Ministerie van Defensie

Digitale Transformatie Strategie

Gevechtskracht door rekenkracht

Inhoudsopgave

1.	**Introductie: gevechtskracht door rekenkracht**	**5**
	Ambitie: gevechtskracht voor de warfighter	6
	Leeswijzer	6
2.	**Drijvende krachten van de strategie**	**7**
	Recente ontwikkelingen: Waarom versnellen noodzakelijk is	7
	Conclusie: snelheid omhoog met focus op nieuwe ontwikkelingen	8
3.	**Speerpunt | Communicatie & digitale samenwerking**	**10**
4.	**Speerpunt | Digitaal fundament**	**12**
5.	**Speerpunt | Data, AI en Autonomie**	**14**
6.	**Speerpunt | EMS, Cyber en redundantie**	**17**
7.	**Speerpunt | Digitaal aanpassingsvermogen**	**19**
8.	**De force multiplier: integratie tussen de speerpunten**	**21**
9.	**Veranderaanpak, risico's en mitigerende maatregelen**	**24**
Bijlage A: Digitale trends		**26**
Bijlage B: begrippenlijst		**28**
Bijlage C: referenties		**30**

1. INTRODUCTIE: GEVECHTSKRACHT DOOR REKENKRACHT

In de Defensienota 2024 'Sterk, Slim, Samen' is de urgentie geschetst om te bouwen aan een Slimme en Sterke Krijgsmacht die zorgt voor de noodzakelijke afschrikking. De afgelopen jaren is de veiligheidssituatie in Europa verder verslechterd. De verwachting dat de wereld fragmenteert naar een multipolaire orde met concurrerende blokken die machtspolitiek bedrijven, is in een stroomversnelling geraakt. In deze wereld wordt steeds meer naar Europa gekeken om haar eigen veiligheid op orde te brengen om de stabiliteit op het Europese continent te kunnen waarborgen. Kortom de focus verschuift sterker naar hoofdtaak 1[1]: het kunnen verdedigen van het Koninkrijk en NAVO-grondgebied tegen een technologisch capabele tegenstander.

Tegelijk is er een versnelling van digitale innovatie in het militaire domein. Data, AI en autonome systemen spelen hierin een dominante rol, maar gaan hand in hand met andere technologische ontwikkelingen zoals de toenemende kracht van cyberdreigingen, militarisering van het ruimtedomein, congestie in het Elektro Magnetisch Spectrum (EMS) en hybride dreigingen, waaronder aanvallen op datakabels en manipulatie van informatie. Als Defensie onvoldoende meekomt in deze snelle technologische ontwikkelingen dan is het conflict van de toekomst al verloren.

In de Defensienota 2024 staan drie strategische doelen centraal: (1) Defensie is voorbereid op een grootschalig militair conflict in het NAVO-verdragsgebied, (2) Defensie is klaar voor het gevecht van de toekomst en past zich aan veranderende dreigingen en conflictvoering aan en (3) Defensie staat klaar voor nationale taken en ondersteuning van civiele autoriteiten. Het realiseren van deze ambitie en het invulling geven aan onze hoofdtaken vereist dat Defensie digitale technologie sneller dan de tegenstander weet om te zetten in gevechtskracht. Kortom: gevechtskracht door rekenkracht.

[1] De andere twee hoofdtaken zijn (2) bescherming en bevordering van internationale rechtsorde en stabiliteit en (3) het leveren van militaire bijstand aan civiele autoriteiten bij de handhaving van de openbare rechtsorde, alsmede bij rampenbestrijding en crisisbeheersing (Defensienota 2024).

Ambitie[1]: gevechtskracht voor de warfighter

Defensie moet gevechtskracht leveren om af te schrikken en indien nodig om te vechten, in alle omstandigheden. De omstandigheden variëren van statische gebouwen zoals hoofdkwartieren die verbonden zijn met glasvezelnetwerken tot speciale eenheden die zonder voertuigen door vijandelijk gebied verplaatsen. De digitale transformatie moet de gevechtskracht in alle omstandigheden versterken door Defensie beter dan de tegenstander in staat te stellen om:

- Geïntegreerde effecten te realiseren samen met civiele en militaire partners over domeinen heen;
- Informatie- en beslisdominantie te bereiken;
- Continu nieuwe en huidige technologie te combineren naar meer gevechtskracht.

Deze strategie focust zich op vijf speerpunten:

1. *Communicatie & digitale samenwerking*: Veilig en interoperabel kunnen communiceren over domeinen (land, zee, lucht, cyber, ruimte) en met strategische partners (militair en civiel).
2. *Digitaal fundament*: Toegang bieden tot opslag- en rekenkracht in alle omstandigheden; Defensiebrede processen digitaliseren als basis om verder op te innoveren.
3. *Data, AI en autonomie*: Geïntegreerd beeld op kunnen bouwen & datagedreven besluiten kunnen nemen; AI en autonome systemen effectief kunnen inzetten en door-ontwikkelen.
4. *EMS, cyber en redundantie*: Beschermen van de digitale informatieketen tegen interne en externe verstoringen.
5. *Digitaal aanpassingsvermogen*: Sneller dan de tegenstander nieuwe en huidige technologie om kunnen zetten in gevechtskracht.

Het realiseren van deze effecten vereist integrale verandering van zowel specifiek militaire IT als Defensiebrede kernprocessen zoals inkoop, personeel, logistiek en gezondheidszorg die cruciaal zijn voor het voortzettingsvermogen en strategische besluitvorming. Het gaat om het vinden van de snelste en meest toekomst-bestendige route naar het vergroten van de gevechtskracht – nu en op termijn.

Leeswijzer

Het doel van deze strategie is het vergroten van de gevechtskracht van Defensie. In hoofdstuk 2 worden de belangrijkste drijvende krachten onder deze strategie benoemd. In de daaropvolgende hoofdstukken worden de vijf speerpunten uitgewerkt. In deze hoofdstukken wordt het belang van dit speerpunt in relatie tot gevechtskracht gelegd waarna de concrete maatregelen per speerpunt worden gegeven. Vervolgens wordt in hoofdstuk 8 stil gestaan bij de samenhang: integratie tussen de vijf speerpunten zorgt ervoor dat de gevechts-kracht sterk toeneemt. Tot slot wordt in hoofdstuk 9 stilgestaan bij de benodigde randvoorwaarden, middelen, risico's en mitigerende maatregelen.

