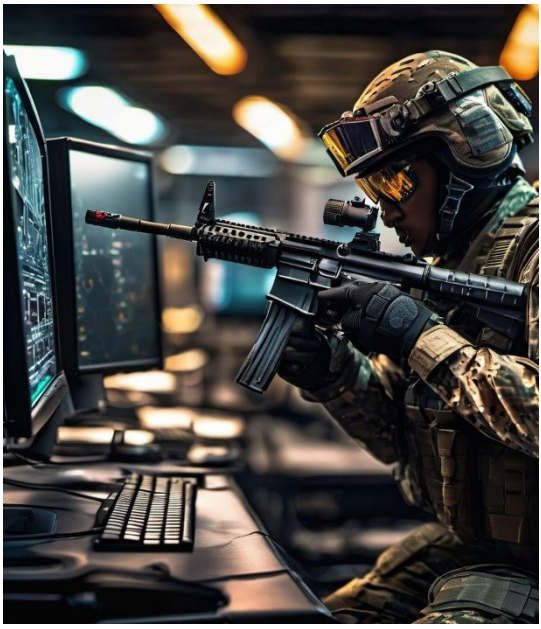
[2] *OODA-loop: observe, orient, decide, act*

Data readiness is hierbij van cruciaal belang; de gegevens moeten voorbereid worden om bruikbaar te zijn voor nieuwe technologieën. Kenmerkend voor kwaliteitsvolle data zijn nauwkeurigheid, consistentie, integriteit en toegankelijkheid. Om data-ondersteunde besluitvorming te kunnen integreren in alle operationele en functionele processen, moeten de noodzakelijke richtlijnen voor het registreren en beheren van kwaliteitsvolle data gedurende de gehele levenscyclus worden vastgelegd in een coherent databeleid. Expertise en toepassingen op het gebied van data-exploitatie dienen zodanig toegankelijk en gebruiksvriendelijk te worden gemaakt dat alle geautoriseerde gebruikers er optimaal gebruik van kunnen maken. Daarnaast moet de uitwisseling van data worden bevorderd door een samenwerkingscultuur aan te nemen.

De onderliggende digitale infrastructuur moet voldoende robuust, schaalbaar en veilig zijn om grote hoeveelheden data betrouwbaar en snel te kunnen transporteren. Systeembeheerders worden daarbij geconfronteerd met grote uitdagingen wanneer ze de onontbeerlijke interfaces realiseren tussen oudere systemen en nieuwe, opkomende technologieën. Digitale interoperabiliteit tussen de verschillende (wapen)systemen, doorheen de interne organisatie en met externe partners, moet worden versterkt door standaardisatie-inspanningen te intensiveren. Daarbij is het essentieel om interoperabiliteitsvereisten uit nationale, coalitie-, EU- en NAVO-normering en -richtlijnen te identificeren en te integreren.

Het belang van digitale expertise en cultuurverandering

Naarmate militaire operaties steeds meer gedigitaliseerd worden, moet het militair personeel over bijkomende vaardigheden beschikken om nieuwe technologieën, digitale hulpmiddelen en systemen te kunnen bedienen en onderhouden. De uitdaging ligt in het gelijke tred houden met de technologische vooruitgang en ervoor zorgen dat al het personeel, ongeacht de functie of de graad, over de noodzakelijke digitale geletterdheid beschikt. Een organisatiebrede digitale cultuur moet gepromoot worden die innovatie, een correcte gegevensuitwisseling, de adoptie van nieuwe technologieën en het gebruik van data-exploitatie in besluitvormingsprocessen stimuleert en beloont.



© T. Hansen on Pixabay

Medewerkers op alle niveaus moeten de basisprincipes van correct databeheer aanleren. Het is bijvoorbeeld belangrijk om te begrijpen hoeveel kwalitatieve data noodzakelijk is om artificiële intelligentie-oplossingen effectief te trainen.

In parallel moet extra geïnvesteerd worden in gespecialiseerde digitale expertise, extra financiële stimuli moeten ingevoerd worden om digitaal talent aan te trekken en te behouden. De organisatiestructuren voor digitale expertise moeten hertekend worden om aansturing, flexibiliteit, effectiviteit en efficiëntie te optimaliseren. Voor de digitale ondersteuning van defensieorganisaties moet, met inachtneming met de militaire specificiteit, een correct evenwicht gezocht worden tussen interne expertise, gemengde defensie-/private industrieteams, contractanten en consultants.

Technologische oplossingen en diensten moeten verworven worden op een efficiëntere en flexibelere manier. Een cultuuromslag is nodig om de overstap te maken van een bureaucratisch en risicomijdend aanbestedingsbeleid naar een meer wendbare, marktconforme aanpak. Die inspanningen moeten in evenwicht gebracht worden met passend toezicht.

