




Ministerie van Defensie

Departementaal I-plan Defensie 2025-2027

Versie	1.0
Datum	3 december 2024
Status	definitief

Colofon

	Bestuurstaf Chief Information Office
Locatie	Den Haag - Plein-Kalvermarktcomplex Kalvermarkt 32 's-Gravenhage
Postadres	Kalvermarkt 38 2511 CB 'S-GRAVENHAGE MPC 58B
Contactpersoon	
Versie	1.0

Inhoud

1	Inleiding—5
2	Rijksbrede prioriteiten—7
2.1	I in het Hart; Verbeteren van digitale uitvoerbaarheid van beleid—7
2.2	Versterken digitale weerbaarheid;—7
2.3	IHH; Informatiehuishouding op orde—7
2.3.1	Archivering chatberichten:—7
2.3.2	E-mailarchivering:—8
2.4	Data & Algoritmen; aanpak algoritmen & AI - Algoritmeregister—8
3	Prioritaire doelstellingen—9
3.1	Digitale transformatie—9
3.2	Multidomein optreden (MDO)—10
3.3	Versterken continuïteit IT—10
3.3.1	Grensverleggende IT—11
3.3.2	FOXTROT—12
3.3.3	ROGER—12
3.3.4	Defensie Open op Orde—12
3.4	Elektromagnetisch spectrum—12
3.5	Data science & artificial intelligence—12
3.6	Cyber en digitale weerbaarheid—13
3.7	Interoperabiliteit—14
3.8	Wendbare organisatie—15
3.8.1	CIO-stelsel—15
3.8.2	Personeel—15
3.8.3	Robotisering—16
3.8.4	Aanbesteding—16
3.8.5	Gereedstelling—16
3.9	Conclusie—16
4	Financiële paragraaf—17
5	Referenties—18

Aanleiding

Naar aanleiding van verschillende documenten en onderzoeken, waaronder de Kabinetsreactie commissie Elias, de Beleidsreactie onderzoeken IV-governance Rijk en het Besluit toekomst Bureau ICT-toetsing (BIT), is aan de Tweede Kamer toegezegd dat departementen een meerjarig informatieplan opstellen^{1, 2}. In het Besluit CIO-stelsel 2020³ is het meerjarig departementaal informatieplan (I-plan) verankerd en zijn de taken voor de departementale CIO, de departementale CISO, CIO-Rijk en CISO-Rijk hieromtrent opgenomen.

Het interdepartementale CIO-beraad heeft het Kwaliteitskader Meerjarige Departementale Informatieplannen⁴ vastgesteld dat op 1 januari 2022 in werking is getreden. Dit kwaliteitskader bevat een nadere uitwerking van de inhoud van het informatieplan en het proces van aanlevering. Het Kwaliteitskader wordt continu doorontwikkeld. Dit plan is gebaseerd op het bijgestelde Kwaliteitskader van april 2024, waaraan een nieuw hoofdstuk rijksbrede prioriteiten is toegevoegd.

Ieder departement levert jaarlijks een departementaal I-plan op met daarin de prioritaire doelstellingen op het gebied van de informatievoorziening van het ministerie voor de komende drie jaren. Een indicatief aantal hierbij is tussen de vijf en acht doelstellingen.

Het doel van het departementale informatieplan is niet een overzicht van alle lopende projecten, maar inzicht in de belangrijkste ontwikkelingen en plannen op het gebied van de IT en digitalisering. Defensie heeft op relevante deelgebieden reeds specifieke meerjarige strategieën en plannen. Dit I-plan schetst de verbinding hiertussen en biedt daarmee inzicht in de digitale transformatie van Defensie.

1 Inleiding

De maatschappelijke taak van Defensie is om Nederland veilig te houden. Fysieke en digitale dreigingen nemen steeds verder toe. Het digitale domein wordt in toenemende mate gebruikt om politiek-strategische doelstellingen te forceren onder de grens van het gewapend conflict. Staten proberen hun (politieke) invloed te vergroten, zowel via cyberaanvallen als door continue beïnvloeding van mensen en groepen. Daarnaast zetten onze tegenstanders volop in op de mogelijkheden van data science en AI voor het moderniseren van hun krijgsmachten. Ook maken niet-staatelijke actoren in toenemende mate gebruik van technologische ontwikkelingen die een dreiging vormen voor de vitale infrastructuur.

De Defensienota 2024 onderkent drie strategische doelstellingen voor Defensie voor de komende jaren:

- Defensie is voorbereid op een grootschalig militair conflict in het NAVO-verdragsgebied
- Defensie is klaar voor het gevecht van de toekomst en past zich aan veranderende dreigingen en conflictvoering aan
- Defensie staat klaar voor nationale taken en ondersteuning van civiele autoriteiten

Terwijl de (digitale) dreiging rap toeneemt heeft Nederland 30 jaar lang bezuinigd op Defensie wat diepe sporen heeft nagelaten in zowel het IT landschap als het verandervermogen. Om onze grondwettelijke taken effectief te kunnen blijven uitvoeren, en te vechten voor een veilige toekomst, zullen we dus niet alleen beter moeten worden in het stroomlijnen van informatie om snelle en goede besluiten te nemen. We zullen ook onze organisatie en ons optreden moeten aanpassen aan de veranderende dreiging- en informatieomgeving en het verandervermogen moeten herstellen. Tegelijkertijd biedt digitalisering ook kansen om bij te dragen aan de vernieuwing van Defensie, waaronder optimaliseren van de bedrijfsvoering en het ondersteunen van besluitvorming met behulp van data en nieuwe technologische ontwikkelingen als quantum computing of cloudtechnologie.

Zoals aangegeven in de Defensienota 2024⁵ werkt Defensie aan het aanpassen van de organisatie aan het veranderde dreigingsbeeld. Vanuit hoofdtak 1, de verdediging van het eigen en Navo-grondgebied, moet Defensie optimaal zijn voorbereid op een conflict met een technologisch geavanceerde tegenstander. Om in alle domeinen slim en geïntegreerd samen te kunnen werken zijn digitale transformatie en technologische ontwikkelingen randvoorwaardelijk. De komende periode wordt hiervoor een digitale transformatiestrategie ontwikkeld. Ook werkt Defensie aan de Wet op de gereedstelling, waarmee belemmeringen worden weggenomen om in het informatiedomein aan gereedstelling te kunnen doen.