2. DRIJVENDE KRACHTEN VAN DE STRATEGIE

Sinds het rapport Defensie Duurzaam Digitaal uit 2021[II] zijn de eerste stappen gezet om jarenlange onderinvestering in de IT van Defensie te herstellen. De richting die Defensie een aantal jaar terug heeft ingezet is samen te vatten als:

- *Versterken van de basis*, onder andere door modernisering van infrastructuur, communicatiemiddelen, digitale weerbaarheid, datakwaliteit en versterken van de IV organisatie.
- *Slimmer gaan optreden*, onder andere door het opbouwen van een netwerk van sensoren, data, AI en digitale innovatie.
- Beter *geïntegreerde effecten* kunnen bereiken samen met civiele en militaire partners, onder andere met behulp van initiatieven op interoperabiliteit.

Dit heeft geleid tot concrete resultaten en een versterkte IV organisatie. Tegelijk is dit niet langer voldoende om de huidige geopolitieke realiteit en technologische ontwikkelingen het hoofd te bieden.

Recente ontwikkelingen: Waarom versnellen noodzakelijk is

Toenemende competitie en dreiging[III]

De strategische context is fundamenteel veranderd. De Russische inval in Oekraïne en de assertieve koers van China leiden tot een structureel hogere dreiging. Defensie verschuift van expeditionaire inzet naar robuuste collectieve verdediging van NAVO-gebied, terwijl digitale dreiging permanent aanwezig is. Cyberaanvallen, sabotage en beïnvloeding vergen digitale weerbaarheid, informatievoorsprong en flexibiliteit. Technologische en informatiesuperioriteit zijn randvoorwaardelijk voor afschrikking en verdediging.

Toenemende eisen vanuit de NAVO voor inzetbaarheid en interoperabiliteit

De NAVO versnelt haar inzetbaarheid, met het *NATO Force Model* (NFM). Dit vraagt om digitale interoperabiliteit[2], zodat Defensie digitaal effectief geïntegreerd kan opereren binnen bondgenootschappelijke netwerken. Gegevensuitwisseling, snelle besluitvorming en cyberveiligheid zijn hierbij doorslaggevend. De adoptie van gezamenlijke standaarden met partners voor digitale infrastructuur en *federated mission networking* (FMN) is essentieel om een geloofwaardige afschrikking en effectieve Defensie te realiseren.

Verschuiving naar hoofdtaak 1

De strategische focus van Defensie verschuift naar hoofdtaak 1: het verdedigen van het eigen en bondgenootschappelijk grondgebied. Hoogwaardige cyberverdediging, geïntegreerde inzet van drones en AI, en robuuste, storingsbestendige communicatie zijn hierbij cruciaal.

[2] Gaat hier specifiek om technische interoperabiliteit: kunnen systemen en netwerken met elkaar communiceren en worden zelfde definities gebruikt t.b.v. effectief data uitwisselen en analyseren.

Daarnaast neemt het belang van mobiliteit en het verminderen van digitale signatuur sterk toe. Kortom gereedheid voor hoofdtaak 1 vereist een fundamenteel andere digitale infrastructuur dan voor vredesmissies.

Op **1 juni 2025** voerde Oekraïne de geavanceerde operatie "Spider's Web" uit: met **117 FPV-drones**, deels AI-gestuurd, werden strategische Russische luchtmachtbases aangevallen – inclusief diep in Siberië, meer dan 4.000 km van het front. Drone-operators lanceerden de systemen en bestuurden ze via het lokale 4G netwerk, waarbij de drone met behulp van AI deels zelfstandig richting het doel konden vliegen en deze aanvallen. De combinatie van mens en AI is cruciaal doordat de grote afstand anders te veel vertraging op zou leveren voor effectieve besturing door een operator. Gebruik van het lokale netwerk maakt detectie moeilijker. Deze operatie illustreert het gevecht van de toekomst waarin AI, autonomie, civiele middelen, menselijke creativiteit en lef steeds nauwer samengaan.

Klaarmaken voor conflict van de toekomst

Digitalisering van het gevechtsveld gaat snel. Digitale trends[3] [IV] die komende jaren een grote impact hebben:

- Gevecht om connectiviteit: beschermen, opsporen en verstoren van communicatiekanalen. Dit gevecht breidt zich uit naar het ruimtedomein, fysieke infrastructuur zoals onderzeekabels en het elektromagnetische spectrum.
- (Semi) autonome systemen, in het bijzonder drones en zwermtechnologie.
- Toenemende kracht en complexiteit van cyberaanvallen, specifiek wanneer Quantum technologie doorbreekt.
- Toenemende transparantie, bijvoorbeeld door toename sensoren en OSINT (open source intelligence). Dit wordt gecombineerd met verminderd belang van geografische afstanden (geen veilige plek meer).
- Steeds beter wordende AI gedreven analyses en beslisondersteuning, gecombineerd met AR / VR (Augmented Reality / Virtual Reality) visualisatie.
- Meer Europese strategische autonomie in zowel hardware- als softwareketens.

In de bijlage is een visueel overzicht van de belangrijkste digitale trends opgenomen.

Conclusie: snelheid omhoog met focus op nieuwe ontwikkelingen

Defensie heeft haar eigen verandersnelheid in relatie tot de huidige *capability gaps* geanalyseerd. Daarnaast is geleerd van digitale transformatie strategieën van NAVO partners[V]. Op basis van deze analyses wordt geconcludeerd dat:

- De ingezette richting is nog steeds valide, maar aanscherping is nodig om actuele ontwikkelingen mee te nemen bijvoorbeeld rondom AI, drones, EMS en soevereiniteit.
- Het verander- en innovatietempo moet sterk omhoog om mee te gaan in de snelheid die landen als Oekraïne, China en Rusland laten zien.

[3] In de bijlage is een visueel overzicht van de belangrijkste digitale trends opgenomen.

Tegelijkertijd moet Defensie altijd operationeel zijn en digitale veiligheid en stabiliteit vormen hierbij een randvoorwaarde. We moeten dus snel veranderen terwijl de stabiliteit en veiligheid van kernsystemen geborgd blijft. Waar Defensie op moet focussen om dit te bereiken wordt hieronder in de speerpunten uitgewerkt. Elk speerpunt eindigt met een aantal concrete maatregelen. Gezien de snelheid van de ontwikkelingen op zowel geopolitiek als technologisch vlak zullen deze maatregelen en het effect jaarlijks worden geëvalueerd en waar nodig bijgesteld op basis van actuele ontwikkelingen. Zo blijft de strategierealisatie zelf ook flexibel.

3. SPEERPUNT | COMMUNICATIE & DIGITALE SAMENWERKING

Bijdrage aan gevechtskracht

Het eerste speerpunt richt zich op het vermogen om veilig en effectief digitaal te kunnen communiceren en samenwerken. Zowel tussen operationele domeinen (land, zee, lucht, ruimte, cyber), civiele als militaire partners. Dit maakt betere samenwerking mogelijk wat leidt tot meer snelheid en flexibiliteit om effectief te reageren in verschillende scenario's. Daarnaast is het randvoorwaardelijk voor het kunnen uitwisselen van data, informatie en besluiten zodat de Krijgsmacht een informatievoordeel heeft ten opzichte van de tegenstander.

