Kennis- en innovatieagenda Veiligheid

"Samen organiseren, samen innoveren, één doel"

oktober 2019, finale versie

Topsector High Tech Systemen en Materialen, Team Dutch Digital Delta, Topsector Creatieve Industrie, Topsector Logistiek en Topsector Water & Maritiem

Inhoudspgave

Colofon

Aan de samenstelling van deze KIA Veiligheid is door velen over de gehele kennisketen een bijdrage geleverd. De organisatie van de uitvraag is gecoördineerd door een kernteam bestaande uit Jan Pieter Mook (min. J&V); Auke Venema en Juan Irausquin (min. Defensie); Mark Lengton, Koen de Pater en Katja Primozic (min. EZK); Leo Warmerdam (topsector HTSM); Bart Ahsman (topsector creatieve technologie); Fred Boekhorst (Dutch Digital Delta); Albert Veenstra (topsector Logistiek), Marnix Krikke (topsector Maritiem); Wiebe Brandsma (provincie Zuid Holland); Christiane Klöditz en Janneke van Kersen (NWO). De uitwerking van de MMIP's is geleid door coördinatoren (Tjarda Krabbendam en Egbert Jan Sol (TNO); Martijn Catz (Fronteer); Ubo Termote (Airbus DS) en diverse leden uit het kernteam), in stevig overleg met een breed eco-systeem aan deelnemers uit ministeries, lokale overheden, kennisinstellingen en bedrijfsleven. Hans van Vliet (TNO) heeft de redaktie van de KIA getrokken.

1 Voorwoord

De Nederlandse overheid heeft in het kader van het nieuwe missiegedreven topsectoren- en innovatiebeleid nadruk gelegd op vier maatschappelijke thema's: landbouw, water en voedsel; gezondheid en zorg; energietransitie en duurzaamheid; en veiligheid. Vijfentwintig missies zijn opgesteld door vakdepartementen in consultaties met vele partijen en topsectoren en vervolgens goedgekeurd in april 2019 door het kabinet. De topsectoren hebben deze missies verder uitgewerkt in vier thematische Kennis en Innovatie Agenda's (KIA's), uitmondend in Meerjarige Missiegedreven Innovatie Programma's (MMIP's). Uitvoering van de MMIP's in de vele vormen van publiek-private samenwerking draagt bij aan het bereiken van de gestelde missie-doelen, leidt tot het benutten van economische kansen voor grote en kleinere bedrijven, zowel in binnen- maar vooral ook in buitenland.

De voorliggende Kennis en Innovatie Agenda (KIA), opgesteld door betrokken topsectoren High Tech Systemen en Materialen, Creatieve Industrie, Logistiek, Water & Maritiem en Team Dutch Digital Delta, is een unicum voor het *security* domein. Het in gezamenlijkheid programmeren, uitvoeren en aanjagen van de kennisontwikkeling en innovatie zal versterkend werken voor brede sectoren en biedt grote kansen op meer maatschappelijke impact en grotere economische bedrijvigheid. Daarmee leveren we gezamenlijk tevens het bewijs van de succesfactoren van het topsectoren beleid.

Marc Hendrikse,

Boegbeeld topsector HTSM

2 Inleiding

"De economische kansen van de maatschappelijke uitdagingen en de ambitie om een vooraanstaande rol te spelen op een aantal sleuteltechnologieën zijn de centrale uitgangspunten in de vernieuwde topsectorenaanpak. (...) Door gezamenlijk missies te formuleren, maken we de kennisvraag expliciet en bevorderen we samenwerking en krachtenbundeling om maatschappelijke uitdagingen aan te pakken en economische kansen beter te benutten." (Kamerbrief over het Missiegedreven innovatiebeleid, 13 juli 2018)

Nederland moet voor zijn burgers een veilig land blijven om te wonen, te werken en te leven. Een veilige samenleving is niet vanzelfsprekend. Nederland staat de komende decennia voor complexe uitdagingen.[5] *Dat vraagt om een proactieve houding en een innovatieve aanpak om potentiële dreigingen tegen te gaan. Hierbij moeten we gebruikmaken van de nieuwste wetenschappelijke inzichten, (sleutel) technologieën en toepassingen en aandacht hebben voor ethische en maatschappelijke vragen, en fundamentele en structurele aspecten van veiligheidskwesties. In het veiligheidsdomein zal steeds een combinatie van nieuw technisch, digitaal, sociaal, maatschappelijk, juridische, gedragswetenschappelijke, organisatorisch, sociaalpsychologisch en (geo)politieke onderzoek nodig zijn. Dat kan als we intensief samenwerken tussen overheid*[6]*, bedrijfsleven*[7] *en kennisinstellingen*[8]*, ook op Europees niveau. Want dan kunnen we (potentiële) tegenstanders steeds een stap vóór blijven: "always ahead of the threat''.* (Missiedocument thema Veiligheid, maart 2019)

2.1 Missiegedreven innovatiebeleid

In juli 2018 heeft het kabinet een missiegedreven innovatiebeleid voor het nieuwe topsectorenbeleid vastgesteld. Veiligheid is een van de vier maatschappelijke thema's die daarin centraal staan, naast inzet op *sleuteltechnologieën* en *sleutelmethodologieën*. Een missiegedreven aanpak helpt om onderzoek en innovatie tijdig te richten op actuele en relevante onderwerpen. Doordat missies op elkaar bouwen, ontstaat meer coherentie en impact, en wordt versnippering van innovatie beperkt.

Binnen het thema Veiligheid zijn onder leiding van het Ministerie van Defensie en het Ministerie van Justitie en Veiligheid acht missies gedefinieerd[1], die vragen om (toegepaste) innovaties . Dit is gedaan in nauwe samenwerking met het Ministerie van Economische Zaken en Klimaat, de topsectoren, kennisinstellingen en het bedrijfsleven. De missies vergen de ontwikkeling van nieuwe kennis en innovaties die bijdragen aan een veiliger samenleving, een weerbaarder Nederland, én die economische kansen creëren, ook op de exportmarkt. De overkoepelende ambitie is (potentiële) tegenstanders steeds een stap vóór blijven: *"always ahead of the threat''* met slimme oplossingen in dienst van een veilige maatschappij.

Het thema Veiligheid is afgebakend tot *security*[2]. Ook binnen deze beperking heeft het thema een grote reikwijdte; uiteenlopend van het verdedigen tegen dreigingen van buiten, het voorkomen van georganiseerde criminaliteit, het beschermen van kritieke infrastructuren en digitale veiligheid tot veiligheid op straat. Hiervoor is het nodig gebruik te maken van de nieuwste wetenschappelijke

[1] https://www.topsectoren.nl/missiesvoordetoekomst/documenten/kamerstukken/2019/april/29-04-2019/missiedocument

[2] Cambridge Dictionary: protection of a person, building, organization, or country against threats such as crime or attacks by foreign countries. Het verzoek van het kabinet om omgevingsveiligheid te adresseren in de thematische KIA's is nog niet verwerkt in deze KIA Veiligheid. De topsectoren staan open voor overleg en uitwerking hiervan in het vervolgtrajekt.

inzichten, (sleutel)technologieën en toepassingen met aandacht voor ethische en maatschappelijke aspecten. Daarbij zullen vaak combinaties nodig zijn van meerdere kennisgebieden, zowel technologisch, sociaal-maatschappelijk als organisatorisch. Meerdere wetenschappelijke disciplines en topsectoren moeten hiervoor samenwerken. Doorpakken op het thema Veiligheid vergt dus nieuwe partnerschappen, tussen bedrijven en universiteiten als organisaties, maar ook persoonlijk: de digitale expert met de gedragswetenschapper, de composietenspecialist met de veiligheidsfunctionaris, de elektronisch ontwerper met de expert die nieuwe marineschepen ontwikkelt. Een uitdaging die onderzoekers en innovators graag aangaan, zoals blijkt uit de in dit document vastgelegde kennis- en innovatieagenda.

2.2 Van missies naar kennis- en innovatieagenda

De missies voor Veiligheid zijn in 2019, door hetzelfde samenwerkingsverband dat de missies heeft gedefinieerd, uitgewerkt naar de Kennis- en Innovatieagenda (KIA) Veiligheid. Hierbij hebben de betrokken topsectoren (Topsector High Tech Systemen en Materialen, Team Dutch Digital Delta, Topsector Creatieve Industrie, Topsector Logistiek en Topsector Maritiem) het voortouw. Er is intensief samengewerkt met alle betrokkenen: de eerder genoemde ministeries, bedrijven, waaronder MKB, brancheverenigingen, kennisinstellingen, NWO en regio's.

Een succesvol innovatiebeleid wordt gevoed door multidisciplinariteit en is in haar basis vraaggedreven. Maar daarnaast ook aanbodgedreven met oog voor fundamenteel onderzoek dat later en op dat moment nog onbedoeld tot innovaties leidt zoals bijvoorbeeld de sleuteltechnologieën laten zien. Deze KIA Veiligheid beschrijft de ambitie van de betrokken topsectoren om met samenhang een bijdrage te leveren aan essentiële innovaties en valorisatietrajecten voor de missies en daarmee bij te dragen aan het aanpakken van maatschappelijke opgaven op het gebied van Veiligheid als wel het verdienvermogen van Nederland. De kennis- en innovatieagenda is vastgelegd in de vorm van meerjarige missiegedreven innovatieprogramma's (MMIP's).

Een aantal van de missies vraagt een oplossingsrichting met een combinatie van technologische en sociale factoren. Onderzoek met multidisciplinariteit kan helpen om draagvlak te verzekeren voor innovatierichtingen. Daar komt bij dat veiligheid vaak een gedragscomponent heeft, en een veiliger gedrag van burgers en professionals bereikt moet worden niet alleen via regels en richtlijnen maar ook via psychologie en *nudging*.

Voor de betrokkenen is de opstelling van de KIA Veiligheid een eerste gelegenheid geweest om met de breedte en diversiteit van vijf topsectoren de uitdagingen van de ministeries van Defensie en Justitie en Veiligheid te adresseren. Voor een aantal missies beginnen we vanaf een pril samenwerkingsniveau. Voor andere missies maken we gebruik van innovatieketens die al geruime tijd bestaan.

In het kader van deze KIA zijn per missie teams samengesteld met vertegenwoordigers van bedrijfsleven, kennisinstellingen en ministeries. Deze teams hebben een analyse gemaakt van lopende PPS'en en hierop en op de doelen van de missie een voorstel gebouwd voor doorzetting dan wel versterking van de programmering. In deze analyse is nadrukkelijk onderscheid gemaakt tussen onderzoek, ontwikkeling, demonstratie en implementatie. Details zijn te vinden in hoofdstuk 2.

Deze KIA is vooral een eerste ijkpunt van de samenwerking tussen ministeries en topsectoren. Eén waarop alle betrokkenen graag verder bouwen om verdere uitdieping en verzwaring van de MMIP's te bereiken. In die zin is het missiegedreven innovatiebeleid rond het thema Veiligheid al te

verklaren als een succes: Uiterst relevante innovatieprogramma's gaan gecoördineerd worden en bijdragen aan het vervullen van de gestelde missies.

2.3 Bijdrage topsectoren

Deze kennis- en innovatieagenda maakt duidelijk *dat* en *wat* de topsectoren kunnen bijdragen aan veiligheid. En daarnaast *hoe* dat kan. De topsectoren vinden het een voorwaarde hier als collectief continuïteit aan te geven, samen met de ministeries. Ze willen blijven investeren in het gezamenlijk realiseren van de missies: samen organiseren, samen innoveren, één doel. De MMIP's richten zich op publiek-private samenwerking en staat open voor iedereen. Daarbij zetten we in op realisme én ambitie. Realisme vanuit werkelijk lopende innovatieprogramma's en ambitie vanuit de baanbrekende uitdagingen in de missies.

De betrokken topsectoren leveren multidisciplinaire bijdragen vanuit verschillende elkaar versterkende expertises:

- Met het ontwikkelen, produceren en exporteren van innovatieve producten is de Topsector Hightech Systemen en Materialen een essentiële motor en aanjager van de Nederlandse economie en een aanjager van technologische innovatie. Door krachtenbundeling tussen bedrijven, kennisinstellingen en overheid wordt in de Nederlandse hightechsector een cruciale bijdrage geleverd aan het oplossen van maatschappelijke uitdagingen.
- ICT en internet zijn in toenemende mate motoren voor innovatieve producten en diensten en daarmee voor economische groei. Vanuit de Nederlandse positie in de wereldtop van digitale economieën richt *Team Dutch Digital Delta* zich op het realiseren van gesynchroniseerde informatiesystemen waarin big data, interoperabiliteit, data fusie en artificiële intelligentie bijeengebracht worden. Zowel snelheid van het besluitvormingsproces als transparantie en uitlegbaarheid zijn kernaspecten van dergelijke genetwerkt systemen.
- De mensgerichte aanpak van de *Topsector Creatieve Industrie* zorgt voor een integrale aanpak waarin sociale normen en gedragsverandering in acht worden genomen als basis van een effectieve aanpak. Het betrekken van verschillende stakeholders (cocreatie en participatie) leidt tot *e*ffectiever innoveren. Methodisch ontwerpen via probleemgedreven innoveren middels een centrale vraagarticulatie vanuit de veiligheidsbehoefte van veiligheidsprofessionals én burgers geeft een voorsprong. Communicatie als wapen verhoogt het bewustzijn: handelingsperspectief en systeemverschuiving.
- De unieke manier waarop in de *Topsector Logistiek* naar de wereld gekeken wordt is het frame van de ketens en netwerken: het ontwerpen en inrichten van ketens en netwerken, de rol van verbindingen en knooppunten, en de manier waarop aansturing van processen mogelijk wordt door het verbinden van informatie, beslissingsondersteunende tools, en het inzicht en begrip van mensen. Met defensie wordt al volop samengewerkt in de logistiek: de logistiek van onderhoud en reparatie, en de logistiek van reserveonderdelen voor materieel.
- *TKI Maritiem* is breed en omvat scheepsbouwindustrie, offshore, zeevaart, zeehavens, (zee-) visserij, Koninklijke Marine, binnenvaart, jachtbouw, watersport, maritieme toeleveranciers, de waterbouwers, kennisinstellingen en opleidingsinstituten.

2.4 Leeswijzer

Hoofdstuk 3 van dit document presenteert het *Wat* van deze kennis- en innovatieagenda: de meerjarige missiegedreven innovatieprogramma's (MMIP's). Wat bieden de topsectoren om de door

de Ministeries van Defensie en Justitie en Veiligheid geformuleerde missies voor veiligheid te realiseren?

In hoofdstuk 3 nemen we de missie titels integraal over[3], en vanuit het perspectief van de topsectoren formuleren we de Meerjarige Missiegedreven InnovatieProgramma's (MMIP's).

Hoofdstuk 4 beschrijft het *Hoe* van deze kennis- en innovatieagenda: de uitvoering van de innovatieprogramma's. Hoe zorgen we samen voor het realiseren en laten landen van de kennis- en innovatie uit de agenda in het gehele ecosysteem van gebruikers, overheid, bedrijven en kennisinstellingen? Welke onderzoeksvragen moeten beantwoord worden om bijvoorbeeld marktcreatie en inbedding in regio's te kunnen realiseren?

In hoofdstuk 5 gaan we in op het vervolg en vatten we de MMIP's samen.

[3] Een uitgebreide beschrijving van de missies is te vinden op https://www.rijksoverheid.nl/documenten/publicaties/2019/04/26/missies

3 Meerjarige missiegedreven innovatieprogramma's

De Kennis- en Innovatieagenda Veiligheid bestaat uit acht Meerjarige missiegedreven innovatieprogramma's (MMIP's) die zijn gekoppeld aan de acht missies uit het Missiedocument Veiligheid van de Ministeries van Defensie, Justitie en Veiligheid en Economische Zaken en Klimaat van 26 april 2019. De MMIP's beschrijven de door 'missieteams' vanuit de betrokken topsectoren, in afstemming met de ministeries, uitgewerkte agenda voor kennis en innovatie als antwoord op de behoeften vanuit de desbetreffende missie.

Elk van de MMIP's bestaat uit een aantal deelprogramma's die focussen op een specifiek onderdeel voor kennis- en innovatie. Voor elk MMIP is in de volgende paragrafen een overzicht weergegeven van de activiteiten in de kennis- en innovatieagenda, onderscheiden naar de fasen onderzoek, ontwikkeling, demonstratie en implementatie.

Onderstaande tabel geeft een overzicht van de MMIP's en deelprogramma's gekoppeld aan de missies.

Tabel 3.1: Overzicht van de MMIP's en deelprogramma's in de KIA Veiligheid

Missies	**MMIP's en deelprogramma's**
1. Integrale aanpak van georganiseerde criminaliteit	MMIP 1: Integrale aanpak, digitaal gedragen, van interventies, tools en data • 1.1: Interventies en organisatie • 1.2: Real time digitale observatie en ondersteuning • 1.3: Bruikbare data en handelingsperspectief
2. Maritieme hightech voor een veilige zee	MMIP 2: Maritime security • 2.1: Smart kill-chains - Radar en geïntegreerde sensorsuites • 2.2: Smart operations • 2.3: Smart manning & automation • 2.4: Zero emission and survivable warships • 2.5: Smart design and maintenance • 2.6: Smart concepts
3. Veiligheid in en vanuit de ruimte	MMIP 3: Voor veiligheid in en vanuit de ruimte • 3.1: Robuuste plaatsbepaling- en tijdsynchronisatiesystemen • 3.2: Nationale situational awareness, surveillance & tracking capaciteit • 3.3: Grondgebonden situational awareness capaciteit • 3.4: Laser voor veilige communicatie en vergrote transmissiecapaciteit • 3.5: (Gedeeltelijk) eigen satellietcapaciteit met tijdige en veilige toegang
4. Cyberveiligheid	MMIP 4: Cyberveiligheid • 4.1: Bestrijden cybercrime • 4.2: Bevorderen ontwikkeling cybercompetenties • 4.3: Defensieve cybertechnologie • 4.4: Offensieve cybertechnologie • 4.5: Ketenweerbaarheid en governance
5. Genetwerkt optreden op land en vanuit de lucht	MMIP 5: Informatiegestuurd en genetwerkt optreden • 5.1: Innovatie in ontwerp en aansturing van netwerken • 5.2: Informatie als wapen • 5.3: Aansturing van genetwerkte logistieke operaties • 5.4: Counter DRAM (Drone, Rocket, Artillery & Mortar) • 5.5: Smart service logistics
6. Samen sneller innoveren voor een adaptieve krijgsmacht	MMIP 6: Innovaties voor een adaptieve krijgsmacht • 6.1: Toepassing van robots/autonome systemen/drones (RAS/RPAS) • 6.2: 3D-printen voor onderdelen, lokale bouw en materiaalontwikkeling • 6.3: Energiesystemen & circulariteit

7.	Data en intelligence	MMIP 7: Data en intelligence • 7.1: Privacy-bestendige informatiedeling • 7.2: Beslissingsondersteuning
8.	De veiligheids-professional	MMIP 8: Gekwalificeerde en gekwantificeerde veiligheidsprofessionals • 8.1: Qualified-self, Digitaal wapenen middels nieuwe (leer)methodes • 8.2: Quantified-self, Meetbare prestatie en vitaliteit van veiligheidsprofessionals • 8.3: Digitaal uitgerust - Waarneming en communicatie • 8.4: Reframing veiligheid

Samenhang MMIP's en deelprogramma's

De MMIP's en deelprogramma's staan niet los van elkaar. Onderliggende (sleutel)technologieën en -methodieken worden in verschillende deelprogramma's gebruikt. Hiermee versterken de MMIP's elkaar en richt de KIA Veiligheid zich op een coherente bijdrage aan de realisatie van de missies. De relatie tussen de MMIP's en sleuteltechnologieën wordt besproken in paragraaf 4.7.

