NIVP

NIDV Informatie Voorziening Platform

Ambitie 2021 – 2025

Table of Contents

1 INLEIDING 3

2 OMGEVING 5

2.1 OVERHEID 6
2.1.1 DEFENSIE - KRIJGSMACHT 6
2.1.1.1 Defensienota 2018 6
2.1.1.2 Defensievisie 2035 7
2.1.1.3 Defensie Industrie Strategie 7
2.1.1.4 Defensie IT strategie 2019 -2024 8
2.1.1.5 Defensie Cyberstrategie 2018 10
2.1.1.6 EU Cyber-Strategie 11
2.1.1.7 Defensie Innovatie 11
2.1.1.8 Aandachtspunten Defensie m.b.t. ICT 13
2.1.1.9 De koude oorlog in het vijfde domein: cyber 14
2.1.2 JUSTITIE EN VEILIGHEID - POLITIE, IFV/ VEILIGHEIDSREGIO'S, NCTV 15
2.1.2.1 Politie Innovatie 18
2.1.2.2 Politie Aandachtspunten 18
2.2 BEDRIJVEN 19
2.2.1 BESCHRIJVING ICT SECTOR 19
2.2.2 ANALYSE DEELNEMENDE BEDRIJVEN NIVP 20

3 AMBITIE NIVP IN HAAR ROL TUSSEN OVERHEID EN BEDRIJVEN / KENNISINSTITUTEN 21

3.1 ALGEMEEN 21
3.2 SPECIFIEK 22
3.3 SAMENVATTING 25

4 NIVP ORGANISATIE 26

4.1 NIVP PLATFORM BESTUUR 26

5 BIJLAGEN 27

5.1 BIJLAGE A OVERZICHT ICT- GERELATEERDE DMP-PROJECTEN, DEFENSIE PROJECTEN OVERZICHT 2020. 28
5.2 BIJLAGE B ICT-VERNIEUWING BINNEN POLITIEPORTEFEUILLES 29
5.3 BIJLAGE C BESTUUR NIVP 38
5.4 BIJLAGE D NIVP DEELNEMERS EN HUN CAPABILITIES 39
5.5 BIJLAGE E INNOVATIEAFDELINGEN BINNEN DE NEDERLANDSE KRIJGSMACHT 41
5.6 BIJLAGE F LIJST VAN AFKORTINGEN 43

1 Inleiding

Dit document beschrijft de ambitie, de prioriteiten, de werkwijze en de concrete activiteiten van het NIVP. Dat wordt gedaan door te analyseren hoe de beleidsvoornemens en de ICT-behoeften van Defensie en de andere civiele publieke veiligheidsdiensten enerzijds en de capaciteiten van de Nederlandse ICT-bedrijven en kennisinstituten anderzijds, het beste op elkaar aansluiten en welke rol het NIVP op dat grensvlak kan vervullen.

Hoofdstukken 2.1 (overheid) en 2.2 (bedrijven en kennisinstituten) vormen de analyse. In hoofdstuk 3 wordt een conclusie (ambitie) geformuleerd, eerst in algemene zin (3.1) en dan specifiek (3.2)

In dit document zijn IV en ICT-synoniem.
Hieronder een korte afbakening van de hoofdrolspelers en het IV-domein.

Overheden
Krijgsmacht (Koninklijke Marine, Koninklijke Landmacht, Koninklijke Luchtmacht en Koninklijke Marechaussee, Defensie Materieel Organisatie, Defensie Ondersteunings Commando, Bestuursstaf), Justitie en Veiligheid (Politie, Politiedienstencentrum, NCTV, en IFV/Veiligheidsregio's)

NL-defensie- en veiligheidssector
Onder de Nederlandse defensie- en veiligheidssector worden bedrijven geschaard die producten, software, technieken en diensten ontwikkelen en leveren aan de hiervoor genoemde overheidsdiensten. Ook de kennisinstellingen worden tot de sector gerekend.

NIDV
Op het grensvlak van de samenwerking tussen overheid, bedrijfsleven en kennisinstellingen, met betrekking tot defensie en veiligheid, speelt de Stichting Nederlandse Industrie voor Defensie en Veiligheid (NIDV) een unieke rol. De NIDV is opgericht door de ministeries van Buitenlandse Zaken, Defensie en Economische Zaken en Klimaat. Het is de enige brancheorganisatie van Nederlandse bedrijven die producten en diensten leveren op het gebied van nationale en internationale veiligheid. Inschakeling van het Nederlandse bedrijfsleven bij orders van de krijgsmacht en de civiele publieke veiligheidsdiensten is één van haar kerntaken.

NIVP
Voor de uitvoering van haar kerntaak maakt de NIDV onder meer gebruik van platforms waarin bedrijven en kennisinstellingen zijn verenigd die actief zijn binnen hetzelfde segment van de markt. Eén van die platforms is het ICT-georiënteerde NIDV Informatie Voorziening Platform (NIVP). Het NIVP richt zich dus op Informatica- en communicatietechnologie waaronder ook *Artificial Intelligence* en *Data Analytics* begrepen worden.

Belang van het ICT-domein [1]
In 2019 had Nederland de derde meest geavanceerde digitale economie van Europa en gold als vierde meest concurrerende economie van de wereld. Met de 'Nederlandse Digitaliseringsstrategie' geeft het kabinet-Rutte III richting aan de Nederlandse digitaliseringsagenda. De prioriteiten van het kabinet liggen onder andere op het thema artificiële intelligence (AI), en de hiermee samenhangende groei in de vraag naar data. Van alle nieuwe digitale technologieën wordt van AI de grootste impact verwacht op de economie, welvaart en maatschappij in de komende jaren.

In hoog tempo transformeert digitale technologie onze (kennis)economie, maatschappij en ons dagelijks leven. Nieuwe digitale toepassingen zoals *cloud-computing*, 3D-printing en robotica vinden hun weg in het Nederlandse bedrijfsleven. ICT-toepassingen gaan hand in hand met onderzoek en ontwikkeling (R&D) en innovatie, die van fundamenteel belang zijn voor de Nederlandse economie die vooral op kennis concurreert. Steeds meer Nederlanders zijn dagelijks online voor hun werk, om contact te houden met hun sociale netwerk, hun bankzaken te regelen, informatie te zoeken of voor vermaak. Nieuwe technologieën zorgen er ook voor dat de manier van werken verandert. De COVID19-pandemie heeft dat veranderingsproces nog eens aanzienlijk versneld.

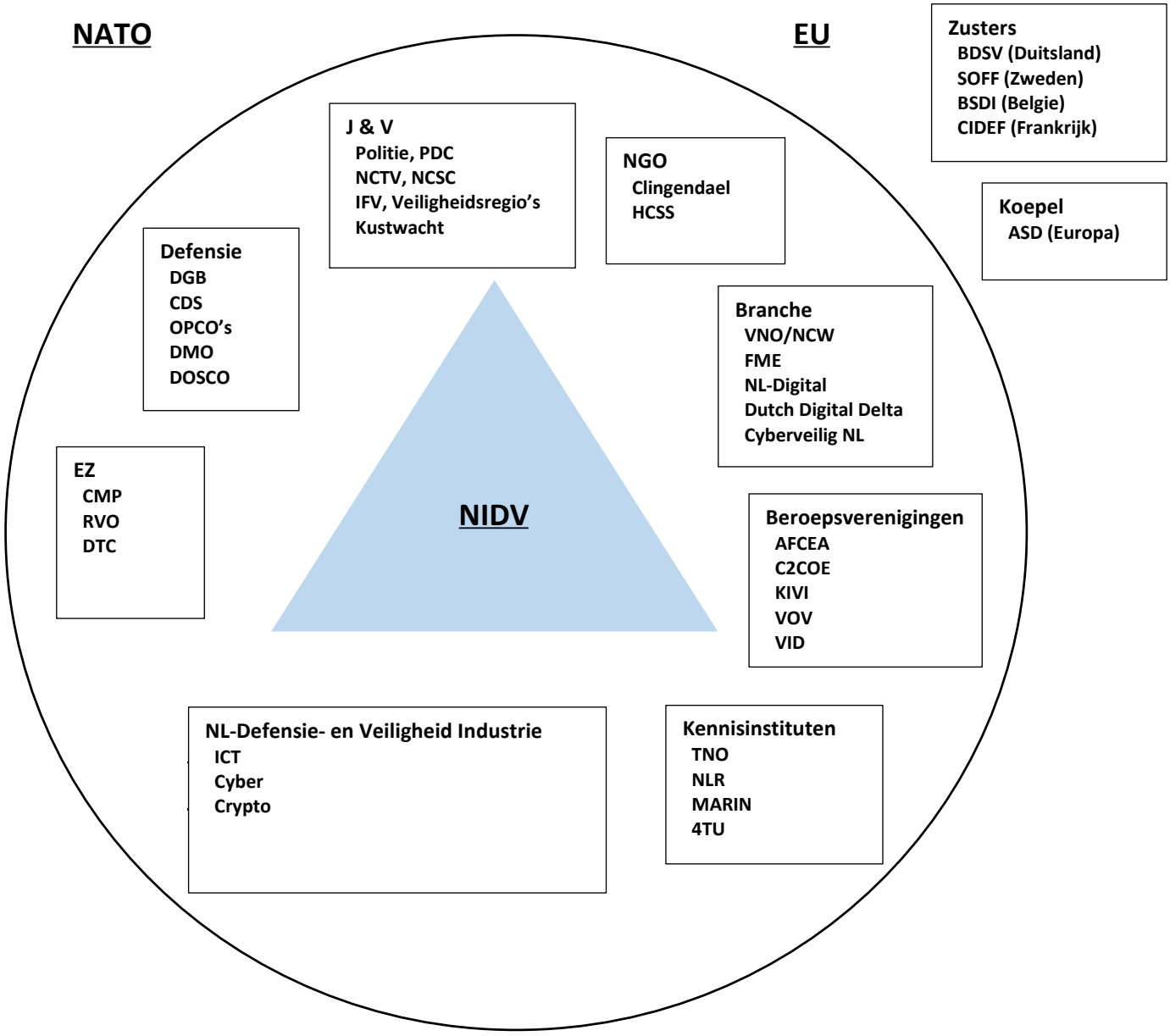
[1] Bron: Centraal Bureau voor de statistiek (CBS) – 10e editie van ICT, kennis en economie – oktober 2020

Ook onze defensie- en veiligheidsdiensten maken in sterk toenemende mate gebruik van digitale systemen en digitale infrastructuur. Die bieden ongekende nieuwe mogelijkheden, maar brengen ook nieuwe kwetsbaarheden met zich mee. Vandaar dat ook de bescherming van onze digitale infrastructuur en van digitale data van steeds groter belang wordt. Het belang van cyberdomein wordt inmiddels algemeen onderkend, zowel defensief (cybersecurity) als offensief in het kader van militaire operaties.

Gelet op de snelheid van de ontwikkelingen op ICT- en Cyber-gebied werkt de Nederlandse overheid op dat terrein nauw samen met de industrie en kennisinstellingen. Dat kan ook, want Nederland beschikt over een sterk groeiende innovatieve ICT-sector. In 2018 hebben Nederlandse bedrijven en instellingen bijna € 16,6 miljard gespendeerd aan R&D (totaal van ICT en andere sectoren) en werden hieraan 157.000 arbeidsjaren besteed. Bijna een kwart van het R&D-personeel werkt in de ICT-sector. De bruto toegevoegde waarde van de ICT-bedrijven groeide in 2018 sterker dan die van de Nederlandse economie als geheel!

2 Omgeving

De NIDV verricht haar werkzaamheden binnen de zogenaamde Gouden Driehoek van overheid, bedrijfsleven en kennisinstituten. Daarnaast onderhoudt de NIDV contacten met diverse andere brancheorganisaties, zusterorganisaties in binnen- en buitenland, is zij aangesloten bij de Europese koepel *AeroSpace and Defence Industries Association of Europe* (ASD) en overlegt zij met internationale organisaties zoals de NAVO en de EU. Het NIVP is binnen de NIDV specifiek gericht op de ICT-sector. In de onderstaande afbeelding wordt de omgeving van het NIVP schematisch weergegeven. In de volgende paragrafen wordt nader ingegaan op de kenmerken, beleidsvoornemens en ICT-behoeften van de belangrijkste spelers in die omgeving.



2.1 Overheid

De Nederlandse regering onderkent het strategische belang van digitalisering voor de Nederlandse samenleving en voor de Nederlandse economie. Dat blijkt uit de in 2018 gepubliceerde en sindsdien jaarlijks geüpdatete Nederlandse digitaliseringsstrategie. Daarin wordt de ambitie uitgesproken om “digitale koploper van Europa te worden”. Het kabinet zet daarom in op een aanpak met twee sporen, namelijk maatschappelijke en economische kansen benutten en versterken van het fundament voor digitalisering. Het tweede spoor bevat twee elementen die ook voor de defensie- en veiligheidssector bijzonder relevant zijn, namelijk grensverleggend onderzoek en innovatie en het op orde brengen van de digitale veiligheid.

2.1.1 Defensie - Krijgsmacht

2.1.1.1 Defensienota 2018

https://www.defensie.nl/downloads/beleidsnota-s/2018/03/26/defensienota-2018
In de Defensienota 2018 spreekt Defensie de ambitie uit om een adaptieve, informatiegestuurde organisatie te zijn. Dat houdt in dat de organisatie in staat wil zijn om alle relevante informatie op ieder gewenst niveau tijdig te verwerven, te verwerken en te verspreiden opdat men zo veel mogelijk met de juiste middelen, op het juiste moment op de juiste plaats kan zijn. Robuuste ICT is daarbij niet alleen een strategische *enabler, transformer* en *game changer*, maar wordt zelfs aangemerkt als ‘hoofdwapensysteem’. Defensie kiest er dan ook voor om fors te investeren in cyber, inlichtingen, ICT, informatievergaring en in het gehele informatiedomein. Die keuze blijkt ook uit BIJLAGE A Overzicht ICT- gerelateerde DMP-projecten, Defensie Projecten Overzicht 2020. Voor uitbreiding van de cyberslagkracht wordt vanaf 2021 structureel een bedrag van M€ 20 gereserveerd. En in de jaren 2018 t/m 2033 wordt cumulatief maar liefst M€ 1.794 geïnvesteerd in ICT-voorzieningen.

Bij het doen van die investeringen kiest Defensie ervoor om intensiever samen te werken met bondgenoten en strategische partners, andere overheidsorganisaties, maatschappelijke organisaties en het bedrijfsleven op het gebied van personeel, kennis en innovatie, de aanschaf en het onderhoud van materieel en bij oefenen, trainen en inzet. Samen met het ministerie van Justitie en Veiligheid (J&V) wil men de civiel-militaire samenwerking herijken. Tevens wil men de weerbaarheid van de samenleving vergroten en onze vitale infrastructuur en de digitale veiligheid van ons land beter beschermen. (Ook van de zijde van de Cyber Security Raad werd onlangs opgeroepen tot meer samenwerking tussen civiele organisaties en Defensie.)

Bij aanbestedingstrajecten is Defensie voornemens om artikel 346 VWEU ruimhartig te interpreteren en zo het nationale veiligheidsbelang te laten meewegen. Indien het gaat om *proven technology*, kiest men wat verwerving betreft voor de uitgangspunten ‘snel, tenzij’ en ‘van de plank, tenzij’. Verwerving van niet-defensiespecifieke spullen en dienstverlening wordt waar mogelijk overgelaten aan externe partijen. Onderzoek naar nieuwe dreigingen én kansen door nieuwe technologieën krijgen voorrang. En Defensie haakt aan bij het Europese Defensiefonds en het Missiegedreven Topsectoren- en Innovatiebeleid. Wat dat laatste betreft is met name het thema Veiligheid relevant voor het NIVP. Binnen dat thema worden namelijk verschillende meerjarige missiegedreven innovatieprogramma’s (MMIPs) gedefinieerd, zoals 4) Cyber, 5) Genetwerkt optreden op land en vanuit de lucht, 6) Adaptieve krijgsmacht en 7) Data en intelligence.