Dit meerjarig informatieplan (I-plan) van Defensie is een update van het [Defensie I-plan 2023-2026](#)⁶ en is bedoeld om de belangrijkste prioriteiten op het gebied van deze digitale transformatie voor de periode 2025-2027 weer te geven. Deze versie van het departementale i-plan neemt een aantal concepten mee uit de Defensienota 2024. De volgende versie wordt volledig gebaseerd op de nieuwe Defensienota en de digitale transformatiestrategie.

De geschetste prioriteiten vormen de beleidsopgave van Defensie in het I-domein. Dit wordt uitgewerkt in hoofdstuk 0. De doelstellingen hangen met elkaar samen en zijn niet los van elkaar te zien. Daarom worden om te beginnen de overkoepelende

begrippen digitale transformatie en multidomein optreden (MDO) toegelicht. Ten tweede wordt ingegaan op het versterken van de continuïteit en het *future fit* maken van de basis IT en bijbehorende infrastructuur. Daarbij is aandacht voor informatiehuishouding, een rijksbrede prioriteit. Daarna worden data science en artificial intelligence behandeld als belangrijke enablers voor de transformatie. De digitale ontwikkelingen brengen zowel risico's als kansen met zich mee in het cyberdomein, wat prioriteit op cyber (weerbaarheid) noodzakelijk maakt. Daarna wordt over de as van interoperabiliteit de samenwerking met onze bondgenoten en partners in binnen en buitenland besproken. Tot slot wordt aandacht besteed aan het personeel, werkwijzen en de wendbare organisatie die nodig zijn om deze prioriteiten tot uitvoering te brengen.

In hoofdstuk 2 wordt ingegaan op de rijksbrede prioriteiten voor 2025.

2 Rijksbrede prioriteiten

In dit hoofdstuk wordt aangegeven op welke wijze Defensie invulling geeft aan de vastgestelde rijksbrede prioriteiten voor 2025⁷.

2.1 **I in het Hart; Verbeteren van digitale uitvoerbaarheid van beleid**

In een snel veranderende digitale wereld stimuleert, richt en toetst de CIO de digitale transformatie van Defensie. De CIO heeft zitting in de Bestuursraad, is rechtstreekt geplaatst onder de Secretaris-Generaal en heeft een zelfstandige beleidsbevoegdheid. Hierdoor wordt de CIO in een vroegtijdig stadium betrokken bij beleidsontwikkelingen, ook van andere domeinen.

Defensie heeft de Integrale beleidscyclus (IBC) vastgelegd in een aanwijzing. Onderdeel daarvan is de integrale afstemming met alle stakeholders, waaronder de CIO. Ook wordt de CIO betrokken bij alle materieelprojecten. In 2025 evalueert de CIO of en welke verbeteringen er vanuit CIO-perspectief gewenst zijn.

Defensie beschikt over een eigen Defensiebreed CIO-stelsel. In dit stelsel worden naast de departementale CIO ook CIO's decentraal bij defensieonderdelen onderkend.

2.2 **Versterken digitale weerbaarheid;**

Defensie moet onder alle omstandigheden, ook bij cyberaanvallen of een kinetisch conflict, digitaal veilig kunnen werken en operaties kunnen uitvoeren. Daarvoor wordt de digitale infrastructuur van Defensie versterkt. Defensie verhoogt daarnaast de eigen digitale weerbaarheid door te investeren in cyberbewustzijn en bijbehorend gedrag van personeel.

Defensie besteedt al aandacht aan digitale weerbaarheid in basistrainingen of bewustwordingsprogramma's voor specifiek doelgroepen, zoals militairen en IT-personeel. Deze trainingen en programma's worden in de komende periode uitgebreid naar alle defensie medewerkers.

Voor de verdere activiteiten rondom cyber, NIS2 en digitale weerbaarheid zie para 3.6.

2.3 **IHH; Informatiehuishouding op orde**

IHH is onderdeel van het programma Defensie Open op Orde (DOO). Dit wordt verder uitgewerkt in paragraaf 3.3.4. Voor IHH zijn twee rijksbrede prioriteiten vastgesteld: Archivering van chatberichten en van e-mail.

2.3.1 *Archivering chatberichten:*

De archivering van chatberichten wordt projectmatig aangepakt vanuit het programma Defensie Open op Orde. Dit project bestaat uit 3 deelprojecten:

- In Chatkuis worden nieuwe chatberichten geautomatiseerd en op afstand veiliggesteld. Het gaat hierbij om circa 200 medewerkers die onder de nog vast te stellen selectielijst worden aangemerkt als sleutelfunctionaris. Implementatie wordt verwacht in Q1 2026.
- In ChatDuTo worden chatberichten duurzaam toegankelijk gemaakt in een beheerd archiefsysteem. Implementatie wordt verwacht per Q3/Q4 2026
- In ChatHistorie worden eerdere handmatig veiliggestelde berichten duurzaam toegankelijk gemaakt. Implementatie wordt verwacht per Q1/Q2 2027.

Defensie zoekt de samenwerking met het rijksbrede chatberichtenproject van RvIHH.

Defensie blijft in de tussentijd uitvoering geven aan de tijdelijke instructie chatberichten bewindspersonen zoals vastgesteld in de ministerraad. De nieuwe bewindspersonen zijn hierover geïnformeerd.

2.3.2

E-mailarchivering:

Defensie heeft een concept selectielijst opgesteld voor het archiveren van e-mails. Zodra de rijksbrede PAR-procedure is voltooid en de nieuwe handreiking is vastgesteld zal Defensie de selectielijst zo nodig aanpassen en vaststellen.

Er wordt door het SSC-ICT gewerkt aan een technische voorziening voor het veiligstellen van de e-mailboxen die daarna als voorbeeld wordt gebruikt voor de implementatie bij Defensie. De implementatieplanning wordt gekoppeld aan de uitrol van het nieuwe Defensiebrede documentmanagementsysteem DefDoc.