3.1 Missie: Integrale aanpak van georganiseerde criminaliteit

Omschrijving missie[4]

In 2030 is het zicht op illegale activiteiten en geldstromen zodanig verhoogd dat georganiseerde criminaliteit riskant en slecht lonend is.

Waar gaat deze missie over

Georganiseerde ondermijnende criminaliteit is ontwrichtend voor de samenleving. De bestrijding van de vindingrijke en georganiseerde criminaliteit wordt effectiever als overheid, bedrijfsleven en burgers intensiever en gerichter samenwerken. Op basis hiervan kunnen innovatieve interventiemodellen ontstaan. De inzet van data-onderzoek om misdaadfenomenen en activiteiten in beeld te brengen is noodzakelijk. Uitdagingen zijn de mogelijkheden en beperkingen om bestaande data van publiek en private instanties te gebruiken en het binnen bestaande juridische kaders omzetten van deze data bij preventie, opsporing en vervolging.

Benodigde kennis en innovatie

De kennis- en innovatiebehoeften liggen op het gebied van 'zicht', 'inzicht' en 'interventie'. Zicht betreft sensoren en observatietechnieken voor (heimelijke) monitoring en detectie zowel in het fysieke als het digitale domein en mogelijk in lastige omstandigheden (in de nacht en bij slecht weer). Inzicht betreft het kunnen voorspellen van toekomstige ontwikkelingen. Met daarbij modellen voor het duiden van de effecten van mogelijke interventies. Hiervoor is het gewenst waarnemingen en databronnen van verschillende spelers - privacy-bestendig – te kunnen combineren en analyseren. Voor analyses is het gewenst ook psychologische gedragskunde toe te passen. Interventie betreft nieuwe modellen en inzichten voor het versterken van burgerparticipatie, het modelleren van de vermogens van de tegenstander, beïnvloedingsmogelijkheden (*nudging*) en het verhogen van de kwaliteit van verhoren.

[4] Een uitgebreide beschrijving van de missies is te vinden op https://www.rijksoverheid.nl/documenten/publicaties/2019/04/26/missies

The game has changed. Enerzijds vindt vermenging plaats van de fysieke en de digitale wereld, waar anderzijds ook de boven- en onderwereld steeds meer in elkaar overgaan. Dit resulteert in een (nieuwe) wereld waarin criminelen zich onzichtbaar wanen en door slim gebruik van anonieme tools (ten behoeve van cybercrime) en nieuwe businessmodellen (onder andere *counterfeit*; namaak van medicatie en elektronica) uit handen van de instanties weten te blijven. Het medicijn: zichtbaarheid. Door de digitale transformatie van criminaliteit vraagt deze missie om sterke aandacht voor het digitale domein. Om in de kennis- en innovatiebehoefte te voorzien geven we prioriteit aan digitaal gefaciliteerde samenwerkingen en de ontwikkeling van bruikbare digitale toepassingen. Digitale innovaties transformeren de manier waarop we leven en werken en kunnen bijdragen aan vreedzaam samenleven met door de maatschappij gedragen oplossingen. Zonder deze maatschappelijke betrokkenheid en medewerking is een overheidsaanpak - ook als deze eenduidiger en effectiever wordt georganiseerd - gedoemd te mislukken.

Voor het maken van een collectieve vuist is een effectieve integrale aanpak nodig die centraal geregisseerd is en, ondersteund door helder beleid, zowel landelijk als regionaal geïmplementeerd kan worden: een aanpak die zichtbaarheid van normafwijkend gedrag vergroot én met name voorkomt. Het reactieve én proactieve vermogen moeten omhoog. *(Deelprogramma 1 - Interventies en organisatie)*

Naast het 'verbinden van alle ogen' zullen deze ogen ook vooral veilig moeten kunnen worden ingezet. Collectief ontwikkelde digitale oplossingen (apps, krachtige sensoren, platforms) zullen real-time en privacy-*proof* en binnen de juiste juridische kaders moeten ondersteunen én voorspellen (wearables, implementatie in gebouwde omgeving) als de nieuwe olie voor deze integrale machine. *(Deelprogramma 2 - Real time digitale observatie en ondersteuning)*

Door met meer stakeholders en middels nieuwe modellen integraal op te treden is het van belang dat toepassingen zoals verzamelde en gecombineerde data altijd ten behoeve van de eindgebruiker zijn. Met gemakkelijk te implementeren en interpreteren data zal de informatiepositie ter bestrijding van criminaliteit versterkt worden en wordt de verschillende gebruikers handelingsperspectief geboden. *(Deelprogramma 3 - Bruikbare data en handelingsperspectief)*

3.1.1 MMIP: Integrale aanpak, digitaal gedragen, van interventies, tools en data

Dit MMIP heeft als doel de integrale aanpak van georganiseerde criminaliteit te versterken door de zichtbaarheid van normafwijkend gedrag en het reactieve én proactieve vermogen te vergroten Naast de collectieve inventarisatie en ontwikkeling van digitale oplossingen richt het MMIP zich op onderzoek naar de meest effectieve aanpak om data, ten dienste van de menselijke eindgebruiker, om te zetten in interventies.

Met de uitvoering van dit MMIP zijn bestrijders van criminaliteit beter in staat zicht en inzicht op georganiseerde criminaliteit te hebben en effectiever, ondersteund door passende wetgeving en procedures, te kunnen interveniëren. De capaciteiten worden versterkt foor digitaal gefaciliteerde samenwerkingen en bruikbare digitale toepassingen.

Deelprogramma 1: Interventies en organisatie

Onderdeel van dit deelprogramma is onderzoek naar de effectiviteit van integrale preventie mechanismen voor ondermijning. Hoe herkennen we signalen, hoe en welk handelingsperspectief kan worden geboden? Omdat een preventieve aanpak, in combinatie met het verhogen van de

aangiftebereidheid, positief effect heeft op de gestelde ambitie in de missie, zal parallel veldonderzoek gedaan worden naar binnen welke fases/domeinen van het aangifteproces, bijvoorbeeld door middel van *nudging* of *boosting*, gewenst gedrag kan worden gestimuleerd.

Om onderzoeksinzichten ook effectief te testen zullen samen met eindgebruikers verschillende digitale, laagdrempelige en schaalbare oplossingen, zoals digitale trainingen en simulaties, worden gevalideerd in branchespecifieke proeftuinen. Voor de implementatie zullen positief gevalideerde middelen worden ingezet als training en voorbereiding op de-escalatie.

Dit resulteert in verhoogd bewustzijn onder burgers, bedrijven, gemeenten en instanties en vergroot de herkenbaarheid van (nu nog) onzichtbare criminaliteit. Het collectief ontwikkeld handelingsperspectief zorgt daarnaast voor een krachtige top-down én bottom-up aanpak van veiligheid waarbij alle ogen verbonden zijn en het zelfreinigend vermogen wordt gestimuleerd.

Deelprogramma 2: Real time digitale observatie en ondersteuning

Om alle ogen real-time te kunnen verbinden dienen krachtige *digital sensing* oplossingen te worden ontwikkeld, in combinatie met de juiste kaderstellingen. Dit deelprogramma faciliteert deze innovatie door onderzoek naar gerichte privacy-*proof* digitale observatie en de ontwikkeling en demonstratie van nieuwe technologieën (oplossingen) voor het opsporings- en handhavingsdomein. Grootschalige observatie is namelijk duur, privacy gevoelig en beïnvloedt de persoonlijke leefsfeer.

Het programma zal worden versterkt met het opzetten van een consortium om gezamenlijk onderzoek te doen naar de huidige uitdagingen van heterogene informatie-fusie op basis van *deep learning* (*high risk, high gain*). Ten behoeve van een effectieve inzet van deze digitale middelen zullen heldere juridische kaders dienen te worden gedefinieerd. Voor de ontwikkeling hiervan zal een taskforce worden opgezet waar juristen, programmeurs en eindgebruikers samen zullen werken om vroeg in het proces ook niet-technologische randvoorwaarden (bijvoorbeeld privacy, intellectueel eigendom) mee te kunnen nemen in de techniekontwikkeling.

Omdat we pas aan de vooravond van *big data analytics* en *artificial intelligence* staan zal de implementatie van toekomstige geautomatiseerde analyses, voorspellingen en besluitvorming geleidelijk moeten worden onderzocht. Daarvoor is het van belang dat bestaande techniek wordt ingezet en nieuwe techniek wordt ontwikkeld waardoor deze automatische beslissingen altijd traceerbaar, *accountable* en *explainable* blijven. Maar dat vraagt ook om een aanpak van onderzoek, ontwikkeling en validatie in een proeftuin / living lab opzet.

Deelprogramma 3: Bruikbare data en handelingsperspectief

Techniek is de menselijke sensoren al voorbij. Om echter wel te kunnen blijven handelen op basis van data dient deze gemakkelijk geïnterpreteerd te kunnen worden. Dit deelprogramma doet onderzoek naar de meest effectieve manieren waarop data, ten dienste van de menselijke eindgebruiker, kan worden ingezet. Tevens zal een consortium worden samengesteld dat specifiek oplossingen ontwikkelt ten behoeve van beeldverwerking van sensoren, voor de generatie van lokale triggers.

Deelprogramma	Onderzoek	Ontwikkeling	Demonstratie	Implementatie
Interventies en organisatie	• Onderzoek naar effectieve integrale preventie mechanismen ondermijning o.a. t.b.v. schone branches	• Veldonderzoek naar effectiviteit nudging en boosting t.b.v. verhogen aangiftebereidheid	• Proeftuin voor validatie digitale middelen ter verhoging van integrale herkenning criminele signalen	• Introductie van een collectief en schaalbaar handelingsperspectief middels digitale communicatiemiddelen
Real time digitale observatie en ondersteuning	• Gerichte, privacy proof digitale observatie middels molest ongevoelige en tactisch gepositioneerde systemen (beeld, geluid, chemisch, etc. • Heterogene informatiefusie o.b.v. deep learning	• Verkenningen van technologieën voor het opsporings- en handhavingsdomein • Oplossing t.b.v. traceerbaarheid artificial intelligence en advanced data analytics • Zelflerende modellen van fenomenen en netwerken	• Prototyping en proof-of-concepts van technologieën (b.v. hennepgeluidscamera's) voor het opsporings en handhavingsdomein • Taskforce voor opstellen kaders (o.a. juridisch) t.b.v. digital sensing en technologie ontwikkeling • Zelflerende modellen ter ondersteuning van een dynamische ondermijningsmonitor	• …
Bruikbare data en handelings-perspectief	• (Veld) onderzoek naar gebruiksvriendelijke visualisatie en toepassing van data	• Consortium voor multi-sensor beeldverwerking om lokale triggers te kunnen genereren	• …	• …

3.2 Missie: Maritieme hightech voor een veilige zee

Omschrijving missie [5]

In 2035 beschikt Nederland over de marine voor de toekomst. Die beschermt de Nederlandse waarden en welvaart en geeft veilige toegang tot wereldwijde wateren. Zij heeft een antwoord op onvoorspelbare en onvoorstelbare ontwikkelingen in dreiging en technologie en vervult haar missies effectief, efficiënt en flexibel.

Waar gaat deze missie over

De toekomst van Nederland als maritieme handelsnatie is afhankelijk van een veilige zee. De zee is mondiale transportroute, bron van grondstoffen en voedsel en wingebied voor energie tegelijk. Dat maakt de zee en haar kustgebieden kwetsbaar voor competitie, concurrentie en conflicten. Door technologische, geopolitieke en mondiale ontwikkelingen staat de veiligheid op en vanuit zee onder druk. Voor een goed functionerende maritieme veiligheidsketen moeten de Koninklijke Marine en de Kustwacht op alle huidige en toekomstige veiligheidsuitdagingen een antwoord hebben. Een toekomstbestendig en concurrerend ecosysteem van overheid, kennisinstellingen en (maritieme) industrie is hiervoor essentieel.

Benodigde kennis- en innovatie

De kennis- en innovatiebehoeften liggen op het gebied van maritieme hightech, die bijdraagt aan de versterking van slimme operaties en concepten. Zoals met onbemande en autonome middelen, moderne sensoren, missiemanagementsystemen en effectoren. En slimme bemanningsconcepten, slim opwerken, slim onderhoud en materieelbeheer. Op het gebied van slim scheeps-en onderzeeboot ontwerp gaat het om *zero emission* marineschepen, overleefbaarheid, *safety design*, mitigatie voor CBRNe-dreigingen, weerbaarheid, *stealth*-eigenschappen en incasseringsvermogen, nieuwe materialen, lage hydrodynamische weerstand, schokbestendigheid en een zeer lage geluidssignatuur. En daarnaast om gedistribueerde intelligente distributiesystemen en signatuurmanagementsystemen. En tenslotte volledig nieuwe concepten voor de *'navy after next'*.

Het is voor een goed functionerende maritieme veiligheidsketen essentieel dat de Koninklijke Marine en de Kustwacht op alle huidige en toekomstige veiligheidsuitdagingen een antwoord moeten hebben. Daarvoor moeten ze kunnen beschikken over middelen die zijn opgewassen tegen de complexiteit en kracht van de moderne dreiging in die gebieden waar de dreiging zich voor doet. Om te kunnen voorzien in de daarvoor benodigde middelen is een toekomstbestendig en concurrerend ecosysteem van overheid, kennisinstellingen en (maritieme) industrie noodzakelijk.

De nieuwe middelen moeten allereerst effectief en robuust zijn tegen de nieuwe dreigingen die onze belangen kunnen schaden, zoals hypersone en ballistische missielen, lange afstand torpedo's, *swarming* Unmanned Surface Vehicles, etc. Ook moeten de middelen geschikt zijn om in alle denkbare omstandigheden te opereren, zowel in warmere als in koudere gebieden. Bovendien moet het risico van letsel voor de bemanning tot een minimum worden gereduceerd.

De hieronder beschreven onderzoeks- en innovatiegebieden zijn gekozen in discussierondes van industrie, kennisinstellingen en Defensie.

[5] Een uitgebreide beschrijving van de missies is te vinden op https://www.rijksoverheid.nl/documenten/publicaties/2019/04/26/missies

3.2.1 MMIP: Maritime security

Doelstelling van dit MMIP is invulling te geven aan de Defensie Industrie Strategie middels het opbouwen van een sterke basis van Nederlandse kennis en innovatie.

Uitvoering van dit MMIP biedt de Koninklijke Marine en de Kustwacht middelen om op alle huidige en toekomstige veiligheidsuitdagingen een antwoord te kunnen geven. Die middelen moeten zijn opgewassen tegen de complexiteit en kracht van de moderne dreiging in die gebieden waar de dreiging zich voor doet.

Deelprogramma 1: Smart kill-chains - Radar en geïntegreerde sensorsuites

De ambitie is om de schepen van de Koninklijke Marine geschikt te maken om ook de nieuwe dreigingen optimaal het hoofd te kunnen bieden. Daarvoor zijn toekomstbestendige en adaptieve sensoren, missie management systemen en effectoren benodigd. Deze systemen moeten zodanig flexibel zijn dat ze continu aangepast kunnen worden aan de veranderende dreigingen. Voor de ontwikkeling van nieuwe radars en geïntegreerde sensorsuites biedt de roadmap van Platform Nederland Radarland richting. De samenwerking in dit platform waarborgt een sterke kennis- en marktpositie van betrokken partijen en leidt tot unieke en onderscheidende radarproducten met spin-offs naar de civiele markt. Hierdoor kan Defensie over de modernste radar- en geïntegreerde sensorsuites ter wereld beschikken.

In de periode na 2030 moet rekening worden gehouden met een reële dreiging van ballistische *missiles* en andere dreigingen die veel sneller, wendbaarder, onvoorspelbaarder, onvoorstelbaarder en moeilijker te detecteren zijn dan de huidige dreigingen. Hoewel de potentie van de bestaande sensor- en wapencapaciteiten groot is ontbreekt in de periode na 2030 een operationele Integrated Air and Missele Defence (IAMD) capaciteit met simultaan AAW (Anti Air Warfare) en BMD (Ballistic Missile Defense). Dit MMIP beantwoord de wens van het Ministerie van Defensie om sensortechnologieontwikkelingen tijdig te starten en beschikbaar te hebben om een nationale IAMD ambitie na 2030 te kunnen realiseren.

Er zijn vier innovatiegebieden gedefinieerd, namelijk: concepten van radar en geïntegreerde sensorsuites; RF-*frontends*; sensorsignaalprocessing; life-cycle en kostenbeheersing. Wetenschappelijke en technologische doorbraken in dit MMIP zijn noodzakelijk om de gewenste technologische voorsprong en het gewenste TRL niveau rond 2030 te bereiken. Het programma “D-RACE – Advanced Radar Technology (D-ART)” adresseert een aantal van de onderwerpen van de onderzoekslijnen in de Roadmap “Radar en Geïntegreerde Sensorsuites 2030”. D-ART beoogt voor deze onderwerpen een impuls te creëren in de kennisopbouw die een zeer sterk multidisciplinair karakter heeft en gerelateerd is aan vakgebieden als systeem- en architectuurconcepten, RF front-end technologie en algoritmiek. D-ART beoogt een “kickstart” om een technologiedoorbraak te bewerkstelligen als opvolger van de Active Electronic Scanning Antenna technologie wat tot een paradigmaverschuiving moet leiden op radargebied.