Als we hier niet in slagen dan zijn de consequenties voor de Krijgsmacht groot. In het dagelijks leven ervaren we het (tijdelijk) wegvallen van connectiviteit al als zeer disruptief. Voor de Krijgsmacht zijn de consequenties nog groter in het scenario dat de connectiviteit wegvalt tijdens een complexe militaire operatie. In dat scenario is het noodzakelijk dat communicatie en het uitwisselen van informatie met partners beschikbaar is en blijft om de dreiging van een technologisch geavanceerde tegenstander het hoofd te bieden.

Strategische doelen

- Het aantal sensoren en data neemt exponentieel toe. Het moet makkelijker worden om deze gegevens op een veilige manier zowel binnen Defensie als met partners te delen en te integreren tot een gezamenlijk beeld.
- Om systemen en netwerken snel aan elkaar te kunnen koppelen moet er gewerkt worden met standaard communicatiemiddelen, koppelingen en datadefinities. Dit moet centraal gestuurd worden.
- Om de toenemende datastromen goed te faciliteren en communicatiemiddelen robuuster te maken tegen verstoring moet Defensie inzetten op een mix van communicatiemiddelen met voldoende bandbreedte.

Huidige situatie

Er lopen verschillende initiatieven die primair gericht zijn op het vervangen en aanvullen van communicatiemiddelen en netwerken op tactisch niveau. Daarnaast wordt primair vanuit de NAVO de adoptie van gezamenlijke standaarden ten behoeve van digitaal samenwerken gestimuleerd. In gezamenlijke oefeningen zoals CWIX en Osprey[4] wordt concreet geoefend met vernieuwende toepassingen en samenwerking in coalitieverband.

[4] Zie video Osprey (link) of CWIX2025 (link)

Belangrijkste uitdagingen:

- De mix van communicatiemiddelen moet verder worden versterkt met aandacht voor bandbreedte, reikwijdte en fallback opties.
- Satelliet Communicatie (SatCom) moet verder worden versterkt met voorkeur voor soevereine oplossingen, inclusief de benodigde hardware.
- Digitale samenwerking wordt nog te veel gezien als een IT-vraagstuk, zonder de noodzakelijke aanpassing van processen en doctrines.
- Gegevensuitwisseling tussen domeinen en verschillende netwerken moet worden vereenvoudigd.
- De omvang van personeel dat op missie IT ondersteuning kan bieden (CIS en C2 eenheden) moet meegroeien met de krijgsmacht en de toenemende rol van digitale middelen in het optreden.

Aanpak: wat gaan we doen om te versnellen

1.1 Per defensieonderdeel (DO) wordt de beoogde mix van middelen versus huidige situatie in kaart gebracht en geïnvesteerd om de kloof te dichten. Een belangrijke schakel hierin zijn communicatiemiddelen met grote bandbreedte.

1.2 De EU SatCom capaciteit wordt op korte termijn versterkt. Daarnaast wordt er voor de lange termijn een plan gemaakt waarbij rekening gehouden wordt met een toename van sensoren, datastromen en autonome systemen.

1.3 Er wordt voldoende IT kennis en capaciteit geïntegreerd in de operationele eenheden (CIS/C2). Deze blijft meegroeien met de groei van de krijgsmacht en de toenemende digitalisering. Deze eenheden worden eveneens gesteund in hun rol om IT/data kennis breder te delen binnen hun onderdeel.

1.4 Er wordt strakker gestuurd op de standaardisatie van koppelingen en datadefinities, zowel binnen IT als bij inkoop van materieel en vastgoed. De benodigde principes hiervoor worden verankerd in de portfoliosturing en de gezamenlijke architectuurrichtlijnen.

4. SPEERPUNT | DIGITAAL FUNDAMENT

Bijdrage aan gevechtskracht

Het digitaal fundament stelt Defensie in staat om onder alle omstandigheden toegang te hebben tot opslag- en rekenkracht. Dit fundament ondersteunt informatie- en beslisdominantie door *(near)real-time* data-analyse en AI-ondersteuning mogelijk te maken, ongeacht de fysieke locatie. Daarnaast heeft Defensie veel organisatiebrede, ondersteunende processen, zoals voorraadbeheer of logistiek) die cruciaal zijn voor het voortzettingsvermogen, integraal informatiebeeld en strategische besluitvorming. Het verbeteren van deze processen met digitale middelen versterkt het fundament waarop de digitale transformatie wordt gebouwd en vergroot de gevechtskracht.

Als Defensie dit niet doet dan is de consequentie voor de Krijgsmacht dat geavanceerde analyses en nuttige databronnen niet of moeilijk toegankelijk zijn, terwijl de tegenstander hier wel over beschikt. Ondersteuning van de Krijgsmacht met bijvoorbeeld logistiek, HR en voorraden zal minder effectief zijn.

Strategische doelen

- Ontwikkel de verschillende hoog- en laaggerubriceerde infrastructuur en cloud-oplossingen door tot een samenhangend fundament. Doel is dat zowel de operationele als ondersteunende eenheden onder alle omstandigheden een beroep kunnen doen op gedeelde databronnen en rekenkracht.
- Stuur op autonomie ten aanzien van zeggenschap over data en infrastructuur, waarbij realistische afwegingen gemaakt worden tussen korte termijn waarde voor de Krijgsmacht en lange termijn strategische autonomie.
- Digitaliseer organisatiebrede proces-domeinen die de Krijgsmacht ondersteunen. Hierbij kiest Defensie voor standaard-oplossingen met ingebouwde tooling zoals AI, tenzij (militaire) uniciteit maatwerk afdwingt.
- Verminder versplintering in het IT landschap door brede adoptie van standaard pakketten/ technische platformen en uitfasering van onnodig maatwerk en duplicatie van functionaliteit.

Huidige situatie

De belangrijkste lopende initiatieven binnen dit speerpunt zijn de **cloudstrategie**, het programma **GrIT** en het programma **Roger**. Deze initiatieven leveren tezamen zowel een nieuwe infra-structuur als verschillende clouddiensten die op of in samenhang met de infrastructuur worden

ontwikkeld. In dit kader is Defensie bijvoorbeeld in gesprek met verschillende bedrijven over de ontwikkeling van een soevereine cloud en heeft GrIT een Twin datacenter en eerste mobiele rekencentra (XS boxen) opgeleverd. De initiatieven bevinden zich in verschillende ontwikkelingsstadia.