Opmerking: Het beleid staat, maar moet worden versterkt om het daadwerkelijk te laten slagen. Nodig is dat de overheid (J &V, Defensie, EZK) een heldere stip op de horizon zet (met medeneming van het Europese exportmarktspeelveld, strategische autonomie enz.), afdoende (extra) financiële middelen toekent voor onderzoek of verwerving en intern coördinatie inzake het MMIP goed organiseert. Ook is het van belang deze zaken goed te communiceren met zowel het bedrijfsleven (C-level) als kennisinstellingen, om wensen en verwachtingen op elkaar af te stemmen. Daarnaast is het nodig dat het bedrijfsleven zich op basis van voorgaande committeert aan de vigerende kennis- en innovatieagenda of op zijn minst aangeeft zich daar voor in te willen spannen want het bedrijfsleven moet er natuurlijk wel zijn qua betreffend MMIP. Als dat in Nederland afwezig is het bijna onmogelijk om nationaal economische kansen te creëren.

Kort samengevat biedt de Defensienota 2018 volop kansen voor de Nederlandse ICT-sector.

2.1.1.2 Defensievisie 2035

https://www.defensie.nl/downloads/publicaties/2020/10/15/defensievisie-2035
Uit de tien beschreven inrichtingsprincipes zijn voor wat betreft ICT de volgende twee relevant:
- Gezaghebbende informatiepositie (veel en goede data)
- Multidomein en geïntegreerd optreden (dus ook qua data genetwerkt)

Opmerking: Er staat geschreven: “als we alles zo goed mogelijk inrichten dan is er structureel € 13 miljard tot € 17 miljard extra nodig.”
Het ligt helaas niet in de lijn der verwachting dat die extra middelen er in die omvang komen en tegelijkertijd wordt er in de visie geen keus in prioriteit of omvang gemaakt (voor ICT of anderszins).

2.1.1.3 Defensie Industrie Strategie

https://www.defensie.nl/downloads/beleidsnota-s/2018/11/15/defensie-industrie-strategie
Naast de Defensienota beschrijft ook de Defensie Industrie Strategie (DIS2018) die in 2018 door het kabinet Rutte III is vastgesteld, de basis van kennisinstellingen en bedrijven die is benodigd om Nederland een zekere mate van autonomie in de inkoop en instandhouding van militaire capaciteiten te laten behouden. Een basis die ervoor zorgt dat de kennis, technologie en capaciteiten in huis zijn om onze militairen in staat te stellen hun werk veilig, efficiënt en effectief te laten doen en om een rol van betekenis te kunnen spelen in de samenwerking met andere landen, al dan niet als toeleverancier van grote buitenlandse bedrijven.

IT is voor Defensie een belangrijk hoofdwapensysteem. Het is een strategische *enabler* en een *transformer*. De mogelijkheden van IT ontwikkelen zich wereldwijd in een razend tempo. In alle sectoren veranderde er veel in korte tijd. Het bleek een *game changer* met ongekende én richtinggevende invloed op primaire en ondersteunende processen in vrijwel alle organisaties. Op de verschillende pagina’s vermeldt de DIS2018:

P17:
AI, Cyber, Electromagnetische analyse (EMA), *Quantumcomputing* en sensoren zijn dusdanig kritiek voor de informatievoorziening dat nationaal ontwikkelend vermogen noodzakelijk is. Nederland dient te kunnen beschikken over technologie die haar in staat stelt om veilig (digitaal) te communiceren en opereren.

P21:
De mate waarin informatie van diverse sensorsystemen kan worden verzameld en verwerkt en de snelheid waarin geïnformeerde besluiten kunnen worden genomen, is essentieel voor de slagvaardigheid van de krijgsmacht. Informatie is veelal geheim en moet goed worden beschermd. Tegelijk is interoperabiliteit van informatiesystemen met vertrouwde partners gewenst. Basissystemen voor het combineren, verwerken, beheren en opslaan van informatie zijn in belangrijke mate op de markt beschikbaar, maar moeten worden toegespitst op militaire doeleinden en worden geïntegreerd in netwerken en platformen. Dit willen we, vanwege de noodzaak informatie te kunnen beschermen, in nationaal verband doen of eventueel op basis van internationale samenwerking. Vooral in het maritieme domein kunnen we informatieverwerkingssystemen nationaal verankeren. Dit maakt deel uit van de capaciteit om systemen te integreren

P 21:
Communicatiesystemen in basisconfiguratie en communicatiediensten zijn voor zowel zee, land en lucht in belangrijke mate op de markt beschikbaar. Op het gebied van beveiliging en robuustheid zijn vaak specifieke militaire eisen aan de orde, maar daarbij is een beroep op de militaire markt mogelijk. In een aantal gevallen zijn delen of componenten van communicatiesystemen specifiek nationaal en hoog gerubriceerd. Hiervoor vinden we dat industriële capaciteiten nationaal georganiseerd moeten zijn, omdat niet alle gerubriceerde informatie kan worden gedeeld met partners en er toezicht moet worden gehouden op staatsgeheimen en de beveiliging ervan. Vanwege de nauwe relatie met systeemintegratie bij platformen kunnen we vooral in het maritieme domein delen van communicatiesystemen nationaal verankeren. De componenten kunnen evenwel ook door vertrouwde partners worden aangeleverd. Hoewel de noodzaak voor land- en luchtsystemen niet anders is, speelt daar de Nederlandse (kleine) maat en internationale operationele samenwerking een belangrijke rol in de besluitvorming.

P24:
Het cyberdomein is een relatief nieuw domein. Dat dit domein van groot belang is voor de nationale veiligheid staat buiten kijf. Hoewel bedrijven in principe zelf verantwoordelijk zijn voor hun cybersecurity staat de verantwoordelijkheid voor de Nederlandse overheid als het gaat om de bescherming van vitale sectoren - zeker wanneer er statelijke actoren in beeld zijn - niet ter discussie.

P24:
De Nederlandse kennisinstellingen en industrie hebben een sterke basis in de technologieën die nodig zijn voor cyberweerbaarheid, zoals chipdesign, crypto, ICT en netwerken. De sector verricht op meerdere technologiegebieden fundamenteel en toegepast onderzoek. In de nieuwe cyberstrategie wordt uitgebreid op dit domein ingegaan.

P26:
Defensie zal samen met de industrie aan het concept “open innovatie” invulling gaan geven. Hiertoe wordt een beroep gedaan op het innovatieve vermogen van onze (internationale) partners, maar ook op het innovatieve vermogen van kennisinstellingen, bedrijfsleven, hogescholen en universiteiten.

P34:
Het versterken van coördinatie voor Nederlandse inbreng Europese initiatieven (EDF, EDAP, PESCO): De Europese commissie zet in op een meer intensieve samenwerking voor gezamenlijke ontwikkeling van defensiecapaciteiten via o.m. de ontwikkeling van een sterke concurrerende en innovatieve Europese defensie technologische en industriële basis.

P34:
Op basis van de markt- en kennispositie van de Nederlandse defensie-industrie op de internationale defensie markt wil Nederland op termijn bij de top 10 van Europese landen behoren ten aanzien van de toegekende middelen uit het EDF. Dit vraagt om een gestructureerde en afgestemde nationale inzet en strategie op Europese ontwikkelprogramma’s voor defensie capaciteiten.

Interdepartementale Coordinatie Groep
Inmiddels hebben EZK en Defensie een high level Interdepartementale Coördinatiegroep (ICG) ingesteld voor bovengenoemde en gerelateerde Europese defensie programma’s. Onderdeel van de versterking van de coördinatie is een Bijzonder Vertegenwoordiger om de belangen van het Nederlandse defensie gerelateerde bedrijfsleven binnen dergelijke programma’s goed te behartigen. De NIDV neemt in deze ICG deel.

Simulatie
Met een simulatienetwerk kunnen militairen beter worden voorbereid op het uitvoeren van missies. Dit leidt ook tot kostenbesparingen. Het NIVP wil bijdragen aan een simulatie-infrastructuur waarmee Defensie snel en gericht een missie kan simuleren, als onderdeel van een gedistribueerd internationaal simulatienetwerk (Mission Training through Distributed Simulation). Dat betekent onder meer dat bouwstenen moeten worden gemaakt voor het ontwikkelen van scenario’s, voor het hergebruik van scenario’s en van modellen van woonomgevingen en militair materieel. Ook kunnen cyberdreigingen worden gerepresenteerd en kunnen waarborgen worden ingebouwd voor het op elkaar aansluiten van simulatieomgevingen. Ook In het EDF en PESCO wordt ingezet op Rapid Development, Simulation, AR/VR. Onderzocht wordt of een werkgroep onder het NIVP kan worden opgericht.

Een beschrijving van de innovatie aanpak van Defensie en van de wijze waarop die is georganiseerd is opgenomen in paragraaf 2.1.1.7

2.1.1.4 Defensie IT strategie 2019 -2024

De keuze van de Defensienota om IT te beschouwen als hoofdwapensysteem wordt in de Defensie IT-strategie 2019-2024 nader uitgewerkt. Maar dit document is niet openbaar.

Uit de Defensienota, de DIS en de IT-strategie blijkt op meerdere plaatsen duidelijk de uitgestoken hand van Defensie naar het bedrijfsleven en de kennisinstituten. In ieder geval qua intentie, maar niet altijd qua financiële middelen. Verder moet aangetekend worden dat Defensie de markt weliswaar nodig heeft om IT-dienstverlening te leveren en de continuïteit daarvan te waarborgen, maar dat ze altijd een deel van de IT-dienstverlening tot op zekere hoogte zelfstandig moet kunnen uitvoeren vanwege het specifieke karakter van de militaire organisatie.

Concreet gaat het bij de implementatie van de Defensie IT-strategie om een ecosysteem
- om in het kader van de adaptieve krijgsmacht personeel en materieel uit te wisselen tussen Defensie en markt;
- Strategische samenwerking met marktpartijen;
- Een nieuwe IT-infrastructuur;
- Meer mobiele devices en apps:
- Introductie van cloudtechnologie;

- Nieuwe balans tussen centrale, decentrale en lokale IT-samenhangende militaire *capabilities* en IT-*capabilities*;
- Een groter innoverend vermogen door experimenteren en een innovatieagenda.

Op 2 april 2021 heeft het ministerie van Defensie in antwoord op kamervragen de volgende bijlagen gepubliceerd:

- "Scenario's en ontwikkelpaden IT-investeringen van Defensie" Scenario's en ontwikkelpaden IT-investeringen van Defensie | Rapport | Rijksoverheid.nl
- "Defensie duurzaam digitaal" Defensie Duurzaam Digitaal | Rapport | Rijksoverheid.nl

Hieruit bljjkt:

- Het meeste geld is bestemd voor de grote programma's GrIT (1,7 mld), FOXTROT (2,4 Mld), Cyber (3,2 mld) en IGO (16,1 mld).
- In de periode 2021 – 2025 is er investeringsruimte van opgeteld bijna 2 Mld; de behoefte ligt > 4 Mld hoger.
- De digitale transformatie waar Defensie voor staat is geen 'IT-probleem' maar heeft brede impact. Er is lef nodig, risico's accepteren. De klassieke, op beheersing gerichte manier van werken belemmert de realisatie van ambities
- Voor het versterken van het realisatievermogen zijn met name data en cyber specialisten nodig.
- De arbeidsmarkt is krap (iedereen zit te springen om IT personeel) en aan de andere kant heeft het absorptievermogen van Defensie / JIVC ook een grens

2.1.1.5 Defensie Cyberstrategie 2018

https://www.defensie.nl/downloads/publicaties/2018/11/12/defensie-cyber-strategie-2018
Een grotere afhankelijkheid van IT brengt voor de krijgsmacht ook kwetsbaarheden met zich mee. Vandaar dat de bescherming van de eigen IT-infrastructuur en het ontregelen of verstoren van de IT-infrastructuur van mogelijke tegenstanders belangrijke aandachtspunten zijn. Daarover gaat de Defensie Cyberstrategie 2018. Aan de hand van die strategie investeert Defensie in cybercapaciteiten om:

- Te allen tijde de baas te zijn van haar eigen IT- en wapensystemen en haar digitale weerbaarheid te verzekeren;
- Nog beter te weten wie onze nationale veiligheid in het digitale domein bedreigen;
- Over meer mogelijkheden te beschikken om digitale aanvallen te verstoren of af te schrikken;
- Samen met civiele partners de veiligheid van Nederland en van onze vitale infrastructuur en processen te waarborgen in het geval van een onverhoopt militair conflict waarbij digitale aanvalsmiddelen worden ingezet;
- Digitale middelen doelgericht in te zetten om in het kader van militaire operaties het overwicht te krijgen en te behouden (gebruik van IT als wapensysteem).

P15:
Defensie intensiveert vanaf 2019 de middelen voor onderzoek op het terrein van cyber. Van bijna 4 miljoen euro de afgelopen jaren zal Defensie met ingang van 2019 bijna 6,5 miljoen euro per jaar in cyberonderzoek investeren. Daar waar mogelijk wordt dat samen met andere departementen gedaan, zoals ook is aangekondigd in de Nederlandse Digitaliseringsstrategie.

Een zijstap is relevant naar het HCSS Rapport “Naar een Cybercapaciteiten portfolio voor de Koninklijke Landmacht”
https://www.hcss.nl/report/naar-een-cybercapaciteitenportfolio-voor-de-koninklijke-landmacht

P3
De Nederlandse defensieorganisatie heeft het afgelopen decennium forse stappen gezet in het ontwikkelen van strategieën, structuren, capaciteiten en een doctrine voor het cyberdomein. Tegelijkertijd liggen er nog belangrijke uitdagingen in dit snel ontwikkelende domein. Diverse bondgenoten en tegenstanders hebben een voorsprong in zowel de omvang als in de strategische en operationele inbedding van militaire cybercapaciteiten. Defensie werkt aan de ontwikkeling van defensieve en offensieve cybercapaciteiten op verschillende niveaus. Het Defensie Cybercommando DCC is hierbij het leidend orgaan. DCC is tevens het aangewezen organisatieonderdeel om, bij gegeven mandaat, offensieve operaties uit te voeren. Sinds juli 2018 valt het DCC direct onder de Commandant der Strijdkrachten, waar het voorheen was ondergebracht bij de Landmacht (als single-service manager). Sinds 2019 positioneert het DCC zich meer als strategische effectenbrenger en richt zich minder op tactische effecten. Hierdoor ontstaat er een vacuüm dat door de Operationele Commando’s moet worden opgevuld. De Landmacht bezint zich daarom op haar eigen rol in het cyberdomein, het elektromagnetische spectrum en de bredere informatieomgeving. De leidende gedachte is dat verkrijgen, aanwenden en inzetten van cyber en elektromagnetische capaciteiten steeds meer een randvoorwaarde is voor succes in het (land)optreden.

De CLAS Visie “Optreden voor de Landmacht: Manoeuvreren in de Informatieomgeving” is niet openbaar, maar uit een artikel in de Militaire Spectator https://www.militairespectator.nl/thema/editoriaal/manoeuvreren-de-informatieomgeving en het visiedocument van HCSS https://hcss.nl/sites/default/files/files/reports/Playing%20to%20Your%20Strengths.pdf kunnen we afleiden dat Informatie Gestuurd optreden (IGO) een topprioriteit is.

IGO kan worden gedefinieerd als: alle relevante data en informatie kunnen verwerven, verwerken en delen om tijdig inzicht, overzicht en begrip te verkrijgen. Het gaat hierbij om zowel de dagelijkse bedrijfsvoering als de operationele omgeving. Met als doel militaire besluitvorming en militair optreden te kunnen realiseren’. Het begrip ‘militair’ kan ruim gezien worden want de tegenstander kan door fysieke slagkracht) beïnvloed worden, maar evengoed (via informatie) zijn wil, gedrag en/of perceptie.