Deelprogramma 2: Smart operations

Het is de wens om onder, op en boven water een aantal taken van het schip zelfstandig en deels autonoom te laten uitvoeren door onbemande systemen. De komende jaren zal de Koninklijke

Marine in toenemende mate gebruik maken van onbemande systemen, met als katalysator de introductie van de nieuwe mijnenbestrijdingscapaciteit. De ambitie is om de komende jaren geleidelijk functionaliteit toe te voegen aan de onbemande systemen.

Kennis en innovatievragen zijn: Welke technologie voor zelfstandig en autonoom optreden moet verder ontwikkeld worden, aansluitend op ontwikkelingen in het civiel maritieme domein, bijvoorbeeld op de gebieden autonoom varen en drone technologie voor survey. Welke procedures, doctrines en tactieken zijn nodig voor de inzet van onbemande en autonome middelen in *stand-off/swarming* operaties.

Deelprogramma 3: Smart manning & automation

Het deelprogramma Smart Manning & Automation wordt gedreven door de afname van de bemanningsomvang en de technische kennis aan boord van schepen van de Koninklijke Marine, terwijl de variëteit en complexiteit van de taken toeneemt. Daarnaast is er een grote druk op terugdringen van *life cycle* kosten. Daardoor is er een noodzaak om remote diensten te versterken en functies aan boord vergaand te automatiseren en te robotiseren in een missiegerichte architectuur van adaptieve systemen, ruimtelijk en functioneel geïntegreerd. Er zal ook grotere vraag komen naar ontwikkeling van simulatorfaciliteiten aan de wal (voor opleiding, training, opwerking en missie voorbereiding), maar ook aan boord (met behulp van VR en AR), zodat de schepen zich kunnen richten op hun primaire taken. Het is de wens van de KM om een architectuur beschikbaar te krijgen die de bestaande *stovepipe*-systemen (zoals het Combat Management System, Bridge Management System en het Platform Management System) integreert en alle informatie aan boord van het schip beter toegankelijk maakt.

Kennis- en innovatievragen: Hoe wordt de informatie over de scheepstoestand en de omgeving van het schip beter toegankelijk voor de bemanning. Wat zijn de drempels voor integreren van uiteenlopende monitoring, Command & Control systemen en hoe kunnen die geslecht worden. Op welke wijze kan de walorganisatie een beeld opbouwen en ingezet worden voor advisering. Hoe kunnen dynamische mens – machine teams gevormd worden en welke eisen stelt dat aan de automatisering en opleiding/training.

Deelprogramma 4: Zero emision and survivable warships

Het deelprogramma *zero emission and survivable warships* gaat uit van de doelen voor emissiereductie in de Defensie Energie- en Omgevingsstrategie (DEOS) 2019. Daarnaast kan de inzet van nieuwe voorstuwingstechnologie significante signatuurreducties (akoestisch, thermisch) opleveren, wat een groot effect heeft op de toekomstige overleefbaarheid van marineschepen. Nieuwe wapentechnologie (zoals lasers) vragen op korte termijn zeer hoge vermogens. Dit vraagt een andere aanpak van de energie distributie. Ook leveren energie gedistribueerde systemen met autonome capaciteiten verlaging van de kwetsbaarheid. Systemen kunnen ook na schade blijven werken doordat intelligentie en energievoorziening gedistribueerd is opgezet.

Kennis- en innovatievragen: Welke alternatieve brandstoffen zijn beschikbaar (of kunnen worden ontwikkeld) om de vermindering van emissies en de onafhankelijkheid van fossiele brandstoffen te bereiken? Welke weerstandsreductie methoden en voortstuwingsystemen kunnen worden ontwikkeld, bv door de inzet van *biomimitics*? Welke energieopslag (zoals batterijen en supercondensatoren), energie omzettingssystemen (zoals brandstofcellen en aangepaste

brandstofmotoren), emissiereductiemethoden, nieuwe (hybride) voortstuwingsconfiguraties kunnen worden ontwikkeld, gekoppeld met de scheepshydrodynamica (*hydro-systems integration*) en geïntegreerd in het totale scheepssysteem? Hoe kunnen signaturen worden verminderd gezien de ontwikkelde nieuwe sensortechnieken. Op welke wijze kan de informatie over de actuele status van de signaturen verkregen worden. Hoe kan die informatie gebruikt worden voor het geven van operationele adviezen en uiteindelijk autonome opvolging daarvan in war-time en *peace-time* mode. Is onafhankelijke, gerichte lokale en duurzame energievoorziening en koeling haalbaar. Is onafhankelijke, gerichte, betrouwbare en veilige draadloze data uitwisseling haalbaar in schepen? Hoe kunnen Smart Survivability sensoren verplaatst worden naar de constructie en zelfvoorzienend gemaakt worden.

Deelprogramma 5: Smart design and maintenance

In het deelprogramma *Smart design and maintenance* is de eerste ambitie om in het ontwerpstadium een *digital twin* beschikbaar te kunnen krijgen om specificaties te verifiëren en voor de ontwikkeling van operationele- en bemanningsconcepten. Het niveau van de modellen wordt gedurende de bouw en operationele inzet verrijkt zodat het inzetbaar is voor familiariseren, opleiden, opwerken, trainen en missie voorbereiding (en het bevorderen team skills). De digital twin modellen kunnen eveneens worden ingezet voor technisch-logistieke optimalisatie en voor advisering van bemanningen aan boord, gebruik maken van mogelijkheden van de nieuwste Virtual Reality (VR) en Augmented Reality (AR) technieken. Modelling & Simulation door simulatie is het concept van de toekomst. Het brengt flexibiliteit, tactische voorsprong en kostenbeheersing onder handbereik. De ambitie op het gebied van smart maintenance is om te komen tot een zero maintenance concept op meerdere tijdschalen voor schepen en voor systemen die langere tijd autonoom opereren. Het onderhoud tijdens missies moet geëlimineerd worden zodat de bemanning zich kan richten op haar primaire taken. Dat vraagt om een uitbreiding van de Maritime Support Centre aan de wal, die paraat moet zijn voor advisering van de schepen over onderhoudsvraagstukken.

Kennis- en innovatievragen: Hoe creëren we een betrouwbare Modelling & Simulation omgeving voor complexe maritieme operaties op zee. Hoe koppelen we deze omgeving aan het gedrag van de bemanning. Hoe zetten we deze omgeving effectief in voor conceptontwikkeling, ontwerp, opleiding, training, opwerking en missie voorbereiding. Wat zijn de implicaties zijn van een *zero maintenance* concept op meerdere tijdschalen voor schepen en voor systemen die langere tijd autonoom opereren. Hoe kunnen *remote asset management*, robotisering, nanotechnologie en 3D-printing bijdragen aan het zero maintenance concept. Hoe zou een Maritime Support Centre ingericht moeten worden.

Deelprogramma 6: Smart concepts

Om de dreiging op zee altijd vooruit te zijn, moet de marine van de toekomst een antwoord hebben op onvoorspelbare en onvoorstelbare ontwikkelingen in dreiging en technologie. De vereist de ontwikkeling van volledig nieuwe concepten en operaties voor de *'navy after next'* op basis van Risicodragend Verkennend Onderzoek.

Kennis- en innovatievragen: Hoe bepalen we de toekomstige technologische dreigingen bij potentiële vijanden en hoe reageren we daarop? Welke nieuwe technologische ontwikkelingen zijn er en welke mogelijkheden bieden die om onze eigen slagkracht en overleefbaarheid te verhogen?

Deelprogramma	Onderzoek	Ontwikkeling	Demonstratie	Implementatie
Smart kill-chains - Radar en geïntegreerde sensorsuites	• Meerjarenprogramma D-RACE Advanced Radar Technology (D-ART), TRL 1-3, 2019-2024	• Een breed scala van gerichte nationale en internationale studieopdrachten in diverse consortia om TRL niveau stapsgewijs te verhogen naar TRL4. Periode 2019 - 2027	• Functionele demonstratie van AAW en BMD mogelijkheden m.b.v. een Evolution Design Model, periode 2025-2027, TRL 5 • Demonstratie van paradigmaverschuiving m.b.v. een technologiegedreven Evolution Design Model, periode 2028-2030, TRL 5	• Productontwikkeling, TRL>5
Smart operations	• Methoden voor bepaling operationele mogelijkheden en beperkingen van inzet onbemande systemen • Bepalen van behoefte aan informatie en van daaruit voortkomende eisen aan data en datafusie • Bepalen van de beste mix aan middelen in een toolbox	• Technologie voor onbemande en autonome systemen mede ontwikkelen en beoordelen • Datafusie en omzetten naar informatie voor toepassings-mogelijkheden met oplopende complexiteit • Ontwikkeling simulatie- en Kunstmatige Intelligentie technieken voor boven- en onderwaterautonomie	• Beproevingen uitvoeren en opdoen operationele ervaring met state of the art unmanned systemen op zee	• Als eerste stap implementeren van aangekochte systemen op een mijnenbestrijdingsvaartuig
Smart manning & automation	• Het onderzoeken van mogelijkheden voor vorming van dynamische mens – machine teams • Het bepalen van de behoefte aan data en informatie • Het ontwikkelen van autonome functionele ketens	• Het aanpassen van de bedrijfsvoering aan steeds verder gaande automatisering en autonomisering • Geleidelijke integratie van Command & Control, platform en communicatie-systemen • Ontwikkeling van simulator, VR en AR systemen; Real time inzicht in herstelprioriteiten • Ontwikkeling van remote diensten vanaf de wal	• Aantonen van mogelijkheden en beperkingen van simulatorfaciliteiten aan de wal l • Uittesten van datastandaardisatie en koppeling van systemen	• Integratie van brug – en platform monitoring en control systemen op nieuwe schepen
Zero emission and survivable warships	• Relatie tussen vermindering van emissies en van signaturen • Onderzoek aan energieopslag, energie omzettingssystemen en emissiereductiemethoden	• Analyse van alternatieve en synthetische brandstoffen (zoals Methanol, Ammonia en Waterstof) en de daarbij horende risico's (zoals tijdens Bevoorraden op Zee)	• Uittesten van oplossingen en bepaling risico's van nieuwe concepten in een simulatieomgeving • Het testen van deeloplossingen voor gedistribueerde	• Vervanging Van Kinsbergen en havensleepboten bieden kansen voor eerste toepassing emissieloze voortstuwing • Het verwerken van gedistribueerde systemen

	• Ontwikkeling van nieuwe weerstandsreductie en voortstuwingstechnieken (o.a. biomimitics) • Dynamisch gedrag van energiesystemen die gebruik maken van duurzame brandstoffen en systemen voor opslag van energie • Het onderzoeken van de mogelijkheden voor on-board actuele informatie over de status van alle signaturen • Het onderzoeken van mogelijkheden voor autonome opvolging van adviezen op het gebied van signatuurreductie • Relatie tussen vermindering van emissies en van signaturen	• Ontwikkeling van simulatie en testopstellingen voor nieuwe energieopslag, energie omzettingssystemen en emissiereductiemethoden (zoals de motorenopstelling bij het KIM en het Zero Emission Lab bij MARIN) • Het verder ontwikkelen van een monitoring en adviessysteem voor de status van geselecteerde signaturen • Verlagen van signaturen gezien de ontwikkelingen van nieuwe sensoren	systemen voor voeding en koeling	in de vervanger M-fregatten
Smart design and maintenance	• Ontwikkeling van simulatie en VR/AR technieken om tot een betrouwbare virtuele Modelling & Simulation omgeving te komen • Human factoronderzoek naar vergaand verschuiven van trainingen en opwerken naar de wal • Nagaan wat de implicaties zijn van een zero maintenance concept op meerdere tijdschalen voor schepen en voor systemen die langere tijd autonoom opereren	• Opwerkfaciliteit op de wal waarbij de interne battle en externe battle integraal worden getraind • Gebruik simulaties, simulatoren en VR/AR ten behoeve van smart (concept) design • Inventariseren en selecteren van geschikte health en monitoring technieken • Opzetten van een infrastructuur voor veilige opslag en transfer van data	• Uittesten van VR/ AR technieken voor platformontwerp • Uittesten van deelmodellen die tijdens ontwerpontwikkeld zijn in de operationele fase • Op deelgebieden demonstreren van maintenance op afstand	• Opzetten en ingebruikname van simulatie- en simulator omgevingen zoals het TNO Internal Battle Lab en de MARIN Seven Ocean Simulator • Opzetten van een Maritime Support Centre voor integrale logistieke, technische en operationele begeleiding van de schepen
Smart concepts	• 'Technology watch' van zich ontwikkelende technieken. • Eigen (fundamenteel) onderzoek naar nieuwe technologieën	• Ontwikkeling van vroege innovaties (laag TRL) op basis van nieuwe technieken of innovatief gebruik van bestaande technieken (Risicodragend Verkennend Onderzoek)	• Demonstraties van nieuw ontwikkelde technieken door bedrijven, startups en kennisinstellingen, bij voorbeeld in CODEMO-regeling	• Toepassing nieuwe technieken aan boord in pilots

3.3 Missie: Veiligheid in en vanuit de ruimte

Omschrijving missie [6]

In 2030 heeft Nederland een operationeel inzetbare ruimtevaartcapaciteit voor Defensie en Veiligheid. Ruimtevaartcapaciteit omvat in deze definitie zowel satellieten, infrastructuur op de grond als de mogelijkheid van informatieverwerking.

Waar gaat deze missie over

Met een operationele ruimtevaartcapaciteit kunnen we een essentiële bijdrage aan de veiligheid leveren door: het beschermen van de kritische ruimtevaartinfrastructuur, het optimaal benutten van satelliettoepassingen voor observatie en veilige communicatie en het beschermen tegen dreigingen uit de ruimte. Unieke voordelen van satellieten zijn dat ze kunnen waarnemen zonder de soevereiniteit van een land te schenden en in korte tijd grote oppervlakten kunnen verwerken. Om uit alle satellietinformatie op tijd de juiste conclusies te kunnen trekken, dient het informatieverwerkingsproces (*downstream*) goed ontwikkeld te worden. Tevens dient de infrastructuur robuust genoeg te zijn tegen natuurlijke en vijandelijke dreigingen.

Benodigde kennis- en innovatie

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)). Kennisintensieve technologieontwikkeling voor geminiaturiseerde systemen t.b.v. satellieten en constellaties, voor specifieke ruimtesensoren (thermisch, optisch, radar, laser) als ook een operationele capabiliteit voor SSA, voor elementen van secure laser end–to-end communicatiesystemen en de integratie met radiocommunicatie sluiten nauw aan op de missie. Nieuwe ontwikkelingen en toepassingen voorzien in het geautomatiseerd, actueel, accuraat en betrouwbaar integreren, interpreteren en het veilig communiceren van datastromen en/of daaruit ontsloten informatie voor de operationele inzet.

De kennisvragen en deelprogramma's die aan de orde komen sluiten nauw aan op bovenstaande constatering. De innovatieve kracht van de sector wordt door deze vragen uitgedaagd. Het MMIP 'Veiligheid in en vanuit de ruimte' bevat een vijftal deelprogramma's die hieronder worden toegelicht. Te weten: Robuuste plaatsbepaling- en tijdsynchronisatiesystemen, Nationale Situational Awareness, Surveillance & Tracking capaciteit, Grondgebonden Situational Awareness capaciteit, Laser voor veilige (satelliet) communicatie en grotere datatransmissie capaciteit en Unieke, (gedeeltelijk) eigen satellietcapaciteit met tijdige en veilige toegang.

3.3.1 MMIP: Voor veiligheid in en vanuit de ruimte

Dit MMIP heeft als doel het ontwikkelen van systemen voor observatie ten behoeve van vergrote *situational awareness* en veilige communicatie via satellieten. Dit zowel voor systemen in de ruimte als grondgebonden systemen.

Met de uitvoering van dit MMIP wordt bereikt dat Nederland beschikt over faciliteiten voor observatie en communicatie vanuit de ruimte ten behoeve van defensie en veiligheid.

[6] Een uitgebreide beschrijving van de missies is te vinden op https://www.rijksoverheid.nl/documenten/publicaties/2019/04/26/missies

Deelprogramma 1: Robuuste plaatsbepaling- en tijdsynchronisatiesystemen

Dit deelprogramma voorziet in een gestructureerde aanpak om tot gevalideerde, accurate en betrouwbare tijd- en positie informatie te komen via nationale ontwikkeling tot een robuuste PNT oplossing. De ambitie is dat Nederland uiterlijk in 2030 beschikt over een Robuuste Nationale PNT Oplossing. De komst en doorontwikkeling van Global Navigation Satellite Systemen ("GNSS") zoals het Europese Galileo systeem en het Amerikaanse Global Positioning System ("GPS") hebben eraan bijgedragen dat onze maatschappij zich heeft kunnen ontwikkelen tot onze huidige *'smart economy'*. Dit heeft ook een keerzijde. We zijn ongemerkt in grote mate afhankelijk geworden van de accurate tijd en hoge positienauwkeurigheid waarin deze systemen voorzien. Het geheel van deze systemen en technologie noemen wij hier Positie, Navigatie en Timing ("PNT"). Verwezen wordt naar het I&M rapport Inventarisatie Kwetsbaarheid Uitval Satellietnavigatie van 11 maart 2016 (het "IKUS Rapport") waarin deze afhankelijkheid wordt bevestigd. Het rapport treft alle sectoren en vitale infrastructuren. Een citaat uit het publieke deel van het IKUS Rapport (blz 26 en 27): "Uit het IKUS onderzoek komt naar voren dat het gebruik van GNSS-technologie door de digitalisering van de samenleving verder is toegenomen. De kwetsbaarheid van gebruikers voor GNSS-uitval is daardoor ook toegenomen. Deze wil tot samenwerking (red: tussen sectoren) en inzicht in elkaars kwetsbaarheid is relevant voor het ondervangen van een gesignaleerde systeemkwetsbaarheid rond GNSS. " Een belangrijk deel van het IKUS Rapport is geclassificeerd wat benadrukt dat deze afhankelijkheid van GNSS technologie een fundamentele kwetsbaarheid is voor onze samenleving. PNT moet dan ook beschouwd worden als een kritisch "nutsproduct" met de onderliggende technologieën als strategische sleuteltechnologie. Opbouw en onderhoud van nationale PNT kennis en technologie is dan ook noodzakelijk om de stabiliteit en veiligheid van de Nederlandse samenleving te kunnen blijven garanderen. Een Robuuste Nationale PNT oplossing kan worden gerealiseerd door het gebruik van verschillende (van elkaar) onafhankelijke PNT-technologieën waardoor men zeker weet dat derden hier geen (of nauwelijks) misleidende invloed op uit kunnen oefenen. De technologieën die hiervoor in aanmerking komen zijn inzichtelijk gemaakt in onderstaand MMIP tijdschema. De meest basale vorm is een geïntegreerde oplossing van een traagheidsnavigatiesysteem (INS) en een door encryptie beschermd satelliet navigatiesysteem zoals Galileo PRS. Afhankelijk van de functionele behoefte kan en moet het systeem robuuster gemaakt worden door het gebruik van meer verschillende technologieën.

