Ministerie van Defensie

Departementaal I-PLAN Defensie

2023 - 2026

Colofon

Bestuurstaf
Chief Information Office

Locatie
Den Haag
Plein-Kalvermarktcomplex
Kalvermarkt 32 's-Gravenhage

Postadres
Kalvermarkt 38
2511 CB 'S-GRAVENHAGE
MPC 58B

Versie 1.0

Inhoud

1	Inleiding	5
2	Prioritaire doelstellingen	6
2.1	Digitale transformatie	6
2.2	Informatiegestuurd optreden	7
2.3	Versterken continuïteit IT	8
2.3.1	Grensverleggende IT	8
2.3.2	Foxtrot	8
2.3.3	ROGER	9
2.3.4	Vernieuwing HR IT	9
2.3.5	Defensie Open op Orde	9
2.3.6	Bijdrage aan werkagenda waardegedreven digitaliseren	10
2.4	Data science & artificial intelligence	11
2.4.1	Bijdrage aan werkagenda waardegedreven digitaliseren	11
2.5	Cyber en digitale weerbaarheid	12
2.5.1	Bijdrage aan werkagenda waardegedreven digitaliseren	12
2.6	Interoperabiliteit	13
2.7	Wendbare organisatie	14
2.7.1	Bijdrage aan werkagenda waardegedreven digitaliseren	14
2.8	Conclusie	15
3	Financiële paragraaf	16
4	Referenties	17

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 2020 [3] 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 Informatieplannen [4] 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.

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 tot vijf 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 verschillende 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-statelijke actoren in toenemende mate gebruik van technologische ontwikkelingen die een dreiging vormen voor de vitale infrastructuur.

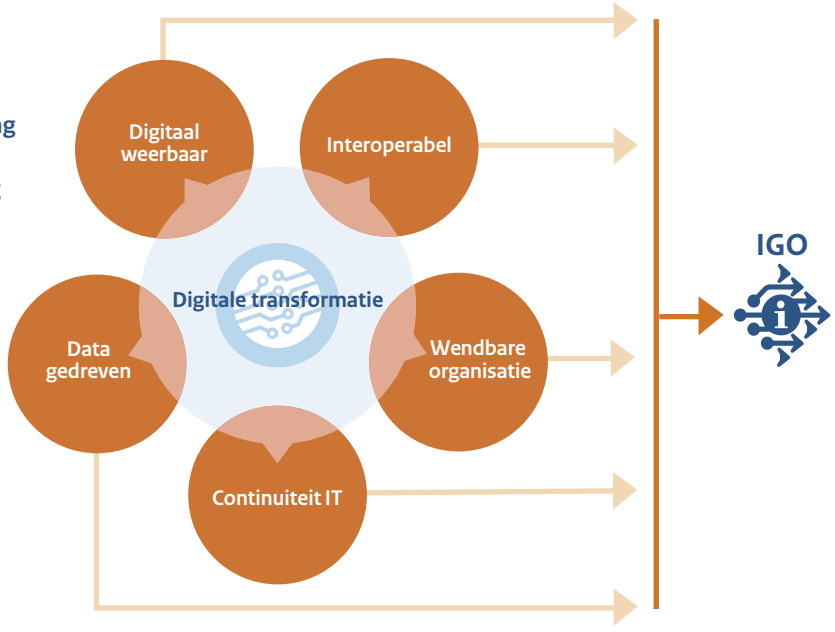
Om onze grondwettelijke taken effectief te kunnen blijven uitvoeren, en te vechten voor een veilige toekomst, zullen we dus niet alleen beter moeten worden in het stroomlijnen van informatie om snelle en goede besluiten te nemen. We zullen ook onze organisatie en ons optreden moeten aanpassen aan de veranderende dreiging- en informatieomgeving. 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.

