Ministerie van Defensie

# Departementaal I-plan Defensie

| | |
|---|---|
| Versie | 1.0 |
| Datum | 5 oktober 2022 |
| Status | Definitief |

# Colofon


| | |
|---|---|
| | Bestuurstaf<br>Chief Information Office |
| Locatie | Den Haag - Plein-Kalvermarktc.<br>Kalvermarkt 32 's-Gravenhage |
| Postadres | Kalvermarkt 38<br>2511 CB 'S-GRAVENHAGE<br>MPC 58B |
| Contactpersoon | Ing. J. Cats MSc<br>*Coord Adv CIO*<br>T +31 6 10015994<br>M +31 6 10015994<br>J.Cats@mindef.nl |
| Versie | 1.0 |

# Inhoud

**1 Inleiding—5**

**2 Prioritaire doelstellingen—6**
2.1 Basis op orde—6
2.2 Informatiehuishouding—6
2.3 Informatiegestuurd optreden—7
2.4 Goed werkgeverschap—8
2.5 Arbeidsextensiviteit—8
2.6 Doorontwikkeling decentraal CIO-stelsel—8
2.7 Relatie tot I-strategie Rijk—9

**3 Financiële paragraaf—10**

**4 Refertes—11**

# Inleiding

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 (kamerstuk 62488). In het Besluit CIO-stelsel (2020) 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 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.

# 1 Inleiding

Zoals aangegeven in de Defensienota 2022 worden landen wereldwijd geconfronteerd met verschillende en toenemende dreigingen. Steeds vaker blijkt er sprake van een hybride machtsstrijd: desinformatie beïnvloedt dagelijks onze democratieën en toenemende cyberaanvallen zijn een continue bedreiging voor vitale infrastructuur en processen.

Om de veiligheid samen met bondgenoten te kunnen verdedigen, transformeert Defensie naar een moderne, technologisch hoogwaardige organisatie met een sneller reactievermogen, groter aanpassingsvermogen en betere gevechtskracht, handelend op basis van de beste informatie.

Om keuzes te maken, brengt Defensie focus aan. Allereerst wordt de basis van de krijgsmacht versterkt. Daarmee worden de gereedheid, inzetbaarheid en wendbaarheid zo snel mogelijk verhoogd. Concreet betekent dit het verbeteren van de arbeidsvoorwaarden voor het personeel, een verdere versteviging van de bedrijfsvoering en versterking van de operationele ondersteuning van de gevechtseenheden.

Met het oog op de toekomst moet Defensie noodzakelijke moderniseringen doorvoeren. Dat betekent dat over de hele linie ingezet wordt op informatiegestuurd optreden, automatisering en robotisering, cyber(security), elektronische oorlogvoering en de (aanwezigheid in) de ruimte.

Deze doelen worden gerealiseerd langs 6 actielijnen:

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 optreden

Het voorliggende meerjarig informatieplan van Defensie geeft inzicht in de belangrijkste prioriteiten op het gebied van IT en digitalisering voor de periode 2022 – 2025.

# 2 Prioritaire doelstellingen

De prioritaire doelstellingen volgen uit de 6 actielijnen. De IT-prioriteiten lopen door alle actielijnen heen, waarbij het zwaartepunt ligt op actielijn 6, informatiegestuurd optreden.

## 2.1 Basis op orde

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 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 werken door ervoor te zorgen dat de juiste informatie op het juiste moment op de juiste plaats is. 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.

De toenemende afhankelijkheid van IT stelt steeds hogere eisen aan de continuïteit, beveiliging en wendbaarheid van IT. Defensie investeert daarom in de modernisering van de IT-infrastructuur voor alle gebruiksomstandigheden. Dit gebeurt samen met de markt. Onder andere met het programma Grensverleggende IT (GrIT) voor het statische en ontplooide domein en met het programma FOXTROT voor het mobiel-tactische domein. Het programma Vernieuwing HR en het programma HR-IT moeten de HR-processen moderniseren en daarmee werving, ontwikkeling en behoud van personeel ondersteunen met moderne en flexibele processen en systemen.

De integrale bedrijfsvoering voor logistiek en financiën wordt gemoderniseerd. Het huidige ERP-systeem bij Defensie is gebaseerd op gedateerde processtandaarden en SAP-software. Er is besloten te migreren naar de nieuwe versie van SAP, te weten SAP S/4HANA. Programma ROGER voert dit uit en zorgt daarmee voor verbeteringen en grote veranderingen in de bedrijfsvoering van Defensie. Er is gekozen voor een aanpak waarbij het systeem eerst technisch wordt overgebracht naar S/4HANA, waarna gefaseerd optimalisaties en standaardisaties plaatsvinden. Uit het eerdere vooronderzoek  is gebleken dat deze aanpak het beste aansluit bij de behoeftes van Defensie.