Deelprogramma 2: Nationale situational awareness, surveillance & tracking capaciteit

De ambitie is de ontwikkeling en bouw van een nationale, operationele Space Situational Awareness (SSA) faciliteit met eigen sensoren. Het nationaal kunnen beschikken over dergelijke middelen, maakt het mogelijk om deel te nemen aan globale SSA-netwerken, waardoor een betere maar ook een gewenste informatiepositie ontstaat. Internationaal is erkend dat SSA een essentiële capaciteit is om de veiligheid in de ruimte en de huidige levensstandaard te waarborgen. SSA kan onderverdeeld worden in Space Surveillance and Tracking (SST) en Space Weather (SPWX), waarbij SST zich richt op het in kaart brengen van alle objecten in het ruimtedomein en SPWX de effecten van de zon beschrijft. Nederland beschikt over de juiste industriële en kennisinfrastructuur op basis waarvan Defensie internationaal een vooraanstaande rol kan spelen op gebied van SSA.

Onze vitale infrastructuur is steeds meer afhankelijk geworden van satellietsystemen: Wat gebeurt er als deze systemen worden bedreigd? Het onvoorstelbare antwoord is dat kritische infrastructuur

zoals b.v. water- en gasdistributie uitvallen, elektriciteitsvoorzieningen ontregeld raken, dat communicatienetwerken uitvallen en, in het kort, ons dagelijkse leven drastisch wordt ontregeld. Het wordt breed onderkend dat dergelijke bedreigingen steeds reëler worden; steeds meer landen beschikken over de daarvoor benodigde middelen. De bedreigingen kunnen bewust geïnitieerd zijn door een tegenstander, zoals het opzettelijk uitschakelen of storen van onze eigen satellieten of satellietverbindingen of bewust veranderen van hun satellietbanen t.b.v., specifieke militaire activiteiten tegen ons vanuit de ruimte, maar ook onvoorspelbaar, zoals het botsen van satellieten die in elkaars baan komen, uitbarstingen van de zon, of het terugvallen van ruimteobjecten naar en op de aarde.

Investeringen in SSA zullen leiden tot een belangrijke operationele capaciteit en opbouw van een vooraanstaande internationale kennispositie voor Nederland. Dit biedt verder ook belangrijke kansen om de exportpositie op het gebied van lange afstandsradar verder uit te bouwen en op de gebieden van *space weather* en Satellite Laser Ranging & Imagery Optical Ground Station een plaats in te nemen. Tot slot kan via deze Nederlandse capaciteit, samenwerking worden opgezet met andere Europese en NATO landen om te komen tot een SSA netwerk. Een eerste basis voor dit soort samenwerkingen is al gelegd door een SSA Sharing Agreement met USSTRATCOM en met het German Space Situational Awareness Center.

Deelprogramma 3: Grondgebonden situational awareness capaciteit

De ambitie behelst de ontwikkeling, validatie, bouw en operatie –via publiek-private samenwerking – van een Sensordata Intelligence Capaciteit. Een veelzijdige, op satelliet data gebaseerde informatiedienst die de actoren in het civiele en militaire veiligheidsdomein periodiek en proactief kan informeren over veiligheidsrisico's en kan ondersteunen bij de uitvoering van haar activiteiten. Operationele benutting van de enorme ontwikkeling van het ruimtesegment en de toepassing van kunstmatige intelligentie vormen de technologische basis van deze Sensordata Intelligence Capaciteit. In onze samenleving worden vitale infrastructuren en kritische, op ruimtevaart gebaseerde, diensten steeds vaker blootgesteld aan risico's van buitenaf. Het voorkomen en beheersen van rampen en incidenten vraagt om monitoringssystemen die door de inzet van satelliet- en ruimtevaarttechnologie in staat zijn risico- en bedreigings-niveaus frequenter en nauwkeuriger in kaart te brengen om de betrokken overheidsinstanties vroegtijdig te kunnen alarmeren en te informeren. Voor het veiligheidsdomein geldt dat Defensie en Justitie en Veiligheid bij het uitvoeren van taken steeds meer informatie gestuurd in plaats van activiteiten gestuurd optreedt, waarbij het snel kunnen beschikken over de juiste informatie over nationaal en grensoverschrijdend activiteiten essentieel is om onze nationale belangen te beschermen en conflicten te de-escaleren: *'always ahead of the threat'*.

De potentie van bestaande en toekomstige satellietsystemen voor grondgebonden Situational Awareness, surveillance en tracking is groot. De waarnemingsfrequentie neemt sterk toe met een steeds groter aantal geplande satelliet missies. Tegelijkertijd neemt de kwaliteit van waarneming toe met de ontwikkeling van nieuwe ruimtesensoren en innovatieve dataverwerkingstechnologie. Daarbij zullen door de sterke ontwikkelingen op het gebied van kunstmatige intelligentie en computerkracht belangrijke stappen worden gezet in de snelle vertaling van al deze data naar bruikbare en tijdige ofwel *actionable* informatie. Kortom een systeem waarmee satellietdata in combinatie met andere data – zoals in-situ sensoren en sociale media – en in combinatie met analyse tools en modellen, worden verwerkt tot informatie waarmee specifieke activiteiten kunnen

worden gedetecteerd, geclassificeerd en voorspeld ter ondersteuning van de veiligheidscyclus: “preparation, prevention, response and recovery”.

Deelprogramma 4: Laser voor veilige communicatie en vergrote transmissiecapaciteit

De doelstelling is de integratie van Secure Space-based Laser Communication capaciteit in nationale strategische en tactische communicatie-infrastructuur. De behoefte aan veilige communicatie infrastructuur is groot. Hoge datastromen voortkomend uit sensoren op satellieten, onbemande en bemande vliegtuigen, op land en zee vragen om steeds meer bandbreedte. Daarnaast is er een groot belang deze informatie op veilige wijze te kunnen delen binnen de betrokken overheidsorganisaties binnen het veiligheidsdomein. Of het nu om *situational awareness*, genetwerkt optreden, de commando keten gaat, gebruikers moeten kunnen vertrouwen op veilige en op behoefte toegespitste communicatie infrastructuur. De vraag naar datatransport / bandbreedte groeit veel sneller dan het beschikbare spectrum (radiogolven) toelaat.

Voor defensie en veiligheid is het van belang om veilige communicatie op orde te hebben. Het ruimtedomein zal daarin een vooraanstaande rol spelen. Space-based laser communicatiesystemen zullen gaan bijdragen aan verhoogde veiligheid in communicatie door bemoeilijking van signaal onderschepping, optimaal gebruik van encryptie op basis van Quantum Key Distribution (QKD) en grote toename van de datacapaciteit. Ook door haar onafhankelijkheid van RF spectrum allocatie vormt het een oplossing voor snel inzetbare, veilige communicatie. Op alle kerngebieden van laser communicatie vindt in Nederland kennisintensieve technologie ontwikkeling plaats die zullen bijdragen aan de realisatie van militaire laser communicatie en aan de integratie daarvan door defensie in een hybride communicatie infrastructuur. De Nederlandse Kennisinstituten en industrie zijn bij uitstek gepositioneerd om internationaal een vooraanstaande rol te spelen in de *supply chain* maar ook in de integratie van optische communicatie in de bestaande netwerken van de (nationale) gebruikers.

Deelprogramma 5: (Gedeeltelijk) eigen satellietcapaciteit met tijdige en veilige toegang

Dit deelprogramma heeft ten doel dat Nederlandse marktpartijen de capabiliteit ontwikkelen om op basis van experimentele *in-orbit* demonstrators en pilotprojecten een operationele capaciteit in de ruimte kunnen leveren én doormiddel van continue innovaties aanvullende niches in te vullen die de nationale inlichtingenpositie structureel versterken.

De ruimte als *ultimate high ground* met vrije vlucht over de gehele aarde, biedt unieke mogelijkheden. Militaire en humanitaire missies in conflictsituaties vragen om informatiedominantie en Situational Awareness, zowel op de grond als in de ruimte, om doelgericht en zo veilig mogelijk uitgevoerd te worden. Er zijn al veel verschillende diensten beschikbaar vanuit de ruimte, maar Nederland heeft niet overal toegang toe. Nederland loopt voorop in de ontwikkeling van kleine satellieten en hightech, geminiaturiseerde sensoren. De industriële, institutionele en academische positie van Nederland is heel goed om genetwerkte satellietconstellaties voor Defensie en Veiligheid verder te ontwikkelen. Wat voorheen kostentechnisch niet haalbaar was, wordt dat nu wel, namelijk het verkrijgen van (deels) eigen, onafhankelijke, ruimtevaartcapaciteit om de inlichtingenpositie te versterken.

Deelprogramma	Onderzoek	Ontwikkeling	Demonstratie	Implementatie
Robuuste plaatsbepaling- en tijdsynchronisatie-systemen	• Opbouwen van kennis en specificatie van een geïntegreerde, robuuste PNT-oplossing bestaande uit een mix van de volgende componenten / technologieën: ○ GNSS inclusief Galileo PRS ○ Sensorfusie ○ Omgevingsherkenning ○ Traagheidsnavigatie ○ Radionavigatie (niet GNSS) ○ Tijd transfer ○ Slimme antennes • Evaluatie van kwaliteit en kwetsbaarheid huidige systemen	• Ontwikkelen van: ○ Nationale Galileo PRS ontvanger technologie ○ Database Matching technologie voor omgevingsherkenning ○ Sensor fusie integratie algoritmes ○ PNT monitoring systeem • Verbeteren van: ○ traagheidsnavigatie ○ time transfer ○ antenne technologie	• Prototype Galileo PRS ontvanger component • Prototype geïntegreerde robuuste PNT oplossing • Overzicht PNT betrouwbaarheid in NL	• Toepassingsgerichte integratie van de eerder ontwikkelde PNT componenten met de juiste balans van robuustheid, betrouwbaarheid en nauwkeurigheid per toepassing
Nationale situational awareness, surveillance & tracking capaciteit	• Fundamenteel onderzoek naar architectuur controle en datacentrum, hardware concepten voor sensoren en software algoritmes voor tracking, detectie, classificatie en fusie van data	• Ontwikkeltrajecten die haalbaarheid van de kritische elementen aantonen: ○ Laser/radar tracking sensors ○ Specifieke detectie- en trackingtechnieken ○ Imaging- en classificatie-technieken ○ Interfacingtechnieken met andere internationale SSA databases en/of faciliteiten ○ Automatische detectie interpretatie en alarmering	• Engineering Development Model, t.b.v. demonstratie van unieke NL SSA capaciteit waaronder o.a.: ○ Laser, actieve en passieve radar/radiotelescopen ○ Specifieke detectie- en tracking algoritmes ○ Geïntegreerde controle functionaliteit	• Operationele SSA-sensorfaciliteiten geïntegreerd met een operationele, permanent bemande controle- en datacentrum (Voorzien is dat dit centrum ook voor R&D doeleinden wordt gebruikt)
Grondgebonden situational awareness capaciteit	• Aanscherping van de vraagstelling vanuit JenV en Defensie • Schaalbare dataservice architectuur voor het Sensor Data Intelligence Platform • Gebruik van Machine Learning (ML) platform voor nauwkeurige detectie/classificatie/predictie • Nieuwe concepten voor de Sensor Data Intelligence Platform (tasking, on-board processing, direct delivery, nieuwe type data)	• Schaalbare dataservice architectuur met gedistribueerde. computing capability en APIs met ground-based data sources • ML platform voor algoritme ontwikkeling / training • Service modellen voor diverse use cases. • Uitwerking nieuwe concepten • Detail ontwerp van het Sensor Data Intelligence Platform.	• Data-services met het Prototype Sensor Data Intelligence Platform voor tenminste 3 (civiele en militaire) use cases	• Installatie & ingebruikname op operationele schaal van het Sensor Data Intelligence Platform

	• Specificaties voor het Sensor Data Intelligence Platform			
Laser voor veilige communicatie en vergrote transmissie-capaciteit	• Fundamenteel onderzoek naar architectuur, laser terminal hardware concepten, encryptie, integratie laser communicatie in bestaande communicatie infrastructuur	• Diverse ontwikkeltrajecten die haalbaarheid van de kritische elementen op gebied van militarisering, laser terminals, encryptie (QKD), integratie met vliegen platformen, en integratie met bestaande RF-infrastructuur (interoperabiliteit, standaarden, protocollen) • Ontwikkeling van atmosfeer modellen en algoritmen voor de voorspelling performance en kwaliteit van laser links	• Engineering Development Model, t.b.v. demonstratie unieke NL capaciteit. • Demonstreren van optisch terminals, links tussen space-based laser terminals en vliegende, varende platformen; demonstratie in combinatie met High Altitude Pseudo Satelliet (HAPS) • Demonstreren van inpassing laser communicatie in RF infrastructuur	• Secure (Space-based) Laser Communication capaciteit geïntegreerd in strategische & tactische communicatie infrastructuur

(Gedeeltelijk) eigen satellietcapaciteit met tijdige en veilige toegang	• Onderzoek naar toekomstige concepten van operatie en (informatie) behoeftes waaruit daartoe gewenste unieke, (deels) eigen satelliet capaciteit geïdentificeerd, gedefinieerd en ontworpen kan worden	• Space payloadsystemen:
		  ○ Radio-frequentie
		  ○ Electro-optisch
		  ○ Meetsystemen
		• Spacecraft technologie:
		  ○ Militaire radio banden
		  ○ Zelfbescherming tegen cyber, interferentie en space debris
		  ○ Benutting van zeer lage aardbanen
		  ○ Payload specifiek
		• Grondsystemen voor gebruikers in het veld, zowel permanent als mobiel
			• In de ruimte valideren van (sub)systemen voor eigen satelliet-capaciteit.
			• Eerste fase focus
			  ○ Beveiligde communicatie
			  ○ Electronic Signal Monitoring
			  ○ Space Weather
				• Gekwalificeerde operationele satelliet en/of satelliet subsysteem producten die kunnen worden afgenomen door behoeftestellers
				• Een innovatieve “responsive supply chain” welke inspeelt op de specifieke behoefte om snel ruimtecapaciteit te kunnen inzetten van operationeel belang

3.4 Missie: Cyberveiligheid

Omschrijving missie [7]

Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren. Door in te zetten op het ontwikkelen van cybersecurity kennis en innovatie streeft Nederland ernaar om binnen vijf jaar in de top 10 van zowel de ITU Global Cybersecurity Index[8] als de National Cyber Security Index[9] te staan.

Waar gaat deze missie over

Digitalisering transformeert wereldwijd economieën en maatschappijen in razendsnel tempo. Nederland heeft een goede uitgangspositie om de economische en maatschappelijke kansen van digitalisering te verzilveren. Digitalisering brengt echter ook (nieuwe) kwetsbaarheden en uitdagingen met zich mee. Kennisontwikkeling en innovatie op het gebied van cybersecurity zijn noodzakelijk om dreigingen in het digitale domein tegen te gaan. Het doel van deze missie is cyberkennis en - kunde in Nederland te versterken, onderzoek en innovatie te faciliteren en een ecosysteem van experts en organisaties te bouwen.
De belangrijkste Nederlandse cybersecurity uitdagingen worden uiteengezet in drie strategieën.
- De Nederlandse Cyber Security Agenda (NCSA)
- De Nederlandse Digitaliseringsstrategie (NDS)
- De Defensie Cyber Strategie (DCS)

De cybermissie richt zich op het ontwikkelen van kennis en innovatie voor (het kunnen anticiperen op) de belangrijkste cyberuitdagingen uit bovengenoemde strategieën. De missie geeft richting aan fundamenteel en toegepast (multidisciplinair) cybersecurity-onderzoek voor zowel de langere als kortere termijn. Daarbij vormen de pijlers van de Nederlandse Cybersecurity Research Agenda (NCSRA) een belangrijke leidraad voor de onderzoeksinspanningen. De pijlers van de NCSRA zijn: Ontwerpen, Verdedigen, Aanvallen, Governance en Privacy. Deze missie snijdt dwars door de negen topsectoren heen (net zoals Dutch Digital Delta dat doet). Een directe link bestaat met de topsector HTSM maar net zo goed is digitale veiligheid een fundament voor (digitalisering van) de andere sectoren. Energievoorziening, watervoorziening, het bancaire systeem, transport, voedselveiligheid en gezondheidszorg kunnen niet functioneren zonder goede cybersecurity.

Kennis- en innovatievragen

Op het gebied van cybersecurity onderzoek en innovatie verbindt de NCSRA III[10] verschillende disciplines met elkaar via de vijf pijlers. Deze vormen voor de hieronder geprioriteerde onderzoeks- en innovatiegebieden een leidraad.