Om alle data te vergaren en te verdelen is een technologisch sterk en veilig Command & Control en ICT systeem nodig. Zo’n systeem moet kunnen werken met statische en mobiele deelnemers en sensoren en ook onder wisselende omstandigheden van de verbindingskwaliteit en met wisselende rubriceringsniveaus.

Om interoperabiliteit te bereiken met systemen van andere (bevriende) landen is het zinvol te werken met een generieke architectuur (bijvoorbeeld de NATO Generic Vehicle Architecture), waarbij ook de integratie van positie, richting en tijd wordt meegenomen. Op NATO nivo wordt de gewenste compatibiliteit van diverse landelijke systemen gevat onder het begrip Federated Mission Networking. De defensiebrede programma’s GrIT en TEN/FOXTROT zijn voorbeeld van werken naar die compatibiliteit.

2.1.1.6 EU Cyber-Strategie

Uit Draft Report 2020/2256(INI) on the state of EU cyber defence capabilities:

P5:
Underlines that a common cyber defence policy and a substantial cyber defence capability are core elements for the development of the European Defence Union; stresses the urgent need to strengthen EU and the Member State cyber defence capabilities.

P7:
Recalls that cyber defence has both military and civilian dimensions; calls on the VP/HR, therefore, to develop an integrated policy approach and close cooperation between the Military CERT-Network and CERT-EU;
Welcomes the Commission's Action Plan On Synergies between civil, defence and space industries, and recalls the close interdependence of these three sectors in cyber defence; notes that, differently from other military domains, cyber space is mainly owned by commercial entities based mostly outside the EU, which leads to industrial and technological dependencies on third parties; strongly believes that the EU needs to increase its technological sovereignty and innovation, investing in the use of new technologies in security and defence such as artificial intelligence (AI) and quantum computing;

2.1.1.7 Defensie Innovatie

Een overzicht van alle innovatie-afdelingen binnen Defensie is opgenomen in 5.5.

2.1.1.7.1 FRONT

Innovatie is voor Defensie altijd belangrijk geweest. Samenwerken met het bedrijfsleven en de kennisinstituten is daarvoor onontkoombaar. Bij alle defensieonderdelen zijn voor innovatie specifieke organisatie-elementen opgericht. Het gaat om organisaties/bureaus aan de voorkant van ontwikkelingen en zijn daarmee van belang voor het NIVP. Het zijn kweekvijvers voor nieuwe concepten, technieken en behoeftestellingen.

Het overkoepelende innovatiebureau van de CDS wordt FRONT genoemd (*Future Relevant Operations with Next Generation Technology & Thinking*). FRONT scout innovatieve technologieën op de commerciële markt op relevantie voor de Nederlandse krijgsmacht. Die marktpartijen zijn voornamelijk startups. FRONT is een initiatief van het ministerie van Defensie, rapporteert rechtstreeks aan de commandant der Strijdkrachten en is opgericht in 2018. Het strekt zich overigens niet alleen uit over innovatieve materieel gerelateerde producten en diensten. Defensie zoekt voortdurend naar innovatieve ideeën om de slagkracht en het voortzettingsvermogen van de krijgsmacht te versterken. FRONTdoor is daarvoor de digitale 'toegangspoort'. Met incubators worden samenwerkingsverbanden aangegaan om innovatieve ideeën en bedrijven te kunnen laten groeien tot een bedrijfsvorm met overlevingskans. Wanneer interessant voor Defensie, wordt een innovatief idee of bedrijf verbonden aan een onderdeel binnen Defensie. Het NIVP draagt industriële partners aan om zo de samenwerking, binnen de keten van bedrijven, te versterken en daarmee de toegevoegde waarde voor Defensie te vergroten.

2.1.1.7.2 NL-AIC Artificial Intelligence Coalitie

Een belangrijke focus van de krijgsmachtdelen op het gebied van innovatie betreft *artificial intelligence*. De NIDV en haar deelnemers kunnen bijdragen aan dat innovatieproces door onder meer hun aansluiting bij de Nederlandse AI Coalitie[2] (https://nlaic.com). De NIDV is inmiddels aangesloten. Een van de toepassingsgebieden van NL-AIC is Defensie, waarvoor de NIDV samen met de kennisinstituten en het bedrijfsleven use cases gaat ontwikkelen. Daartoe zullen naar het idee van het EDF en het thema Veiligheid, gouden Driehoekjes worden gevormd om een ecosysteem te vormen voor uiteenlopende AI-onderwerpen.

2.1.1.7.3 Missiegedreven innovatie- en topsectorenbeleid

Het missiegedreven innovatie- en topsectorenbeleid is voor de gehele Nederlandse industrie – dus niet alleen Defensie – maar met name het thema Veiligheid relevant voor het NIVP. Voor dat thema worden concreet de volgende ambities genoemd:

- In 2035 beschikt Nederland over de marine van de toekomst. In staat om flexibel te reageren op onvoorspelbare ontwikkelingen.

[2] Directeur NIDV neemt deel in de AI adviesraad van het ministerie van Defensie en van de NL-AIC werkgroep Defensie

- In 2030 werkt de krijgsmacht volledig genetwerkt met andere diensten en met integratie van nieuwe technologieën om sneller en effectiever te kunnen handelen dan de tegenstander.
- Vraag en aanbod worden sneller bij elkaar gebracht om kort-cyclisch succesvolle innovaties te implementeren.
- In 2030 verzamelen veiligheidsorganisaties nieuwe en betere data, waardoor men de dreiging steeds een stap voor is.

Binnen het thema veiligheid zijn verschillende meerjarige missiegedreven innovatieprogramma's (MMIPs) gedefinieerd die terug te vinden zijn in de Kennis en Innovatie Agenda Veiligheid (KIA-Veiligheid). Bij de vorming daarvan heeft de NIDV bijgedragen door onder meer Gouden Driehoekjes (overheid, bedrijfsleven, kennisinstituten) te vormen waarin de MMIPs werden uitgewerkt.

Integrale aanpak georganiseerde criminaliteit met onder meer MMIP's gericht op digitale observatie en bruikbare data

De veiligheidsprofessional met MMIP's gericht op digitaal wapenen en digitaal uitgerust zijn.

Maritieme hightech voor een veilige zee
Om te kunnen voorzien in de benodigde middelen om op alle huidige en toekomstige veiligheidsuitdagingen antwoord te kunnen geven, is een toekomstbestendig en concurrerend ecosysteem van overheid, kennisinstellingen en (maritieme) industrie noodzakelijk. Er zijn in dat verband vier innovatiegebieden gedefinieerd, namelijk: concepten van radar- en geïntegreerde sensorsuites; RF-frontends; sensorsignaalprocessing; life cycle en kostenbeheersing.

Veiligheid in en vanuit de ruimte
De kennis- en innovatiebehoeften liggen op zowel het gebied van de upstream (de infrastructuur in de ruimte) en de downstream (data verwerking naar actionable informatie op de grond) als ook op het snijvlak daarvan (veilige communicatie, Space Situational Awareness (SSA).

Cyberveiligheid
De cybermissie richt zich op het ontwikkelen van kennis en innovatie voor (het kunnen anticiperen op) de belangrijkste cyberuitdagingen uit de Nederlandse Cyber Security Agenda, de Nederlandse Digitaliseringsstrategie en de Defensie Cyber Strategie. De missie geeft richting aan fundamenteel en toegepast (multidisciplinair) cybersecurity-onderzoek voor zowel de langere als kortere termijn.

Genetwerkt optreden op land en vanuit de lucht
Voor commanderen en coördineren van informatiegestuurd en genetwerkt optreden (C2: Command & Control) zijn nodig: sensor- en datafusie, een robuust en hoogwaardig interoperabel communicatienetwerk en C2-ondersteunende systemen die besluitvorming ondersteunen. Het gaat ook om het genetwerkt optreden van Robot Autonomous Systems (RAS), waarbij mens-machine interactie van belang is, en genetwerkt optreden om de tegenstander via het internet, het elektromagnetisch spectrum en sociale media te beïnvloeden (Informatie als wapen).

Samen sneller innoveren voor een adaptieve krijgsmacht
De toepassing van het samen sneller innoveren ligt op een groot aantal gebieden waaronder: robotica en autonome systemen, nieuwe energievoorziening en toepassingen van verklaarbare kunstmatige intelligentie (AI), big data en analyse technieken voor snellere besluitvorming en snelheid van handelen, maar ook het verkrijgen van inzicht in intenties en gedrag. Daarnaast biotech-toepassingen voor het vergroten van menselijk presteren, *Additive Manufacturing* (3D-printing), nieuwe materialen en productie-en ontwerpmethodieken en *Internet of Things*.

Data en intelligence
De kennis- en innovatiebehoeften liggen op het gebied van observeren, analyseren, beslissen en handelen/kwaliteitsborging. Voor observeren gaat het om ontwikkelen van nieuwe sensoren en beter gebruik maken van bestaande sensoren en databronnen. Analyseren

betreft data-integratie, data analysemethodes, voorspellende modellen en sense making. Gebruik van AI voor bijvoorbeeld beeldherkenning. Beslissen vraagt om datavisualisatie en beslissingsondersteunende modellen.

2.1.1.8 Aandachtspunten Defensie m.b.t. ICT

Uit interviews met ICT-functionarissen van Defensie komt naar voren dat haar ICT te maken heeft met de volgende specifieke uitdagingen, aandachtspunten en kwetsbaarheden:

- Technische beperkingen in het veld.
  - *Low connectivity*. De snelheden voor datatransport zijn laag en er is *latency* bij satellietverbindingen.
  - Beperkte bandbreedte en wegvallen van verbinding (ook door ECM van de vijand).
  - Beperkte opslag: hoe kleiner het platform, hoe minder mogelijkheden er zijn voor veilige en robuuste opslag van informatie.
  - Beperkte verwerking: hoe kleiner het platform, des te minder verwerkingscapaciteit. Daarom is een afweging nodig tussen het hebben van een centraal datacentrum versus *edge computing*.

- OT en IT moeten - net als bij de civiele industrie - convergeren (onderscheid tussen ‘groene IT’ en ‘witte IT’ vervaagt). Dit geldt ook voor de ervaringen van de eindgebruiker. Veel traditioneel witte diensten zijn in het veld nodig en vice versa. Maar de omstandigheden in het veld zijn dusdanig anders dat de diensten technisch of functioneel niet hetzelfde kunnen zijn.

- Internationaal is weinig compatibiliteit en weinig standaardisatie.
  Er is op veel vlakken genoeg standaardisatie (STANAGs), maar nationale industriepolitiek en *legacy* drijven landen ertoe deze beperkt te volgen, waardoor nationale silo’s ontstaan. Ook zien we dat NATO-standaarden soms inferieur zijn aan de *proprietary* technologie van de industrie. Daardoor kiezen landen ook vaak niet voor STANAGs. Daarom is het belangrijk om aan te blijven sluiten bij en zelfs richting te geven aan grote initiatieven als Federated Mission Networking (FMN) . Een voorbeeld daarvan is TEN/Foxtrot, een groot bi-nationaal programma met de ambitie om snel en flexibel te ontwikkelen samen met de industrie (spirals) en kan een voorbeeld zijn voor FMN in NATO verband.

- De rolverdeling tussen JIVC en industrie is nog onduidelijk. De krijgsmacht wil adaptief zijn en dus samenwerken met de industrie, maar echte coöperatie (wederzijdse afhankelijkheid) is lastig door onbekendheid met als star ervaren juridische aanbestedingskaders. Daardoor blijft samenwerken vaak steken in het klassieke rolpatroon opdrachtgever - toeleverancier. Zowel overheid als industrie zoekt naar betere (flexibeler) samenwerkingsvormen waarbij er al in een vroegtijdig stadium (voordat er aanbesteding komt) interactie is. Het GriT—project biedt hierbij overigens perspectief. Daarin zijn IBM, ATOS en Unica en tientallen toeleveranciers verenigd in het Athena-netwerk.

- Juist bij IT gaan de technologische ontwikkelingen in hardware en software zo snel dat de klassieke vorm van aanbesteden (eerst volledig specificeren en dan pas bestellen) verouderde producten levert (als nu een iPhone wordt besteld via de klassieke aanbestedingsregels, wordt deze over één of twee jaren geleverd. Dan is inmiddels de iPhone 14 al beschikbaar op de markt). Er is continue vernieuwing van IT nodig. Dat vraagt naast een IT-omgeving/architectuur die dat aankan, ook organisatorische veranderingen bij JIVC en de OPCO’s (omgaan met innovaties moet onderdeel zijn van training en opleiding). Voor Ten/Foxtrot komt dan al gauw de vraag aan de orde: ‘Welke inkoopinstrumenten passen hierbij’ ?

- Van belang is voorts dat bij veel wapensystemen en platformen de IT is geïntegreerd met de hardware. De levensduur van het platform is vele malen langer dan die van de IT. Door de verregaande integratie is het moeilijk de IT los van het platform te vernieuwen. Maar kort-cyclische innovaties zijn ook hier hard nodig. Dit vergt nadrukkelijk aandacht.

- De van oudsher natuurlijke verdeling tussen land, lucht en zee werkt nog steeds door. Zo zijn er aparte datacenters in respectievelijk Woensdrecht, Stroe en Den Helder. Op zich geen

probleem, als de data maar gedeeld en geaggregeerd kunnen worden.

- Er zijn veel data (verzameld) maar daarbij staat een overkoepelend en samenhangend beeld maken voor analyse of IGO nog in de kinderschoenen. Veel van deze data zijn onbruikbaar, omdat ze niet goed gelabeld zijn of in onbruikbare formats opgeslagen. De hoeveelheid te verwerken data zal (exponentieel) toenemen door steeds meer sensoren zoals drones. Databeheer en eigenaarschap moeten dus door de hele organisatie worden doorgevoerd.

- Balans vinden in regelgeving rondom privacy en de wens tot dreigingskennis is een must. Het gaat hier niet alleen om privacy, maar om allerlei regelgeving en belangen, zoals *intellectual property rights*, economisch/commercieel, staatsgeheim, etc. Het is van belang gecontroleerde toegang tot data goed te regelen, zowel intern Defensie als met partners. Balans vinden in gemak/noodzaak van Cloud versus de wens tot veiligheid verdient grote aandacht. Dat vergt een goede afweging tussen Private Cloud / Public Cloud, waarbij ook de nationale, EU- of NATO-aspecten moeten worden betrokken. Hierbij is de hamvraag: ‘Kan hoog-gerubriceerde info in public cloud staan?’ (Ter info: De US NAVY start in 2021 voor 72.000 gebruikers met cloud computing bij Amazon).

- Essentieel bij opslag en encryptie en verwerking van data is dat dit veilig gebeurt. Het belang van nationale veiligheid kan vereisen dat de Nederlandse regering hierover de volledige, zo niet mogelijk maximale zeggenschap heeft en houdt. Daarmee kan maximale garantie worden gegeven op strategische soevereiniteit. Als opslag en encryptie en verwerking van data niet op Nederlands grondgebied met Nederlands personeel kan plaatsvinden, zijn andere waarborgen nodig om zo veel mogelijk aan deze eis tegemoet te komen en de voor NL belangrijke gegevens onder NL jurisdictie te houden (hetgeen betekent dat je niet voor een rechter in USA, Rusland of China eindigt bij een dispuut). Het belang van nationale veiligheid noodzaakt dat de inkoopstrategie op basis van art. 346 VWEU wordt vastgesteld.

2.1.1.9 De koude oorlog in het vijfde domein: cyber

Er is een koude oorlog gaande in het vijfde domein, cyber. Rusland bemoeide zich eerder met de Amerikaanse verkiezingen en ook bij de SolarWind-hack werd al snel hun richting op gewezen. Toch roept geen enkel land dat een dergelijke cyberaanval een oorlogsdaad is. Veel landen maken gebruik van staatshackers om informatie van andere landen buit te maken of zelfs kritische infrastructuur te saboteren. Indien ze de cyber-aanvallen op eigen land als oorlogsdaad bestempelen, dan roepen ze het over zich af dat hun eigen cyberactiviteiten ook als oorlogsdaad kunnen worden gezien. Daardoor zouden ze dit wapen niet meer kunnen inzetten zonder gevaar van escalatie van het conflict naar de andere domeinen (Land, Zee, Lucht, Ruimte). Hard slaan betekent ook incasseren.