## 2.2 Informatiehuishouding

Ook de informatiehuishouding van de defensieorganisatie wordt gemoderniseerd. Informatie moet vindbaar en bruikbaar zijn. Defensie wil daarmee de wendbaarheid verbeteren. Snel de juiste informatie vinden en gebruiken zal besluitvorming versnellen en het reactievermogen verbeteren. Daarmee versterkt Defensie zowel de commando- als de bedrijfsvoering.

Daarnaast helpt een betere informatiehuishouding om transparanter te zijn. Defensie wil transparant zijn en investeert daarom in het voldoen aan de Wet open overheid (Woo). De informatiehuishouding wordt verbeterd door te investeren in informatiemanagement en archivering, waaronder de missie-archieven.

Defensie stimuleert het intern en extern delen van niet-vertrouwelijke informatie en investeert in de modernisering van de IT-systemen die deze doelstellingen ondersteunen.

Besluitvorming voor het uitvoeren van de taken van Defensie moet plaatsvinden op basis van betrouwbare en actuele informatie. Dit maakt ook de informatievoorziening aan het parlement en de samenleving beter. Voor de inspanningen op dit gebied sluit Defensie aan bij het Rijksbrede programma Open op Orde en zal een verouderd IT-systemen voor documentmanagement worden vervangen.

## 2.3 Informatiegestuurd optreden

Militaire conflicten digitaliseren. Wapensystemen worden steeds meer uitgerust met digitale technieken waaronder slimme sensoren, navigatie, systemen voor data-opslag en data-verwerking en communicatiesystemen om verbindingen op te bouwen. De hoeveelheid data neemt enorm toe, maar ook de complexiteit om deze systemen te gebruiken en onderhouden. De informatietechnologie (IT) die relevant is voor Defensie zal zich de komende jaren snel blijven ontwikkelen.

De defensieorganisatie moet informatie sneller verkrijgen dan de tegenstander. Informatiedominantie is essentieel om effectief te kunnen optreden. Sneller en slimmer verkrijgen van informatie is van groot belang, om vervolgens de informatie te verwerken, selecteren en analyseren en doelgericht te verspreiden. Commandanten kunnen hierdoor gericht beslissen en sturen en zo succesvol optreden in conflicten en crises: dat is de kern van informatiegestuurd optreden.

De IT-infrastructuur wordt onder andere met de programma's GrIT en FOXTROT zodanig gemoderniseerd dat informatie snel en veilig verwerkt en uitgewisseld kan worden en de koppelingsmogelijkheden met partners worden vergroot. De mobiele communicatiemiddelen worden vervangen, zodat eenheden beter veilig met elkaar en met internationale partners en bondgenoten kunnen communiceren.

### Data

Defensie investeert in moderne ondersteunende systemen en software die op de IT-infrastructuur beschikbaar wordt gesteld. Daarbij worden ook technologieën voor data science en Artificial Intelligence (AI) beschikbaar gesteld. Defensie ontwikkelt kaders en richtlijnen met oog voor juridische en ethische afwegingen. Defensie werkt samen met kennisinstellingen, industrie, NAVO en EU om nieuwe kansen op dit vlak te benutten.

Omdat de kwaliteit van data randvoorwaardelijk is om moderne data-technologieën in te kunnen zetten heeft Defensie de datagovernance geactualiseerd. De datagovernance regelt de taken en verantwoordelijkheden voor het beheer en de verspreiding van data.

### Cyber

Defensie moet opgewassen zijn en blijven tegen de almaar groeiende cyberdreigingen. Dit stelt hoge eisen aan de digitale weerbaarheid. Realisatie van het cyber uitvoeringsplan draagt bij aan het verhogen van de cyber readiness van Defensie.

Door invoering van het NIST-framework wordt een robuuste aanpak van de digitale weerbaarheid bereikt. Het inrichten van een SOC-toren (Security Operating Center) leidt tot een goede interne organisatie voor de digitale weerbaarheid.

## 2.4 Goed werkgeverschap

Defensie voert tussen nu en 2025 stapsgewijs een nieuw HR-model in. De IT-systemen die nodig zijn om het nieuwe HR-model te ondersteunen, worden gemoderniseerd.

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. 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 daarom geleidelijk en stapsgewijs opgelost moeten worden. Het programma Vernieuwing HR en het programma HR-IT moeten de HR-processen moderniseren en daarmee werving, ontwikkeling en behoud van personeel een impuls geven.

## 2.5 Arbeidsextensiviteit

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 mensen 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.