- Ontwikkelen van kennis over cybercrime en betrokken daders;
- Versterken van het gerechtvaardigd vertrouwen in digitalisering: Aanpakken van cybercrime, valideren van supply chain security van ICT en de systemen die ICT gebruiken, valideren van informatie (identificeren van fake news), valideren van (buitenlandse) security technologie, quantum safe crypto, integratie van cybersecurity in de verschillende topsectoren (en hun maatschappelijke en economische omgevingen), security by design – inherent veilige digitalisering;

[7] Een uitgebreide beschrijving van de missies is te vinden op https://www.rijksoverheid.nl/documenten/publicaties/2019/04/26/missies
[8] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
[9] https://ncsi.ega.ee/
[10] https://www.dcypher.nl/national-cyber-security-research-agenda-iii-ncsra-iii-2018

- Bevorderen van veiliger digitaal gedrag: Versterken van de weerbaarheid van burgers tegen beïnvloeding via het digitale domein, vergroten van het inzicht in en de kennis van ontwikkelingen van digitale en gedigitaliseerde activiteiten, het vergroten van de handelingsperspectieven met betrekking tot digitale en gedigitaliseerde dreigingen, verbeteren van governance van cybersecurity (en ICT, quantum, AI enz.) door beleids- en besluitvormers;
- Verminderen van de schaarste aan cybersecurity capaciteit: Naast opleiding en training ook automatisering van cybersecurity taken, optimaliseren van werkprocessen, pooling & sharing van cybersecurity professionals, kennis en (ondersteunende) middelen, meer focus en preventieve maatregelen, certificering en regulering van professionals;
- Versterken van offensieve en defensieve cybercapaciteiten: Sterke fysieke en digitale 'dijken' om vitale processen en infrastructuur (ICT, drinkwater, dijken, energie), meetbaar maken van politie-interventies in het digitale domein, valideren offensieve technologie, cybersecurity van wapensystemen, specifieke *high assurance* middelen (digitale soevereiniteit), verantwoord beproeven van kritieke digitale systemen en de impact van langdurige uitval;
- Het voorkomen van uitval van fysieke kritieke systemen ten gevolge van een cyberaanval in een keten.

Hoewel deze missie zich richt op het ontwikkelen van kennis en innovatie voor de belangrijkste cyberuitdagingen van Nederland, kunnen we dat niet alleen. Internationale samenwerking met partners en de private sector is noodzakelijk en ook aansluiting bij kennis en innovatie programma's van intergouvernementele organisatie zoals de EU, VN en NAVO zijn op dit vlak is wenselijk.

Benodigde kennis- en innovatie

De opbouw van digitale weerbaarheid vraagt veel van de Nederlandse samenleving. Om digitale ontwrichting te voorkomen en schade te beperken bij incidenten, moeten in een groot deel van de samenleving capaciteiten opgebouwd worden. 'Capacity building' is daarom een kernbegrip voor cyberveiligheid, en een belangrijk aspect van de indexen die genoemd zijn in de missie-omschrijving (de *ITU Global Cybersecurity* Index en de *National Cyber Security Index*). Deze indexen kijken naar een breed palet van relevante zaken zoals de wetgeving rondom cybersecurity, de staat van technologie bij organisaties, de samenwerking tussen partijen, en het maatschappelijke innovatie-vermogen. De Nederlandse kennis- en innovatieprocessen moeten daarop inspelen.

Inhoudelijk is cybersecurity is een breed werkterrein, en kent veel dynamiek en maatschappelijke aandacht. Digitale technologie ontwikkelt zich snel, en daarmee ook de operationele, bestuurlijke en maatschappelijke uitdagingen om Nederland weerbaar te maken tegen digitale dreigingen. Om defensief en offensief voldoende slagkracht te kunnen blijven ontwikkelen is een sterk kennis- en innovatie landschap cruciaal, waarbij technische wetenschappen, gedragswetenschappen, organisatie- en bestuurskunde elkaar vinden en samen opbouwen naar een digitaal weerbare samenleving. In dit landschap vinden kennispartners, bedrijfsleven en kwetsbare organisaties elkaar, en ontstaan effectieve innovatieketens die opbouwen naar defensieve en offensieve capaciteiten.

De veranderlijkheid van het cybersecurity landschap maakt het lastig om een vastomlijnd onderzoeksprogramma op te stellen. Een missie-gedreven aanpak helpt om cybersecurity onderzoek en -innovatie tijdig te richten op actuele en relevante onderwerpen. Door binnen innovatie ecosysteem gezamenlijk innovatie-missies te definiëren, en commitment te krijgen op de opvoering daarvan door partners, ontstaan sterke innovatie-ketens. Doordat missies op elkaar bouwen, ontstaat meer coherentie en impact, en wordt versnippering van innovatie beperkt.

We hanteren de volgende *uitgangspunten* bij de vertaling van de Missie Cyberveiligheid naar het Meerjarig Missie-gedreven Innovatie Programma (MMIP) Cyberveiligheid:

- Onderzoek en innovatie vindt plaats in een samenwerking in de driehoek overheid, kennisinstellingen en bedrijfsleven, met waar nodig en mogelijk regie op doorontwikkeling.
- Tussen nationale - en internationale onderzoek- en innovatie-activiteiten wordt zoveel mogelijk synergie gecreëerd.
- Een expliciete relatie met sleuteltechnologieën cybersecurity en quantum-technologie wordt nagestreefd.
- De focus ligt op het verkrijgen van een overzichtelijk, financierbaar en bemensbaar aantal onderwerpen en programma's, zodat daadwerkelijk stappen naar impact gemaakt kunnen worden.
- Digitale soevereiniteit is een belangrijke leidraad bij de keuze van onderwerpen waarop focus gelegd wordt: op welke onderwerpen moet Nederland zelf kennis- en innovatie kunnen opbouwen, en op welke onderwerpen mogen we vertrouwen op buitenlandse ontwikkelingen en producten?

Deze uitgangspunten vormen de basis voor de invulling van de missie-gedreven aanpak, en gaan leiden tot een versnelling van het innovatieproces in het cybersecurity domein.

3.4.1 MMIP: Cyberveiligheid

Het MMIP Cyberveiligheid heeft tot doel de kennisontwikkeling en innovatie te bewerkstelligen die nodig is voor een digitaal weerbaar Nederland. Dit moet voortkomen uit een nauwe samenwerking tussen overheid, kennisinstellingen en bedrijfsleven en is verbonden aan de uitvoering van de Nederlandse Cybersecurity Agenda en de Defensie Cyber Strategie 2018[11].

Met de succesvolle uitvoering van het MMIP Cyberveiligheid kent het Nederlandse cybersecurity innovatie ecosysteem in 2030 een duidelijke vorm, en laat het zien dat Nederland in staat is om urgente uitdagingen effectief het hoofd te bieden (kort-cyclisch), en ook doelgericht aan fundamentele vraagstukken te kunnen werken (lange termijn innovatie). Dit uit zich in een coherente, programma-overstijgend set van onderzoeks- en innovatie-activiteiten, gericht door breed gedragen missies.

Voor de KIA Veiligheid zijn vijf *deelprogramma's* voor Cyberveiligheid geïdentificeerd:

1. Bestrijden cybercrime
2. Bevorderen ontwikkeling cybercompetenties
3. Defensieve cybertechnologie
4. Offensieve cybertechnologie
5. Ketenweerbaarheid en governance

Deelprogramma 1: bestrijden cybercrime

De digitale technologie en de toepassing daarvan heeft een toenemende invloed op het criminele landschap. Nieuwe vormen van criminaliteit ontstaan en bestaande vormen van criminaliteit zijn gedigitaliseerd. Kennis van en inzicht in cybercrime en gedigitaliseerde criminaliteit is nodig om handelingsperspectieven te ontwikkelen en de effectiviteit van genomen maatregelen te beoordelen.

[11] https://www.defensie.nl/downloads/publicaties/2018/11/12/defensie-cyber-strategie-2018

Cybercrime onderzoek bestaat uit een combinatie van mono- en multidisciplinair onderzoek. Onderzoek waarin de ontwikkeling van innovatieve technische tools wordt gecombineerd met de nieuwste psychologische en sociologische inzichten. Bijvoorbeeld de combinatie van technische tools om interventies uit te voeren met studies naar menselijk gedrag. Of onderzoek naar de effectiviteit van de interventies en onderzoek naar de sociale factoren van slachtoffers en daders (denk hierbij aan interventies tegen 'dark markets' en zogeheten waterbedeffecten). Geavanceerde technische tools op basis van de nieuwste technologieën zijn nodig om interventies te plegen, om cybercriminelen op te sporen en kwetsbaarheden te signaleren in technieken die cybercriminelen inzetten.

Daarnaast geldt vaak dat de aanpak van cybercrime en gedigitaliseerde criminaliteit samenwerking vereist tussen een groot aantal publieke- en private partijen. Samenwerking in kennis en innovatieontwikkeling moet leiden tot:

- nieuwe analysemodellen voor het in beeld brengen van cybercrime en gedigitaliseerde criminaliteit,
- analysemodellen en innovatieve interventiestrategieën om nieuwe modi operandi snel te kunnen herkennen,
- technische tools voor het uitvoeren van deze interventies,
- methoden om op basis van data de effectiviteit van oplossingen te kunnen beoordelen.

Deelprogramma 2: bevorderen ontwikkeling cybercompetenties

Voor het bevorderen van de ontwikkeling van cybercompetenties wordt onderscheid gemaakt naar:

1. Het in staat stellen van eindgebruikers om veilig te handelen bij alle activiteiten gerelateerd aan het digitale domein.
2. Capaciteitsopbouw van cybersecurity professionals.

Ad 1: Veilig handelen

Menselijk handelen in het digitale domein is van grote invloed op cyberveiligheid. Een goed slot op de deur van je huis is vanzelfsprekend het hanteren van een sterk wachtwoord voor je digitale systemen niet. Ontwikkeling van kennis over hoe tot een algemeen geaccepteerd handelingskader voor digitaal veilig handelen kan worden gekomen is hierbij essentieel. Daarnaast moeten we het de gebruiker zo makkelijk mogelijk maken. Ontwikkeling van innovatieve producten die gebruikers automatisch veilig laten handelen, stimuleren veilig te handelen of zelfs dwingen veilig te handelen biedt een oplossing. Hoe kunnen bijvoorbeeld technieken als nudging mensen stimuleren maatregelen te treffen om digitaal weerbaarder te worden.

Het ontwerp van digitale diensten en producten is van groot belang bij het stimuleren van digitaal veilig handelen van gebruikers. Door in de ontwerpfase al bewust het product in te richten op veilig handelen wordt de toekomstige gebruiker ontlast of gedwongen veilig te handelen. (Deze strategie linkt nauw met de *security-by-design* principes uit deelprogramma 3)

Ad 2: Capaciteitsopbouw

Het huidige tekort aan capabele cybersecurity professionals, zowel in kwantitatieve als kwalitatieve zin, zal alleen maar toenemen. Structurele aandacht voor cybersecurity onderwijs is nodig om over voldoende cybersecurity professionals te beschikken. Daarbij gaat het om alle onderwijsniveaus. Ook essentiële randvoorwaarden zoals beschikbaarheid van cybersecuritydocenten dient hierbij meegenomen te worden. Uitdaging is om nieuwe aanwas aan cybersecurity professionals continu

aan te laten sluiten bij de vraagzijde uit het bedrijfsleven. Onderzoek naar methoden die de continue adaptatie van cybersecuritykennis in onderwijscurriculum bevorderen is hierbij nodig. Daarnaast vereist dit een goed beeld van de ontwikkelingen op de arbeidsmarkt voor cybersecurity professionals in Nederland.

Cybersecurity kennis is niet alleen voorbehouden aan de cybersecurity beroepsgroep. Ook cybersecurity competenties binnen andere beroepen worden door verder gaande digitalisering steeds belangrijker. Daarmee wordt toevoeging van deze competenties aan onderwijscurricula van belang. Dit alles moet leiden tot een pakket aan concrete korte en lange termijn maatregelen gericht op verdere structurering en professionalisering van het:

1) vakgebied: een heldere definitie van (harde en zachte) cybersecurity competenties[12], eenduidige (internationaal afgestemde) certificering van cybersecurity professionals, duidelijke en aantrekkelijke arbeidsvoorwaarden en loopbaanpaden.
2) kennisgebied: een algemeen geaccepteerde *body of knowledge*[13] en cybersecurity lexicon, voldoende gekwalificeerde docenten en meer samenhang binnen het cybersecurity onderwijs.
3) toepassingsgebied: meer samenwerking aan de vraagzijde van de arbeidsmarkt, waar cybersecurity kennis wordt toegepast en geborgd in een breed spectrum van vakgebieden, en waar binnen organisaties vergroting gewenst is van de cybersecurity compliance.

Deelprogramma 3: defensieve cybertechnologie

Dit deelprogramma richt zich op onderzoek naar het verbeteren van defensieve cybertechnologie. De snelheid van doorontwikkeling van het cybersecurityinstrumentarium moet aansluiten bij de digitale dreiging. De focus ligt enerzijds op het ontwerpen van veilige, geautomatiseerde en privacy vriendelijke systemen en producten en anderzijds op het ontwikkelen van technieken om systemen en producten weerbaar te maken en te houden.

Ondanks toenemende investeringen in cybersecurity, kunnen de meeste organisaties de snelheid en ontwikkelingen van digitale dreigingen nauwelijks bijhouden. Automatiseren van cybersecurity werkzaamheden is een belangrijke oplossing om met beperkte capaciteit alsnog weerbaar te blijven. Kennis en innovatievragen die hieraan gerelateerd zijn:

- het ontwikkelen van manieren om geautomatiseerd kwetsbaarheden te signaleren in broncode's,
- het automatiseren van veel voorkomende stappen in het pentestproces,
- automatisch patchen op applicatielevel,
- het automatiseren van operationele taken van security incident- en dreigingsanalyses,
- het automatisch detecteren of een organisatie wel of niet compliant is ten aanzien van wetgeving, standaarden of eigen beleid.

Nieuwe innovatieve technologieën zoals de toepassing van artificial intelligence / machine learning voor detectie en response processen bieden oplossingen voor het groeiende weerbaarheidsprobleem. Het integreren van artificial intelligence en machine learning in detectie en

[12] Bijvoorbeeld zoals geformuleerd in het NIST SP 800-191 NICE Cybersecurity Workforce Framework: https://csrc.nist.gov/publications/detail/sp/800-181/final
[13] De adoptie van CyBOK (Cyber Security Body Of Knowledge) wordt onderzocht: https://www.cybok.org/about/

response processen kunnen op de lange termijn menselijke inzet vervangen en op de korte termijn het werkproces versnellen. Eerste gesignaleerde toepassingen zijn:

- detectie van botnets met AI,
- machine learning in software vulnerabilities,
- automatische detectie binnen industriële omgevingen zoals bijvoorbeeld in industriële ICS-SCADA systemen.

Essentieel onderdeel binnen dit deelprogramma is onderzoek naar de interactie tussen de mens en geautomatiseerde security tools, onder andere het kunnen blijven doorgronden van geautomatiseerde technieken en het optimaal in kunnen zetten van AI technologie voor cyberveiligheid van organisaties.

Naast artificial intelligence zijn kennisvragen en innovatieve oplossingen tussen post kwantum computing en cybersecurity van belang. Cryptografie en post kwantum cryptografie zijn essentieel voor veilige communicatie, en daarmee een fundament onder digitale weerbaarheid. Gesignaleerde kennisvragen en innovatieopgaven zijn de robuustheid van crypto-algoritmen in post kwantum tijdperk kunnen blijven testen, post kwantum encryptie en post kwantum communicatiemethoden.

Deelprogramma 4: offensieve cybertechnologie

Dit deelprogramma richt zich op onderzoek naar en innovatie van offensieve cybertechnologie. Onderzoek naar offensieve technologie maakt het mogelijk technische en organisatorische middelen te ontwikkelen voor overheidsorganisaties. Dit betreffen organisaties met een wettelijk mandaat om offensief te opereren in cyberspace: bijvoorbeeld voor bestrijding van (cyber-)crime, defensiedoelen of inlichtingen. Het kan hier inhoudelijk gaan om ondersteunende processen en technologie (b.v. voor *'Command & Control'* of efficiënte, controleerbare productie van offensieve cybermiddelen), of om daadwerkelijke aangrijpingsmiddelen. Meer concreet is er behoefte aan technologieën die inzetbaar zijn voor rechtshandhaving. Voor de opsporing en vervolging van (cyber)criminaliteit is sterke behoefte aan de ontwikkeling van technologie om binnen te dringen in een geautomatiseerd netwerk. Ook zijn de toepassing van nieuwe technieken zoals artificial intelligence en kwantum computing en in het verlengde daarvan post kwantum encryptie en cybersecurity ten behoeve van offensieve handelingen centrale onderwerpen in kennis en innovatieopgaven. Digitale soevereiniteit voor de Nederlandse overheid is hierbij een belangrijke overweging.

Deelprogramma 5: ketenweerbaarheid en governance

Risicomanagement van bedrijfsprocessen met ICT beveiliging als integraal onderdeel ervan is essentieel voor de continuïteit van organisaties. De keten waarin de organisatie zich bevindt speelt hierin een grote rol. Het onderlinge afhankelijke en genetwerkte karakter van ICT processen vergt veel van cybersecurity maatregelen. In het bijzonder geldt dit voor de vitale infrastructuur (processen). Uitval van vitale infrastructuur heeft grote cascade effecten. Dit deelprogramma richt zich op kennisvragen en innovatieopgaven naar ketenweerbaarheid, risicomanagement en de bestuurlijke dynamiek rondom cybersecurity.

Cyberdreigingen en risico's worden door vele niet-cyber-ingewijden gezien als technisch en lastig te doorgronden. Ook is de 'business case' van cybersecurity vaak niet helder. Gevolg is dat risico's niet of beperkt worden meegenomen in het risicomanagementproces van organisaties. Onderzoek naar de besluitvorming en de beïnvloeding van management en bestuur inzake het nemen van cybersecurity maatregelen geeft inzicht welke afwegingen genomen worden en hoe hierop ingespeeld kan worden.

Er zijn talrijke instrumenten en maatregelen die bijdragen aan de weerbaarheid tegen cyber incidenten. Om als organisatie tot een juist instrumentarium te komen is inzicht in de effectiviteit van en correlaties tussen instrumenten een must. Het verschaffen van helderheid door een fundamenteel raamwerk te ontwikkelen over de voor- en nadelen van beschikbare instrumenten, zoals het inzetten van penetratietesten, biedt dit inzicht en geeft vervolgens inzichten voor nieuw te ontwikkelen (hybride) vormen. Op basis daarvan kan een (mix van) instrumenten strategisch ingezet, gepromoot, gestimuleerd of geëist worden.