Belangrijkste uitdagingen:

- Verschillende cloudoplossingen moeten beschikbaar gemaakt worden voor diverse omstandigheden (multicloud). Ontbrekende elementen moeten worden ingevuld.
- De cloudmarkt wordt gedomineerd door de VS. In het kader van strategische autonomie, is er een ambitie voor meer Europese samenwerking. Voor diverse clouddiensten is echter nog geen volwaardig Europees alternatief beschikbaar.
- Integratie van nieuwe en huidige infrastructuur en cloudoplossingen naar een samenhangend platform met beveiligde toegang moet nog plaatsvinden.
- Organisatiebrede procesdomeinen bieden nog veel kansen voor verdere digitalisering, m.n. met behulp van betere data integratie en gebruik van AI.

Aanpak: wat gaan we doen om te versnellen

2.1 We realiseren samen met marktpartijen cloudoplossingen waarbij gebruik wordt gemaakt van moderne technologie met Nederlandse hosting en soevereiniteit, die bruikbaar zijn in verschillende gebruiksomstandigheden.

2.2 We geven prioriteit aan de integratie van infrastructuur, cloud en lokale IT-oplossingen zodat er een geïntegreerd infra/cloud platform ontstaat met eenduidige beveiliging en *identity & acces* management laag eromheen.

2.3 We gaan de Cloud strategie actualiseren om het recent toegenomen belang van strategische autonomie te weerspiegelen.

2.4 Defensie gaat investeren in digitalisering van bedrijfsbrede processen met als richtlijn zo min mogelijk maatwerk (configure not customize), tenzij security of unieke samenwerking anders eist[5].

2.5 Defensie ontwikkelt richtlijnen en een toolbox voor het gebruik van gestandaardiseerde koppelingen in verschillende gebruikersomstandigheden. Daarbij worden koppelingen gerationaliseerd als onderdeel van regulier onderhoud (LCM).

2.6 Defensie gaat betere zichtbaarheid en sturing op applicaties creëren door de adoptie van het TIME (Tolerate-Invest-Migrate-Eliminate) of een vergelijkbaar framework.

[5] Randvoorwaardelijk hiervoor is integrale sturing gezien de afhankelijkheden tussen de zestien procesdomeinen en toewerken naar een gedeelde datalaag (single source of truth) inclusief mechanismen om datakwaliteit te borgen.

5. SPEERPUNT | DATA, AI EN AUTONOMIE

Bijdrage aan gevechtskracht

Dit speerpunt draagt primair bij aan gevechtskracht door het mogelijk maken van informatie- en beslisdominantie. Slimme algoritmes gekoppeld en getraind met goede datasets leiden tot betere inzichten en *courses of action* die de tegenstander niet verwacht. Autonome systemen zijn met behulp van AI in staat om, binnen ethische en juridische kaders, zelfstandig besluiten te nemen, met veel hogere snelheid dan mensen dit kunnen. Het belang van het goed leren toepassen van AI kan niet overschat worden.

Als Defensie er niet in slaagt om dit speerpunt te realiseren, dan kan Defensie zich steeds minder goed meten met een technologisch capabele tegenstander. Tegenstanders zullen dan sneller, slimmer en schaalbaarder kunnen opereren met betere integratie van (semi) autonome systemen.

Strategische doelen

- Zorg dat data van voldoende kwaliteit snel ontsloten en gecombineerd kan worden tot relevante inzichten, zonder dat er nog vertragende tussenstappen zoals databewerking nodig zijn.
- Ontwikkel een snel innoverend data ecosysteem bestaande uit kenniscentra, centraal datalab, decentrale datateams en een mix van partners uit de markt. Innovaties worden uitgewerkt binnen de geldende juridische en ethische kaders.
- Pas AI breed toe in zowel militaire als bedrijfsmatige processen, en werk daarbij aan zowel de technische oplossing als de datageletterdheid en adoptievermogen van de organisatie.
- Zorg dat Defensie met behulp van AI internationaal koploper wordt op het vlak van adoptie en continue verbetering van autonome systemen.

Huidige situatie

Onder de vlag van de Defensie Data Science & AI strategie[VI] zijn maatregelen in uitvoering gericht op het vergroten van de datakwaliteit en toepassing van AI in zowel militaire als bedrijfsmatige processen. Daarnaast zijn er verschillende programma's die bijdragen aan vindbaarheid en kwaliteit van data zoals Defensie Open op Orde (DOO) en Roger. Hiermee zijn al tal van initiatieven gelanceerd waaronder de inrichting van een datascience center of excellence, inrichting van decentrale datacellen en de uitrol van een nieuw document-management systeem. Volwassenheids-metingen informatie- en datamanagement[6] leggen verschillende ontwikkelpunten bloot. Tevens heeft Defensie internationaal een sterke rol in het ontwikkelen van ethische en juridische kaders rondom AI.

Belangrijkste uitdagingen:

- *Interne capaciteit*: Decentrale datacapaciteit moet meegroeien met toenemende datastromen en data & AI ambities.
- *IT en data infrastructuur*: Defensie heeft een dataplatform met gedeelde tooling die nog beter kan worden benut. Data uit verschillende bronnen moet nog makkelijker te ontsluiten zijn. Implicaties van b.v. grootschalige drone adoptie voor de IT infrastructuur moet worden uitgewerkt.
- *Visie op C2 (command & control) en data-architectuur*: De C2 visie op de toekomst en daarbij horende data-architectuur moet nog vorm krijgen.
- *Datakwaliteit:* Datakwaliteit en sturing hierop moet continu kunnen verbeteren. Lopende initiatieven op verhogen data volwassenheid kunnen elkaar meer versterken.
- *Samenwerking met de markt:* Dit wordt veelvuldig opgezocht maar is tegelijk complex, o.a. door gebrek aan trainingsdata voor hoog gerubriceerde toepassing en integratie in de gesloten architectuur van Defensie.
- Breed gedeelde *best practices* voor dataintegratie/C2 van Oekraïne zoals het Delta systeem vertalen (zie kader) zich nog beperkt door naar Defensie.

Het Oekraïense Delta-platform groeide in korte tijd uit tot het digitale zenuwstelsel van de krijgsmacht. Dit geïntegreerde commandoplatform combineert realtime informatie uit drones, sensoren, civiele bronnen en inlichtingen, en maakt deze toegankelijk voor eenheden aan het front via veilige tablets en smartphones. Delta toont live de positie van vijandelijke troepen, eigen eenheden en doelen, en stelt commandanten én individuele militairen in staat om sneller, nauwkeuriger en gecoördineerd op te treden. Het systeem is cloud-based, werkt via Starlink en is ontworpen om snel in te spelen op veranderingen in het gevecht. Deze digitale oplossing laat zien hoe data-integratie, situational awareness en adaptieve technologie beslissend zijn op het moderne slagveld.