In de **Defensienota 2022** [5] zijn zes actielijnen gedefinieerd:

1. **Krachtige ondersteuning**
2. **Een goede werkgever, verbonden met de samenleving**
3. **Versterken van specialismen**
4. **Meer Europese samenwerking**
5. **Innoverend vermogen en nieuwe domeinen**
6. **Informatiegestuurd werken en optreden**

De prioriteiten die Defensie stelt in het kader van de digitalisering lopen door alle actielijnen heen. Het zwaartepunt van dit I-plan ligt op actielijn 6, informatiegestuurd werken en optreden.
Dit meerjarig informatieplan (I-plan) van Defensie is een update van het eerste **Defensie I-plan van 2022** [6] en is bedoeld om de belangrijkste prioriteiten op het gebied van deze digitale transformatie voor de periode 2023 - 2026 weer te geven.

De geschetste prioriteiten vormen de beleidsopgave van Defensie in het I-domein. 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 informatiegestuurd optreden (IGO) 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.



2 | Prioritaire doelstellingen

2.1 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 krijgsmacht. 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 kosten van IT;
- Nieuwe technologieën voor operationele inzet en bedrijfsvoering, zoals:
  - Internet of Things;
  - Robotic Process Automation (RPA);
  - Kwantum- en nanotechnologie;
  - Cloudtechnologie.
- Toename van data die verzameld, verwerkt, geanalyseerd, toegepast en gedeeld moet worden;
- Minder onderscheid tussen militair specifieke (operationele) en generieke (bedrijfsvoering) IT;
- 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. Defensie moet zich verhouden tot deze trends. Met de **Defensienota 2022** [5] en de Maatregelennota [7] is gekozen voor een ambitieuze versnelling van de digitale transformatie. Daarom wordt prioriteit gelegd op investeringen die IGO mogelijk maken. Dit uit zich in inzet op innovatie, modernisering van IT, versnelling op het gebied van data science en AI, cybersecurity, en onderliggend hieraan personele groei bij de interne dienstverlener (JIVC) en Defensieonderdelen om het benodigde realisatie- en absorptievermogen op te bouwen.

Dit alles vereist een flinke transformatie, of eigenlijk golven van meerdere transformaties. Veranderingen zullen plaats moeten vinden in strategie, doctrine, leiderschap en cultuur, beleid 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, verwantwoord 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 **Werkagenda Waardengedreven digitaliseren** [8].

2.2 Informatiegestuurd optreden

De digitalisering van Defensie is een essentiële randvoorwaarde voor informatiegestuurd optreden (IGO). De Kamer heeft op 4 juli 2023 de **Beleidsvisie IGO** [9] ontvangen. IGO vormt het fundament onder de keuzes die worden gemaakt in de digitale transformatie. Informatie Gestuurd Optreden (IGO) houdt in dat Defensie in staat is:

1. (Informatie) sneller de juiste informatie verzamelen en analyseren teneinde de situatie beter te begrijpen, zodat
2. (Gestuurd) snellere en betere besluiten genomen kunnen worden, om
3. (Optreden) met de beschikbare (militaire) middelen de gewenste effecten te bereiken.

Het slimmer verwerken van informatie en sneller doorlopen van ons besluitvormingsproces dan de tegenstander kan alleen als eenheden goed in staat zijn informatie uit te wisselen. Het toepassen van data science en AI ter ondersteuning aan menselijke besluitvorming kan er bijvoorbeeld voor zorgen dat informatie zorgvuldig, efficiënt en doelgericht kan worden geanalyseerd. Dit vereist een robuuste en weerbare IT-infrastructuur, goed opgeleide mensen en interoperabele IT- en wapensystemen. Voor IT geldt dat “security by design” in de ontwerpfase en borging hiervan gedurende de gehele levensduur van IT-systemen hierbij het uitgangspunt zijn.

Informatie kan Defensie ook sterker maken. Naast informatie als middel voor de commando- en bedrijfsvoering en informatie als doel voor inlichtingen denkt Defensie ook na over informatie als wapen - door bijvoorbeeld manipulatie van de informatie in vijandelijke systemen met een cyberoperatie - maar ook aan misleiding en strategische communicatie. Om te kunnen blijven winnen, moet de kennis van de informatieomgeving als deel van de operationele omgeving worden vergroot en worden toegepast om het vermogen te versterken. Op alle terreinen, bij alle eenheden en in alle wapensystemen, maar vooral ook in ons strategisch denken.