Het benutten van de vele digitale opportuniteiten vereist een gedisciplineerde aanpak voor brede adoptie, waarbij de risico's zorgvuldig worden overwogen. Om gelijke tred te houden met de snelheid van technologische innovaties, moeten militaire organisaties hun begrip van veiligheidsrisico's verfijnen en hun risicoanalyse verschuiven van een *compliance*- naar een op risico gebaseerde veiligheidscultuur. Een benadering van adaptieve beveiliging kan hierbij een waardevolle rol spelen, door prioriteit te geven aan automatisering en snelle respons, terwijl maximale *compliance* wordt gewaarborgd door middel van continue monitoring en geautomatiseerde detectie van anomalieën.

Het belang van digitale integriteit

Naarmate militaire organisaties steeds meer gedigitaliseerd worden, worden ze ook steeds kwetsbaarder. Een succesvolle cyberaanval of technische storing kan communicatienetwerken ontwrichten, gevoelige informatie compromitteren, besluitvormingsprocessen belemmeren, operationele activiteiten verstoren en zelfs kritieke militaire infrastructuur verlammen of uitschakelen.

De sterke afhankelijkheid voor militaire operaties van digitale infrastructuur benadrukt dan ook het belang om robuuste cyberbeveiligingsmaatregelen te waarborgen, regelmatig kwetsbaarheidsbeoordelingen uit te voeren, te investeren in geavanceerde detectie- en reactiesystemen voor bedreigingen, redundante digitale systemen op te zetten en te onderhouden alsook noodplannen te ontwikkelen om de impact van technische onderbrekingen te mitigeren.

En nu militaire organisaties nieuwe technologieën omarmen, moeten ook ethische overwegingen centraal staan. Hoewel er weinig discussie bestaat over het potentieel van artificiële intelligentie om militaire operaties en besluitvorming te ondersteunen, blijft er binnen de defensiesector bezorgdheid bestaan over de betrouwbare ontwikkeling en implementatie van deze technologie. Dit moet leiden tot inspanningen om een verantwoord gebruik van artificiële intelligentie en de bescherming van persoonsgegevens te codificeren, zowel in nationale als in internationale regelgeving en normen. Ook aan autonome systemen worden veel operationele voordelen toegekend, met ethische implicaties als gevolg alsook de behoefte aan beleid en regelgeving om te bepalen wanneer en hoe deze systemen ingezet kunnen worden.

Conclusie

Nieuwe technologieën leiden tot nieuwe digitale hulpmiddelen die onmisbare troeven worden op het moderne slagveld. Deze technologieën transformeren fundamenteel de manier waarop strijdkrachten communiceren, beslissen en vechten. De toekomst van militaire operaties in het digitale tijdperk zal voornamelijk worden bepaald door het vermogen van militaire organisaties om zich aan te passen aan en optimaal gebruik te maken van de transformerende kracht van opkomende technologieën.

Het is van cruciaal belang dat geautoriseerde gebruikers *realtime* toegang krijgen tot relevante operationele data uit alle functionele domeinen en tot beslissingsondersteunende tools. Dit vereist een volledig genetwerkte organisatie om datasets beveiligd en tijdig uit te wisselen binnen de organisatie en met partners, een organisatiecultuur- en structuur die data-uitwisseling promoot en technologische innovatie faciliteert, een versterkte digitale kennis op alle niveaus doorheen de volledige organisatie, een aangepaste digitale ondersteuningsorganisatie en het correct identificeren van informatiestromen.

Onze eigen defensieorganisatie zal zich dus ook moeten aanpassen aan vernieuwende operationele concepten waarin datagestuurd optreden onontbeerlijk wordt, evenals aan de toenemende snelheid van technologische innovatie. De grootste uitdaging in de komende jaren zal er ongetwijfeld in bestaan digitale transformatie-initiatieven af te stemmen op de gelijktijdige transformatie van vrijwel al onze grote wapensystemen. Onderlinge connectiviteit en interoperabiliteit waarborgen, zowel met bestaande systemen als met systemen van partners, is een uiterst complex proces dat zal mislukken zonder het noodzakelijke beheer en de nodige richtlijnen te definiëren.
Defensie bundelde de noodzakelijke directieven in haar visie voor digitale transformatie. Deze visie combineert inspanningen op het gebied van optimalisatie, modernisering en transformatie, en richt zich op efficiënt databeheer, versterkte digitale expertise, gedigitaliseerde processen en technologische innovatie. De focus ligt hierbij altijd op het maximaliseren van de operationele waarde door de mogelijkheden voor datafusie en effectieve data-exploitatie te vergroten, met inachtneming van de regelgeving op het gebied van data, informatie en cyberbeveiliging. Het plan is dus klaar. Nu nog zorgen dat we op het vooropgestelde "implementatiepad" kunnen blijven.

Trefwoorden: Digitale transformatie, artificiële intelligentie, technologische innovatie