[6] Data en informatie wordt hier door elkaar heen gebruikt. Het onderscheid is complex doordat het contextafhankelijk is of iets geldt als data- of informatie.

Aanpak: wat gaan we doen om te versnellen

3.1 We breiden decentrale datacapaciteit uit in lijn met de exponentiële groei van data en de ambities op het vlak van data en AI. Daarbij creëren we ruimte voor het centrale datalab om snel te kunnen experimenteren met de markt.

3.2 Defensie ontwikkelt een visie met bijbehorend investeringsplan gericht op de digitale infrastructuur die nodig is om grootschalige drone adoptie en bijbehorende datastromen te faciliteren.

3.3 We gaan experimenteren met data en C2 innovaties vanuit b.v. Oekraïne. Na succesvolle experimenten worden deze innovaties verder geïmplementeerd.

3.4 Defensie versterkt het gezamenlijk dataplatform. We ontwikkelen op basis van een goed uitgewerkt C2 concept een breed geaccepteerde data-architectuur die dit C2 concept ondersteunt en sturen op implementatie.

3.5 We gaan meer synergie creëren tussen de verschillende initiatieven die data-volwassenheid van de organisatie vergroten, zodat hierop wordt versneld.

3.6 Defensie vormt een team dat samen met proceseigenaren visualiseert hoe processen eruitzien wanneer de mogelijkheden van robotisering, data science en AI ten volle worden benut. De processen die direct bijdragen aan de gereedstelling en gevechtskracht krijgen hierbij de prioriteit. *Compliance* en *security by design* principes worden direct meegenomen. Defensie stuurt op brede adoptie van vernieuwende oplossingen in combinatie met het afschalen van oude systemen en processen.

6. SPEERPUNT | EMS, CYBER EN REDUNDANTIE

Bijdrage aan gevechtskracht

Naarmate het belang van digitalisering voor de gevechtskracht toeneemt, nemen ook de dreigingen in het cyber-, elektromagnetisch spectrum (EMS) en voor de fysieke infrastructuur toe. Het verstoren van digitale vermogens van de tegenstander heeft immers steeds meer impact op de gevechtskracht. Defensie investeert daarom in EMS, cyberweerbaarheid en redundantie om de ambitie te realiseren.

Als we hier onvoldoende succesvol zijn dan kan de tegenstander ons vermogen om informatietechnologie te gebruiken ernstig verstoren, en daarmee onze vermogens tot geïntegreerd optreden en behalen van een voordelige informatiepositie teniet doen.

Strategische doelen[7]

- Het beschermen van de Defensie informatiesystemen tegen verstoring rekening houdende met nieuwe ontwikkelingen zoals Quantum computing (*post Quantum crypto*).
- Het toepassen van nieuwe beveiligingstechnieken waardoor data veilig delen over verschillende netwerken makkelijker wordt.
- Voorbereid zijn op uitval van systemen en snel kunnen herstellen of omschakelen naar alternatieven (*contingency*).

Huidige situatie

In 2025 komt een nieuwe cyberstrategie uit die een breed pallet aan doelen en maatregelen bevat om zowel Defensieve als offensieve cybercapaciteit te versterken. Defensie werkt al een aantal jaren zeer actief aan versterken van de cyberweerbaarheid, bijvoorbeeld met de implementatie van SOC (security operation center) torens en oefeningen zoals locked shields[8]. Kennis t.a.v. ontwikkeling van capaciteiten in het elektromagnetisch spectrum krijgt recent meer aandacht maar is nog in opbouw. Omwille van vertrouwelijkheid wordt hieronder niet nader ingegaan op de belangrijkste uitdagingen.

[7] Scope DTS beperkt zich tot cybersecurity.
[8] Zie voor meer informatie (link)

In Oekraïne vindt dagelijks een strijd plaats die voor het oog onzichtbaar is: drones vallen uit, signalen verdwijnen, netwerken worden verstoord. Russische elektronische aanvallen dwingen Oekraïense eenheden om voortdurend te improviseren en hun technologie aan te passen. Ze zetten zelf ontwikkelde stoorzenders in, bouwen moeilijk te verstoren mobiele netwerken, switchen automatisch van frequentie en gebruiken drones met glasvezelkabels om buiten bereik van verstoring te blijven. Deze aanpak laat zien hoe belangrijk het is om snel te reageren, creatief te denken en technologie flexibel toe te passen.

Aanpak: wat gaan we doen om te versnellen

4.1 De maatregelen uit de Cyber Strategie 2025 worden geïmplementeerd, waaronder het toepassen van principes van datacentrische beveiliging, zero trust en quantumveilige cryptografie.

4.2 Defensie investeert in zowel interne kennis en capaciteit op het gebied van encryptie en datacentrisch beveiligen als in marktpartijen om de kennis in Nederland te houden. Dataencryptie is een van de sleutels om databeveiliging minder afhankelijk te maken van gescheiden netwerken waardoor het sneller kan stromen naar de plek waar de informatie het meeste voordeel biedt.

4.3 Defensie investeert in een goed werkende organisatie voor het elektromagnetisch spectrum (EMS) om operationele effectiviteit en veiligheid te waarborgen.

4.4 Het life cycle management in brede zin wordt versterkt. Daarbij wordt redundantie gebouwd voor de kritische systemen. De systemen die direct bijdragen aan de gevechtskracht krijgen prioriteit.

4.5 Defensie gaat regelmatig de uitval van kritische systemen en connectiviteit oefenen. Het gaat zowel om oefeningen met militaire als bedrijfsmatige systemen en netwerken.

7. SPEERPUNT | DIGITAAL AANPASSINGSVERMOGEN

Bijdrage aan gevechtskracht

Zoals Oekraïne meermaals heeft laten zien gaat het niet alleen om het hebben van goede digitale middelen maar vooral om het effectief toepassen ervan voor maximaal effect. Het vermogen om continu te zoeken naar manieren om huidige en nieuwe technologie om te zetten in gevechtskracht is cruciaal. Anders geformuleerd: goed geïntegreerde IT en data vormen een steeds krachtiger wapensysteem, maar het heeft alleen effect op de gevechtskracht als Defensie het goed leert gebruiken.

Als Defensie niet succesvol is in het realiseren van dit speerpunt dan loopt Defensie het risico veel IT te bouwen die onvoldoende aansluit bij de operationele behoefte. Potentiële tegenstanders zijn Defensie dan telkens een stapje voor door slimmer gebruik te maken van digitale technologie.