IGO heeft betrekking op zowel het primaire als het secundaire proces; zowel op onze operationele inzet, als op de organisatie en bedrijfsvoering die deze inzet mogelijk maakt.

2.3 Versterken continuïteit IT

Een belangrijke voorwaarde voor informatiegestuurd 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 2019-2024 [10] geeft richting aan deze ontwikkelingen.

De infrastructuur vormt de ruggengraat voor informatiegestuurd optreden 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 hele 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.

De toenemende afhankelijkheid van IT stelt steeds 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.

Defensie heeft vijf 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), de Wet open overheid (Woo) en de privacywet. Op strategisch niveau sturen de Programmaboards de grote IT-programma's aan, met de stuurgroep Digitale Transformatie als escalatieniveau.

2.3.1 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 middels voortgangsrapportages in het kader van de Regeling Grote Projecten [11].

2.3.2 Foxtrot

Met het programma Foxtrot vernieuwt Defensie de communicatiesystemen in het tactisch mobiele domein. Foxtrot legt het fundament voor IGO 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.

2.3.3 ROGER

Programma Roger levert een moderne bedrijfsvoering die voldoet aan de ambitie van Defensie. 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. Dit gebeurt in samenwerking met het programma Vernieuwing HR IT. 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.

2.3.4 Vernieuwing HR IT

Defensie voert tussen nu en 2025 stapsgewijs een nieuw HR-model in. Defensie is het programma Vernieuwing HR IT gestart om de implementatie van het nieuwe HR-model te faciliteren en te voorzien in robuuste en flexibele HR IT waarmee op de langere termijn de werking en continuïteit kan worden geborgd. Het landschap van IT-applicaties die de HR-processen ondersteunen zijn verouderd, steeds lastiger te onderhouden en sluiten niet aan bij de eisen voor het nieuwe HR-model. IT-systemen die nodig zijn om het nieuwe HR-model te ondersteunen, worden daarom gemoderniseerd.
Daarmee worden werving, ontwikkeling en behoud van personeel ondersteund met moderne en flexibele processen en systemen. Door een hoge mate van integratie tussen de programma's ROGER en Vernieuwing HR IT wordt daarnaast het beheer van data en autorisaties op termijn ook gemakkelijker.

2.3.5 Defensie Open op Orde

Het programma Defensie Open op Orde (DOO) draagt in de periode 2021 t/m 2026 bij aan het bereiken van een gezaghebbende informatiepositie als basis voor informatiegestuurd werken en optreden. Het programma DOO bestaat uit vier actielijnen die hieraan bijdragen. Met DOO vergroot Defensie de openheid in en over ons werk:
we kunnen de keuzes en acties van medewerkers - onder soms moeilijke omstandigheden - dan goed uitleggen aan de samenleving waar we voor werken.

Informatiehuishouding

Iedereen moet erop kunnen vertrouwen dat informatie van medewerkers, afdelingen, onderdelen én die van het ministerie altijd juist, compleet, actueel en vindbaar is. Alleen dan kunnen we succesvol samenwerken. Daarom verbetert DOO de informatiehuishouding: door slim gebruik van technologie (zoals de invoering van het documentmanagementsysteem DefDoc) kunnen we informatie beter creëren, opslaan, vinden en archiveren.

Informatieverstrekking

In lijn met nieuwe wet- en regelgeving, zoals de Wet open overheid (Woo), passen we onze informatieverstrekking aan. Defensie wil een transparante organisatie zijn en informatieverstrekking is daar een belangrijk onderdeel van. Daarom maakt ook Defensie steeds vaker actief informatie openbaar.
Dit wordt de komende jaren stap voor stap uitgebreid, in lijn met het rijksbrede beleid.