## 2.6 Doorontwikkeling decentraal CIO-stelsel

De ambities van Defensie op het gebied van Informatie & Informatietechnologie I&T zijn hoog: we streven naar een informatiegestuurde, technologisch hoogwaardige krijgsmacht. In de Defensienota 2022 is gekozen voor een ambitieuze versnelling van de digitale transformatie. Dit uit zich in modernisering van I&T, een versnelling van investeringen op IGO inclusief cybersecurity en onderliggend hieraan personele groei bij JIVC en Defensieonderdelen om het benodigde realisatie- en absorptievermogen op te bouwen. De ambities stellen hogere en andere eisen dan voorheen aan de Defensieorganisatie en aan de inrichting van de IT-functie in het bijzonder. Defensie richt een CIO-stelsel in, waarin er naast een departementale CIO ook CIO’s decentraal bij defensieonderdelen worden onderkend. Dit is een van de verbeteringen in de IT functie en randvoorwaardelijk om ambities te kunnen realiseren.

De (decentrale) Chief Information Security Officer (CISO) en de Chief Data Officer (CDO) zijn eveneens onderdeel van het CIO-stelsel.

## 2.7 Relatie tot I-strategie Rijk

De onderwerpen uit de IT-strategie Defensie (referte 5) en dit I-plan komen terug in de I-strategie Rijk. Thema's als I in het hart van beleid, digitale weerbaarheid, IT-landschap op orde, informatiehuishouding (Open op orde), data (science) en algoritmen, markt en innovatie sluiten op elkaar aan.

Daarbij geldt dat Defensie altijd zal moeten afwegen welke interoperabiliteit prevaleert indien er sprake is van strijdigheid. Defensie moet zowel met NATO-partners als met andere departementen kunnen samenwerken en informatie kunnen delen. De verbeterde IT-infrastructuur vanuit programma GrIT en het programma Federated Mission Networking (FMN) voorzien daarvoor in de noodzakelijke IT-middelen. Ook stelt Defensie hoge eisen aan de cyberweerbaarheid vanwege de dreiging van statelijke actoren. Hierdoor is het niet altijd mogelijk gebruik te maken van rijksbrede voorzieningen. Defensie zal echter zoveel mogelijk gebruik maken van de voorzieningen die rijkbreed beschikbaar zijn en zich zoveel mogelijk conformeren aan rijksbrede afspraken over interoperabiliteit.

# 3 Financiële paragraaf

De defensiebegroting vertoont een stijgende lijn maar ondanks dat moeten er prioriteiten gesteld worden.

Er zullen hierbij afwegingen plaatsvinden tussen vernieuwing, beheer en onderhoud. De uitwerking van die prioriteiten valt uiteen in verschillende projecten en programma's die defensiebreed worden uitgevoerd. Deze programma's en projecten om de doelen van het I-plan te bereiken zijn opgenomen in de Defensiebegroting. Bij de uitwerking van de plannen naar investeringen worden het reguliere planningsproces[1] en het Defensie Materieel Proces (DMP) gehanteerd, en de Kamer vervolgens via die lijn geïnformeerd.

De komende tijd worden de prioriteiten verder uitgewerkt in een intern strategisch IT-plan. Dit zal de basis vormen voor het I-plan Defensie dat in 2023 aan de Kamer wordt aangeboden.

[1] PS&IB-proces (planningssystematiek en investeringsbeheer)

# 4 Refertes


1. Kabinetsreactie naar aanleiding van Commissie Elias – Brief Parlementair onderzoek ICT-projecten bij de overheid - Tweede Kamer, vergaderjaar 2014–2015, 33 326, nr. 13
2. Beleidsreactie onderzoeken IV-governance Rijk en Besluit toekomst BIT - Tweede Kamer, vergaderjaar 2019–2020, 26 643, nr. 656
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
4. Het interdepartementale CIO-beraad heeft met het Kwaliteitskader Meerjarige Departementale Informatieplannen 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.
5. IT-strategie. In 2019 is de IT strategie 2019 – 2024 (Naar een informatie-gestuurde, technologisch hoogwaardige en toekomstbestendige krijgsmacht) uitgebracht
6. Defensienota 2022. Defensienota 2022: Sterker Nederland, veiliger Europa. Tweede Kamer, vergaderjaar 2021–2022, 36 124, nr. 1
7. Maatregelennota Defensie 2022. 20 juli 2022 kenmerk BS2022014950
8. 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
9. Programma Grensverleggende IT (GrIT)
10. Concept Defensiestrategie DataScience en Artificial Intelligence ; roadmap 2023-2025
11. Defensie Cyberstrategie. Investeren in digitale slagkracht voor Nederland