Strategische doelen

- Stimuleer zoveel mogelijke directe interactie en aansturing tussen gebruiker en (interne) leverancier. Dit sluit aan bij het principe dat de commandant zeggenschap heeft over de noodzakelijke middelen voor inzet, inclusief de te ontwikkelen en beheren IT middelen.
- Versterk het strategisch ecosysteem van IT leveranciers en creëer meer ruimte voor rechtstreekse, flexibele afstemming tussen gebruiker en leverancier.
- Stuur op doelarchitectuur en slim hergebruik van technologieoplossingen van binnen als buiten Defensie. Decentrale sturing mag niet leiden tot onnodige complexiteit in het IT landschap.
- Versterk mindset en kennis die past bij een snel innoverende digitale organisatie.

Huidige situatie

Ondanks dat Defensie weer aan het groeien is, zijn de sporen van 20 jaar lang bezuinigen niet zomaar verdwenen. Veel processen voor de IT voortbrenging zijn nog ingericht op een situatie waarin alleen ruimte was voor het hoogst-noodzakelijke onderhoud in plaats van snelle innovatie dicht op de gebruiker. Er zijn binnen Defensie meerdere bewegingen ingezet om de organisatie flexibeler te maken, zoals de inrichting van een CIO stelsel, versterken portfoliosturing en adoptie en sociale innovatie in werkwijzen. Deze strategie gaat daarop door.

Belangrijkste uitdagingen:

- In de bezuinigingsperiode is IT sterk gecentraliseerd en is veel kennis en ervaring weggehaald bij de Defensieonderdelen, terwijl juist voor het omzetten van technologie in gevechtskracht gebruiker en ontwikkelaar zoveel mogelijk direct moeten samenwerken. Dit geldt eveneens voor de Defensiebrede functionele IT.
- Inkoop is al bezig te versoepelen. Specifiek voor IT is er behoefte aan strategische

partnerships die helpen bij Defensiebrede innovatie met bijpassende flexibele contractvormen.
- Op een aantal technologielagen -zoals data- is Defensie al verder in het opbouwen van een ecosysteem met kennispartners, leveranciers en interne capaciteit en sturing. Deze werkwijze zou voor meerdere kritische technologielagen omarmt moeten worden en gecombineerd met andere instrumenten voor samenhangende sturing.
- Binnen de IT keten is er nog veel focus op de processtappen, alle risico's afdekken en het aantal mensen dat diepgaande kennis heeft van zowel IT als operationele doctrines is beperkt. Daarbij moet affiniteit met inzet van digitale middelen en het creatief denken in digitale mogelijkheden sterk verbeteren.

Aanpak: wat gaan we doen om te versnellen

5.1 Defensie zorgt ervoor dat eindverantwoordelijken[9] flexibel de IT-ontwikkeling en het beheer kunnen aansturen die zij nodig hebben voor hun taken. Deze transformatie loopt gefaseerd onder regie van de CDS om zowel decentrale sturing als eenduidigheid in werkwijze en IT landschap te borgen. Dit maakt de weg vrij voor minder grootschalige projecten en programma's, en meer kortcyclische ontwikkeling gericht op concrete effecten.

5.2 Digitale transformatie en innovatie hangen nauw met elkaar samen. In de realisatie van de digitale transformatie strategie wordt daarom de aansluiting gezocht bij D-SII (Defensie Strategie voor Industrie en Innovatie), wat onder meer betekent dat defensie op specifieke technologiegebieden optreed als smart developer

5.3 Defensie creëert/versterkt rondom kritische digitale technologieën[10] de opbouw van een ecosysteem met kennispartners, NAVO-partners, strategische leveranciers en interne capaciteit. Dit ecosysteem wordt samen met de innovatie- en inkoopketen vormgegeven en er wordt actief gestuurd op kennisdeling, hergebruik van technologieplatformen en adoptie van oplossingen en standaarden die tevens de strategische autonomie bevorderen.

5.4 Portfoliomanagement en architectuur worden blijvend versterkt.

5.5 Defensie ontwikkelt de digitale geletterdheid door een mix van opleiding, resultaatsturing, mandaten laag beleggen en uitwisselen van kennis tussen operatie en IT. Daarnaast wordt zoveel mogelijk directe samenwerking in snelle experimenten tussen gebruiker en ontwikkelaar gestimuleerd wat de meest effectieve wijze is om digitale geletterdheid en operationele kennis samen te brengen.

[9] Commandanten van defensieonderdelen en verantwoordelijken voor functionele IT, zoals HR
[10] Bijvoorbeeld Cyber, cloud/Infra, data&AI, EMS, low-code/robotics, crypto&HGI. Rondom deze technologielagen wordt synergie met de initiatieven uit de Defensie Industrie en Innovatie Strategie geborgd.

8. DE FORCE MULTIPLIER: INTEGRATIE TUSSEN DE SPEERPUNTEN

Elk van deze speerpunten draagt bij aan gevechtskracht, maar de impact is veel groter wanneer de speerpunten in samenhang werken. Hoe dit werkt kan het beste uitgelegd worden aan de hand van een voorbeeld. Onderstaand voorbeeld is primair militair, maar dezelfde logica geldt voor ondersteunende en bestuurlijke processen.

Stel dat een MQ9 Reaper data verzamelt, dan moet deze data via een (1) beveiligde verbinding (e.g. tactische datalink) verstuurd worden naar een omgeving waar deze data (2) opgeslagen en geanalyseerd kan worden, bijvoorbeeld een lokaal commandocentrum (edge) of centraal beveiligde cloud omgeving.

Vervolgens wordt data uit verschillende bronnen en van verschillende partners aan elkaar gekoppeld via beveiligde verbindingen en (3) gecombineerd met andere data, zoals satelliet-gegevens en OSINT data met troepen-bewegingen, zodat een gecombineerd real-time beeld ontstaat van het operatiegebied. Vervolgens kan met behulp van geavanceerde analyse- en visualisatiemethoden, zoals AI en AR, handelingsopties worden voorgesteld en scenario's getest. De tegenstander probeert deze informatieketen uiteraard te verstoren met een combinatie van kinetische, EMS en cyberaanvallen waardoor (4) continu gewerkt moet worden aan de cyberveiligheid en redundantie van systemen en processen. Tenslotte zijn zowel de processen als onderliggende technologie continu onderhevig aan vernieuwing, wat betekent dat (5) het creatieve vermogen om deze digitale middelen om te zetten in gevechtskracht uiteindelijk het doorslaggevend verschil maakt. Mens & machine dus.