Een belangrijk onderdeel van cyber risicomanagement is het creëren van een overzicht van dreigingen ten opzichte van bedrijfsrisico's. Onderzocht dient te worden hoe tot een optimaal en geïntegreerd dreigingsbeeld kan worden gekomen. Een dreigingsbeeld op basis van digitale, hybride en (geo)politieke ontwikkelingen. En een methodiek die in staat is om op een dynamische wijze real-time dreigingsbeelden kan genereren. Door onder andere analytische modellen door te ontwikkelen wordt beter gebruik gemaakt van data en ontstaan betere risico-indicatoren.

Om de ketenweerbaarheid van Nederland te versterken tegen digitale ontwrichting is continue kennisontwikkeling naar het krachtenveld in het digitale landschap nodig. Om tot versterkte ketens te komen is inzicht nodig in hoe tot effectieve informatie-uitwisseling gekomen kan worden. Informatie-uitwisseling over actuele dreigingen en incidenten tussen organisaties. Deze informatie-uitwisseling dient daarbij ondersteund te worden door de ontwikkeling van veilige en privacy-vriendelijke informatie-uitwisselingstechnieken. Een volgende stap is het creëren van handelingsperspectieven voor elke individu of organisatie in de keten. Het ontwikkelen van realistische oefeningen en testen met de nieuwste technieken en dreigingen rondom digitale verstoringen op zowel lokaal, regionaal niveau als in een keten is daarbij essentieel.

Deelprogramma	Kennisopbouw (TRL[14] niveau 1 t/m 3)	Kennistoepassing (TRL niveau 4 t/m 6)	Kennisgebruik (TRL niveau 7 en 8)	Implementatie (TRL niveau 8 en 9)
Bestrijden cybercrime	• Onderzoek naar de effectiviteit van interventies die cybercrime opsporen en kwetsbaarheden signaleren in de technieken van cybercriminelen. • Onderzoek naar de sociale factoren van slachtoffers en daders in verhouding met bestaande en nieuwe interventies.	• Ontwikkeling van mono en multidisciplinaire analysemodellen voor het in beeld brengen van cybercrime en gedigitaliseerde criminaliteit. • Ontwikkeling van mono en multidisciplinaire analysemodellen en interventie strategieën om nieuwe modi operandi snel te herkennen. • Ontwikkeling van handelingsperspectieven en technische tools voor het tegengaan van cybercrime en gedigitaliseerde criminaliteit • Ontwikkeling van methoden om op basis van data de effectiviteit	• Proeftuinen voor demonstreren en valideren handelingsperspectieven voor het tegengaan van cybercrime en gedigitaliseerde criminaliteit • Proof of concept voor het in beeld brengen van cybercrime en gedigitaliseerde criminaliteit door middel van sensoren en informatie-uitwisseling	• Implementeren van handelingsperspectieven en tools voor het tegengaan van cybercrime en gedigitaliseerde criminaliteit

[14] Technology Readiness Level

		van oplossingen te kunnen beoordelen.		
Bevorderen cyber-competenties	• Onderzoek naar effectief beïnvloedingsbeleid hoe tot een algemeen geaccepteerd handelingskader gekomen kan worden. • Onderzoek hoe methodes als nudging kunnen worden ingezet om het cybersecurity instrumentarium te versterken. • Onderzoek naar hoe cybersecuritycompetenties in onderwijscurricula kunnen worden opgenomen. • Onderzoek naar de arbeidsmarkt voor cybersecurity-professionals en aansluiting van relevante opleidingen.	• Ontwikkeling van innovatieve producten die gebruikers automatisch veilig kunnen laten handelen, stimuleren veilig te handelen of dwingen veilig te handelen. • Ontwikkeling van een human capital agenda voor cybersecurity, inclusief integrale benadering met toolkit aan instrumenten voor individuele organisaties.	• Demonstratie van secure design tooling voor veilige/ privacy vriendelijke informatie-uitwisseling en opslag • Demonstratie van de impact op taak- en -activiteitreductie op basis van demonstratie (deels) geautomatiseerd instrumenten	• Aangepaste of nieuwe digitale producten en diensten waarmee digitaal veilig werken geen extra handelingen van de eindgebruiker kost • Implementatie van relevante cybersecurity aspecten in bestaande scholing- en opleidingstrajecten. •
Defensieve cyber-technologie	• Onderzoek naar geavanceerde en automatische defensieve cybertechnologie. • Onderzoek naar de interactie tussen de mens en geautomatiseerde security tools. • Onderzoek naar de effecten en toepassing van post kwantum computing op cybersecurity. • Onderzoek naar de robuustheid van crypto-algoritmen in post kwantum tijdperk • Onderzoek naar de beperkingen van het automatiseren van cybersecurity handelingen en hoe met deze beperkingen om te gaan. • Onderzoek naar en toepassing van security-by-design (waaronder identity mngt) in IoT • Onderzoek naar uniek identificeerbare chips voor kleinschalig gebruik in gerubriceerde toepassingen t/m grootschalig in IoT	Ontwikkelen van technologieën voor: • Het automatiseren van signaleren en corrigeren van kwetsbaarheden in software (b.v. via cyber reasoning systeem) • Het automatiseren van patchen van kwetsbaarheden in software • Het automatiseren van veel voorkomende stappen in het penetratietest proces. • Het automatiseren van operationele taken in security incident en dreigingsanalyses. • Het automatiseren van detecteren of organisaties compliant zijn aan wetgeving, (eigen gestelde) standaarden. • Detectie van Botnets met AI. • Security detectie technologie voor binnen industriële systemen. • Beveiliging van laag en hoog gerubriceerde informatie d.m.v. o.a. (quantum safe) encryptie, detectie, identity management.	Prototypering van ontwikkelde technologieën voor: • Het automatiseren van signaleren en corrigeren van kwetsbaarheden in software. • Het automatiseren van patchen van kwetsbaarheden in software. • Het automatiseren van veel voorkomende stappen in het penetratietest proces. • Het automatiseren van operationele taken in security incident en dreigingsanalyses. • Het automatiseren van detecteren of organisaties compliant zijn aan wetgeving, (eigen gestelde) standaarden. • Detectie van Botnets met AI. • Security detectie binnen industriële systemen. • Proof of concept demonstratie van (deels) geautomatiseerd Security Operations Center (SOC) in proeftuin bij bijv. een MSSP	• Ingebruikname van geavanceerde en automatische defensieve cybertechnologie

	• Onderzoek naar (on)mogelijkheden eigen standaarden op basis van bestaande standaarden.			
Offensieve cyber-technologie	• Onderzoek naar concepten en methoden voor offensieve cybertechnologie voor uitvoering van de wettelijke taken van de overheid. • Fuzzing, root cause analysis, risk assessment of vulnerabilities, etc. • En daarnaast: andere landen ontwikkelen met veel inzet automatische cyberwapens: onderzoek naar deze capaciteiten t.b.v. de eigen verdediging.	• Ontwikkeling van technologie of processen voor offensieve doeleinden • Testen en evaluatie van bestaande systemen	• Beproeving van prototypes van offensieve (hulp-) middelen	• Ingebruikname en exploitatie van offensieve cybertechnologie
Keten-weerbaarheid en governance	• Onderzoek naar besluitvorming en beïnvloeding van management en bestuur inzake het nemen van cybersecurity maatregelen. • Onderzoek naar de effectiviteit en correlaties tussen cybersecurity instrumenten. • Onderzoek naar het modelleren en voorspellen van cyberrisico's, cascade-effecten in een proces-/organisatieketen • Onderzoek naar effectieve informatie-uitwisseling over dreigingen en incidenten tussen organisaties binnen geldende regelgeving.	• Ontwikkeling van een methodiek die op dynamische wijze een realtime geïntegreerd dreigingsbeeld kan genereren. • Ontwikkeling van een fundamenteel raamwerk over de voor en nadelen van cybersecurity instrumenten en de interactie tussen deze instrumenten. • Ontwikkelen van veilige en privacy vriendelijke informatie-uitwisselingstechnieken • Ontwikkelen van realistische oefeningen en testen op basis van de nieuwste technieken en gesignaleerde dreigingen.	• Proeftuinen voor het demonstreren van effectief toepassen van het ontwikkelde fundamentele raamwerk risicomanagement en maatregelen. • Demonstratie van realistische oefeningen en testen op basis van de nieuwste technieken • Beproeven van nieuwe technieken en ontwikkelde procedures tijdens cyberincidentmanagement trainingen en oefeningen. • Verzamelen en ter beschikking stellen van longitudinale cybersecurity datasets t.b.v. onderzoek en beleidsondersteuning.	• Gestructureerde en beargumenteerde wijze van inzetten van een effectief cybersecurity instrumentarium • Effectieve cybersecurityinformatie en incidentuitwisseling tussen organisaties. • Regelmatig en effectief oefenen, testen en evalueren op basis van de nieuwste technieken en gesignaleerde dreigingen. • Onderhoud datasets.

3.5 Missie: Genetwerkt optreden op land en vanuit de lucht

Omschrijving missie [15]

In 2030 werkt de krijgsmacht volledig genetwerkt met andere diensten en met integratie van nieuwe technologieën, zoals onbemande systemen, elektromagnetisch spectrum en *social media*, waardoor we de *decision loop* sneller en beter dan de tegenstander doorlopen.

[15] Een uitgebreide beschrijving van de missies is te vinden op https://www.rijksoverheid.nl/documenten/publicaties/2019/04/26/missies

Waar gaat deze missie over

Er is een toenemende mate van verbondenheid tussen nationale en internationale veiligheid en dit zorgt ervoor dat de veiligheidsorganisaties meer met elkaar genetwerkt zullen moeten samenwerken. Met volgende generaties sensoren en vurende systemen wordt het steeds moeilijker om onzichtbaar of buiten de invloed van tegenstanders te blijven. Essentieel voor het winnen van conflicten is dat we in staat zijn om sneller en beter informatie te vergaren, te analyseren, samen te brengen en te delen dan onze tegenstanders. Genetwerkt optreden vraagt om het integreren van nieuwe technologieën in het optreden en nieuwe operatieconcepten. Experimenteren, trainen en oefenen zijn belangrijk om te bepalen hoe technologieën het optreden kunnen veranderen, maar ook om te bezien welke technologieën ontwikkeld zouden moeten worden.

In de uitwerking van het MMIP is besloten alle robot gerelateerde programmering onderdeel tea maken van MMIP: Innovaties voor een adaptieve krijgsmacht (MMIP 6.1).

Benodigde kennis- en innovatie

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*). Voor genetwerkt optreden tegen Rockets, Artillery of Mortars (RAM) vliegtuigen en drones speelt capaciteit op gebied van preventie, detectie, classificatie, neutralisatie en opsporing een belangrijke rol. Het genetwerkt optreden vraagt om concepten en technologieën om *slimme en robuuste logistiek* effectief in te richten.

De ambitie is om in deze KIA in te zoomen op de onderwerpen die vooral in een militair/politie-civiele samenwerking onder te brengen zijn. Daarvoor zijn binnen genetwerkt optreden de volgende onderwerpen geselecteerd:

- *Command & Control*: Deelprogramma 1: *Innovatie in ontwerp en aansturing van netwerken*;
- *Robot autonomous systems (RAS), en Remotely Piloted Airborne Systems (RPAS)*: Een belangrijk deel hiervan valt onder de missie Adaptieve krijgsmacht;
- *Informatie als wapen*: Deelprogramma 2: Informatie als wapen;
- *Genetwerkt optreden met capaciteiten tegen Rockets, Artillery of Mortars (RAM) en Unmanned Aerial Systems (UAS)*: Deelprogramma 4: *Counter DRAM (Drone, Rocket, Artillery & Mortar)*. Daarnaast zitten delen van deze kennisvraag in de missie *Adaptieve krijgsmacht* en in de missie *Data en Intelligence*.
- *Slimme en robuuste logistiek*: Deelprogramma's 3 *Aansturing van genetwerkte logistieke organisaties* en 4 *Smart service logistics*.
- *Vergroten slagkracht*: de vraagstukken rondom het effectiever inzetten van wapensystemen/-platformen (waaronder de veiligheidsprofessional, de militair) hebben in deze missie betrekking op het creëren van een snellere *sensor-to-shooter link*. Deze kennisvraag wordt meegenomen in Deelprogramma 1.

3.5.1 MMIP: Informatiegestuurd en genetwerkt optreden

De doelstelling van dit MMIP is om de krijgsmacht en andere veiligheidsorganisaties effectief te laten functioneren in genetwerkte omgevingen. Uiteindelijk moet hierdoor de slagkracht van deze organisaties worden vergroot.

In 2030 moet dit blijken uit het feit dat defensieonderdelen en andere veiligheidsorganisaties in staat zijn voor een willekeurige operatie, alsmede voor de *going concern* activiteiten, snel een acceptabel niveau van netwerk integratie te behalen en te behouden, voor zowel de communicatie, de *situational awareness*, de inzet van informatie als wapen, en de operationele processen.

Deelprogramma 1: Innovatie in ontwerp en aansturing van netwerken

Een belangrijke voorwaarde voor genetwerkt optreden is het tot stand brengen van netwerken voor communicatie, datacollectie en – analyse en de aansturing van operationele activiteiten. Dit heeft parallellen met de civiele wereld, waar de mensen steeds meer genetwerkt raken in privé en werkomstandigheden door de toegenomen digitalisering en afhankelijkheid van mobiele en data (3G en in de toekomst 4G) netwerken. Steeds meer sensoren op verschillende plekken in de maatschappij en privé raken verbonden om processen te automatiseren, zoals Internet of Things (IoT). Dat draagt bij aan bewaken en beveiligen, *tracken en tracen* van distributie en vervoer, voor bewaken van de dijken etc. etc.

Ook zijn er crisis situaties waarvoor netwerken voor humanitaire hulp moeten worden ingericht, net als in de festivalwereld, waar ook in korte tijd grote festivalterreinen worden ingericht en weer worden afgebouwd. Daarnaast is er een parallel met de meer reguliere wereld van *supply chains* en logistiek, waar communicatie en de integratie van informatiesystemen ook aan de orde van de dag is.

Dit deelprogramma richt zich op het inrichten van een aantal militair/civiele initiatieven gericht op het grootschalig integreren van communicatie, data en informatienetwerken waarmee vervolgens effectief informatiegestuurd optreden kan worden ondersteund.

Belangrijke onderzoeksvraagstukken gaan over de mogelijkheden voor *smart connectivity* in reguliere en uitdagende omstandigheden, de rol van standaardisatie daarbij, en ook de mogelijkheden voor de inzet van Artificial Intelligence bij het herkennen van datastructuren en het faciliteren van connectiviteit. Daarnaast is er onderzoek vereist naar de manier waarop onder verschillende omstandigheden informatie gecombineerd en gerepresenteerd kan worden om uiteindelijk *situational awareness* en *situational understanding* te verkrijgen.

Daarnaast speelt de vraag hoe krijgen Defensie en Politie goed inzicht in de situatie met alle sensoren (Internet of Things) die er zijn, en met alle sensoren die de veiligheidsorganisaties zelf ter beschikking hebben zoals de F35, diverse onbemande vliegtuigen en voertuigen, radar, satelliet en diverse andere sensoren bv bij de eenheden zelf op voertuigen of in een groep. Er komt steeds meer data ter beschikking en hoe gaan we uit al deze big data, zowel militair, civiele en open source databases de relevante informatie halen en delen in de relevante netwerken?

Concrete initiatieven zijn o.a.: inventarisatie bestaande oplossingen voor dataconnectiviteit in nationale en internationale operaties; toepassingen datafusie technieken; inrichting basisinfrastructuur voor delen van grote datasets van sensordata; miniaturisatie van communicatiemiddelen en –netwerken en User Interface ontwikkelingen zoals Watson, geografisch weergave, apps, etc.

Deelprogramma 2: Informatie als wapen

Informatie als wapen bevat specifieke onderzoeksvragen rondom sociale media analyse, gedragswetenschappen, en de invloed van de digitale wereld op de werkelijke wereld. De digitale wereld is dusdanig verweven met de werkelijke wereld, dat ook voor crisissituaties en conflicten dit niet meer los van elkaar kan worden gezien.

Het gaat niet alleen om informatie, percepties en standpunten/intenties van groeperingen die digitaal worden beïnvloed en verspreid. Maar ook de samenleving is inmiddels volledig afhankelijk van de digitale wereld, zoals vrijwel alle maatschappelijke functies ook digitaal uitgevoerd of ondersteund worden zoals financiële processen, nutsvoorzieningen, handel, productieprocessen etc. Internet of Things is een ontwikkeling die sterk doorzet in ons gehele dagelijks en professionele leven. Dat betekent risico's voor onszelf in Nederland, maar ook kansen voor de inzet van dit soort middelen in conflictgebieden.

Facebook, Instagram tot en met gewone (*spam/phishing*) mails zijn omgevingen die snel veranderen en die door tegenstanders, maar ook door de eigen veiligheidsorganisaties als wapen (kunnen) worden ingezet. Hoe herken en spot je (potentieel) gevaarlijke trends in sociale media en hoe kun je daarop effectief reageren? De kennis en innovatie vragen betreffen hier niet alleen technische vragen (beta/software engineering), maar ook een meer mens, cultuur en marketing gericht insteek (gamma/alfa) met aandacht voor (groeps-)psyche in het virtuele/digitale domein. Deze kennis kan door de veiligheidsorganisaties ook intern worden toegepast in project en programmasituaties waar sturing nodig is voor resultaat.

Concrete initiatieven betreffen: aansluiten bij sociale media analyse; In beeld brengen van moderne marketinginzichten ten aanzien van beïnvloeding koopgedrag; reikwijdte gedragsanalyse, -wetenschappen en antropologische methodieken bepalen en *big data analytics* met *data science*.

Deelprogramma 3: Aansturing van genetwerkte logistieke organisaties

Initiatieven in dit thema zijn gericht op het realiseren van Command & Control concepten voor de logistiek in complexe operationele situaties. Deze situaties worden gekenmerkt door een structuur waarin omgeving, voertuigen/middelen en lading, in de context van een specifieke operationele doelstelling, de drie belangrijke dimensies zijn. De Command & Control structuur dient te beschikken over relevante informatie op deze drie niveaus, alsmede oplossingen voor inter-organisationele uitwisseling van data, en andere sturingsinformatie.