Signalen herkennen

Het doel van deze actielijn is dat de medewerkers van Defensie, op alle niveaus, externe en interne signalen proactief oppakken en opvolgen.
Het programma DOO maakt deze nieuwe manier van werken mogelijk met ICT-instrumenten en advies over nieuwe werkwijzes. Dit vergroot het anticiperend vermogen van de organisatie en maakt ons dus wendbaarder. Ook kan Defensie op deze manier proactiever informatie delen als blijkt dat daar behoefte aan is.

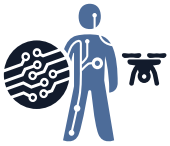
I-vakmanschap

Het programma DOO vergroot ter ondersteuning van de andere actielijnen het informatievakmanschap, zodat alle medewerkers bewust en transparant met informatie kunnen werken.
Door de vereiste kennis en vaardigheden te verankeren in opleidingen, trainingen en leiderschapsontwikkeling zorgen we voor duurzame gedragsverandering.

2.3.6 Bijdrage aan werkagenda waardegedreven digitaliseren

De ontwikkelingen op het gebied van versterken continuïteit IT dragen bij aan de volgende sporen van de werkagenda:

- 2.2 Borgen van privacy, verantwoord datagebruik en vergroten transparantie over gegevensverwerking en -uitwisseling
- 4.1 Verbeteren informatiehuishouding voor openbaarheid van bestuur
- 4.2 Verbeteren gegevenshuishouding voor burgers en organisaties
- 4.3 Versterken ICT-organisatie en -systemen van het Rijk



2.4 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** [12] en de onderliggende routekaart investeert Defensie in de integratie van Data Science en AI in haar processen. Zo ontwikkelt Defensie een hooggerubriceerde 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. Tot slot investeert Defensie in een Data Science Center of Excellence bij de Nederlandse Defensie Academie waar de aanstelling van een hoogleraar Data Science ervoor zorgt dat 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. Via de Uitvoeringsagenda Innovatie en Onderzoek krijgen Data Science en AI daarom prioriteit en wordt de samenwerking met kennis- en innovatiepartners in ecosystemen versterkt.

Deze ontwikkelingen dwingen ons gezamenlijk te werken aan (internationale) regulering en standaarden die voldoen aan onze ethische en juridische standpunten. Defensie zet daarom in op bilaterale en multilaterale samenwerking op dit vlak.

2.4.1 Bijdrage aan werkagenda waardegedreven digitaliseren

De ontwikkelingen op het gebied van data science & artificial intelligence dragen bij aan het volgende spoor van de werkagenda:

- 2.3 Anticiperen op nieuwe digitale technologie
- 3.3 Algoritmes reguleren

2.5 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.

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.

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 kennisinstituten 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 EZ.

Verder herziet Defensie in de komende periode de **Defensie Cyberstrategie uit 2018** [13]. 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.

2.5.1 Bijdrage aan werkagenda waardegedreven digitaliseren

De ontwikkelingen op het gebied van cyberveiligheid draagt bij aan het volgende spoor van de werkagenda:

- 2.4 Versterken cybersecurity

2.6 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 basisvoorwaarden 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 frequentiemanagement. 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 en EU-grondgebied.

Bijdrage aan werkagenda waardengedreven digitaliseren

De ontwikkelingen op het gebied van data science & artificial intelligence dragen bij aan het volgende spoor van de werkagenda:

- 2.3 Anticiperen op nieuwe digitale technologie
- 2.4 Versterken cybersecurity

2.7 Wendbare organisatie

Naast de technische kant van de digitale transformatie zijn ook organisatorische en culturele aspecten onderdeel van de digitale transformatie. Defensie heeft daarom het CIO-stelsel ingericht en werkt aan de verdere invulling 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.

Het rapport **Defensie Duurzaam Digitaal** [14] 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 extra profielen 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 is 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 2023 [15] onder andere over de vulling van IT-personeel.

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.