Samengevat wordt gesproken over een zogenaamde 'technologie stapel' (*'technology stack'*), dat een continu ontwikkelend wapensysteem vormt. Dit wapensysteem moet beschermd worden (oranje laag) en mensen moeten het zowel goed leren inzetten als helpen om het continu te verbeteren (buitenste laag)[11].

[11] Onderstaande logica komt eveneens terug in digitale transformatie strategieën van andere krijgsmachten, zoals van de UK of de NAVO datastrategie.


1. Coms & samenwerking
2. Digitaal fundament
3. Data, AI & autonomie
4. EMS, Cyber en redundantie
5. Aanpassingsvermogen
AI, Autonomie & decision-support
Datafusie
Integratielaag
Infra & cloud
Communicatie & samenwerking
Informatie- en Beslisdominantie
Geïntegreerde effecten

Consequentie voor de strategie

- Mensen maken het verschil. IT is net als een wapensysteem een middel dat gevechtskracht kan leveren, en hoe beter mensen in staat zijn dit middel te gebruiken hoe meer gevechtskracht het oplevert. Training, oefening en directe interactie tussen ontwikkelaar en gebruiker is dus cruciaal.
- De bovenste lagen zijn beperkt effectief als de onderste lagen niet op orde zijn. Basis op orde blijft daarmee komende jaren prioriteit. Idealiter vindt er wel geleidelijk een verschuiving plaats richting een steeds hoger tempo en ruimte voor innovatie.
- IT is een force multiplier waaraan elke dag door duizenden mensen hard wordt gewerkt, van binnen en buiten Defensie. Sturing op samenhang blijft daarom noodzakelijk, juist om binnen deze kaders meer decentrale vrijheid en directe samenwerking mogelijk te maken.

9. VERANDERAANPAK, RISICO'S EN MITIGERENDE MAATREGELEN

Aan de strategie wordt een uitvoeringsplan gekoppeld. Dit uitvoeringsplan geeft concreter invulling aan de beoogde veranderdoelen binnen defensie inclusief de financiële consequenties, monitoring en borging. Besluitvorming hierover wordt via het reguliere proces gerealiseerd. Dit uitvoeringsplan is al in ver gevorderd stadium en activiteiten die binnen de huidige kaders en mandaten plaats kunnen vinden worden reeds in gang gezet, er is immers geen tijd te verliezen.

Risico's & mitigerende maatregelen

Consequenties van het mislukken van de speerpunten zijn reeds genoemd in de betreffende hoofdstukken. De strategie moet dus lukken om dit te voorkomen. Onderstaande risico's zijn daarom primair gericht op de realisatie.

Risico	Mitigatie
Onvoldoende financiele middelen en/of menskracht (o.a. door arbeidsmarktkrapte) voor de versnelling van de digitale transformatie.	Investeringsbehoefte wordt in lijn met ambities nader uitgewerkt in een financiele en personeelsforecast[12]. Daarnaast wordt op de genoemde doelen slim samengwerkt met de markt.
Gedeeltelijke decentralisatie van de IT ontwikkeling leidt tot verdere fragmentatie van het IT landschap waardoor de transformatie vastloopt.	Combinatie van versterken architectuur, centrale portfoliosturing en het werken met technologieplatformen levert tegelijk voldoende sturing op samenhang en hergebruik. Daarnaast wordt de decentralisatie gefaseerd ingezet, beginnend blij CLAS, CLSK en een functionele IT keten.
Organisatorische randvoorwaarden voor het realiseren van het beoogde aanpassingsvermogen worden onvoldoende ingevuld.	Lopende gesprekken hierover vertalen naar concrete voorstellen in het uitvoeringsplan en afhechten in de bestuursraad.
Implementatie loopt vast door teveel prioriteiten tegelijk en onduidelijke resultaten.	Met behulp van uitvoeringsplan en portfoliomanagement sturen op zowel tempo als focus. Impact volgen in te ontwikkelen digitaal gereedheid dashboard van defensie.
Weerstand tegen de verandering (not invented here).	Topmanagement hulp vragen bij uitdragen transformatieboodschap. Nauw blijven betrekken van het defensie CIO stelsel en veranderkundige / communicatie ondersteuning voor de lijn bieden.

[12] In 2021 is het rapport Defensie Duurzaam Digitaal naar de kamer gegaan (kamerstuk 31 125, nr. 118). Hier wordt in 2025 een update op gemaakt geactualiseerd naar de huidige situatie en doelstellingen.

BIJLAGE A: DIGITALE TRENDS

Digitale trends

In de huidige conflicten zien we verschillende trends en ontwikkelingen die in toenemende mate een rol gaan spelen in conflicten.

Connectiviteit onder druk

Digitale connectiviteit is de levensader van de moderne oorlogsvoering. Een betrouwbaar, interoperabel en robuust digitaal netwerk komt steeds meer onder druk te staan door de huidige intensivering van jamming en sabotage.

EW
24 miljard (2028) investeringen in wapens bedoeld voor Electronic Warfare (EW) dat is 40% meer dan 2021.

Jamming
Jamming laat de hit rate van moderne wapens (bijvoorbeeld HIMARS en drones) dalen naar minder dan **10%**

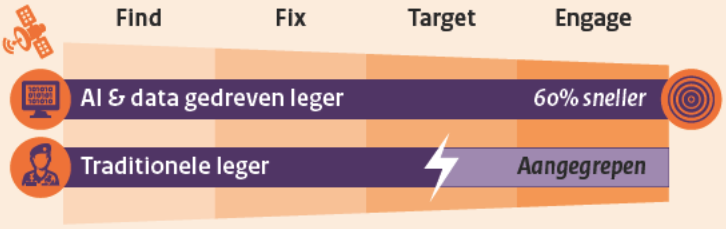
Autonome systemen domineren

Autonome systemen, zoals drones, kunnen tegen relatief lage koste snelle, nauwkeurige en effectieve aanvallen uitvoeren. Ze domineren hiermee het huidige slagveld en hinderen de manoeuvres van reguliere troepen.

70% van militaire verliezen wordt veroorzaakt door drones.

AI versnelt het gevecht

Kunstmatige intelligentie versnelt de verwerking van data en de identificatie van doelen, wat effectiever optreden mogelijk maakt. AI verkort niet allen de herkentijd, maar vergroot ook de effectiviteit van daaropvolgende aanvallen dankzij verbeterde decision support.



Cyber is kritiek

Onze afhankelijkheid en verwevenheid met IT-systemen maakt deze tot een interessant doelwit voor (cyber)aanvallen door vijanden. Up-to-date IT-systemen, quantum-resistente encryptie en fallback-opties vormen het fundament van onze digitale weerbaarheid.