2.4

Data & Algoritmen; aanpak algoritmen & AI - Algoritmeregister

Defensie vindt het belangrijk om waar mogelijk transparant te zijn over het gebruik van algoritmes. Daarom wordt er gewerkt aan het inventariseren van algoritmes en het publiceren van algoritmes die in het Algoritmeregister kunnen worden geplaatst. Het is aannemelijk dat veel algoritmes van Defensie vallen onder de uitzonderingsgrond genoemd in categorie D van de Handreiking Algoritmeregister. Niet alle algoritmes kunnen worden gepubliceerd. Deze afweging moet zorgvuldig gemaakt worden in verband met mogelijke veiligheidsrisico's bij het publiceren van bepaalde informatie.

Defensie heeft een algoritme procesmodel ontwikkeld waarbij voor elke stap in het proces rollen en verantwoordelijkheden inzichtelijk zijn gemaakt. Defensie maakt daarbij een onderscheid tussen algoritmes die onderdeel zijn van een experiment en algoritmes die in producties draaien. Defensie-onderdelen starten per 2025 met het registreren van hun algoritmes in productie in het interne algoritmeregister dat Defensie heeft ontwikkeld. De focus ligt in eerste instantie op het identificeren van verboden en hoog risico algoritmes volgens de AI verordening, en op algoritmes met directe rechtsgevolgen voor betrokkenen. In de loop van 2025 en 2026 zullen ook andere algoritmes worden geïnventariseerd, bijvoorbeeld algoritmes die hoogerubriceerde informatie (HGI) verwerken of algoritmes die beïnvloeden hoe de overheid een betrokkene of groep classificeert. Met het inventariseren en registreren wordt het voor Defensie-onderdelen makkelijker om te identificeren welke algoritmes in het Algoritmeregister kunnen worden gepubliceerd.

3 Prioritaire doelstellingen

3.1 Digitale transformatie

Militaire conflicten digitaliseren. Wapensystemen worden steeds meer uitgerust met digitale technieken waaronder slimme sensoren, navigatie, systemen voor dataopslag en dataverwerking en communicatiesystemen om verbindingen op te bouwen. De hoeveelheid data neemt enorm toe, maar ook de complexiteit om deze systemen te gebruiken en onderhouden. Defensie is volledig afhankelijk van informatietechnologie (IT); zonder IT geen moderne krijgsmacht. Anders gezegd, digitalisering is *core business* voor Defensie en een kwestie van leven en dood. De IT die relevant is voor Defensie zal zich de komende jaren snel blijven ontwikkelen. Daarin zien we een aantal trends:

- Gewijzigde en veranderende digitale dreiging;
- Toename van gebruik en daarmee samenhangende kosten van IT;
- Toenemend belang van innovatie- en verandervermogen om voor te blijven lopen in vergelijking met technologisch hoogwaardige tegenstanders
- Nieuwe technologieën voor operationele inzet en bedrijfsvoering, zoals:
 - Internet of Things;
 - Robotic Process Automation (RPA);
 - Quantum- en nanotechnologie;
 - Cloudtechnologie.
- Toename van data die verzameld, verwerkt, geanalyseerd, toegepast en gedeeld moet worden; AI als versneller in analyse en patroonherkenning
- Minder onderscheid tussen militair specifieke (operationele) en generieke (bedrijfsvoering) IT;
- Intensivering van de strijd om het EMS (Elektro Magnetisch Spectrum)
- Toenemende invloed van beperkt aantal (grote) tech bedrijven
- Groeiende noodzaak voor samenwerking met de markt, andere departementen en buitenlandse defensieorganisaties;
- Stevige concurrentie op de IT-arbeidsmarkt.

De ambities van Defensie op het gebied van informatie en IT zijn hoog: we streven naar een informatiegestuurde, technologisch hoogwaardige krijgsmacht die sneller en slimmer kan opereren dan potentiële tegenstanders. Defensie moet zich verhouden tot deze trends.



Figuur 1: digitale transformatietempel

Met de [Defensienota 2022⁸](#), het rapport [Defensie Duurzaam Digitaal⁹](#) en de [Maatregelennota¹⁰](#) is gekozen voor een ambitieuze versnelling van de digitale transformatie. Dit is met de Defensienota 2024 nog eens een keer versterkt. Het doel is om met behulp van (digitale) innovatie en vernieuwing een significante bijdrage te leveren aan de gevechtskracht van Defensie. Daarom wordt prioriteit

gelegd op investeringen die multidomein optreden (MDO, zie paragraaf 3.2) mogelijk maken. Dit uit zich in inzet op innovatie, modernisering van IT, versnelling op het gebied van data science en AI, cybersecurity, versterking business continuïteit, beheersing van het EMS-domein, en onderliggend hieraan personele groei en slimmere samenwerking door de hele IT keten om het benodigde realisatie- en absorptievermogen op te bouwen. De inhoudelijke aandachtsgebieden van de digitale transformatiestrategie zijn weergegeven in Figuur 1: digitale transformatietempel.

Dit alles vereist een flinke transformatie, of eigenlijk golven van meerdere transformaties. Veranderingen zullen plaats moeten vinden in strategie, doctrine, leiderschap en cultuur, beleid, wet- en regelgeving, werkwijzen en opleidingen, bedrijfsvoering, veiligheid en in IT- en wapensystemen. Daarbij is Defensie zich ten alle tijden bewust van belangrijke waarden als privacy, rechtmatigheid, transparantie, verantwoord datagebruik en betekenisvolle menselijke controle.

Deze veranderingen zijn primair gericht op de uitvoering van de taken van Defensie binnen de samenwerking met bondgenoten binnen de NAVO en EU. Daar waar relevant wordt tevens invulling gegeven aan de rijksbrede I-strategie.

3.2 Multidomein optreden (MDO)

Defensie zet in op multidomein optreden (MDO) met als doel een militair voordeel te behalen en te behouden op potentiële tegenstanders. Multidomein optreden is een manier van denken en werken - een operationeel concept - voor het optreden van de krijgsmacht. Het concept slaat een brug tussen strategische doelstellingen en operationele en tactische militaire activiteiten, door uit te gaan van te bereiken effecten. Dit vraagt om sterke innovatie en een gebalanceerde krijgsmacht die in staat is om domeinoverstijgend fysieke, virtuele en cognitieve effecten te realiseren, in samenhang met niet-militaire activiteiten. Het optreden van de krijgsmacht is daarbij informatiegestuurd: proactief op basis van een goed begrip van de omgeving en continu aangestuurd en bijgestuurd op basis van actuele informatie. Zo maakt de krijgsmacht optimaal gebruik van informatie(technologie) voor snellere besluit- en bevelvoering dan de tegenstander. Dit gaat hand in hand met de digitale transformatie van Defensie en vereist verandering van mens en gedrag, processen en technologie. Defensie blijft dan ook investeren in de modernisering van commandovoering en het verder implementeren van de in 2022 geformuleerde maatregelen.