Het is ook in Nederland tijd voor actie. Het zou gevaarlijk naïef zijn te veronderstellen dat wij geen mogelijk doelwit zijn in deze koude cyberoorlog. Wat deze missie extra uitdagend maakt voor defensie is dat in het domein cyber, anders dan op het land, ter zee en in de lucht, onze strijdkrachten niet zelf de verdediging op zich kunnen nemen. Veel van de netwerken en infrastructuur die mogelijk doelwit zijn van een aanval door statelijke actoren zijn namelijk in eigendom van en in beheer bij bedrijven en consumenten. De luchtmacht verdedigt fabrieken tegen bombardementen vanuit de lucht, in cyberspace moeten bedrijven dat helemaal zelf doen. En de systemen worden geleverd en onderhouden door technologiebedrijven. En die delen daarmee de volledige verantwoordelijkheid voor de beveiliging daarvan.

Deze gedistribueerde verantwoordelijkheid voor de verdediging van Nederland in het cyber domein hoeft niet perse een probleem te zijn. Je kan het zelfs als een voordeel zien dat de verantwoordelijkheid en middelen niet bij één partij liggen. Terroristennetwerken en criminele organisaties zijn moeilijk te verslaan omdat ze opereren als gedistribueerde netwerken; georganiseerd in autonome cellen zonder een duidelijke hiërarchie. In de kern is het dus goed voor de weerbaarheid van Nederland dat de verantwoordelijkheid voor verdediging bij defensie, justitie, politie, binnenlandse zaken, inlichtingendiensten en vooral bij meerdere, min of meer zelfstandige bedrijven ligt, zoals technologiebedrijven, nutsbedrijven, telco’s, fabrieken en financiële instellingen.

Het is dan wel zaak dat de autonome cellen in dit verdedigingsnetwerk, net als bij de criminelen en terroristen, goed met elkaar samenwerken en vrij informatie delen met elkaar. De overheid moet

daarvoor niet een leidende maar een faciliterende rol innemen in het veilig houden van Nederland met betrekking tot cyberdreiging en zich realiseren dat netwerkbeheerders en technologiebedrijven een cruciale rol spelen met ieder een eigen verantwoordelijkheid. En tenslotte zorgen dat Nederland, of in ieder geval Europa, onafhankelijk is van andere werelddelen voor de bewaking van haar staatsgeheimen

2.1.2 Justitie en Veiligheid - Politie, IFV/ Veiligheidsregio's, NCTV

Uit het Strategisch Omgevingsbeeld 2020 van het ministerie van J&V:
https://www.rijksoverheid.nl/actueel/nieuws/2021/02/01/strategisch-omgevingsbeeld-bundelt-ontwikkelingen-en-perspectieven-in-het-jenv-domein
Het omgevingsbeeld werd samengesteld op basis van analyse van 100 recente publicaties van het ministerie, trendbureaus, de wetenschap, kennisinstellingen en planbureaus. Deze analyse is aangevuld met inzichten en perspectieven van diverse experts, van binnen JenV en daarbuiten. Zo is gesproken met Politie, IND en NCSC, maar ook met vertegenwoordigers uit de wetenschap en het bedrijfsleven.

Ook in dit document zien we – voor wat betreft ICT – de toenemende digitalisering die naast vele voordelen helaas ook meer criminaliteit brengt en meer landelijke en internationale afstemming over bescherming vergt.

Afstemming over gebruik van de cloud voor Politie wil het ministerie van J&V samen met de markt uitzoeken (à la GrIT bij Defensie).

Uit het rapport "Nederlandse strategische autonomie en cybersecurity" van de Cyber Security Raad 18-02-2021

P4:
Een sterkere samenhang van beleid en expliciete prioritering van digitale strategische autonomie is niet alleen wenselijk maar ook noodzakelijk. Bovendien zou het een grote waarde hebben om het reactief handelen te combineren met proactief monitoren en anticiperen. Dit zou ook inhouden om meerdere beleidsterreinen en belangen hecht met elkaar te verbinden, met sturing vanaf het hoogste niveau (Whole-of-Government).
De verschillende departementen zouden op beleids- en operationeel niveau hun samenwerking permanent moeten maken. Het herzien van de organisatie en governance in verband met digitale strategische autonomie is een ambitieuze stap. Niettemin, het langere termijnperspectief is verankering in organisatie en governance van de Nederlandse overheid.

Dit betekent o.a. een sterke verbinding van (beleid en uitvoering van) het ministerie van Defensie met andere ministeries.

Uit de jaarverantwoording 2019 van de Politie aan de Tweede Kamer (20 mei 2020)

P18:
Digitale criminaliteit: Op het web neemt de digitale criminaliteit toe. Hacking is tegenwoordig gemeengoed, zoals voorheen fietsendiefstal. De bestrijding van cybercriminaliteit versterken, verdient daarom alle aandacht. Vaak werkt een publiek-private aanpak aantoonbaar het effectiefst bij het bestrijden van deze criminaliteitsvorm. Daarom investeert de politie in dergelijke publiek-private samenwerking.

P20:
Wat betreft digitale opsporing, forensische opsporing en financieel rechercheren steeg het tempo waarmee de politie zijinstromers voor deze specialismen werft. Zij kunnen nu een versnelde politieopleiding volgen die speciaal is toegesneden op hun functie. Deze nieuwe medewerkers vullen deels de gaten op die de komende jaren ontstaan door de grote pensioenuitstroom van opsporingsmedewerkers.

P21:
De politie beschikt over steeds meer gegevens uit steeds meer bronnen. Om deze grote hoeveelheden data optimaal te kunnen gebruiken, werkt het korps op verschillende plaatsen met bigdatatechnologie. Voorbeelden daarvan zijn het programma Raffinaderij en het Criminaliteits-anticipatiesysteem (CAS). De Raffinaderij biedt rechercheurs en analisten de mogelijkheid om snel grote hoeveelheden politiegegevens in onderlinge samenhang te analyseren en visualiseren. Dat versnelt en verbetert de waarheidsvinding in de opsporing. Na een aantal jaren te hebben gedraaid als proefproject, werkte het korps in 2018 en 2019 stapsgewijs aan het verder invoeren en in de organisatie inbedden van de Raffinaderij.
Het CAS bepaalt waar en wanneer zich de grootste kans op bepaalde delicten voordoet. Op basis van talloze gegevens berekent het CAS waar en wanneer die kans statistisch gezien bovengemiddeld is. Een CAS-kaart is een slimmere hotspotkaart en helpt om – op basis van deugdelijk onderbouwde informatie – capaciteit optimaal in te zetten. Alle regionale politie-eenheden namen het CAS in 2018 en 2019 in gebruik.

P29:

De politie verruimde de bestrijding van cybercriminaliteit verder naar een aanpak binnen alle eenheden. Hierdoor ontstaat landelijke dekking bij het tegengaan van high tech, reguliere en veelvoorkomende cybercriminaliteit. Het Team High Tech Crime (THTC) bestrijdt complexe, innovatieve en georganiseerde vormen van cybercriminaliteit. De cybercrimeteams in de eenheden richten zich op reguliere en veelvoorkomende cybercriminaliteit, in nauwe samenwerking met de districten en basisteams. In 2019 is door alle teams in het land gezamenlijk gestart met de eenheidsoverstijgende aanpak van fenomenen en dadergroepen, zoals afgesproken in de veiligheidsagenda.

De THTC-onderzoeken van 2019 laten zien dat het gebruik van geavanceerde digitale middelen niet beperkt blijft tot cybercriminaliteit in enge zin (zoals hacking). Ook buiten het domein van cybercriminaliteit hanteren criminelen zulke middelen steeds vaker om misdrijven te plegen en af te schermen. Professionele (cyber)criminele dienstverleners spelen hierbij een belangrijke rol. Bijvoorbeeld beheerders van online drugsmarktplaatsen of aanbieders van versleutelde PGP-telefoons. Het terugdringen van dergelijke dienstverlening vereist vaak complexe en innovatieve bestrijdingsvormen met een hightech component.

De overheid werkt toe naar een netwerk van tien operationeel en technisch verbonden meldkamers, die elkaars taken vloeiend kunnen overnemen. Van denken naar doen luidde het motto in 2019. Vooruitlopend op de definitieve sturingsstructuur op basis van de Wijzigingswet meldkamers is de governance in werking gebracht. Het Bestuurlijk Meldkamerberaad en het Strategisch Meldkamerberaad vormen de landelijke gremia op bestuurlijk en strategisch niveau. Het Disciplineoverleg (waarin de vier meldkamergebruikers zitting hebben) en het Hoofden Meldkameroverleg (waarin de tien meldkamerlocaties vertegenwoordigd zijn) voeden beide meldkamerberaden. Het overleg van de kwartiermakers Bedrijfsvoering geeft richting aan het beheer van de meldkamers.

Uit het halfjaarbericht van de minister van Justitie & Veiligheid aan de tweede kamer (29 mei 2020)
(geeft een eerste overzicht van de stand van zaken bij de politie)

Het beheer van de meldkamers is per 1 januari 2020 overgegaan naar het onderdeel Landelijke Meldkamer Samenwerking van de politie. Daarnaast zal de overdracht van het beheer van het vernieuwde C2000, naar verwachting, per 1 juli 2020 worden overgedragen aan de politie.

In mijn brief van 3 december 2019 heb ik aangegeven dat de politie haar werkwijze voor het ontwikkelen en gebruiken van artificiële intelligentie de komende periode zal inrichten conform het door de politie en OM opgestelde Kwaliteitskader Big Data. In de beantwoording van schriftelijke vragen van uw Kamer heb ik u toegezegd dit Kwaliteitskader aan uw Kamer te doen toekomen na vaststelling door de korpsleiding van politie. Het Kwaliteitskader is een intern document dat de politie en het OM gebruiken om hun werkprocessen rondom het gebruik van big data toepassingen op een zorgvuldige wijze in te richten.

Uit bijlage 2 van bovengenoemd halfjaarbericht: kwaliteitskader big data:

Dit kwaliteitskader is een product van het programma Toekomstbestendig Opsporen en Vervolgen, opgesteld in nauwe samenwerking tussen Politie en OM. De opzet van dit kwaliteitskader is meerledig. De benaming Kwaliteitskader Big Data is specifiek gekozen omdat dit kader verschillende doelen dient. Het is zowel een beschrijvings- als een toetsingskader. Het is geen voorschrijvend kader of ‘control framework’. Het kader wil op een methodologische wijze vooral inzichtelijk maken hoe een Big Data project of activiteit is opgezet, wordt uitgevoerd en welke ‘checks and balances’ aanwezig zijn

Van belang is dus dat de overheid al in een vroeg stadium hierbij de industrie betrekt. Juist doordat de industrie praktijkervaring heeft met ontwikkeling van producten welke moeten voldoen aan juridische-ethische regelgeving.

Het Wetboek van Strafvordering en de Politiewet geven de voorschriften voor het verzamelen van gegevens. De Wet politiegegevens geeft de voorschriften voor het verwerken van deze gegevens voor zover het politiegegevens betreft. Het uitgangspunt is dat het gebruik van Big Data-technologie altijd is gebaseerd op rechtmatig verkregen, verwerkte en gecombineerde informatie. De verwerking en analyse van gegevens (automatisch of handmatig) is controleerbaar, reproduceerbaar en kritisch toetsbaar. Algoritmen en modelparameters die voor bijvoorbeeld risicotaxatie en toekomstverwachtingen worden gebruikt zijn bekend, wetenschappelijk getoetst en controleerbaar (inzichtelijk en transparant). Een belangrijk uitgangspunt is dat altijd wordt voldaan aan de wet en dat dit ook inzichtelijk is. Het Openbaar Ministerie (OM) en de politie nemen, na de beantwoording van (de vragen in) het kwaliteitskader en het geschetste plan van aanpak van het Big Data initiatief of project, gezamenlijk een moreel standpunt in over het gebruik en de inzetbaarheid van de technologie en de daaruit voortvloeiende informatie.

Uit bijlage 2 van bovengenoemd halfjaarbericht: ICT-vernieuwing binnen politieportefeuille:
Zie overzicht in Bijlage 5.2

Uit Kamerbrief met bijlage: Adviesopdracht: “Hoe verder met het programma vernieuwend registreren?”

Het Programma Vernieuwend Registreren (PVR) komt voort uit het per eind 2017 afgeronde Aanvalsprogramma Informatievoorziening Politie. De huidige registratieve politiesystemen zijn onvoldoende toekomstvast om de door de politie gewenste vernieuwing te realiseren. Door PVR worden de bestaande registratieve politiesystemen vervangen zodat agenten en rechercheurs optimaal worden ondersteund bij het eenmalig vastleggen en meervoudig gebruik van deze gegevens op een

eenduidige en gebruiksvriendelijke manier. Daarnaast maakt PVR het mogelijk om nieuwe technieken te integreren zoals het gebruik van multimedia (spraakdata en beeldmateriaal).
In maart 2020 heb ik uw Kamer geïnformeerd over de navolgingswijze op het BIT-advies aangaande OPP/PVR2. De politie heeft door een externe partij, Deloitte, laten onderzoeken op welke wijze het BIT-advies zo goed mogelijk kan worden geïmplementeerd. Dit onderzoek is begin september afgerond. Met de afronding van dit onderzoek wordt invulling gegeven aan het advies van het BIT de opzet te heroverwegen. Ik stuur u het eindrapport als bijlage van deze brief mee.
Het advies van Deloitte luidt:
"Wij achten - onder voorwaarde dat OPP zich voor Winkeldiefstal bewijst op functionaliteit, stabiliteit en schaalbaarheid - continuering van OPP op basis van RDF3 het meest aantrekkelijke scenario voor de politie. Wij zien haalbare mitigerende maatregelen voor de geïdentificeerde risico's en stellen vast dat door de verwevenheid van RDF in OPP het loslaten van deze technologie betekent dat de politie opnieuw moet beginnen. Bij het continueren van OPP op basis van RDF adviseren wij de politie actief beleid te voeren om maatwerkcomponenten te vervangen door gangbare technologie. Tevens adviseren wij om de huidige complexiteit van OPP te reduceren door de inrichting van "Offline Werken" te vereenvoudigen en richting de toekomst onnodige complexiteit te voorkomen. Ten slotte adviseren wij enkele gerichte verbeteringen door te voeren in het IT-voortbrengingsproces zodat de politie kan profiteren van het productiviteitspotentieel van OMT/ODT4."

In het algemeen kan gesteld worden dat er bij Politie aandacht is voor het groeiende aandeel van ICT gerelateerde criminaliteit, maar ook dat de eigen digitalisering van taken tot efficiëntie leidt en kansen biedt, en meehelpt om de afnemende menskracht (uitstroom van agenten) deels te compenseren. Net zoals bij defensie kan ook bij Politie de MMIP's kansen bieden. Zie 2.1.1.7.3

IFV, Instituut Fysieke Veiligheid (nieuwe naam: Nederlands Instituut Publieke Veiligheid, NIPV)
Binnen deze organisatie is netcentrisch werken een begrip. Daarbij moeten vele IT- systemen gekoppeld worden of nieuw ontwikkeld om een landelijk dekkend crisis management systeem te verkrijgen. De beheersfunctie van de veiligheidsregio's en brandweerregio's, zijn -- anders dan bij de krijgsmacht en de politie -- overwegend decentraal belegd. De inkoopfunctie en de verantwoordelijkheden voor instandhouding van materieel, kunnen bij centraal beheer naar verwachting efficiënter worden uitgevoerd, waarbij de DVI ook een substantiële rol kan worden toebedeeld.