De ontwikkeling van de oplossingen om deze informatie te verkrijgen, en te combineren in relevante sturingsinformatie is onderdeel van de opgave binnen dit onderzoeksthema. Hierbij wordt voortgebouwd op technisch onderzoek dat elders in innovatieagenda's wordt uitgevoerd (MJPs voor de sleuteltechnologieën, andere missies in de veiligheidsagenda).

In PPS-verband zal aansluiting worden gezocht bij relevante initiatieven in de civiele wereld, bijvoorbeeld bij de manier waarop de grote retailers hun aanvoerlijnen en winkelbelevering organiseren, hoe de logistieke structuren van de voedselbanken functioneren, hoe in de bouw de logistiek rondom bouwsites wordt ingericht en hoe grote logistieke dienstverleners hun pan-Europese transportnetwerken aansturen. De technische universiteiten in Nederland hebben een gezamenlijk programma op het thema *resilience engineering*. In de Nederlandse creatieve industrie

is heel veel kennis over het managen van de lokale footprint van festivals en de logistiek van opbouw en afbouw. Bij al deze civiele situaties spelen netwerkcommunicatie, integratie van informatie over infrastructuur, voertuigen, lading, en klanteisen, de integratie van nieuwe technologie – geavanceerde planningstools en autonome voertuigen – en continue onzekerheid ook een grote rol.

Specifiek in de wereld van infrabeheer is er veel kennis over de proliferatie van storingen en problemen in het netwerk, en het beheersen van calamiteiten in delen van het netwerk. Tevens zijn er verschillende partijen actief op het gebied van robuuste, flexibele, tijdelijke, netwerk uitbreidingen en koppeling van verschillende infrastructuren (bijvoorbeeld 4G *hotspot* aan een Satcom terminal, etc.)

Concrete initiatieven zijn: inventarisatie wat er al gebeurt vanuit defensie/JenV met de private sector op dit specifieke gebied, en kennismaking met civiel genetwerkt optreden; ontwikkeling gezamenlijke aanpak opbouw-afbouw missies/events/humanitaire hulp. Integratie circulair opereren met effectief en doelgericht inrichten van netwerken en faciliteiten en onderzoek naar Command & Control voor gecombineerde bemande/onbemande netwerken van voertuigen en equipment in civiel/militaire omgevingen.

Deelprogramma 4: Counter DRAM (Drone, Rocket, Artillery & Mortar)

Hoewel de drones een aantal specifieke eigenschappen hebben die mogelijk een andere aanpak vragen dan de ander drie dreigingen is er juist ook veel overlap. Als dreiging worden deze systemen op afstand ingezet. Daardoor noodzaakt het tot het monitoren van een groot gebied in en om het te beschermen object of gebied. Het gebruik van al aanwezige sensoren en netwerken met uitbreidingen als *smart decentralised/clustered processing/analysis* maakt het mogelijk om de dreiging vroegtijdig te ontdekken en tegen acties te ondernemen. Overigens dient er ook rekening gehouden te worden met de toename in mogelijkheden/dreigingen door autonome voertuigtechnieken. De gedachte aan een zelfrijdende bomauto die eerst zelf een stuk door een stad manoeuvreert is niet heel onrealistisch.

Counter DRAM vergt innovatieve toepassing van bestaande middelen en ontwikkeling van nieuwe sensoren en analyse/waarschuwingssoftware. In de civiele sector wordt al onderzoek gedaan en geëxperimenteerd met het koppelen van vele camera's en het (automatisch) volgen van objecten /personen door een groter gebied. Tevens zijn er al toepassingen van beeldverwerking die bepaald gedrag kunnen herkennen of als ongewoon kunnen labelen waarop dan weer vervolg acties genomen kunnen worden. Ook toepassing van 3D audio sensoren en goedkope korte afstand radar systemen die in grotere getalen samen een groot gebied in de gaten kunnen houden komen op de markt en kunnen een mogelijke bijdrage leveren. In alle gevallen is de rol van de mens die moet werken met deze deels autonome technologie ook een aandachtspunt.

Op het gebied van counter DRAM lopen onderzoeksprogramma's bij de verschillende onderzoeksinstituten en zowel defensie als politie zijn aangehaakt. Daarbij zijn vooral de traditionele defensiegerelateerde industrieën betrokken en is de netwerk aanpak nog onderbelicht. Er zijn dan ook mogelijkheden om andere PPS-bedrijven aan te laten haken met kennis en producten op het gebied van beeldherkenning en smart tracking. De rol van de mens haakt aan bij vergelijkbare vraagstukken in tal van andere industriële sectoren.

Deelprogramma 5: Smart service logistics

Veiligheidsorganisaties beschikken over uitgebreide vloten van voertuigen, werktuigen en wapensystemen waarvan de beschikbaarheid cruciaal is voor het uitvoeren van de diverse veiligheidstaken. Naast onderzoek over bijvoorbeeld slimmer onderhoud, *design for maintainability* en gebruik van innovatieve (zelfreparerende) materialen, is de organisatie van de onderhoudsprocessen, en de beheersing van de stroom onderdelen en de planning van technici ook belangrijk. In het civiele domein, vaak in samenwerking met Defensie, is al veel onderzoek gedaan op het vlak van initiatieven van de zogenaamde service logistiek. Dit onderzoek schuift op naar geavanceerde beslissingsondersteuning bij aankoop en onderhoudsbeslissingen, en het ontwikkelen van voorspelmodellen op basis van deelsysteem data (*predictive maintenance*).

Op het gebied van *smart service logistics* lopen er op dit moment bij Defensie initiatieven bij de Marine, de Luchtmacht (rondom de F35) en de Landmacht. De ambitie in dit MMIP is ook om de kennis op het gebied van *smart service logistics* te centraliseren, en zoveel mogelijk uit te wisselen tussen krijgsmachtonderdelen en andere veiligheidsorganisaties.

In het veiligheidsdomein zijn er twee grote uitdagingen op het gebied van *smart service logistics*: enerzijds het daadwerkelijk breed implementeren van beschikbare kennis en modellen. Voorwaarde hiervoor is onder andere dat de beschikbare data over systemen selectief en bewust gedeeld wordt, en dat ook kennis en ervaring met praktische toepassingen breed worden gedeeld. De tweede uitdaging is om de voortgang in de analytische en beslissingsondersteunende systemen te koppelen aan operationele logistieke besluitvorming. Om dit concreet te maken: je kunt wel voorspellen wanneer een bepaalde onderhoudsactie nodig is, maar wanneer wordt die dan ook echt bij een technicus ingepland? Het oplossen van deze uitdagingen draagt bij aan het beter controleren van de kosten die gemoeid zijn bij de aanschaf en inzet van grote assets.

Naast de logistieke organisatie van onderhoud kan ook het onderhoudsproces zelf geïnnoveerd worden. Daarbij spelen *virtual reality*, *digital twinning*, en andere kennisondersteunende oplossingen een belangrijke rol.

Concrete initiatieven betreffen: smart maintenance kennisuitwisseling veiligheidsdiensten breed; ontwikkelen *smart maintenance scenarios* nieuwe fregatten, inclusief logistieke organisatie; ontwikkelen *smart maintenance control tower* F35; ontwikkelen publiek-privaat vlootbeheer voor onderhoud en instandhouding voor de landmacht.

Deelprogramma	Onderzoek	Ontwikkeling	Demonstratie	Implementatie
Innovatie in ontwerp en aansturing van netwerken	• Hoe ziet een optimale basis data/informatie infrastructuur voor genetwerkt optreden eruit?	• Toepassingen 5G in het inrichten van nieuwe communicatie-netwerken • Data fusie infrastructuur / voertuigen / payload	• Transformatie data naar tastbare situational awareness met gebruikmaking van nieuwe representatie-mogelijkheden (VR, twinning, …)	• Inzetten bestaande tools voor standaard data uitwisseling, authenticatie en autorisatie
Informatie als wapen	• Gevoeligheid van mensen voor memes en subliminale berichten • Effectiviteit van fake news	• Effectiviteit van sociale media en marketing technieken voor veiligheidsoperaties, • Gerichte beïnvloeding van koopgedrag, leefpatronen, keuzegedrag, radicalisering, agressie • Elektromagnetisch spectrum	• Data integratie en situational awareness, • Inzet van twitter, facebook, instagram als communicatiekanaal naar groepen	• …

Aansturing van genetwerkte logistieke organisaties	• Geavanceerde, geautomatiseerde tools voor connectiviteit van netwerken, extreem onzekere logistieke netwerken, • identificatie van het zwakste punt in netwerken • Wat is de relatie tussen robuustheid en adaptiviteit?	• Leren van opbouw missies/festivals; Command & Control in hybride (bemand/ onbemande) netwerken	• Efficiënte logistieke operaties in vervoer en opslag, op basis van nieuwe technologie, • Samenwerking logistieke operaties in samenwerking met civiele partners, delen voertuigen, outsourcing	• Logistieke oplossingen en software of the shelf
Counter DRAM (Drone, Rocket, Artillery & Mortar)	• Onderzoek naar nieuwe rekenprocessen voor monitoring	• Scenario-analyse onbemande wapensystemen	• Bestaande sensoriek benutten in Counter DRAM acties	• …
Smart service logistics	• Overschakelen van predictive maintenance naar daadwerkelijke logistieke operaties	• Real time data gebruik bij service logistieke operaties • Grensoverschrijdende operaties voor service logistiek vanuit Nederland (F35)	• Optimalisering van maintenance en repair van fregatten, vliegtuigen, landvoertuigen	• Preventive maintenance planning voor schepen en vliegtuigen

3.6 Missie: Samen sneller innoveren voor een adaptieve krijgsmacht

Omschrijving missie [16]

Om samen sneller te innoveren moet er een permanent fijnmazig innovatienetwerk ontstaan waarbij vraag en aanbod bij elkaar worden gebracht om vervolgens kort-cyclisch succesvolle innovaties te implementeren. Het stimuleren van innovaties op basis van (sleutel)technologie leidt tot toepassingen in civiele domeinen en de benutting van oplossingen door civiele organisaties.

Waar gaat deze missie over

Om adaptiviteit te bereiken is een langdurig stabiel fijnmazig innovatienetwerk nodig om vraag en aanbod bij elkaar te brengen met stevige verbindingen tussen de operationele eindgebruikers, de topsectoren en kennisinstituten. Daarnaast moet er ruimte zijn voor de ontwikkeling van nieuwe samenwerkingsvormen, incentives en instrumenten die zijn toegesneden op de wensen van bedrijven die voor en met Defensie werken. Er is een grote behoefte aan samen sneller innoveren. Het scheppen van de juiste voorwaarden en/of juridische kaders voor kort-cyclische innovaties is van belang. Defensie biedt in het kader van Concept Development & Experimentation ruimte voor experimenteren. Innovatie en adaptiviteit vragen om inzicht in het organiseren van het innovatieproces zoals het samenbrengen van de (beoogde) eindgebruikers en de product ontwikkelaars, alsmede en onderzoek naar organisatiekundige vragen vanuit een integraal perspectief van idee tot aan inkoop en gebruik.

Benodigde kennis- en innovatie

Samen sneller innoveren vraagt om beoordelingskaders voor het accepteren van innovaties, gemeenschappelijke protocollen voor het matchen van vraag en aanbod en ecosystemen voor innovaties. 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. Deze drie onderwerpen: Robots, Drones and autonome systemen, 3D-printing en energiesystemen worden hieronder uitgewerkt.

Robots en autonome systemen alsmede drones (Remotely Piloted Aerial Systemd (RPAS), Unmanned Aerial Vehicles (UAV))) en *counter drones measures* heeft een focus op systemen t.b.v. *mule-logistics*, verkenning, bewaking, etc. Het kent onderzoeksvragen op het gebied van intuïtief gebruik, (semi-) autonoom gedrag, robuustheid (o.a. tegen *jamming*, maar ook onderhoud/inzetbaarheid), automatisering en data analyse met als doel mens extensiviteit (minimale tijdsinspanning en maximale productiviteit door operator(s), efficiëntie) en maximaal effectiviteit. Om dit mogelijk te maken zijn ook (nieuwe) sensortechnieken, veilige communicatie sensor-(*edge*)data verwerking en afstemming decentrale (*edge*) verwerking en effectieve informatie uitwisseling/disseminatie naar genetwerkt optreden/hoger informatie platformen nodig. Denk bij sensor techniek niet alleen aan *vision*, herkenningssensoren, maar ook aan gas/stof/chemische/materiaal detectie (*sneufel*)

[16] Een uitgebreide beschrijving van de missies is te vinden op https://www.rijksoverheid.nl/documenten/publicaties/2019/04/26/missies

sensoren en sensoren die ook in averse omgeving (’s nachts, bij slecht weer of b.v. verhullende rook) betrouwbare informatie kunnen geven.

Een ander belangrijk onderdeel voor samenwerking met bedrijfsleven is (het op locatie) *3D-printing* van (reparatie) onderdelen, multi-materiaal printen en te bouwen onderkomens en bescherming, maar ook printen van voedsel/medische verzorging, (individuele) persoonsbescherming, voertuig bescherming, camouflage/misleiding, etc. En niet alleen voor specifiek militaire toepassing, maar ook in het geval van humanitaire missies. Toepassingen met metaal printen, voedsel printen en beton printen in de industrie zijn al volop in ontwikkelingen, inclusief de te gebruiken beschikbaarheid van CAD informatie (*digital twinning*) en print equipment systemen. Uitdagingen liggen hier op het gebied van materiaal gebruik en inzet van disruptieve materialen, maar ook het hergebruik van (plastic) afvalmateriaal en lokaal beschikbare grondstoffen en biomaterialen. Omgevingen/toepassingsgebied hiervoor zijn reparatiewerkplaatsen, maar ook de kampen in uitzendingsgebieden. Daarnaast ligt er de uitdaging om in deze context ook specifieke en geavanceerde 3D-printtechnologie die op meer centrale locaties kunnen worden uitgevoerd. Voorbeelden zijn hele precieze *printing* t.b.v. *stealth* oppervlaktes of herstel van *composite* elementen, printen van sensoren en extra sterke kunststoffen (met lange vezels) en het printen van camouflage en antiballistische structuren. In aanvulling hierop wordt actief gekeken naar geavanceerde materialen. Deze materialen kunnen bijvoorbeeld nieuwe eigenschappen tonen, zoals verbeterde sterkte en stijfheid of verminderde zichtbaarheid voor externe sensoren.

De operationele energie strategie van defensie (OES) alsmede het bredere vraagstuk van energie voor de soldaat, commando post/voertuigen, maar ook generiek aandrijving/voortstuwing van voertuigen, vliegtuigen, fregatten is een derde focus gebied. Alternatieve energiebronnen en (logistieke) voortstuwing zijn gericht op het verkleinen van de milieu footprint van defensie en andere veiligheidsorganisaties, en daarmee het verkleinen van de afhankelijkheid van schaarser wordende fossiele energiebronnen, voor mobiel optreden, faciliteiten, alsmede voor (defensie/humanitaire) missies en in kampen. Dit is een onderwerp dat ook (gedeeltelijke) invulling geeft aan (*energie/circulariteits*) opgaven uit het klimaatakkoord. De uitdaging bestaat eruit dat er verschillende mogelijkheden zijn voor de inzet van nieuwe energiebronnen. Vragen zijn daardoor niet zozeer technisch van aard, maar gaan over de juiste keuze onder bepaalde omstandigheden. Daarbij spelen de business case, maar ook de continuïteit van energievoorziening een rol.

Op basis van bovenstaande beschrijving n.a.v. diverse discussies met defensie en industrie vertegenwoordigers worden als eerste stap in de kennis investeringsagenda (KIA veiligheid – missie 6) de volgende drie kennisvragen (KV1-KV3) als eerste in het MMIP opgepakt:

1. Robot and Autonomous Systems/Onbemande-op afstand bediende systemen (RAS/RPAS);
2. 3D printen en disruptieve materialen;
3. Energie/Circulariteit.

3.6.1 MMIP: Innovaties voor een adaptieve krijgsmacht

Dit MMIP heeft als doel de adaptiviteit van de krijgsmacht te verhogen door concrete innovaties te realiseren op het gebied van: robots en autonome systemen, 3D-printing en energie/circulariteit. Met het realiseren van deze innovaties wordt bijgedragen aan het samen kort-cyclisch tot succesvolle innovaties te komen; *practice what you preach*.

Met de uitvoering van dit MMIP wordt bereikt dat de adaptiviteit van de krijgsmacht wordt vergroot. Dit door het realiseren van innovaties op geselecteerde (sleutel)technologiegebieden, die elk hun bijdrage hebben aan het versnellen en wendbaarder maken van operaties.

Deelprogramma 1: Toepassing van robots/autonome systemen/drones (RAS/RPAS/UAV)

Hier is samenwerking met Nederlandse robot spelers (o.a. leden Holland Robotics), sensor/instrumentatie bedrijven en ICT bedrijven met focus op AR/VR (augmented/virtual reality) zoals *digital twinning* en simulatie (cobot/telemanipulatoren) en *data analytics* (kunstmatige intelligentie/*machine learning*) AI/ML van belang. Waar robots vaak in schone en goed gedefinieerde/gecontroleerde/¬bekende omgevingen worden toegepast ligt hier de nadruk op toepassing chaotische/veranderende/vuile omgevingen. Vuile omgevingen met stof, water, modder, zout zijn ook bekend in de agro (precisie landbouw), de container terminals met autonome voertuigen in de Rotterdamse haven en maritieme wereld. En sensoren moeten betrouwbaar, ook in mensonvriendelijke omgevingen (brand, gaslucht/explosie gevaar) blijven werken. Er wordt door kennisinstellingen en industrie gewerkt aan nieuwe type sensorsystemen die ook bij slecht zicht optimale resultaten behalen, bijvoorbeeld voor reddingsmissies. Op termijn kan dit leiden tot een situatie waarbij juist slecht weer ingezet kan worden als voordeel en is de technologie ook buiten UAV's van toepassing. EMC-verstoring maar ook cyber security van dergelijk systemen is ook in de industrie een belangrijk onderwerp. TNO en NLR werken al samen met defensie op dit gebied in eigen programma's. Maar ook voorzien wij samenwerking met onderwijsinstellingen (universiteiten en in het bijzonder hogescholen) die reeds langer actief zijn op het gebied van bijvoorbeeld voetbalrobots in Eindhoven, drones in Twente, of alternatieve (vlieg/vaar/..) systemen zoals in Delft. Daarnaast zijn er Digital Innovation Hubs voor robotica zoals i-Botics en RIMA, AI en in Smart Industry verband fieldlabs met een aansluiting bij dit onderwerp, niet alleen op technisch innovatie vlak, maar ook op sociale innovatie (skills) gebied. De uitdaging is nu op met robot en ICT leveranciers gezamenlijk plannen en concrete projecten op te stellen cq tot uitwisselbare/gelijk standaarden te komen van platforms, interfaces, componenten (batterij packs) e.d. Tot slot is ook de ontwikkeling van sensoriek en interface voor *detect and evade* technologie van belang

Deelprogramma 2: 3D-printen voor onderdelen, lokale bouw en materiaalontwikkeling

Dit onderdeel vergt samenwerking met 3D grondstof, 3D printmachinebouw en productie bedrijven die 3D onderdelen printen in de range van metaal, kunststof, bouw, voedsel, en multimaterialen alsmede de veelal luchtvaart georiënteerde bedrijven op het gebied van composieten. Ten aanzien van de engineeringsaspecten (ontwerp data en *digital twin* opslag) zal ook hier betrokkenheid van ICT leveranciers nodig zijn. Net als bij deelprogramma 1 zullen ook hier onderwijsinstellingen (universiteit/hogeschool) bij kunnen dragen, alsmede meerdere smart industrie fieldlabs op het gebied van 3D printen en op het gebied van composieten.