3.3 Versterken continuïteit IT

Een belangrijke voorwaarde voor multidomein optreden is het moderniseren van de IT-infrastructuur van Defensie. De infrastructuur vormt de basis voor alle IT van Defensie en omvat de datacentra, netwerken, werkplekken en mobiele middelen. De Defensie IT-strategie 2019-2024¹¹ geeft richting aan deze ontwikkelingen. Deze IT-strategie wordt in 2025 geactualiseerd, in samenhang met de eveneens te publiceren Digitale Transformatie Strategie.

De infrastructuur vormt de ruggengraat voor het optreden van Defensie, met alle technische voorzieningen om gegevens te verzamelen, op te slaan, te verwerken en te delen. De infrastructuur is niet alleen voor de operationele inzet van belang, maar ook voor de reguliere bedrijfsvoering en ondersteuning. De gehele organisatie moet continu informatiegestuurd kunnen werken. Hiervoor moet de juiste informatie op het juiste moment op de juiste plaats zijn. De omvang en het belang van IT-voorzieningen zijn daarom de afgelopen jaren steeds groter geworden en dat stelt steeds hogere eisen aan de IT-infrastructuur en de bijbehorende beveiligingsaspecten.

Recente verstoringen door bijvoorbeeld de CrowdStrike-update en de NAFIN-storing laten zien dat de maatschappij en Defensie in steeds grotere mate afhankelijk zijn van IT. Dat betekent dat er extra moet worden geïnvesteerd in *Business Contingency Plans*, scenario's bij verstoring, verbeteren samenwerking crisisstructuren bij IT-verstoringen en oefenen en trainen op grote verstoringen.

De toenemende afhankelijkheid van IT stelt niet alleen hogere eisen aan de continuïteit, maar ook aan de beveiliging en wendbaarheid van IT. Defensie investeert daarom in de modernisering van de IT-infrastructuur voor alle gebruiksomstandigheden. Dit gebeurt samen met kennisinstellingen, industrie en bondgenoten. Deze samenwerking is noodzakelijk om gebruik te kunnen maken van de laatste technologische ontwikkelingen, waaronder *quantum computing* en cloudtechnologie, en daarnaast ook interoperabiliteit te realiseren.

Om de continuïteit van inzet en bedrijfsvoering te garanderen, worden de beschikbaarheid, betrouwbaarheid en schaalbaarheid van IT-systemen door middel van cloudtechnologie vergroot. Cloudtechnologie ondersteunt ook het werken met data en AI en biedt kansen voor innovatie, digitale veiligheid en arbeidsextensief werken. Cloudtechnologie draagt bij aan het slimmer en beter zijn dan de tegenstander. De Defensie Cloudstrategie kiest voor een multi-cloud aanpak en geeft richting aan de cloudontwikkelingen bij Defensie en het zoeken naar de noodzakelijke balans tussen de kansen en risico's. Bij een keuze voor een cloudomgeving kan dit de eigen cloudomgeving van Defensie zijn (private) of een cloudomgeving van een Cloud Service Provider (sovereign/public cloud). Gezien de wereldwijde ontwikkeling richting cloud is het adagium, cloud tenzij...

Defensie heeft vier grote IT-programma's ingericht die structurele veranderingen moeten doorvoeren in zowel processen als de IT om de continuïteit te versterken en de ambitie van de digitale transformatie mede waar te kunnen maken en compliant te zijn met de geldende wet- en regelgeving op het gebied van informatie, zoals de Archiefwet, de Algemene Verordening Gegevensbescherming (AVG) en privacy regelgeving, en de Wet open overheid (Woo). Uitgangspunt bij de ontwikkeling van nieuwe IT-systemen is *security* en *privacy by design*. Op strategisch niveau sturen de Programmabords de grote IT-programma's aan, met de bestuursraad Digitale Transformatie als escalatieniveau.

3.3.1 *Grensverleggende IT*

Het Programma Grensverleggende IT (GrIT) vervangt een groot gedeelte van de IT-infrastructuur van Defensie. Deze vernieuwing vormt het fundament voor verdere transformatie van het IT-landschap. Defensie rapporteert sinds 2022 over GrIT door middel van een basisrapportage en halfjaarlijkse [voortgangsrapportages](#) in het kader van de Regeling Grote Projecten¹².

De versterkte focus van Defensie gericht op hoofdtaak 1 heeft ook gevolgen voor het programma GrIT. Bij de herijking van het programma GrIT in 2024 heeft de operationele militair prioriteit gekregen. De doelstellingen van GrIT zijn aangescherpt zodat ze gericht zijn op het zo snel mogelijk waarde leveren voor de Krijgsmacht.

Om de complexiteit van de aansturing van het programma te vereenvoudigen en te sturen richting werkende oplossingen worden na de herijking drie gebruikersgroepen/pijlers onderscheiden:

- Pijler 1: Ontplooid operationele IT voor de OpCo's;
- Pijler 2: IT voor JIVC, voor IT-dienstverlening aan de defensieonderdelen;
- Pijler 3: IT voor alle eindgebruikers.

3.3.2 *FOXTROT*

Met het programma FOXTROT vernieuwt Defensie de communicatiesystemen in het tactisch mobiele domein. FOXTROT legt het fundament voor MDO in het tactisch mobiele landdomein door connectiviteit en exploitatie van informatie te realiseren op een robuuste, flexibele en veilige manier. De operationele gebruiksomstandigheden zijn veranderd, de huidige systemen kennen in toenemende mate instandhoudingsproblemen en de interoperabiliteit tussen eenheden en met bondgenoten is met de huidige middelen beperkt. Een groot deel van de draadloze transmissiemiddelen die nodig zijn om in mobiele gebruiksomstandigheden de commandovoering te kunnen ondersteunen worden daarom vervangen. De focus ligt nu op herstel en verbetering van connectiviteit voor genetwerkt optreden door het scheppen van infrastructurele randvoorwaarden.