250.000 Oekraïense inwoners zonder stroom door een Russische cyberaanval in 2015.

4315 Russische cyberaanvallen in 2024 op Oekraïne.

Strategische autonomie noodzakelijk

Europa's afhankelijkheid van technologieën die uit niet-Europese landen worden gehaald maakt ons kwetsbaar. Dit vraagt om een zorgvuldige afweging tussen innovatie, interoperabiliteit en soevereine controle.

95% van de Europese cloudmarkt is in handen van aanbieders uit niet-EU-landen.

BIJLAGE B: BEGRIPPENLIJST

■ Defensie Duurzaam Digitaal (DDD)	Analyse en kamerstuk uit 2021 op basis waarvan is besloten om de structurele onderinvestering in IT te repareren, te gaan investeren in een aantal organisatorische randvoorwaarden (portfoliosturing, CIO stelsel) en in Cyber en AI.
■ SatCom (Satellite Communication)	Communicatiesystemen die via satellieten data-verbindingen tot stand brengen. SatCom is onmisbaar als robuuste communicatieverbinding voor militaire operaties over grote afstand.
■ EMS (Electro Magnetic Spectrum)	Het totale spectrum van elektromagnetische golven (radio-golven, microgolven, infrarood, licht, ultraviolet, röntgen en gammastraling). In militaire context gaat het vaak om de frequentiebanden die gebruikt worden voor communicatie, radar en sensoren. Beheersing van (en bescherming tegen) vijandelijke verstoring in het EMS is essentieel voor moderne oorlogsvoering. Bescherming bestaat in de praktijk meestal uit het kunnen schakelen tussen meerdere middelen en frequenties.
■ Cyber	Het digitale domein waarin Defensie opereert, zowel Defensief (beschermen van eigen netwerken en systemen) als offensief (verstoren of binnendringen van vijandelijke systemen). Cyber is onlosmakelijk verbonden met moderne oorlogsvoering en wordt gebruikt voor spionage, sabotage en beïnvloeding. De DTS zal, wanneer er gerefereerd wordt aan cyber, voornamelijk doelen op Defensieve cyber.
■ Datacentrische beveiliging	Een beveiligingsstrategie waarbij data zelf versleuteld (gecodeerd) en beschermd wordt, in plaats van enkel het systeem of netwerk waar de data op staat. Hierdoor blijft de informatie ook beveiligd wanneer deze wordt verplaatst, gedeeld of op andere netwerken wordt gebruikt.
■ Zero Trust	Een beveiligingsmodel waarbij geen enkel onderdeel of persoon in het netwerk standaard ‘vertrouwd’ wordt. Alles en iedereen moet zich blijven authenticeren en verifiëren, ongeacht eerdere toegangsrechten. Dit minimaliseert het risico van ongeoorloofde toegang en beperkt de impact van mogelijke inbreuken.

■ Data-architectuur	De manier waarop data binnen een organisatie wordt gestructureerd, beheerd en ontsloten. Het omvat onder andere datamodellen, databronnen, opslag, governance en beveiliging. Een goede data-architectuur vereenvoudigt het delen van informatie, het toepassen van AI en het realiseren van interoperabiliteit.
■ Life Cycle Management (LCM)	Het gestructureerd beheren van IT-systemen en -toepassingen gedurende hun hele levenscyclus – van ontwerp, ingebruikname en onderhoud tot uitfasering. Door LCM goed uit te voeren, wordt de stabiliteit, veiligheid en toekomstbestendigheid van het IT-landschap gewaarborgd en kan nieuwe technologie sneller worden ingevoerd.
■ De operatie	Hiermee wordt breed verwezen naar mensen en processen die gebruik maken van IT middelen om doelen en taken te realiseren die bijdragen aan de gereedheid en gevechtskracht van defensie.
■ Defensieonderdelen (DO'en)	Hieronder vallen in elk geval de Operationele Commando's van land, zee en luchtstrijdkrachten, de KMAR, DOSCO en COMMIT. SOCOM, DCC en de bestuurstaf hebben eveneens zeer specifieke IT behoeften en het kan zinvol zijn deze mee te nemen in de maatregelen om IT te decentraliseren: dit wordt nader uitgewerkt in uitvoeringsplan. De MIVD is een onderdeel dat qua IT aansturing al vergaand is gedecentraliseerd.

BIJLAGE C: REFERENTIES

[I] Sluit aan op kernthema's uit de Defensienota 2024 en de NAVO digitale transformatie strategie. Tevens gebaseerd op recente inzichten m.b.t. rol van data en innovatie in het conflict van de toekomst, waaronder:

- Allen, J. R., Hodges, F. B., & Lindley-French, J. (2021). *Future War and the Defence of Europe*. Oxford University Press.
- Price, B. R. (2024). *Decision advantage and initiative: Completing Joint all-Domain Command and Control. Air & Space Operations Review, 3*(1), 60–74.
- The Economist. (2024, 20 juni). AI will transform the character of warfare. *The Economist*
- Bondar, K. (2025, 6 maart). *Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare*. Center for Strategic and International Studies.
- NATO Allied Command Transformation, Università di Bologna, & Istituto Affari Internazionali. (2021). *NATO decision-making in the age of big data and artificial intelligence*. NATO ACT.
- U.S. Army Futures Command. (2025). Achieving decision dominance: The arduous pursuit of information advantage in the era of AI and data warfare. *Military Review*, January–February, 12–25.
- NATO Allied Command Transformation. (2025, 2 mei). *Multi-Domain Operations and Digital Transformation: Enabling Converged Effects in the Modern Battlespace*. NATO ACT.
- Krepinevich, A. F. (2024, December 16). *Military innovation on the global stage: Lessons from the past*.
- Kotila, B., Drezner, J. A., Bartels, E. M., Hill, D., Hodgson, Q. E., Huilgol, S. S., Manuel, S., Simpson, M., & Wong, J. P. (2023). *Strengthening the defense innovation ecosystem* (RR-A1352-1). RAND Corporation.

[II] Defensie Duurzaam Digitaal uit 2021 (Kamerstuk 31 125, nr. 118).

[III] The Hague Centre for Strategic Studies (HCSS): De Strategische Monitor 2025

[IV] O.a. NATO EDT's (link), the Age of multidomain threats (NATO HQ SACT), TNO technologie verkenning Defensie (2024), Emerging technology trends for defence and security (2020)..

[V] O.a. van de NAVO (link), UK (link), Canada (link), Denemarken, Duitsland, België en de US (link) – hiervan zijn ook recentere documenten bestudeerd.

[VI] Data Science en AI strategie 2023–2027, kamerstuk 36 592, nr. 1.

Ministerie van Defensie

Juli 2025