2.7.1 Bijdrage aan werkagenda waardegedreven digitaliseren

De ontwikkelingen op het gebied van wendbare organisatie draagt bij aan het volgende spoor van de werkagenda:

- 4.2 Verbeteren gegevenshuishouding voor burgers en organisaties
- 4.3 Versterken ICT- organisatie en -systemen van het Rijk

2.8 Conclusie

Door in te zetten op bovengenoemde prioritaire doelstellingen werkt Defensie in de periode van 2023-2026 aan een technologisch hoogwaardige krijgsmacht, die informatiegestuurd kan optreden en geeft daarmee tevens invulling aan onderwerpen uit de **I-strategie Rijk** [16], de **I-strategie routekaarten** [17] en de **Werkagenda Waardengedreven Digitaliseren** [8]. 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** [13], de IT-strategie Defensie [10], de **Defensiestrategie Data Science en AI** [12].

3 | 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** of het **Defensiematerieelbegrotingsfonds.**

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)** en publicatie op het **Rijks ICT-dashboard.**

4 | 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 met 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.

5 Defensienota 2022: Sterker Nederland, veiliger Europa - Tweede Kamer, vergaderjaar 2021-2022, 36 124, nr. 1 **https://www.tweedekamer.nl/downloads/document?id=2022D22236**

6 Departementaal I-plan Defensie - Tweede Kamer, vergaderjaar 2021-2022, 36 124, nr. 9 **https://www.tweedekamer.nl/downloads/document?id=2022D45925**

7 Maatregelennota Defensie 2022. 20 juli 2022, kenmerk BS2022014950

8 Werkagenda Waardengedreven Digitaliseren - Tweede Kamer, vergaderjaar 2022-2023, 26 643, nr. 940 **https://www.tweedekamer.nl/downloads/document?id=2022D45419**

9 Beleidsvisie Informatiegestuurd Optreden - Tweede Kamer, vergaderjaar 2022-2023, 36 124, nr. 35 **https://www.tweedekamer.nl/downloads/document?id=2023D30539**

10 IT-strategie 2019 - 2024: Naar een informatie-gestuurde, technologisch hoogwaardige en toekomstbestendige krijgsmacht, kenmerk BS2019004089

11 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**

12 Defensiestrategie Data Science en Artificial Intelligence - Tweede Kamer, vergaderjaar 2022-2023, 31 125, nr. 125
https://www.tweedekamer.nl/downloads/document?id=2023D25036

13 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

14 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

15 Stand van Defensie najaar 2023 - Tweede Kamer, vergaderjaar 2022-2023, 36 410 X, nr. 5
https://www.tweedekamer.nl/downloads/document?id=2023D37746

16 Nieuwe I-strategie Rijk 2021-2025 - Tweede Kamer, vergaderjaar 2020-2021, 26 643, nr. 779
https://www.tweedekamer.nl/downloads/document?id=2021D32099

17 I-strategie Rijk 2022 - 2025: Routekaarten - Tweede Kamer, vergaderjaar 2022-2023, 26 643, nr. 899
https://www.tweedekamer.nl/downloads/document?id=2022D31432

18 Begroting van het ministerie van Defensie (X) voor 2024 - Tweede Kamer, vergaderjaar 2022-2023, 36 410 X
https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorstel-details&qry=wetsvoorstel%3A36410X#wetgevingsproces

19 Begroting van het Defensiematerieelbegrotingsfonds (X) voor 2024 - Tweede Kamer, vergaderjaar 2022-2023, 36 410 K
https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorstel details&qry=wetsvoorstel%3A36410K#wetgevingsproces

20 Defensie Projectenoverzicht 2023 - Tweede Kamer, vergaderjaar 2022-2023, 27830, nr. 417
https://www.tweedekamer.nl/downloads/document?id=2023D37694

21 Het Rijks ICT-Dashboard bevat een overzicht van ICT-projecten bij Defensie en wordt jaarlijks in september geüpdatet.
https://www.rijksictdashboard.nl/