3.3.3 *ROGER*

Het programma Roger zorgt voor het moderniseren van de materieel logistieke en financiële bedrijfsvoering en levert een effectieve bijdrage aan de gereedstelling, ondersteuning en inzet van militaire eenheden. Een onderdeel daarvan is de overgang naar de nieuwe versie van SAP, S/4HANA. De technische conversie naar S/4HANA heeft op 1 juli 2022 plaatsgevonden en sinds begin 2023 zijn de eerste gebruikers al gestart met het gebruik van S/4HANA. De komende jaren worden S/4HANA en de vernieuwde bedrijfsvoeringsprocessen beheerst en stapsgewijs verder ingevoerd in samenwerking met alle defensieonderdelen.

3.3.4 *Defensie Open op Orde*

Het programma Defensie Open op Orde (DOO) maakt van informatie onze kracht. Via actielijnen en een netwerk van *liaison officers* bij alle Defensieonderdelen verhogen we het volwassenheidsniveau van de informatiehuishouding, als opmaat naar een gezaghebbende informatiepositie. Door middel van nulmetingen bij ieder Defensieonderdeel ontstaat een goed beeld van de volwassenheid van de informatiehuishouding. Daaraan worden concrete acties gekoppeld in actieplannen per DO.

3.4 **Elektromagnetisch spectrum**

Het elektromagnetisch spectrum (EMS) voor radiofrequenties is van strategisch belang voor Defensie. Draadloze communicatie, radar, sensoren en commandovoering zijn namelijk afhankelijk van voldoende EMS-ruimte voor Defensie. Door toenemende schaarste loopt Defensie strategische risico's. Daarom gaat Defensie investeren in kennis en kunde op dit terrein. Er wordt een interne EMS-autoriteit opgericht om te zorgen dat Defensie in vredessituatie en bij operaties zo effectief mogelijk gebruik kan maken van radiofrequenties en hiervoor over de juiste mensen, middelen en concepten beschikt.

3.5 **Data science & artificial intelligence**

Defensie heeft te maken met een grote verschuiving van traditionele naar hoogtechnologische oorlogsvoering. Moderne (wapen)systemen zijn bijna niet inzetbaar zonder Data Science en AI waarbij het gebruik van informatie een steeds prominentere en strategische rol vervult. Er worden nieuwe eisen aan het militair optreden gesteld; niet alleen met betrekking tot het eigen vermogen van de krijgsmacht, maar ook de manier waarop Defensie reageert op (verstorende) technologische ontwikkelingen van potentiële tegenstanders en andere actoren.

Via de [Defensiestrategie Data Science en AI 2023-2027](#)¹³ en de onderliggende routekaart investeert Defensie in de integratie van Data Science en AI in haar processen. Zo ontwikkelt Defensie een hoogerubriceerde IT-infrastructuur voor

datadeling en verwerking. Dit stelt de krijgsmacht in staat relevante informatie op het juiste moment bij de juiste persoon te krijgen. Defensie heeft beleid voor algoritmes ontwikkeld en richt nu de beoordeling en het toezicht op algoritmes in samen met de Functionaris Gegevensbescherming en de Beveiligingsautoriteit.

Bij Defensie werken diverse data science afdelingen aan oplossingen met operationele meerwaarde die direct bijdragen aan hoofdtak 1. De afdeling Datascience & AI Technology Accelerator bij COMMIT zet zich in om diverse (randvoorwaardelijke) zaken uit de Defensiestrategie Data Science en AI te realiseren en ondersteunt Defensieonderdelen met tools zodat zij zelfstandig data science en AI kunnen toepassen.

Tot slot investeert Defensie in een Data Science Center of Excellence bij de Nederlandse Defensie Academie zodat deze technologie plaats krijgt in de militaire opleidingen en het onderzoek. Defensie zet in op het aantrekken, ontwikkelen en behouden van talent om de afhankelijkheid van externe partijen te beperken.

Meer dan ooit kijkt Defensie naar bondgenoten, kennisinstellingen en de industrie om samen te werken. Daarom wordt de samenwerking met kennis- en innovatiepartners in ecosystemen versterkt. Zo heeft Defensie bijvoorbeeld het Data Science Centre of Excellence (DSCE) bij de Nederlandse Defensieacademie opgericht. Het Center of Excellence is het knooppunt waar al het (wetenschappelijke) onderzoek en onderwijs bij elkaar komt en direct wordt gekoppeld aan de defensiepraktijk. Het Center of Excellence is ook onderdeel van het ecosysteem Mindlabs in Tilburg. Zo kan Defensie samen met andere (kennis)partners en start-ups werken aan vraagstukken op het gebied van data science en kunstmatige intelligentie. Ook wordt er geïnvesteerd in onderwijs op het gebied van Data Science & AI in een militaire context. Zo is er bijvoorbeeld een leergang data, een masterclass cyber en data voor de Defensietop, en een defensiebreed project om datageletterdheid te vergroten. Tegelijkertijd heeft Defensie een data science omgeving neergezet voor laaggerubriceerde data die het mogelijk maakt om data science toepassingen te ontwikkelen, testen en in productie te brengen. De data science omgeving voor hoogerubriceerde informatie wordt op korte termijn opgeleverd. Randvoorwaardelijk voor succesvolle data science en AI zijn een gedegen data governance organisatie en data management use-cases. Defensie kent hier een stevige basis maar blijft investeren in manieren om deze randvoorwaarden slimmer te beleggen in de organisatie.

3.6 Cyber en digitale weerbaarheid

De maatschappelijke digitalisering biedt ongekende mogelijkheden om beter en sneller met elkaar gegevens en informatie uit te wisselen, samen te werken en het functioneren van (complexe) systemen mogelijk te maken. Maar daarmee is het ook een domein geworden van mensen, organisaties en landen die hier misbruik van maken. Cyberproblemen en cyberaanvallen zijn dagelijks nieuws. Het cyberdomein (cyberspace) is door de NAVO en de EU reeds geruime tijd onderkend als operationeel domein, naast land, zee, lucht en ruimte.