RB&W
RB&W is een multi-disciplinair kennisnetwerk voor veiligheid www.rbenw.nl

Verhogen cyberweerbaarheid
Cybercrime gaat over het stelen van persoonsgegevens, banktegoeden en bedrijfsgevoelige informatie, identiteitsfraude en het verstoren van vitale processen door kwaadwillenden. Cybersecurity gaat over het beschermen van kroonjuwelen/data rondom productieproces en producten. Voorkomen van uitval/sabotage. Stelen van data/banktegoeden en bedrijfsgevoelige informatie. Het bedrijfsleven werkt samen in het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) om de cyberweerbaarheid te verhogen omdat ogenschijnlijk kleine incidenten grote gevolgen kunnen hebben. Het Digital Trust Center-programma is onderdeel van het Landelijk Dekkend Stelsel en is gericht op het versterken van de cyberweerbaarheid van het niet-vitale bedrijfsleven en het vergroten van het bewustzijn. De Rijksdienst voor Ondernemend Nederland (RVO) heeft en subsidieregeling voor ondernemers in niet-vitale sectoren die hun cyberweerbaarheid willen verhogen. Brancheorganisaties bieden aan hun leden hulp bij het verhogen van cyberweerbaarheid. Voor defensie betekent cyberweerbaarheid niet enkel defensief optreden maar ook offensief.

De Cyber Security Raad (CSR) is een nationaal en onafhankelijk adviesorgaan van het kabinet en bedrijfsleven (via het kabinet) en is samengesteld uit hooggeplaatste vertegenwoordigers van publieke en private organisaties en de wetenschap. De CSR zet zich op strategisch niveau in om de cybersecurity in Nederland te verhogen. De CSR heeft de volgende taken: gevraagd en ongevraagd verstrekken van advies aan de regering en private partijen; adviseren over de implementatie van de nationale cybersecuritystrategie; het leveren van een bijdrage aan de Nationale Cyber Security Research Agenda; en adviseren van de crisisorganisatie in Nederland tijdens grootschalige cyberincidenten. De CSR wordt voorgezeten door Pieter-Jaap Aalbersberg covoorzitter namens de publieke sector en Hans de Jong covoorzitter namens de private sector (VNO-NCW)

De CSR heeft in januari het rapport "Nederlandse strategische autonomie en cybersecurity" uitgebracht (uitgevoerd door buro iivii). En in maart 2021 heeft zij een dringende oproep gedaan voor € 1 Miljard extra budget voor Cybersecurity en meer samenwerking tussen Defensie en Politie; voor bedrijven is Cybersecurity *Chefsache*

2.1.2.1 Politie Innovatie

Missiegedreven innovatie en topsectorenbeleid Zie 2.1.1.7.3

Politie en Wetenschap – Onderzoeksprogramma 2020.
Dit document beschrijft voornamelijk projecten met universiteiten, in de onderzoeksfeer, en is daarmee nu nog niet relevant voor de industrie.

IPEEK International Police Expertise, Education and Knowledge exchange.
Deze stichting richt zich op kennisontwikkeling en overdracht tussen politie en veiligheidsdiensten door professional gaming.

DITSS
Het Dutch Institute for Technology, Safety & Security. DITSS heeft zich de afgelopen jaren ontwikkeld als zogenoemde triple helix onderneming. In co-creatie met verschillende partijen, zoals ministeries, provincies, gemeenten, Politie, veiligheidsregio's, wetenschap, bedrijven en burgers werkt zij aan het analyseren van veiligheidsvraagstukken en het zoeken naar of samen ontwerpen van innovatieve oplossingen.
Het is een onafhankelijke, transparante en facilitaire regie- en uitvoeringsorganisatie die zich richt op het publiek belang. DITSS verbindt publieke en private partijen met elkaar om veiligheidsvraagstukken door middel van vooral technologische, maar ook sociale innovaties, op te lossen

DITSS werkt samen met haar publieke opdrachtgevers en partners aan nieuwe innovatieve producten. De nadruk ligt hierbij op technologische innovaties, maar er is ook altijd oog voor de omgeving (organisaties en samenleving) waarin dit product wordt toegepast. Zo wordt er bijvoorbeeld gekeken of er andere netwerksystemen, processen, competenties, vormen van (in)formeel leiderschap nodig zijn om maatschappelijk rendement te kunnen halen. Want veel aandacht voor sociale innovatie vormt het fundament van het succes van DITSS.

Kortweg gezegd is DITSS een organisatie die voor een ecosysteem zorgt voor innovaties / ideeën die de politie aanlevert. DITSS en NIDV hebben sinds 2020 een samenwerkingsintentie. Momenteel wordt binnen de Korpsleiding van de Politie over de toekomst van DITSS nagedacht.

2.1.2.2 Politie Aandachtspunten

Net als bij Defensie zoekt ook de Politie naar nieuwe wijzen van samenwerken met de markt. Vanzelfsprekend moet er een kern van expertise in huis zijn: De politie heeft ongeveer 75 ontwikkelteams (van ongeveer 7 personen). Er lopen een paar honderd projecten. Waarvan de belangrijkste zijn:

- LMS Landelijke Meldkamer Samenwerking (met Brandweer, ambulance, IFV)
- PVR Programma Vernieuwend Registreren
- DTOPS Digitale Transformatie Opsporing Politie en Strafrechtketen. Loopt al negen jaar.
- GI Generieke Infrastructuur. Is enkele jaren geleden gebouwd. (Een soort GrIT zoals bij defensie). Hierop moeten de applicaties (nog) geladen gaan worden.
- C2000 Opvolging van dit communicatiesysteem wordt vanuit DG?? van J&V gecoördineerd.

De belangrijkste punten uit de portefeuille in Bijlage 5.2

- **Opsporing:** Onderzoek ketenbrede biometrie
- **Vernieuwend Registreren**: Het vernieuwen (en daarmee vervangen) van (twaalf) operationele registratieve legacy-systemen
- **Intelligence:** Implementatie van Advanced Analytics tooling welke bijdraagt aan het analyseren van grote hoeveelheden data.
- **Dienstverlening:** Doorontwikkeling omnichannel, toepassing chatbot in combinatie met live chat (webcare) en 2D contact.

- **Digitalisering en Cybercrime:** Investeren in Sensing techniek. Onderzoek naar brede toepasbaarheid van sensoren (waaronder in Smart Cities).

- **Vreemdelingen, mensenhandel en migratiecriminaliteit:** Standaard Intelligence Tooling t.b.v. het Nationaal Vreemdelingen Informatie knooppunt, het Expertisecentrum Mensen handel en Mensensmokkel, de backoffice identificatie en registratie en informatiedeling met keten en ketenpartners in een op te richten intelligence cluster Migratie.

- **Bedrijfsvoering:** Lange Termijn Informatievoorziening Bedrijfsvoering.
  Lange Termijn Capaciteitsmanagement systeem ter vervanging van BVCM en BCM

Uitbesteding van werk heeft de stap gemaakt van inhuur van personen naar inhuur van teams. De keuze van de teamleden werd veelal door de politie gedaan en niet door de opdrachtnemer. Dat was dus in zekere zin een 'uren' inhuur waarbij de verantwoordelijkheid voor het slagen van een project bij de politie zelf lag. Tegenwoordig hanteren zij ook resultaatafspraken in de realisatie van software. Hierbij worden scrum-teams samengesteld door de leveranciers zelf, waarmee de leverancier medeverantwoordelijk is voor het slagen van een project.

Er is een Raamovereenkomst Applicatie Diensten, die onlangs opnieuw is aanbesteed, en waaraan een zestal (grote) industrie-partijen deelnemen. Deze zou gebruikt kunnen worden als platform om nog meer met de industrie te gaan bouwen in plaats van teams in te huren. Om zo een publiek-private-samenwerking vorm te geven, waarbij (een deel van) de resultaatverantwoordelijkheid bij de industrie kan liggen.

Voor zzp-ers en voor individuele projecten is er het dynamische aankoopsysteem. Ook System Integrators kunnen hier hun aanbiedingen doen, voor bijv. detachering

Zowel Defensie als Politie zetten in toenemende mate drones in, waarbij zij verschillende aanschafcriteria hanteren. Hier kan vroegtijdige gezamenlijke afstemming met de industrie mogelijk een efficiëntievoordeel bieden.

2.2 Bedrijven

2.2.1 Beschrijving ICT sector

De ICT-sector bestaat uit drie onderdelen: de ICT-industrie, de groothandel in ICT-apparatuur en de ICT-dienstensector. De ICT-industrie omvat bedrijven die voornamelijk informatie- en communicatieapparatuur ontwerpen en produceren. Tot de groothandel in ICT-apparatuur behoren bedrijven die handelen in software, computers en overige elektronica, zoals telecommunicatieapparatuur. Ze leveren deze producten hoofdzakelijk aan dealers en andere niet-eindgebruikers. De ICT-dienstensector bestaat uit bedrijven die het proces rondom elektronische informatieverwerking en communicatie ondersteunen. Zij maken bijvoorbeeld software, verzorgen de telecommunicatie of leveren advies.

De meeste bedrijven in de ICT-sector zijn actief als dienstverlener. Eind 2019 waren dit er in Nederland ruim 70.000 (= 90% van het totaal). Een klein aantal multinationals bepaalt het beeld van de Nederlandse ICT-industrie. Deze grote, vaak internationaal opererende, bedrijven vallen deels onder de Nederlandse industrie; een flink deel ervan is qua uiteindelijk bestuur/eigendom in het buitenland.

Gezamenlijk heeft de ICT-sector een aandeel van 4,4 % in het totale aantal Nederlandse bedrijven. De bruto toegevoegde waarde van ICT-bedrijven groeide in 2018 sterker dan die van de Nederlandse economie als geheel. Op alle onderdelen van de ICT-sector was er groei op dit vlak. In 2019 waren 452.000 ICT'ers werkzaam in diverse bedrijfstakken van de Nederlandse economie. Gezamenlijk investeerden Nederlandse bedrijven en overheden bijna € 29,5 miljard in ICT.

Voor ICT onderhoudt de NIDV banden met de Technische Universiteiten en TNO.

De deelnemers in het NIVP zijn vermeld in 5.4

2.2.2 Analyse deelnemende bedrijven NIVP

- Goede samenwerking met kennisinstituten
- Kennis van zaken van toepassingsdomein
- Nederlandstalig
- Sommige projecten zijn Dutch eyes only
- Samenwerkingsframework is voorhanden

3 Ambitie NIVP in haar rol tussen overheid en bedrijven / kennisinstituten

Hoofdstukken 2.1 (overheid) en 2.2 (bedrijven en kennisinstituten) vormden de analyse. In dit hoofdstuk wordt op grond van de bevindingen in genoemde hoofdstukken een conclusie geformuleerd, eerst in algemene zin (3.1), dan specifiek (3.2)

3.1 Algemeen

De rol van het NIVP is om op IV gebied - net als de NIDV dat voor andere domeinen doet - te verbinden en aan te jagen voor interactie tussen overheid, kennisinstellingen en bedrijven op het gebied van veiligheid en defensie. Het NIVP helpt haar deelnemers de ICT-ontwikkelingen te volgen, te begrijpen en te kunnen toepassen in het veiligheidsdomein. En ook hoe de Nederlandse en Europese wet- en regelgeving voor privacy daarbij van toepassing is. Ook de onderliggende hardware voor communicatie, zoals radio's, satellietverbindingen, vallen onder ICT en daar is binnen het NIVP aandacht voor. In klassieke termen was het NIVP oorspronkelijk een platform voor- *Command, Control, Communications, Computers.*

ICT evolueert nog steeds bijzonder snel. Zowel in hardware als in software. ICT is tot in de haarvaten van de samenleving doorgedrongen. Een smartphone is in ieders bezit en ook apparaten zijn verbonden met het wereldwijde internet (iOT). De hedendaagse uitdagingen zijn:

- Overzicht behouden van de bijna exponentieel toenemende hoeveelheden opgeslagen data en dataverkeersstromen. En om daaruit snel een situatiebeeld te destilleren waarop geacteerd kan worden om Nederland veilig te houden voor agressie van staten of criminelen (Informatie Gestuurd Optreden genoemd (IGO)). ICT biedt zelf weer oplossingen om overzicht te verkrijgen uit de door haar gegenereerde stortvloed van data. Door middel van zeer snelle computers, Data Analytics en Artificial Intelligence, kan de voor mensen te arbeidsintensieve taak om overzicht te krijgen, tot op zekere hoogte door 'machines' worden gedaan.

- Een tweede uitdaging is dat met het vergroten van de capaciteit en complexiteit van systemen en hun groeiende interconnectiviteit tevens het aantal 'deuren' toeneemt waardoor kwaadwilligen ingangen kunnen vinden Het lijkt een onuitroeibaar kwaad dat continu alertheid en maatregelen vereist. ICT is zowel een hulp als een deur voor de vijand. De wereld - dus ook Nederland - is een strijdtoneel van voortdurende cyberaanvallen en cyberverweer. Het NIVP helpt deelnemers bij het vinden van bedrijven die de juiste beveiligingen kunnen leveren (RAST-PRO, het NIDV Register ABDO Security Technology Providers). En het NIVP faciliteert verspreiding van dreigingsinformatie vanuit NCSC en DTC naar onze deelnemers.

- Essentieel bij opslag en verwerking van data is dat dit veilig gebeurt. Het belang van nationale veiligheid kan vereisen dat de Nederlandse regering hierover de volledige, zo niet mogelijk maximale zeggenschap heeft en houdt. Daarmee kan maximale garantie worden gegeven op strategische soevereiniteit. Als opslag en verwerking van data niet op Nederlands grondgebied met Nederlands personeel kan plaatsvinden, zijn andere waarborgen nodig om zo veel mogelijk aan deze eis tegemoet te komen. Het belang van nationale veiligheid noodzaakt dat de inkoopstrategie op basis van art. 346 VWEU wordt vastgesteld.

Het is handig om de rol van het NIVP te beschouwen in de verschillende formele fasen waarmee de overheid (vooral Defensie) werkt. Hierna is een beschrijving van de fasen in algemene zin.

Fasen in samenwerking overheid en industrie

Fase 1: Pre-commerciële consultatiefase (inclusief innovatie)
Fase 2: Behoeftestelling door de overheid/gebruiker/klant
Fase 3: Aanbesteding
Fase 4: Instandhouding

FASE-1: Pre-commerciële Consultaties (PCC).

Het NIVP faciliteert in fase-1 de informatie-uitwisseling tussen overheid, kennisinstellingen en bedrijven. Gelet op de grote nadruk die in de verschillende beleidsdocumenten wordt gelegd op “innovatie” en “structurele samenwerking tussen overheid en industrie”, is deze fase (ook) voor de IT-sector van groot belang. Het doel van deze fase is het bevorderen van de samenwerking binnen het ‘gouden ecosysteem’, door met elkaar vroegtijdig concepten te verkennen zodat synergie wordt gerealiseerd. Tevens kunnen in deze fase mogelijke samenwerkingsvormen worden verkend.

In voorkomend geval kan tussen fase 1 en fase 2 een pilot of een demo van een nieuw product of systeem worden ontwikkeld. De ontwikkeling van een pilot of demo vermindert de risico’s voor de klant en vergroot de kansen voor de leverancier.

FASE-2: Behoeftestelling
In deze fase worden behoeftestellingen geformuleerd door de overheid. De industrie kan op basis van de kennis die zij heeft vergaard in fase-1 binnen het NIVP bespreken in hoeverre er onderling kan worden samengewerkt om te zijner tijd een contract van de overheid te krijgen. Dit vanzelfsprekend binnen de ruimte die de mededingings- en aanbestedingsregels bieden.

FASE-3: Aanbesteding
Deze fase gaat van start zodra er een behoeftestelling op de markt is gezet. De NIDV helpt daarin de industrie zoals vanouds om zaken te doen met de overheid, door te informeren, te bemiddelen, matchmaking te organiseren etc. Daarbij wordt ernaar gestreefd om de inkoopstrategie voor een project in een zo vroeg mogelijk stadium te doen vaststellen. Mocht een contract, dat aan industriële participatie onderhevig is, worden gegund aan een buitenlands bedrijf, dan faciliteert de NIDV middels matchmaking om Nederlandse bedrijven te laten aansluiten, in het bijzonder om invulling van IP-verplichtingen mogelijk te maken.