Cyber en elektronische oorlogsvoering, ook wel cyber- en elektromagnetische activiteiten (CEMA), zijn onlosmakelijk verbonden met moderne oorlogsvoering. Kennis rond dit onderwerp kan zowel offensief als defensief worden ingezet voor het verzamelen van inlichtingen, het beschermen van mensen en platformen, maar ook in het ontzeggen van capaciteiten aan de tegenstander of als afschrikking. Daarom versterkt Defensie de kennis en kunde op dit terrein.

Defensie werkt gestaag voort aan het verbeteren van de cyber readiness. Daarbij gaat het niet alleen om het vergroten van de cyberveiligheid van de eigen

netwerken en (wapen)systemen, maar speelt Defensie ook een rol om in samenwerking met civiele en internationale partners Nederland digitaal veilig te houden. Bovendien moet de krijgsmacht tijdens een gewapend conflict in staat zijn om in coalitieverband cyberoperaties uit te voeren en te synchroniseren met activiteiten op zee, land, in de lucht en in de ruimte.

Defensie draagt intern zorg voor het synchroniseren van activiteiten in het cyberdomein om de inlichtingenpositie, de digitale weerbaarheid, de offensieve capaciteiten en de rechtshandhaving gelijktijdig te versterken. Centraal in deze ontwikkeling staat het verder uitbouwen en versterken van het interne netwerk van operatiecentra - de zogeheten 'SOC-toren' - die niet alleen op elkaar, maar ook op de operatiecentra van nationale en internationale partners zijn aangesloten. In hun samenwerking dragen deze centra zorg voor een goede *situational awareness* en een *situational understanding* van het domein. Een uitbreiding van interne, nationale en internationale oefeningen moet de spankracht van dit netwerk continu testen.

De digitale weerbaarheid betreft een bijzonder omvangrijk aandachtsgebied. Om alle benodigde activiteiten integraal te kunnen oppakken en de juiste prioriteiten te stellen, werkt Defensie aan een separaat Uitvoeringsplan Digitale Weerbaarheid. In dit plan worden onder meer alle activiteiten van het NIST Cybersecurity Framework, de Network and Information Security Directive 2 (NIS2) en de Baseline Informatiebeveiliging Overheid 2 (BIO2), maar ook de actielijnen vanuit de NAVO, de EU en de Nederlandse Cybersecurity Strategie (NLCS) in samenhang gezien. Daarnaast wil Defensie met dit plan ook relaties definiëren tussen de eigen 'SOC toren' en het rijksbrede SOC stelsel, met de life cycles van wapensystemen en met kennis en innovatie. Daar waar Defensie als veiligheidsorganisatie afwijkt van het landelijke beeld, wordt dit ook in kaart gebracht. Het plan wordt in de eerste helft van 2025 afgerond.

Omdat Defensie onmogelijk zelfstandig alle ontwikkelingen kan bijhouden, is gekozen voor de inrichting van een Cyber Innovation Hub. Deze hub moet in de komende periode de brug slaan naar vooral nationale private en civiele bedrijven, onderwijsinstellingen en kennisinstellingen om op die wijze de behoeftes van Defensie en de ontwikkelingen op de markt op elkaar te binden. De hub is ook verbonden met nationale initiatieven op dit gebied, zoals het programma dcypher van EZK.

Verder herzielt Defensie de [Defensie Cyberstrategie uit 2018](#)¹⁴. Ook de te voeren strategie moet inspelen op de snelle ontwikkelingen in het cyberdomein en richting en samenhang van defensieplannen- en activiteiten op dit gebied waarborgen.

3.7 Interoperabiliteit

Defensie werkt met veel verschillende partners samen. Interoperabiliteit betekent dat we technisch in staat zijn samen te werken met bondgenoten (NAVO en EU), interdepartementaal, kennisinstellingen, de markt en intern Defensie. Dat vergt moderne (communicatie) hulpmiddelen, goede afspraken en duidelijkheid over rubriceringsniveaus. Interoperabiliteit is dan ook een van de belangrijkste voorwaarden voor de digitale transformatie van Defensie.

Zonder technische mogelijkheden voor interoperabiliteit is gezamenlijk informatiegestuurd optreden niet mogelijk. De verbeterde IT-infrastructuur vanuit programma GrIT en FOXTROT, alsmede het programma Federated Mission Networking (FMN) voorzien daarvoor in de noodzakelijke IT-middelen. Defensie onderzoekt momenteel de hieraan gerelateerde uitdagingen op het gebied van frequentie management. Frequentieruimte moet worden gevonden in overleg met een aantal andere belanghebbende departementen.

Defensie stelt daarnaast hoge eisen aan de cyberweerbaarheid en informatie-uitwisseling tijdens (interdepartementale) crisissen vanwege de dreiging van statelijke actoren. In de praktijk blijkt dat uitwisseling van gerubriceerde informatie-uitwisseling niet altijd op efficiënte wijze mogelijk is binnen de rijksoverheid, aangezien de meeste departementen gebruik maken van rijksbrede voorzieningen die deze mogelijkheid niet bieden. Defensie zal echter zoveel mogelijk gebruik maken van de voorzieningen die rijksbreed beschikbaar zijn voor zover informatie-uitwisseling mogelijk is conform de geldende rubriceringsniveau's van de NAVO en zich zoveel mogelijk conformeren aan rijksbrede afspraken over interoperabiliteit. Het belang van militaire interoperabiliteit binnen NAVO weegt daarbij extra zwaar, omdat die standaarden noodzakelijk zijn bij het verdedigen van het Nederlands, NAVO en EU grondgebied.

3.8 Wendbare organisatie

3.8.1 CIO-stelsel

Naast de technische kant van de digitale transformatie zijn ook organisatorische en culturele aspecten onderdeel van de digitale transformatie. In essentie moet het vermogen van Defensie om digitale initiatieven om te zetten in geïmplementeerde oplossingen sterk worden verbeterd. Defensie heeft daarom het CIO-stelsel ingericht en werkt aan de verdere doorontwikkeling daarvan. In het stelsel worden naast een departementale CIO ook CIO's decentraal bij defensieonderdelen onderkend. Dit is een van de verbeteringen in de IT-functie en de inbedding hiervan in de hele organisatie. De (decentrale) Chief Information Security Officer (CISO) en de Chief Data Officer (CDO) zijn eveneens onderdeel van het CIO-stelsel. Defensie heeft daarnaast ook al een Chief Privacy Officer (CPO) aangesteld. In het kader van wendbaarheid evalueert en verbetert Defensie daarom de komende periode de gehele IT-governance.

3.8.2 Personeel

Het rapport [Defensie Duurzaam Digitaal](#) stelt dat een toename van personeel noodzakelijk is. Defensie zet hierop in met werving, opleiding in eigen huis via de IT-academy en samenwerking met het bedrijfsleven. Defensie wil hiermee uitbreiding van het IT-personeel bij de defensieonderdelen en JIVC realiseren. De vraag naar mensen en middelen zal geleidelijk en stapsgewijs opgelost moeten worden. De personele vulling van de IT-organisatie staat onder druk: er zijn kwalitatieve en kwantitatieve tekorten om de ambities te realiseren. Vooral de behoefte aan IT-capaciteit voor beheer en ontwikkeling van bedrijfsvoeringssystemen, data (science) en cyber is groot. Maar ook voor projectmanagement, technologie voor verbindingen (connectivity) en militaire IT is er de komende jaren steeds meer behoefte aan deskundig IT-personeel.

De door Defensie gewenste profielen voor extra capaciteit zijn schaars op de arbeidsmarkt, mede omdat de vraag naar IT-professionals in de markt sneller toeneemt dan het aanbod en er de komende jaren veel kennis zal uitstromen door natuurlijk verloop. Hierdoor is er sprake van krapte op de arbeidsmarkt die voor Defensie voelbaar is. Het werven, opnemen en inwerken van medewerkers kost tijd. Pas na het volledig inwerken van nieuw personeel kunnen zij bijdragen aan de instandhouding en vernieuwing van de IT van Defensie. Defensie rapporteerde in de [Stand van Defensie Najaar 2024](#)¹⁵ onder andere over de vulling van IT-personeel.

Samen met OCW en EZ geeft Defensie invulling aan de vierde aanbeveling uit het [AWTI-rapport Kennisoffensief voor Defensie](#)¹⁶ door later in 2025 structurele

samenwerkingsverbanden aan te gaan met het HBO en MBO op schaarse personeelscategorieën zoals IT.

3.8.3 *Robotisering*

Door intensiever gebruik te maken van kennis, innovatie en nieuwe technologie kan Defensie arbeidsextensiever worden. Automatisering, digitalisering en robotisering kunnen helpen om bepaalde soorten werk veiliger en makkelijker te maken. Daardoor kunnen mensen zich concentreren op zaken die menselijke vaardigheden vereisen, zoals interactie, inlevingsvermogen en ethische afwegingen. De komende jaren investeert Defensie in technologie en werkwijzen die het werk van onze mensen veiliger maken. Doel is om de medewerkers van Defensie in staat te stellen zich te concentreren op die taken waar menselijke interactie onvervangbaar is. Bij het arbeidsextensiever werken zal in het begin het accent liggen op de ondersteunende processen. Defensie voert projecten uit om robotisering toe te passen voor administratieve taken en doet experimenten om medewerkers veiliger en gezonder te laten werken.

In de digitale transformatie strategie wordt invulling gegeven hoe Defensie van 2025 verder kan bouwen aan het digitaal verandervermogen.

3.8.4 *Aanbesteding*

De huidige regelgeving zit ons in de weg bij de inkoop van technologie en IT. Defensie onderzoekt de mogelijkheden om dit anders aan te pakken. Ook zetten we in op meer geïntegreerde samenwerking met "trustee partners" zoals KPN. Tot slot willen we innovatie zoveel als mogelijk uit de markt halen in plaats van dit zelf te doen.

3.8.5 *Gereedstelling*

Defensie zet in op het gebruik van nieuwe, deels innovatieve technieken en werkwijzen. De huidige regelgeving (zoals de UAVG) beperkt de inzet van deze middelen tijdens de gereedstelling. Ook het gebrek aan ruimte in het EMS (zie paragraaf 3.4) belemmert de gereedstelling, met de bijbehorende onaanvaardbare risico's. Defensie heeft behoefte aan andere spelregels en onderzoekt de mogelijkheden daartoe.

3.9 **Conclusie**

Door in te zetten op bovengenoemde prioritaire doelstellingen werkt Defensie in de periode van 2025-2027 aan de digitale transformatie naar een technologisch hoogwaardige krijgsmacht die optimaal is voorbereid op een conflict met een technologisch geavanceerde tegenstander en geeft daarmee tevens invulling aan onderwerpen uit de [I-strategie Rijk](#)¹⁷ en de [I-strategie routekaarten](#)¹⁸. Thema's als I in het hart van beleid, digitale weerbaarheid, IT-landschap op orde, informatiehuishouding (Open op orde), data (science) en algoritmen, samenwerking met de markt, innovatie en interoperabiliteit sluiten aan bij de doelstellingen in dit I-plan, de [Defensie Cyberstrategie](#)¹⁴, de IT-strategie Defensie¹¹ en de [Defensiestrategie Data Science en AI](#)¹³.

4 Financiële paragraaf

Deze financiële paragraaf bevat uitsluitend kwalitatieve informatie. De programma's en projecten om de doelen van het I-plan te bereiken zijn of worden opgenomen in de [Defensiebegroting](#)¹⁹ of het [Defensiematerieelbegrotingsfonds](#)²⁰.

De Defensiebegroting vertoont een stijgende lijn, ook voor exploitatie en investeringen in het IT-domein. Desondanks moeten er prioriteiten gesteld worden. Defensie zoekt hierbij de balans tussen vernieuwing, beheer en onderhoud.

Voor het uitwerken van de plannen naar investeringen hanteert Defensie reguliere processen, waaronder het Defensie Materieel Proces (DMP). Over de planning en financiën van IT-projecten wordt de Kamer onder andere geïnformeerd via het [Defensie Projectenoverzicht \(DPO\)](#)²¹ en publicatie op het [Rijks ICT-dashboard](#)²².