FASE 4: Instandhouding
Deze fase biedt kansen voor bedrijven die diensten aanbieden op het gebied van software maintenance. Ook in deze fase helpt de NIDV bedrijven om zaken te doen met de overheid en kunnen bedrijven binnen het NIVP bespreken in hoeverre hierbij onderling kan worden samengewerkt.

In alle vier de fasen handelt het NIVP in de geest van de Defensienota 2018, die spreekt van: “intensiever samenwerken met onze bondgenoten en strategische partners, andere overheidsorganisaties, maatschappelijke organisaties en het bedrijfsleven - niet alleen als vanouds bij aanschaf en onderhoud van materieel, maar ook op het gebied van personeel (adaptieve krijgsmacht), kennis en innovatie en bij oefenen, trainen en inzet.”
Doel is volgens de nota het opzetten van een langdurige structurele samenwerking – lange lijnen naar de toekomst. De DIS2018 beschrijft de stabiele basis van kennisinstellingen en bedrijven die daarvoor nodig is. De NIDV en het NIVP geven daar invulling aan door de samenwerking tussen bedrijven en overheden en tussen bedrijven onderling (incl. OEM’s) te faciliteren, te ondersteunen en te informeren.

Ook voor Politie geldt dat zij steeds meer de samenwerking met industrie zoekt en intensiveert.

3.2 Specifiek

Op grond van de beschouwingen in de voorgaande hoofdstukken, en de beperkte capaciteit van het NIVP kiest zij voor:

Nadruk (qua tijd en inspanning) op acteren aan de voorkant (FASE 1)
In Fase1 kan de NIVP het meeste waarde toevoegen omdat in latere fasen de aanbesteding steeds meer uitgekristalliseerd raakt en het creëren van kansen voor de Nederlandse industrie lastiger wordt. Het NIVP kiest daarom voor:

Lange termijn
Vroegtijdig bij de behoeftestellers interactie met bedrijfsleven stimuleren. Zo mogelijk *roadmaps* opstellen van defensie, politie, en IFV/Veiligheidsregio’s en delen met de industrie en de kennisinstellingen.
Voor 2021 is een beoogde JIVC/NIDV industriedag in 2021 een belangrijk nieuw concept als een bouwsteen om de samenwerking van Defensie en de ICT-industrie op een hoger plan te

tillen. Afstemmen en samen nieuwe wegen vinden waarin JIVC en de industrie elkaar vertrouwen en begrijpen. Dit is nodig omdat bijvoorbeeld uit “scenario’s en ontwikkelpaden IT-investeringen van Defensie” blijkt:

- De digitale transformatie waar Defensie voor staat is geen ‘IT-probleem’ maar heeft brede impact. Er is lef nodig, risico’s accepteren. De klassieke, op beheersing gerichte manier van werken belemmert de realisatie van ambities
- Voor het versterken van het realisatievermogen zijn met name data en cyber specialisten nodig. De arbeidsmarkt is echter krap (iedereen zit te springen om IT personeel) en aan de andere kant heeft het absorptievermogen van Defensie / JIVC ook een grens.

Projecten
Een voorbeeld van een project in Fase1 is TEN/Foxtrot. Tesamen met onze Duitse zusterorganisatie BDSV wil het NIVP de industrie hierop optimaal aangesloten houden.

Ook over het GrIT project wil NIVP een dag organiseren om het MKB in contact te brengen met het consortium ATOS, IBM, Unica dat hoofdaannemer is.

Thema’s
Omdat AI een belangrijk en opkomende technologie - en ook ethisch thema - is geworden wil het NIVP haar achterban ook hierin informeren over ontwikkelingen door deelname in de Defensiewerkgroep van de NL-AIC. Stimuleren van interactie binnen de gouden driehoek om use cases te ontwikkelen.
Voor thema’s kunnen ook meetings met overheid en industrie georganiseerd worden. Bijvoorbeeld: Cyberweerbaarheid, IGO, nieuwe ontwikkelmethoden zoals low code development.

Juridische angels
In de praktijk blijkt/blijft vroegtijdige interactie van overheid en industrie juridische angels en voetklemmen te hebben. Vooral bij ICT dat zich zo snel ontwikkelt, is dit probleem te groot om te laten voortbestaan. Te strakke juridisering moet teruggeschroefd worden:
Nieuwe vormen van vroegtijdig en flexibel samenwerken met de industrie
Opzetten van een onderzoekswerkgroep (inkopers, contractmanagers, beleidsmakers, aanbestedingsjuristen, industrie, kennisinstellingen) voor betere vormen van inkoop door flexibilisering van de juridische kaders.
Stimuleren van starten van proefprojecten met deze flexibeler inkoopvormen (FASE 1 en 2)
Launching customership, innovatief partnerschap, pre-commercial-procurement, groter belang hechten aan het toepassen van artikel 346 VWEU. Ondersteuning in dit proces door dieper de behoeftestellingen in te duiken, bijvoorbeeld d.m.v. een thema week: “Hacking government bureaucracy and how to deliver faster value to the end-users?”. Uitwisseldagen om een meer vrije stroom van informatie en uitwisseling te realiseren. Open innovatie werkplaatsen (eco systeem) op Defensie- of Politieterrein creëren waarin industrie- en defensie-eindgebruikers op vaste momenten samenkomen om ideeën te bespreken, proof-of-concepts te bedenken, prototypes te bouwen en feedback op te halen. Ook om technici vaker uit hun veilige comfortzone te halen en “in het veld” met de eindgebruikers te praten.

En met mindere prioriteit: (omdat de nadruk ligt op acteren aan de voorkant)

Industrie aangesloten houden op lopende projecten (FASE 3 en 4) zodat de industrie weet wanneer (en welke soort) mankracht en expertise van de industrie nodig is (om ingehuurd te worden door de overheid)

- GrIT Project. Het consortium IBM, ATOS, UNICA hebben via het Athena netwerk contact met tientallen toeleveranciers.
- De upgade van SAP naar HANA
- De update van Peoplesoft HR systeem bij Defensie
- Politieprojecten. Zie Politie Aandachtspunten 2.1.2.2

Opvolging van het project CyberWeerbaarheid begeleiden.

NIDV heeft twee projecten gestart rondom ABDO (Algemeen Beveiligingsvoorschrift Defensie Opdrachten), een verzameling regels waaraan een toeleverancier van Defensie moet voldoen.

In het NIDV-project Cyberweerbaarheid is een framework voor een ABDO-register geïmplementeerd en de promotie is gestart. Ook voor de haalbaarheid van een ABDO Cloud wordt overlegd met de MIVD.

Dit register, RAST-PRO genoemd (Register ABDO Security Technology Providers) biedt bedrijven die aan ABDO (met name de ICT en Cyber aspecten) willen voldoen, de mogelijkheid om hiervoor betrouwbare leveranciers te vinden. Het Buro Industriële Veiligheid van de MIVD – die de uiteindelijk goedkeuring afgeeft - geeft deze informatie niet omdat zij zich niet in de markt wil mengen.

De relatie van de ABDO-eisen tot die van de Amerikaanse CMMC (Cybersecurity Maturity Model Certification) is proactief opgepakt om de regelgeving voor de Nederlandse industrie zo eenvoudig mogelijk te houden. CMMC omhelst een aantal regels voor cyber hygiëne. DoD eist sinds 1 juni 2020 in de gehele toeleverancierskete voor nieuwe contracten dat bedrijven voor CMMC zijn gecertificeerd door een officiële certificerende (markt-)partij. Het CMMC geldt voor controlled unclassified Information en bestaat uit 5 levels, waarbij ML5 het hoogste en ML1 het laagste is. Deze 5 levels passen alle binnen TBB4 (Te Beschermen Belang) van de ABDO, het laagste niveau van het Nederlandse). DoD heeft met het CMMC de standaard bepaald, maar de uitvoering wordt aan de markt overgelaten. Voor het CMMC is een ‘Accreditation Body’ (AB) ingesteld (www.cmmcab.org). Deze AB kan bedrijven accrediteren als C3PAO (CMMC 3-Party Assessment Organization). Een C3PAO mag op haar beurt certificaten afgeven voor zowel CMMC als hogere rubriceringen. Veel Amerikaanse cybersecurity bedrijven zijn geïnteresseerd om de status van C3PAO te krijgen. Het CMMC gaat ook voor buitenlandse leveranciers gelden. Ter voorbereiding van de Nederlandse bedrijven heeft D-NIDV met de DEFMAT W’ton op 30 maart 2020 een VTC gehouden met de binnen DoD direct verantwoordelijke voor de implementatie van CMMC.

Afgesproken is dat NIDV de CMMC-eisen met die van ABDO zou vergelijken. Inmiddels is dat afgerond. Eén van de conclusies is dat alle eisen in CMMC kunnen worden ingevuld door de IT en cybersecurity Technologie leveranciers in het Register.

Het NIVP wil samenwerken met andere organisaties die de belangen van IT-bedrijven behartigen voor overheden: Samenwerking is nodig omdat de NIDV klein van omvang is en omdat een eenduidige stem vanuit de industrie duidelijker en krachtiger is naar Politie en Defensie

- AFCEA
- NL-Digital
- Cyberveilig Nederland
- Dutch Digital Delta
- VNO/NCW Platform Defensie en Bedrijfsleven
- KIVI Defensie werkgroep
- HSD
- RB&W

Vakinhoudelijke ontwikkelingen volgen
Door de secretaris van het NIVP d.m.v. van webinars en cursussen, hoofdzakelijk op het gebied van Cyber en AI.

3.3 Samenvatting

In 2.1 zijn de overheden Defensie, Politie beschreven vanuit ICT-oogpunt. IGO en Cyber zijn belangrijke thema's. Evenals de door juridische spelregels bemoeilijkte samenwerking met de industrie. Daarna volgde in 3.1 een beschouwing over de beste wijze waarop het NIVP de stimulerende rol tussen die overheden en de industrie kan faciliteren. Er wordt onderscheid gemaakt tussen de verschillende fase waarin samenwerking is: Pre commerciele consultatie, behoeftestelling, aanbesteding en instandhouding. Gekozen wordt om de nadruk te leggen op interactie in de eerste fase, want daar kan het meeste waarde worden toegevoegd. De NIVP zal zich inzetten om:

- het maken van roadmaps te faciliteren,
- interactie in fase 1 voor specifieke projecten in behoeftestellingsfase
- thema dagen rond technologische of organisatorische issues
- stimuleren van acties om juridische angels in de samenwerking weg te nemen

4 NIVP Organisatie

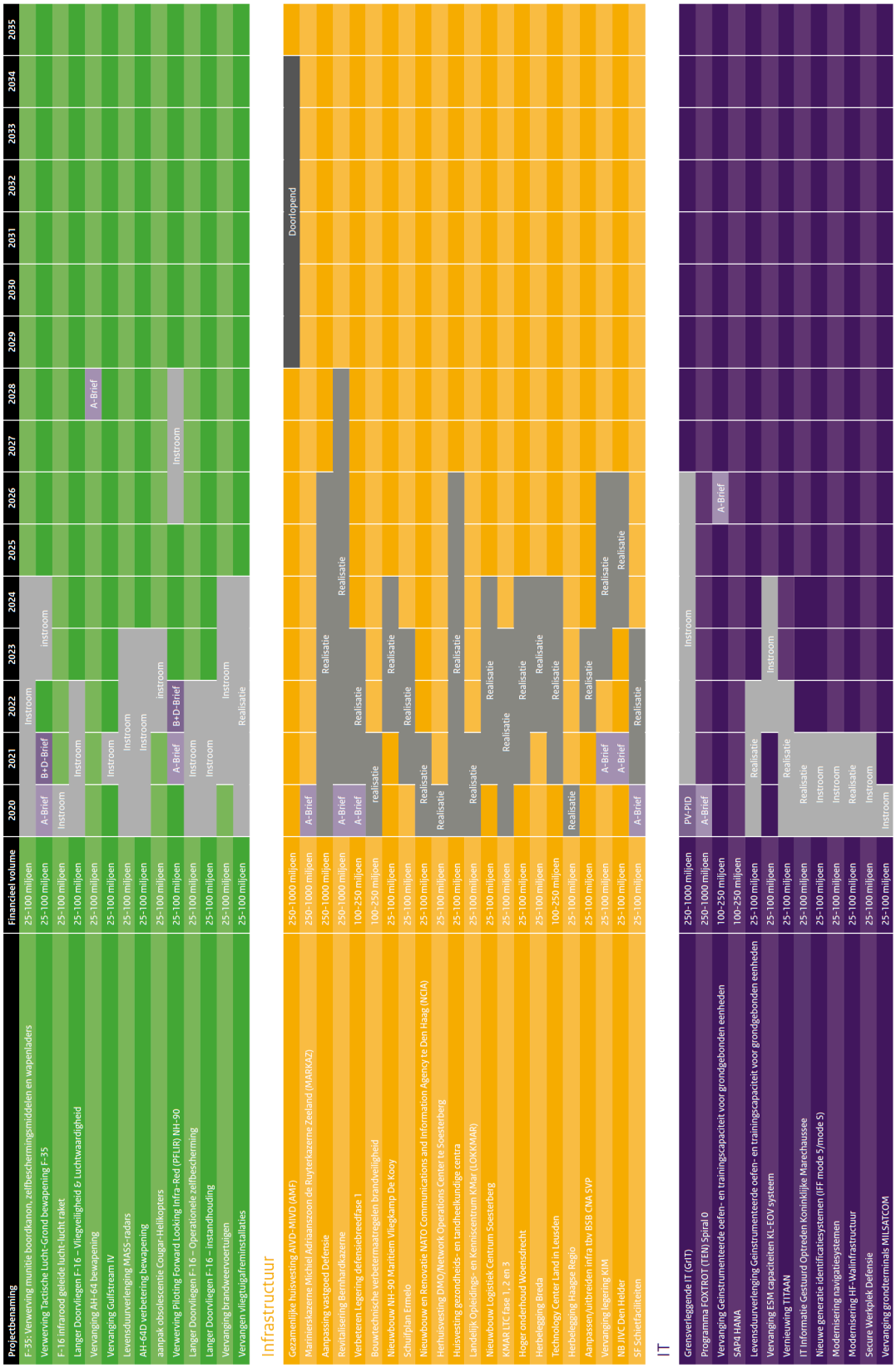
Het NIDV Informatie Voorziening Platform (NIVP) zorgt dat overheden, IT-bedrijven en kennisinstellingen elkaar ontmoeten, informeren en enthousiasmeren over toepassen van digitale technologie bij Defensie, Politie en andere publieke veiligheidsorganisaties. De wereld - dus ook Nederland - is een strijdtoneel van voortdurende cyberaanvallen en cyberverweer. Het NIVP helpt bedrijven - die volgens de ABDO-eisen - aan defensieprojecten werken bij het vinden van de juiste beveiligingen (met RAST-PRO (Register ABDO Security Technology Providers van de NIDV)). Het NIVP faciliteert verspreiding van dreigingsinformatie vanuit NCSC en DTC naar onze deelnemers. Het NIVP stimuleert de interactie tussen overheden, bedrijven en kennisinstellingen om IT-ontwikkelingen te volgen, te begrijpen en toe te passen. Met daarbij aandacht voor de Nederlandse en Europese wetten en richtlijnen op het gebied van dataprivacy. Ook de hardware voor communicatie, zoals radio's en satellietverbindingen, valt onder het NIVP. In klassieke termen is het NIVP dé plek voor C4ISR - Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance.

4.1 NIVP Platform bestuur

Zie Bijlage 5.3

5 Bijlagen

5.1 BIJLAGE A Overzicht ICT- gerelateerde DMP-projecten, Defensie Projecten Overzicht 2020.



5.2 BIJLAGE B ICT-vernieuwing binnen politieportefeuilles

Hierin wordt per portefeuille geschetst wat de doelstellingen van de vernieuwing zijn en wordt een toelichting gegeven op de realisatie in 2019 en de voorziene ontwikkelingen in 2020 en verder (op basis van de portefeuilleplannen). De te realiseren ICT- vernieuwing voortkomend uit het regeerakkoord kan hier onderdeel van zijn. In dit overzicht zijn alleen die portefeuilles opgenomen welke een substantiële IV component in zich dragen. Voor de portefeuilles Contra Terrorisme, Extremisme en Radicalisering (CTER), Ondermijning, Zorg en Veiligheid, Conflict en Crisisbeheersing, Financiële en Economische Criminaliteit (FINEC) en Gebied gebonden Politiezorg (GGP) geldt dat de ICT-vernieuwing waarvan gebruik wordt gemaakt met name binnen de andere portefeuilles wordt gerealiseerd. In deze bijlage is de stand van zaken tot en met december 2019 weergegeven.

Naast de hierna genoemde portefeuilles met een substantiële IV-component, zijn de resultaten op de volgende portefeuilles vermeldingswaardig. Voor de portefeuille conflict en crisisbeheersing betreft dat de Live gang Ketenvoorziening Voetbal (KVV), ten behoeve van ondersteuning Persoonsgerichte Aanpak van hooligans en de ondersteuning van de wedstrijdvoorbereiding. Voor de portefeuille Gebiedsgebonden politiezorg is een app en koppeling met de Blue Spot Monitor opgeleverd binnen de Locatie Gebaseerde Informatie (LGI). LGI zorgt er voor dat (wijk)agenten op basis van hun geo positie belangrijke informatie krijgen over hun omgeving, subjecten en aandachtsgebieden.

Hoofdportefeuille (doel):	Gerealiseerd in 2019:	In ontwikkeling (2020 en verder):	In voorbereiding c.q. onderzoek naar innovatieve mogelijkheden voor de toekomst:
Opsporing Vernieuwing in de opsporing richt zich op: • sneller en makkelijker informatie uitwisselen in de strafrechtketen; • vergroten doelgerichtheid en kwaliteitopsporing door invoering van moderne, gebruikersvriendelijkere interfaces en verdere digitalisering van de strafrechtketen; • vermindering van de administratieve lasten; • implementatie gemoderniseerd Wetboek van Strafvordering. Hierbij wordt aangesloten bij de beoogde vernieuwingen uit de Ontwikkelagenda Opsporing.	• Uitbreiding Zicht op Zaken; gegevenskoppeling BVH en BOSZ met Geïntegreerd Processysteem Strafrecht. • Verwerving nieuw systeem t.b.v. interceptie (tapsysteem). • App Mijn Onderzoek voor delicten diefstal en stalking als proeftuin ontwikkeld. • Uitrol laptops voor 1e lijns medewerkers Forensische Opsporing (mobiel werken en administratieve lastenverlichting). • Toekomstgericht infrastructuurontwerp interceptie gereed. • Verwerving kwaliteitsmanagementsysteem Forensische Opsporing. • In gebruikname verwijzingsportaal bankgegevens t.b.v. opsporing door politie. • Geautomatiseerde koppeling verwijzingsportaal bankgegevens vanuit Summ-IT. • Gezamenlijke monitor re-work met OM i.h.k.v. “In één keer goed” is gerealiseerd. • Pilot lokale opslag Audio Visuele Registratie (AVR).	• Mobiel audio verhoor (mobiele aangiften en verhoren auditief kunnen opnemen). • Uitbreiding functionaliteit Summ-IT: Digitaal dossier en digitale handtekening, internetmonitoring voor digitale wijkagent, koppelvlakken met de BOD- en, digitale communicatie sporen, Beslag in beeld. • Afronden implementatie biometriesysteem; uitfaseren HAVANK. • Implementatie van een nieuw interceptiesysteem. • Ontwikkelen van een Toolkit Zeden; informatiesysteem rondom kinderporno, landelijke database kinderporno. • Systeemintegratie FO, NFI en OM, forensisch informatie systeem, NFIDENT • Opstellen inhoudelijke impactanalyse en voorbereiden pilots ten behoeve van de modernisering van het wetboek van strafvordering. • Implementatie Kwaliteitsmanagementsysteem Forensische Opsporing.	• Onderzoek ketenbrede biometrie voorziening. • Multimedia toepassen in het opsporingsveld. • Digitale samenwerkingsruimte ZSM. • Opsporingscommunicatie: administratie rondom het delen en tonen van video’s en foto’s t.b.v. opsporingsonderzoeken. • Kwaliteit van gegevens: registratie in en het gebruik van applicaties standaardiseren ten behoeve van gegevensuitwisseling met ketenpartners. Digitale Transformatie Opsporing Politie in Strafrechtketen (DTOPS)

Hoofdportefeuille (doel):	Gerealiseerd in 2019:	In ontwikkeling (2020 en verder):	In voorbereiding c.q. onderzoek naar innovatieve mogelijkheden voor de toekomst:

Vernieuwend Registreren
Kern van de opdracht van het programma Vernieuwend Registreren is:
• Het vernieuwen (en daarmee vervangen) van (twaalf) operationele registratieve legacy- systemen;
• met als belangrijke doelen het vergroten van gebruikersvriendelijkheid, de mogelijkheid bieden van het eenmalig vastleggen en het meervoudig hergebruik van gegevens;
• waardoor de beheerlasten van deze groep systemen verlaagd worden.
	• Executie en signalering:
	  • Zaakstroom Strabis (strafrechtboetes) in gebruik genomen op Executie en Signalering (E&S).
	  • Koppeling met ketenpartners binnen E&S technisch gereed.
	  • Nieuwe werkwijze 'signalering' is ingeregeld. Hiermee is het Executie- en Signaleringsproces verbeterd en de samenwerking met het CJIB versterkt.
	  • Signaleringen zijn overgezet van OPS naar E&S en OPS is niet meer operationeel.
	  • Ontsluiting naar KMar en BuZA.
	  • Mobiele app opgeleverd.
	• Mobiele toepassingen:
	  • Functionaliteiten voor Verkeersongevallen-registratie (VOR) gerealiseerd en geïmplementeerd.
	  • Plaats Delict Onderzoek (PDO) is gerealiseerd.
	  • GTPA/ GDPA (geweld tegen/door politie ambtenaren) gerealiseerd. Deze functionaliteit is via MEOS te gebruiken.
	• Winkeldiefstal:
	  • (Tijdelijke) koppeling OPP-BVH en OPP – GMS is gerealiseerd.
	  • Claimen van GMS melding in OPP is gerealiseerd.
	  • De eerste versie van Melding wordt in 4 pilotteams beproefd.
	• Kernregisters
	  • Bouw van kernobjecten Natuurlijk Persoon en Locatie voor proces Winkeldiefstal gerealiseerd.
		• OPP-functionaliteiten:
		  • Bouw 'Melding', Aangifte' en 'Aanhouding' geschikt voor proces Winkeldiefstal.
		  • Aangifte onbekende dader (VVC OD), voorheen Aangifte via Intranet (AVI).
		  • Aangifte Winkeldiefstal (AWI).
		  • Direct Proces Verbaal.
		• Kernregisters
		  • Bouw van kernobjecten Niet-Natuurlijk en Goed voor proces Winkeldiefstal realiseren.
		• Beheer OPP
		  • Migratie functionaliteit e-Briefing en E&S naar platform 2.0.
		• Persoonsgebonden Aanpak (PGA)/Amazone
		  • Vaststellen van landelijk werkproces voor monitoring en registreren van personen en groepen in context van PGA en Amazone (registratiesysteem veelplegers en andere doelgroepen).
		• Mobiele toepassingen
		  • De ontwikkeling van de functionaliteit ProCo (professioneel controleren).
		• Het inrichten van een uniforme werkwijze voor implementatie van opgeleverde functionaliteiten in de eenheden.
			• Mogelijke innovatieve oplossingen (vanuit andere portefeuilles) worden in overweging genomen (indien binnen de kaders van Vernieuwend Registreren haalbaar) bij de uitwerking van de gestandaardiseerde werkprocessen.
			• De komende jaren zullen de functionaliteiten van de operationele registratieve legacy-systemen stapsgewijs worden vernieuwd op het OPP-platform
			Op 14 november is het BIT rapport gepubliceerd, waarop de Min. van Justitie en Veiligheid op 14 december een reactie heeft gegeven. De consequenties voor het Programma Vernieuwend Registreren worden nader onderzocht.

Hoofdportefeuille (doel):	Gerealiseerd in 2019:	In ontwikkeling (2020 en verder):	In voorbereiding c.q. onderzoek naar innovatieve mogelijkheden voor de toekomst:
Intelligence Tijdige, integere intelligence van en voor de politie en haar partners uit interne en externe gegevens bronnen.	• Landelijke uitrol criminaliteitsanticipatiesysteem (CAS); waarmee de benodigde politie capaciteit bepaald kan worden voor een specifieke buurt en of regio tijdens een bepaalde periode. • Doorlopende ontsluiting nieuwe gegevensbronnen en koppeling aan het politie data platform voor gebruik in de zoekprogramma's. • Blue View 4.0 (zoekmachine waarmee men informatie uit verschillende systemen kan vinden) geïmplementeerd en Blue View 2.0 uitgefaseerd. • Met betrekking tot de Commercial Off The Shelf pakketten (COTS) analysetooling is er een compleet overzicht van tools, gebruikers en kosten om hierop te kunnen sturen. • De nieuwe omgeving voor project raffinaderij is opgeleverd en alle gebruikers werken op de nieuwe omgeving. • Er is een samenwerking gestart tussen de IV- organisatie en het Team High Tech Crime (THTC) ten behoeve van Analytical Data Services (ADS). • Het PolitieDataPlatfom is technisch gereed. Er is een PEN-test uitgevoerd en de bevindingen worden verwerkt. Daarmee is de basis voor het ontsluiten van bronnen gereed.	• Implementatie van Advanced Analytics tooling welke bijdraagt aan het analyseren van grote hoeveelheden data. • Uitwisseling van gegevens met veiligheidsdienst o.b.v. art. 24 Wpg is mogelijk. • Analytical cases voor Cybercrime en CTER. Hierbij wordt inzicht verworven door het combineren en analyseren van grote hoeveelheden data, ten behoeve van slimmer en effectiever politiewerk. • Realiseren functionaliteit, gebruikmakend van het PolitieDataPlatform.	• Experimenten in Real Time Intelligence-labs. • Investeren in nieuwe technologie. • Onderzoek naar verdere professionalisering data- science met als doel meer toepassingen van het gebruik van big data. • De voorziening BlueView zal in 2020 en 2021 in gebruik worden genomen binnen de opsporing. Daarmee zal het aantal gebruikers stijgen naar circa 20.000.

Hoofdportefeuille (doel):	Gerealiseerd in 2019:	In ontwikkeling (2020 en verder):	In voorbereiding c.q. onderzoek naar innovatieve mogelijkheden voor de toekomst:
Dienstverlening Het uitbreiden van de mogelijkheden voor digitale dienstverlening aan onder andere de burger. Uitgangspunt is: 'Dienstverlening op maat'.	• Uitbreiding van de mogelijkheden van Internetaangifte met meer delictsoorten. Internetaangifte voor internetoplichting is nu mogelijk. • Met registratie (BVH) en monitoring wordt in het opsporingsproces en bij online aangiften de werkwijze 'individuele beoordeling' ondersteund. Met deze werkwijze kunnen professionals in de strafrechtsketen beter de kwetsbaarheid van slachtoffers beoordelen en maatregelen ter bescherming inzetten. • AVI (aangifte via intranet) module buiten gebruik gesteld i.v.m. verouderd platform en aangepaste wet- en regelgeving. Aangiftes kunnen nu alleen nog rechtstreeks verwerkt worden in BVH. • Het Virtuele Callcentrum, dat de Regionale Service Centra ondersteunt bij het meldingenproces, is technisch ingericht. Op dit moment werken 3 Regionale Call centers virtueel. Hierdoor kan de werklast bij de RSC's makkelijker over de eenheden worden verdeeld. Tevens kan een hoger serviceniveau van de politie naar de burgers worden bewerkstelligd. • Totstandkoming data.politie.nl waarop open data van de politie gepubliceerd wordt. • Pilot chatbot Wout afgerond en wordt geëvalueerd. • Chatbot Wout is gekoppeld met Servicemodule. • Workforce management en quality assurance voor Regionale Service Centra mogelijk gemaakt. • Webservice opgeleverd voor ketenslachtoffer portaal. • Ondersteuning van het meldingenproces door middel van een integrale coördinatievoorziening: onderdeel volgen is opgeleverd.	• Doorontwikkeling omnichannel, toepassing chatbot in combinatie met live chat (webcare) en 2D contact. • Implementeren webcare bij de eenheden / Regionale Service Centra. • Ontwikkeling authenticatie burgers en bedrijven door aansluiting op eIDAS en eHerkenning (standaard binnen de overheid voor elektronische identificatie). • Implementatie virtuele callcenters overige RSC's. • Onderzoek naar toepassing IDIN als authenticatie mogelijkheid voor burgers. • Ontwikkelen intake van cybercrime. • Realiseren elektronische handtekening van de burger. • Ondersteuning van het meldingenproces door middel van een integrale coördinatievoorziening; onderdeel verdelen bijna gereed, onderdeel voortgang bewaken ingepland. • Toepassing van risicotaxatie instrument Provict bij individuele beoordeling. • Beschermen privacy van slachtoffers in de strafrechtketen.	• Toepassing van Artificial Intelligence mogelijkheden bij de Intake. • Betekenisvolle afhandeling van meldingen en aangiften en terugkoppeling naar burger

Hoofdportefeuille (doel):	Gerealiseerd in 2019:	In ontwikkeling (2020 en verder):	In voorbereiding c.q. onderzoek naar innovatieve mogelijkheden voor de toekomst:

Digitalisering en Cybercrime
Deze portefeuille richt zich op de intensivering van de aanpak van cybercrime, het verder ontwikkelen van het digitaal opsporen en het onderzoeken en toepassen van sensoren voor de politietaak.
	• Realisatie technische voorzieningen voor de digitale opsporing:
	  • De nieuwe omgeving Hansken is live gegaan;
	  • uploaden van data vanuit de teams digitale opsporing mogelijk. Dit brengt informatie sneller naar eindgebruikers;
	  • bijna 65 % van de locaties t.b.v. teams digitale opsporing, Cybercrime teams en de Teams Bestrijding Kinderporno Kindersekstoerisme zijn volledig operationeel opgeleverd en aangesloten op het Digitaal Transferium (helpt rechercheurs bij een goede verwerking van hun inbeslaggenomen data);
	  • Briefcam, een analysetool voor het uitkijken van videobeelden, is na de start in 2018 nu landelijk geheel uitgerold als proof of concept.
	• De Artificial Intelligence agent toepassing (reeds in gebruik bij aangifteproces), wordt nu ook ingezet t.b.v. team 'follow the money'.
	• Er is een prototype voor het doen van aangiften ontwikkeld. Daarbij zijn er ook enkele deelproducten opgeleverd voor het Artificial Intelligence (AI) georiënteerd opnemen van aangiften. In deze innovatieve ontwikkeling wordt verkend welke toegevoegde waarde AI kan leveren voor het aangifteproces.
	• Het Nationaal politielab AI (NPAI) draagt bij aan nationale en internationale 'ecosystemen' c.q. netwerken.
	• De Proeftuinvoorziening voor de ondersteuning van de operationele Sensing is gerealiseerd. Het eerste operationele project is aangesloten.
		• Realisatie technische voorzieningen voor de digitale opsporing.
		• Aanschaf en eerste implementatie van software en systemen binnen de mogelijkheden van de Wet Computercriminaliteit III (CCIII) en de continue doorontwikkeling ervan.
		• De verdere implementatie (incl. voorbereiding ICT-infrastructuur) van het landelijk gebruik van bodycams wordt uitgewerkt en uitgevoerd. Het aanbestedingsproces is inmiddels gestart.
		• De generieke voorziening webcrawling wordt specifiek gebouwd voor gebruik van toepassingen op het darkweb.
		• Brede implementatie Hansken.
			• Investeren in Sensing techniek. Onderzoek naar brede toepasbaarheid van sensoren (waaronder in Smart Cities).
			• Investeren in nieuwe technologie Onderzoek naar brede toepasbaarheid Artificial Intelligence.
			• Webcrawling: internationale samenwerking intensiveren.