5 Referenties

-
- ¹ Kabinetsreactie naar aanleiding van Commissie Elias – Brief Parlementair onderzoek ICT-projecten bij de overheid - Tweede Kamer, vergaderjaar 2014–2015, 33 326, nr. 13, <https://www.tweedekamer.nl/downloads/document?id=2015D03316>
- ² Beleidsreactie onderzoeken IV-governance Rijk en Besluit toekomst BIT - Tweede Kamer, vergaderjaar 2019–2020, 26 643, nr. 656
<https://www.tweedekamer.nl/downloads/document?id=2019D53654>
- ³ Besluit van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van 18 december 2020, nr. 2020-0000730468, tot vaststelling van een kader houdende de organisatie-inrichting van het CIO-stelsel binnen de Rijksdienst (Besluit CIO-stelsel Rijksdienst 2021) – Staatscourant 22 december 2020 – nr. 62488
<https://www.tweedekamer.nl/downloads/document?id=2021D05338>
- ⁴ Het interdepartementale CIO-beraad heeft het Kwaliteitskader Meerjarige Departementale Informatieplannen vastgesteld dat op 1 januari 2022 in werking is getreden. Dit kwaliteitskader is in 2023 herzien en bevat een nadere uitwerking van de inhoud van het informatieplan en het proces van aanlevering. In 2024 is het kwaliteitskader opnieuw bijgesteld en is een nieuw hoofdstuk rijksbrede prioriteiten toegevoegd
- ⁵ Defensienota 2024: Sterk, slim en samen – Tweede Kamer, vergaderjaar 2023–2024 36 592 nr. 1
<https://www.tweedekamer.nl/downloads/document?id=2024D31680>
- ⁶ Departementaal I-plan Defensie 2023-2026. Tweede Kamer, vergaderjaar 2023–2024, 26 643
<https://www.tweedekamer.nl/downloads/document?id=2023D48214>
- ⁷ De rijksbrede prioriteiten zijn vastgesteld in het interdepartementaal CIO-beraad van 15 mei 2024
- ⁸ Defensienota 2022: Sterker Nederland, veiliger Europa – Tweede Kamer, vergaderjaar 2021–2022, 36 124, nr. 1
<https://www.tweedekamer.nl/downloads/document?id=2022D22236>
- ⁹ Defensie Duurzaam Digitaal, inclusief bijlage strategisch P-plan. Integrale analyse van vraag en aanbod IT en consequenties voor investeringen, exploitatie (financiën) en personeel op de korte en de lange termijn, 2 april 2021. Tweede Kamer, vergaderjaar 2020–2021, 31 125, nr. 118
<https://www.tweedekamer.nl/downloads/document?id=2021D20200>
- ¹⁰ Maatregelennota Defensie 2022. 20 juli 2022, kenmerk BS2022014950
- ¹¹ IT-strategie 2019 – 2024: Naar een informatiegestuurde, technologisch hoogwaardige en toekomstbestendige krijgsmacht, kenmerk BS2019004089
- ¹² Basis- en voortgangsrapportage Programma Grensverleggende IT (GrIT) – Tweede Kamer, vergaderjaar 2021-2022, 35 728, nr. 7
<https://www.tweedekamer.nl/downloads/document?id=2022D38598>
- Tweede voortgangsrapportage over het programma Grensverleggende IT (GrIT) 2022 – Tweede Kamer, vergaderjaar 2022-2023, 35 728, nr. 9
<https://www.tweedekamer.nl/downloads/document?id=2023D13229>
- Derde voortgangsrapportage over het programma Grensverleggende IT (GrIT) eerste helft 2023 – Tweede Kamer, vergaderjaar 2022-2023, 35 728, nr. 11
<https://www.tweedekamer.nl/downloads/document?id=2023D39442>
- Vierde voortgangsrapportage over het programma Grensverleggende IT (GrIT) tweede helft 2023 – Tweede Kamer, vergaderjaar 2023 – 2024, 35 728, nr. 14
<https://www.tweedekamer.nl/downloads/document?id=2024D12978>
- Vijfde voortgangsrapportage over het programma Grensverleggende IT (GrIT) eerste helft 2024 – Tweede Kamer, vergaderjaar 2023 – 2024, 35 728, nr. 17
<https://www.tweedekamer.nl/downloads/document?id=2024D36321>

¹³ Defensiestrategie Data Science en Artificial Intelligence – Tweede Kamer, vergaderjaar 2022-2023, 31 125, nr. 125

<https://www.tweedekamer.nl/downloads/document?id=2023D25036>

¹⁴ Defensie Cyberstrategie. Investeren in digitale slagkracht voor Nederland – Tweede Kamer, vergaderjaar 2018-2019, 33 321, nr. 9

<https://www.tweedekamer.nl/downloads/document?id=2018D53918>

¹⁵ Stand van Defensie najaar 2024 – Tweede Kamer, vergaderjaar 2024-2025, 36 600 X nr. 4

<https://www.tweedekamer.nl/downloads/document?id=2024D33633>

¹⁶ AWTI-rapport Kennisoffensief voor Defensie.

<https://www.awti.nl/documenten/adviezen/2024/10/kennisoffensief-voor-defensie/kennisoffensief-voor-defensie>

¹⁷ Nieuwe I-strategie Rijk 2021-2025 – Tweede Kamer, vergaderjaar 2020-2021, 26 643, nr. 779

<https://www.tweedekamer.nl/downloads/document?id=2021D32099>

¹⁸ I-strategie Rijk 2022 - 2025: Routekaarten – Tweede Kamer, vergaderjaar 2022-2023, 26 643, nr. 899

<https://www.tweedekamer.nl/downloads/document?id=2022D31432>

¹⁹ Begroting van het ministerie van Defensie (X) voor 2025 – Tweede Kamer, vergaderjaar 2023-2024, 36 600 X

<https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorstedetails&qry=wetsvoorstel%3A36600-X#wetgevingsproces>

²⁰ Begroting van het Defensiematerieelbegrotingsfonds (X) voor 2025 – Tweede Kamer, vergaderjaar 2023-2024, 36 600 K

<https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorstedetails&qry=wetsvoorstel%3A36600-K#wetgevingsproces>

²¹ Defensie Projectenoverzicht 2024 – Tweede Kamer, vergaderjaar 2023-2024, 27830, nr. 435

<https://www.tweedekamer.nl/downloads/document?id=2024D19115>

²² Het Rijks ICT-Dashboard bevat een overzicht van ICT-projecten bij Defensie en wordt jaarlijks in september geüpdatet.

<https://www.rijksictdashboard.nl/>