Hoofdportefeuille (doel):	Gerealiseerd in 2019:	In ontwikkeling (2020 en verder):	In voorbereiding c.q. onderzoek naar innovatieve mogelijkheden voor de toekomst:
Vreemdelingen, mensenhandel en migratie- criminaliteit Ontwikkelingen op het gebied van vreemdelingen en informatie-uitwisseling met ketenpartners.	• Diverse aanpassingen aan de identificatie- zuil (BVID) waardoor identificatie & registratie van verdachten en (verdachte) vreemdelingen sneller en eenvoudiger verloopt met kwalitatief betere resultaten. • In beheername van de Recherche Analyse Omgeving (RAO) ten behoeve van het Nationaal Vreemdelingen Informatie Knooppunt (NVIK). • Digitalisering van het proces (en betrokken documenten) van vreemdeling rechterlijke staande houding en overbrenging. Dit verbetert de informatiepositie van de politie en ketenpartners. Het betreft een deelresultaat van het programma Digitaal werken in de vreemdelingenketen. • Een analysetool in de vorm van een stoplichtsysteem gerealiseerd, als onderdeel van het programma Herijken Asielproces en identificatie- en registratiestraten. Hiermee is een snellere duiding van kwaadwillende en kwetsbaren mogelijk. • De ontwikkeling van de nieuwe mobiele ID koffers (t.b.v. mobiele identiteitsvaststelling) is afgerond. De eerste koffers zijn opgeleverd t.b.v. buitenlandmissies.	• Project Digitaal Werken in de vreemdelingenketen, met als doel het hebben van een realtime online actueel vreemdelingenbeeld voor iedere medewerker in de keten. • Doorontwikkeling van de Basisvoorziening Identiteitsvaststelling. • Realisatie webcrawler signalen mensenhandel voor het op internet geautomatiseerd detecteren van de meest ernstige misstanden zodat (bestuurlijke) controles en opsporing gerichter en daarmee efficiënter kunnen plaatsvinden. • Programma Grenzen & Veiligheid: Implementeren nieuwe en gewijzigde Europese Verordeningen in lijn met het Europese veranderprogramma Borders & Security ten einde op verantwoorde wijze grens- en migratiebeheer, vreemdelingen handhaving & toezicht en internationale opsporing te kunnen uitvoeren.	• Standaard Intelligence Tooling t.b.v. het Nationaal Vreemdelingen Informatie knooppunt, het Expertisecentrum Mensen handel en Mensensmokkel, de backoffice identificatie en registratie eninformatiedeling met keten en ketenpartners in een op te richten intelligence cluster Migratie. • Redesign Identificatiezuilen i.s.m. TU Delft; het ontwikkelen van een toekomst bestendige zuil ten behoeve van het veiligheidsvraagstuk: - identiteit, wie is hij/zij; - vormt risico voor de openbare orde en veiligheid en/of betrokken bij criminaliteit; - vormt risico voor de Nationale Veiligheid; - asiel, verblijf en terugkeer.

Hoofdportefeuille (doel):	Gerealiseerd in 2019:	In ontwikkeling (2020 en verder):	In voorbereiding c.q. onderzoek naar innovatieve mogelijkheden voor de toekomst:

Bedrijfsvoering
Verbeteren van specifieke voorzieningen voor bedrijfsvoering.
	• Doorontwikkeling Planon release naar Planon LIVE heeft plaatsgevonden.
	• Realisatie nieuw Identity & Access Management systeem;
	  • er is gestart met de opschoning van de top 14 systemen. Er zijn nu 10 systemen opgeschoond.
	  • een nieuwe versie van One Identity (IAM) is geïnstalleerd in het nieuwe domein. Deze versie vervangt de IAM omgeving in het huidige domein en verbetert de geautomatiseerde verwerking van autorisaties.
	• Implementatie tooling voor AVG & WPG registratie.
	• Invoer leeromgeving met tijdelijke oplossing zelfroosteren voor capaciteitsmanagement.
	• Aanpassing systemen op nieuwe cao, waaronder invoering LFU.
	• Vernieuwing en migratie van e-learning trainingen van E-pol naar het Leermiddelenportaal van de PA.
	• Proof of Concept Robotic Process Automation (RPA) binnen Finance.
	• Proof of Concept chatbot t.b.v. Werving & Selectie.
	• Implementatie proces debitcards.
	• Voertuig-Inzicht App waarmee Voertuigbeheer een voertuig kan vinden en informatie m.b.t. gebruik etc. kan worden ingezien.
		• Structurele oplossing voor bewaking PTSS- dossiers en case management t.b.v. schadeafhandeling.
		• Inrichten Business Intelligence (BVI-BV) t.b.v. Politie Academie.
		• Doorontwikkeling Politie Prestatie Dashboard (PPD) gericht op operationele indicatoren voor integrale sturing.
		• Realisatie nieuw Identity & Access Management systeem en start opschoning systemen.
		• Implementatie van elektronische facturatie (E- facturatie).
		• Realisatie nieuw intern portaal: Blue met o.a. BlueTube videokanaal, chatfunctie en één integrale webshop. Inrichten en implementeren oplossing voor Loket Sociale Zekerheid.
		• Rationalisatie huidige tools t.b.v. nieuw proces initiële instroom politiemedewerkers.
		• Realisatie toepassingen Robotic Process Automation RPA binnen andere diensten (Service management, HR).
		• Nieuwe PBF-tooling (Planning, Budgettering, Forecasting) ten behoeve van het programma Doorontwikkeling Begroten & Budgetteren.
			• Lange Termijn Informatievoorziening Bedrijfsvoering.
			• Lange Termijn Capaciteitsmanagement systeem ter vervanging van BVCM en BCM.
			• Lange Termijn Werving & Selectie systeem.
			• Analyse Procure-to-pay proces en benodigde toekomstgerichte systeemondersteuning.

Hoofdportefeuille (doel):	Gerealiseerd in 2019:	In ontwikkeling (2020 en verder):	In voorbereiding c.q. onderzoek naar innovatieve mogelijkheden voor de toekomst:
Techniek	• In het kader van de datacenterconsolidatie is Rekencentrum Noord-West afgebouwd en naar Rekencentrum 3 gemigreerd. • Generieke infrastructuur (GI) is volledig opgeleverd en bruikbaar als generieke landingsplaats voor applicaties. Een ontwikkelversie van de nieuwe biometrievoorziening is geland op de nieuwe infrastructuur. Het is de eerste grote applicatie die landt op de GI. • Programma Confi fase 1 (wordt ICOPS) is vrijwel afgerond voor de Landelijke Eenheid. • Netwerkportaal: firewallverbetering versie 2.1 is afgerond. • Servicemanager (USM), de tool welke Expertdesk vervangt, is live. Laatste functionaliteiten worden begin 2020 opgeleverd.	• In beheer name en saneren eigen beheerde omgevingen (EBO's). • Datacenterconsolidatie is gericht op een zo efficiënt, effectief en veilig mogelijk beheer van applicaties. Rekencentrum Midden is het volgende en laatste rekencentrum dat nog gemigreerd moet worden. • Programma ICOPS, waarmee een landelijke omgeving wordt gerealiseerd waarop veilig gewerkt kan worden met (meer) confidentiële Politie gegevens. • Het Programma Herinrichting Beheer Mobiele ICT heeft tot doel de beschikbaarheid van mobiele ICT middelen te optimaliseren en verstoringen van mobiele ICT zo snel mogelijk te verhelpen, zodat de agent zijn of haar werk ongestoord kan blijven uitvoeren. Aanbesteding en transitie Technisch & Logistiek beheer Landelijke Eenheid lopen op schema. • IV naar de politie cloud. Dit programma realiseert de applicatiemigratie naar de Generieke Infrastructuur. Het programmaplan is goedgekeurd. • Ontwikkeling en implementatie van een nieuwe tool voor de Servicedesk ICT, om tickets te registreren en beheren (service manager). Het is een moderne service management tool die gaat helpen om sneller, beter en makkelijker service te bieden aan alle collega's. • Doorontwikkeling toegang tot politieobjecten. • Ontwikkeling van een voorziening voor generieke logging voortkomend uit wettelijke verplichtingen (AVG en WPG). • Continue ontwikkeling op het gebied van de cyberweerbaarheid van de politie. • Netwerkportaal heeft tot doel om op gecontroleerde wijze, met gebruik van generieke services, netwerkverkeer mogelijk te maken tussen de zones met een verschillend niveau van vertrouwen; inclusief internet.	• Continue scan van technologische mogelijkheden.

5.3 BIJLAGE C Bestuur NIVP

Vz	Bas Morselt, Vice President	Capgemini Nederland
Vz	Wilco Riemersma, Vice President Consulting Services	CGI
Sec	Harry de Groot	NIDV
Lid	Harm Janssen, Key Account Manager Landsystems Domestic	Thales Nederland
Lid	Antoine Smallegange, Sr Business Consultant C4I	TNO
Lid	Daniel de Jager, partner	PWC

Adviseur Ron Nulkes, NIDV

Secretaris: Harry de Groot, NIDV.

5.4 BIJLAGE D NIVP deelnemers en hun capabilities

Accenture	Software development en consultancy	
Airbus Defence & Space Netherlands	Systems en software	
ARVOO Imaging Products	Camera's en image processing	
Atos Nederland	Software development	
Between Staffing Nederland	ICT Detachering	geen NIVP deelnemer
BlackBerry Netherlands	Communication equipment & Security software	
Capgemini Nederland	Software development	
Centric	Software development	
CGI Nederland	Software development	
Cisco Systems International	Communication equipment & Security software	
CityGIS	Geographic software	
Compusult	Simulatie Software	
Contour Advanced Systems	Systems integrator for mission critical systems	
Deloitte	Software development en consultancy	geen NIVP deelnemer
DG Systems	Communication equipment	
EAL (Apeldoorn)	Toegangscontrole en registratie	
Eurotempest	Tempest bestendig maken van equipment	
Fokker Technolgies Holding	Aircraft subsystems	
Fox-IT	Cryptography, Cybersecurity. Detection and response, security assessment, training and consultancy	geen NIVP deelnemer
Green Hills Software	Secure Operating systems. Embedded systems	
Height Technologies	Drones	
ICT Teamwork	ICT Detachering	geen NIVP deelnemer
Ilias	Logistics software	

IBM Nederland	Software development en AI	
Intronics	Computer / Network hardware	
KPN	Communication equipment & Security software	
MarkLogic Netherlands	Geographic software en intelligence	
Network Innovations	Wereldwijde satelliet verbindingsoplossing	
NLR - Netherlands Aerospace Centre	Research & Development	
ON2IT	Cybersecurity	
Opt-NET	Artificial Intelligence	
Ordina	Software development	
Palantir	Big Data / AI	
RHEA	ICT, Engineering, Cyber	geen NIVP deelnemer
Rohde & Schwarz Benelux	Communication equipment & Security software	
Saab Technologies	Systems integrator for surveillance	
SAS Institute	Data analytics en AI oplossingen	
Sandgrain	Authentication and Identification of chips	
Sectra Communications	Comm. equipment & Security software	
Siemens Nederland	Systems en software	
Simac Electronics	Communication equipment	
Software Improvement Group	Software analyse	
S & T Science and Technology	Scientific data solutions	
Stratego	Staffing	

SurCom International	Satcom equipment	
Technolution	Communication equipment & Crypto	
Thales Nederland	Radar, Com equipment en sw development	
TNO Defensie en Veiligheid	Research & Development	
TriOpSys	Software development	
Yacht	Detachering	

5.5 BIJLAGE E Innovatieafdelingen binnen de Nederlandse Krijgsmacht

- Bestuursstaf: FRONT - Verkent civiele en militaire kennis die mogelijk het veiligheidsdomein beïnvloeden.
- Bestuursstaf: DPLAN K&I - Voert Defensiebreed de regie over het ontwikkelen en borgen van kennis en het bevorderen van innovatie.
- Koninklijke Luchtmacht: AIR - Creëert beweging door te inspireren, mobiliseren, faciliteren en samen te doen.
- Koninklijke Landmacht: CD&E - Is een katalysator bij experimenten en samenwerking met partijen buiten Defensie.
- Defensie Materieel Organisatie: MIND - Richt zich op technologische en sociale innovatie en maakt zo de DMO wendbaar en adaptief.
- Defensie Materieel Organisatie: KIXS - Is voor informatievoorziening de natuurlijke partner voor de gehele krijgsmacht.
- Directoraat Generaal Beleid: HDBV - Maakt de besturing, organisatie en informatie van Defensie zo effectief en efficiënt mogelijk.
- Koninklijke Marine: MIC - Ondersteunt en introduceert vernieuwingen in de Koninklijke Marine.
- Koninklijke Marechaussee: MOTOR - Adopteren in een vroeg stadium van technologische ontwikkelingen en daarop anticiperen.
- Defensie Ondersteunings Commando: CS&I - Helpt DOSCO effectiever te maken in de uitvoering van haar kerntaak en biedt een veilige omgeving voor de ontwikkeling van nieuwe concepten.
- Innovative coaches - Is een intrinsiek gemotiveerd netwerk van coaches die mogelijkheden bieden om vraagstukken en ideeën om te zetten in implementeerbare oplossingen met behulp van design thinking.

Defensie en Innovatie

- Binnen defensie opereren verschillende innovatie afdelingen.
  - Elk met een eigen taak of aandachtsgebied.
  - Met elkaar verbonden in gezamenlijke projecten en kennisuitwisseling.
- Netwerk van innovatiecoaches.
  - Opleiding en training
  - Gebruiken design-thinking methodes om gezamenlijk naar innovatieve oplossingen te zoeken.
- Succesvolle innovatie door
  - interne samenwerking, en
  - externe samenwerking

5.6 BIJLAGE F Lijst van afkortingen

AI	Artificial Intelligence
ASD	AeroSpace and Defence Industries Association of Europe
BDSV	Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie
CLAS	Commando Landstrijdkrachten
CLSK	Commando Luchtstrijdkrachten
CDS	Commandant Der Strijdkrachten
CD&E	Concept Development & Experimentation
CMP	Commissariaat Militaire Productie
CBRN	Chemisch, biologisch, radiologisch of nucleair
DMO	Defensie Materieel Organisatie
DOSCO	Defensie Ondersteuningscommando
DGB	Directeur-Generaal Beleid
DIS2018	Defensie Industrie Strategie 2018
DMP	Defensie Materieel Projecten
DTC	Digital Trust Centre
EDF	Europese Defensie Fonds
EZK	Ministerie van Economische Zaken & klimaat
EDTIP	Europese Defensie Technologische en Industriële Basis
FRONT	Future Relevant Operations with Next Generation Technology & Thinking
HCSS	The Hague Centre for Strategic Studies
ICG EDS	Interdepartementale Coördinatie Groep Europese Defensie Samenwerking
IP	Industriële Participatie
IFV	Instituut Fysieke Veiligheid
J&V	Ministerie van Justitie en Veiligheid
LCW:	Logistiek Centrum Woensdrecht
MKB	Midden- en Klein Bedrijf
MLU	Midlife Update
MMIP	Meerjarige Missiegedreven Innovatie Programma's
NCSC	Nationaaal Cyber Security Centrum
NIDV	Stichting. Nederlandse Industrie voor Defensie en Veiligheid
NL-DVI :	Nederlandse Defensie- en Veiligheidsindustrie
NIVP	NIDV Informatie Voorzienings Platform
OEM	Original Equipment Manufacturers PCC : Precommerciële Consultaties
PESCO	Permanente Gestructureerde Samenwerking PDC : Politie Diensten Centrum
RAST-PRO	NIDV-Register ABDO Security Technology Providers
SME	Small and Medium Enterprises
VNO-NCW	Verbond Nederlandse Ondernemingen-Nederlands Christelijk Werkgeversverbond