Daarnaast worden in dit programma samenwerkt om nieuwe materialen te ontwikkelen, waaronder composieten en wordt onderzocht of daarbij ook bijv. plastic afval kan worden ingezet. Dit kan worden ingezet voor nieuwe toepassingen in bestaan de of nieuwe platformen, bijvoorbeeld om gewicht te besparen of functionaliteit aan onderdelen toe te voegen. Ook kan een bijdrage worden geleverd bij de invulling van de behoefte om nieuwe technologieën en systemen te onderzoeken en te ontwikkelingen voor potentiele nieuwe systemen en *fixed wing* of *rotorcraft* platformen, waarbij

actief wordt ingespeeld op de behoefte van de operatie. Door deze ontwikkeling van dergelijke kennis wordt ook afhankelijkheid van Defensie van buitenlandse OEM-ers verminderd.

Deelprogramma 3: Energiesystemen & circulariteit

In PPS verband zal aansluiting gezocht worden bij de ontwikkelingen die in de energie/klimaat missie en de transport- en logistieke sector al plaatsvinden, zoals het experimenteren met allerlei alternatieve energiebronnen, van wind, zonne-energie, tot biogas, waterstof, methanol en mierenzuur. De uitdagingen in de civiele sector gaan over de combinatie van investeringen in voertuigen en het ontwerpen van de toeleveringsnetwerken voor de bewuste energiebron. Vooral voor de stationaire faciliteiten van veiligheidsorganisaties (kantoren, kazernes, warehouses, etc.) is deze situatie vergelijkbaar. Mogelijk onderwerpen zijn op nieuwe generaties batterijen (4-Gen 3D *solid state* batterijen), warmte opslag, *solar fuels*, e.d. In feite alle drie oplossingen om tijdelijke zon- en windenergie overschotten op te slaan in elektriciteit, warmte en koolwaterstoffen.

Concrete initiatieven zijn o.a. het in kaart brengen energievraagstukken defensie en andere veiligheidsorganisaties, en mogelijkheden om te vergroenen, onder de specifieke condities die gelden in de veiligheidsagenda, het ontwikkelen duurzame energieconcepten in de combinatie gebouwen/voertuigen en de inzet op elektrificeren van specifieke activiteiten/voertuigen. Wat worden de standaarden voor batterij opladen, standaardisatie van ophangframes in voertuigen (en elders) liefst uitwisselbaar tussen civiele *automotive* en NAVO-oplossingen.

In dit programma zal ook worden samengewerkt op het ontwikkelen van technologie om elektrische verbindingen (incl. toebehoren) te verbeteren, bijvoorbeeld door componenten te verkleinen, en te vereenvoudigen en te integreren in structuren. Hierdoor wordt het mogelijk om meer informatiesystemen in dezelfde ruimte te plaatsen, waardoor meer informatie kan worden gekoppeld t.b.v. de operatie. Ook het verkleinen van de bescherming van systemen, terwijl deze in extreme omstandigheden moeten werken.

In dit programma willen we oplossingen voor circulariteit onderzoeken zoals waterzuivering en besparing, afval verbranding t.b.v. energieopwekking en circulariteit van tijdelijke/flexibele toepassing voor zowel humanitaire en militaire toepassing. De inschatting is dat hiervoor reeds diverse oplossing in brede zin beschikbaar zijn, maar dat focusseren op de tijdelijke/flexibele toepassing aanpassingen vereisen op het gebied van eenvoud, robuustheid en vergaande minimalisering van transportkosten. Denk hierbij niet alleen aan waterbesparing, maar ook aan hergebruik van plastic waterflessen voor ander toepassingen.

Deelprogramma	Onderzoek	Ontwikkeling	Demonstratie	Implementatie
Toepassing van robots/autonome systemen/drones (RAS/RPAS)	• Swarming, AI, stille robots	• RAS, RPAS, UAV's, drones, sensors fusion	• Schietbaan robot: UAV-systemen	• Selectie C/MOTS platforms
3D printen voor onderdelen, lokale bouw en materiaal-ontwikkeling	• MM 3D-printen, printen antibal. & disrupt. mat	• Large size Beton & bescherming printen, nieuwe vervangings-onderdelen	• Reparatie/thuiskom onderdelen printen, nieuwe vervangings-onderdelen	• COTS 3D-printing
Energie systemen & circulariteit	• 4G batterijen, warmte opslag, solar fuels	• In kaart brengen energie en vergroening opties • Lokale opwekking / opslag	• Elektrisch transport systemen, afval verbranden voor energie opwekking	• Waterzuivering, standaardisatie batterijen

3.7 Missie: Data en intelligence

Omschrijving missie [17]

In 2030 verzamelen veiligheidsorganisaties nieuwe en betere data, met slimmere analyses worden de juiste interventies gedaan en worden ze niet verrast.

Waar gaat deze missie over

Veiligheidsprofessionals moeten beschikken over tijdige, juiste en op maat geselecteerde informatie. Voor het delen van data zijn institutionele kaders nodig om een juiste balans te houden tussen operationele effectiviteit en maatschappelijke spelregels. Verhoogde observatiecapaciteit leidt tot verruiming van het waarnemingsvermogen en een versterking van de informatiepositie. Een hogere analyse-capaciteit is nodig om (grotere hoeveelheden en real-time) informatie te kunnen verwerken tot bruikbare 'intelligence'. Die vormt de basis vormt voor besluitvorming. De beslissingen worden geëffectueerd door het uitvoeren van een interventie. De uitvoering en de effecten daarvan worden gemonitord en kan leiden tot nieuwe analyses en het bijstellen van de interventie. Het proces van observeren tot en met handelen dient met de juiste kwaliteitswaarborgen te worden uitgevoerd.

Benodigde kennis- en innovatie

De kennis- en innovatiebehoeften liggen op de 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. Betrouwbare en privacy bestendige data-uitwisseling tussen veiligheidsorganisaties en databronnen gebaseerd op burgerparticipatie kunnen toepassen. Analyseren betreft data-integratie, data analyse methodes, voorspellende modellen en *sense making*. Gebruik van AI voor bijvoorbeeld beeldherkenning. Beslissen vraagt om datavisualisatie en beslissingsondersteunende modellen. Voor handelen is toetsing van de effectiviteit van handelingen relevant. Voor kwaliteitsborging het bevorderen van de kwaliteit van data en de betrouwbaarheid en reproduceerbaarheid van interpretaties de besluitvorming relevant.

Aanscherping van bovenstaande kennisvragen leidt tot de volgende twee hoofdvragen:

- *Privacy bestendige informatiedeling:* Er bestaat enorm veel data over mensen, afkomstig van uiteenlopende bronnen, die momenteel niet op voorhand in samenhang geanalyseerd wordt, o.a. op grond van privacy en *confidentiality* overwegingen. De kennisvraag is hier om technische oplossingen te vinden om data in samenhang te kunnen analyseren met behoud van geheimhouding van die data.
- *Beslissingsondersteuning:* Om de veiligheidsprofessional te allen tijde optimaal voor te bereiden op een interventie moet een zo accuraat mogelijk inzicht gegeven worden in de situatie waarin gehandeld moet worden. Dat kan real-time *first responder* (bijvoorbeeld de politieagent op de straat) situaties omvatten, maar ook offline analyse, bijvoorbeeld voor Rechtszaken.

[17] Een uitgebreide beschrijving van de missies is te vinden op https://www.rijksoverheid.nl/documenten/publicaties/2019/04/26/missies

3.7.1 MMIP: Data en intelligence

Dit MMIP heeft als doel het realiseren van oplossingen voor privacy-bestendige informatiedeling tussen verschillende partijen en op basis van data en intelligence de juiste beslissingen te kunnen nemen.

Met de uitvoering van dit MMIP wordt bereikt dat incidenten, die we hadden kunnen zien aankomen, nauwelijks meer voorkomen en we zeer weinig voorkomende incidenten met veel impact (waar veel ketenpartners gegevens voor moeten leveren) ondervangen. Verder wordt met de uitvoering van dit MMIP bereikt dat de situatie juist is ingeschat, geheel conform de werkelijkheid en zodanig doorgegeven aan de professional dat die de optimale interventie uitvoert. Alle modellen die daarbij gebruikt worden in de informatiedeling en beslissingsondersteuning zijn geaccepteerd, uitlegbaar, vertrouwd en transparant.

Deelprogramma 1: Privacy-bestendige informatiedeling

Dit deelprogramma beoogt oplossingen te bieden voor de volgende uitdagingen:

Het ontwerpen van een systeemarchitectuur / infrastructuur die data-deling mogelijk maakt. Parallel aan de infrastructuur zal ook een passend governance-model moeten worden ontworpen. De oplossingen moeten gecertificeerd en gestandaardiseerd worden. Tevens zullen kritische systeemeigenschappen goed gedefinieerd en gevalideerd moeten worden, een voorbeeld hiervan is het begrip 'anonimiteit'. Een open vraag is in hoeverre het realiseren van privacy en *confidentiality* de prestaties van beslissingsondersteuning, bias, representativiteit en ongewenste nevenactiviteiten beïnvloed. Onduidelijk is vooralsnog hoe data cleaning op geanonimiseerde data gedaan moet worden. Bovendien kan het anonimiseren van een data set teniet gedaan worden door andere data sets, of door andere informatie elementen in de data set (context informatie).

Het ontwerpen van oplossingen voor data-analyse met behoud van anonimiteit zoals bijvoorbeeld homomorfe encryptie, *multiparty computation* en pseudo- anonimisering]. Het vinden van technisch-wetenschappelijke oplossingen voor uitlegbaarheid, verifieerbaarheid en onweerlegbaarheid van uitkomsten, zowel bij preventieve analyse als bij strafrechtelijke analyse. Hier speelt ook een grote niet-technische component mee. Een mogelijke oplossing voor uitlegbaarheid is het opstellen van hypotheses met een bijbehorende waarschijnlijkheids-afschatting'. Uitlegbaarheid is niet altijd belangrijk, denk aan situaties waarbij een willekeurige keuze mogelijk is, zoals b.v. bagage-inspectie. Speciale aandacht is nodig voor *'deep fakes'*

Het realiseren van schaalbaarheid van de complete informatie-verwerkende keten, waardoor grote hoeveelheden data uit verschillende bronnen snel gecombineerd kunnen worden en tot conclusies kunnen leiden. Heel veel data verzamelen hoeft zeker niet tot betere uitkomsten te leiden, integendeel, het kan problemen opleveren omdat het niet a priori duidelijk is of data representatief is, dan wel vervuild is met irrelevante data. Hoe bruikbaar is data uit het verleden voor het voorspellen van toekomstige situaties, die niet eerder gezien zijn? Schaalbaarheid is ook in maatschappelijk opzicht een uitdaging: Zo kan de Rechterlijke macht per situatie een andere inschatting maken t.a.v. het geleverde bewijs en de onweerlegbaarheid ervan.

Het zorgdragen voor maatschappelijke/ethische/juridische acceptatie m.b.t. deze nieuwe manier van informatie gestuurd werken. Eveneens de consequenties van deze nieuwe manier van werken voor alle betrokkenen in kaart brengen en een pad naar implementatie schetsen. In verband met aansprakelijkheid voor fouten van het AI product zijn keurmerken en certificatie van belang. Het

systeem moet weten en aangeven wanneer het niet meer de juiste kwaliteit van besluit kan nemen. Tegelijkertijd kan een systeem alleen leren als er ook fouten gemaakt mogen worden. Werk dus naar een governance architectuur toe die open is, afgestemd op technische mogelijkheden en nog te ontwikkelen oplossingen.

Deelprogramma 2: Beslissingsondersteuning

Dit deelprogramma beoogt oplossingen te bieden voor de volgende uitdagingen:

Het op het juiste moment beschikbaar maken van alle relevante data, daarop een analyse te kunnen doen om daarmee een preferente interventie met eventuele alternatieven aan te kunnen bieden aan de professional. Belangrijk is ook de conversie van relevante data zodanig dat het combineerbaar wordt met andere data, bij voorbeeld de conversie van natuurlijke taal naar geschreven en geanalyseerde tekst. Analoog is de conversie van video beelden naar 'situatie inschatting'. Hieronder vallen ook de specifiek Nederlandse uitdaging van NL taalherkenning (en al helemaal jargon, Bargoens, lokale dialecten, ..,). Ook bij dit deelprogramma is, (op maat gemaakte voor de situatie) uitlegbaarheid, verifieerbaarheid, traceerbaarheid, en onweerlegbaarheid van de aanbeveling essentieel.

Het vinden van technische oplossingen voor het probleem dat datasets waarop systemen getraind worden, klein en asymmetrisch kunnen zijn, dat terwijl een hele hoge precisie en *recall* wordt gevraagd, immers een *'false negative'* leidt tot het niet nemen van actie waar dat wel nodig was en een *'false positive'* leidt tot actie waar die overbodig was. Hoe kan informatie zodanig aan de professional worden gegeven, dat er zo weinig mogelijk mentale belasting ontstaat en de professional ogen en oren op de omgeving kan blijven richten. Essentieel is om slechts relevante informatie, geen irrelevante informatie aan te bieden.

Deelprogramma	Onderzoek	Ontwikkeling	Demonstratie	Implementatie
Privacy-bestendige informatiedeling	• Data processing op geanonimiseerde data en zeer asymmetrische datasets • Schaalbaarheid • Uitlegbaarheid, verifieerbaarheid, onweerlegbaarheid • Hypothese generatie	• Open Infrastructuur voor data-delen • Transparantie omtrent de nieuwe manier van data-gestuurd werken • Maatschappelijke acceptatie	• Stapsgewijze introductie van nieuwe mogelijkheden op basis van een open infrastructuur	• Aanvankelijke implementatie in die gebieden waar veel te winnen is en relatief weinig uitdaging bestaat [crowd management vs. Lone wolf]
Beslissings-ondersteuning	• Data processing op geanonimiseerde data • Schaalbaarheid & snelheid van data verwerking • Uitlegbaarheid, verifieerbaarheid, onweerlegbaarheid • Hypothese-generatie met waarschijnlijkheids-afschatting • Human interfaces	• Open Infrastructuur voor data-delen • Transparantie omtrent de nieuwe manier van data-gestuurd werken • Maatschappelijke acceptatie	• Stapsgewijze introductie van nieuwe mogelijkheden op basis van een open infrastructuur	• Aanvankelijke implementatie in die gebieden waar veel te winnen is en relatief weinig uitdaging bestaat [crowd management vs. Lone wolf]

3.8 Missie: De veiligheidsprofessional

Omschrijving missie[18]

Het vak van veiligheidsprofessional behoort in 2030 tot de top 10 van meest aantrekkelijke beroepen in Nederland.

Waar gaat deze missie over

Met veiligheidsprofessionals wordt gedoeld op de civiele, militaire en private beroepsgroep die in operationele zin zorg draagt voor het voorkomen van onveilige en onwettige situaties, en optreedt bij incidenten, conflicten en crisissituaties. Vanuit een integrale benadering kan veel gedaan worden aan de verbetering van de toerusting van de veiligheidsprofessional. Bestuurskundige en bedrijfskundige inzichten en kennis vanuit organisatiewetenschappen kunnen helpen bij het versterken van de effectiviteit van de veiligheidsprofessional. Moderne technologie en gedragswetenschappelijke inzichten kunnen de mentale en fysieke weerbaarheid verhogen en bijdragen aan een betere opleiding en selectieprocedure. Verbeteringen zijn nodig op drie terreinen: 1. werving, selectie, opleiding en training; 2. persoonlijke prestatie en 3. weerbaarheid.

Benodigde kennis en innovatie

Kennis- en innovatievragen bij deze missie liggen op het gebied van opleiding, persoonlijke prestatie en weerbaarheid. Bij opleiding, oefenen en trainen wordt gebruik gemaakt van simulatie, VR en AR en/of *serious gaming*. Naast aandacht voor de fysieke component is ook de mentale conditie van belang. Ondersteuning vanuit gedragswetenschappen is essentieel. Persoonlijke prestatie wordt versterkt met technologieën als AR, identificatietechnologie, spraak- en vertaal apps, betere kleding, bewapening, exoskeletten, bepantsering en aanvulling met robots, *agents* en AI-systemen. Weerbaarheid, fysieke prestaties en gezondheid worden doorlopend gemeten, geanalyseerd en voorspeld voor een efficiënt optreden. Onderzoek naar aard en achtergronden van traumatische stoornissen, en de ontwikkeling van programma's om werkgerelateerde klachten te voorkomen.

Om het vak van veiligheidsprofessional ook in 2030 in de top 10 van meest aantrekkelijke beroepen te hebben staan zullen professionals, werkgevers en uitvoeringsorganisaties in het veiligheidsdomein mee moeten met de tijd en zich moeten voorbereiden op toekomstige digitale ontwikkelingen die opleiding, training, persoonlijke prestatie en de weerbaarheid zullen beïnvloeden. Om de duurzame inzetbaarheid en vitaliteit van elke individuele veiligheidsprofessional te waarborgen dienen bovengenoemde stakeholders te worden meegenomen en voorbereid op deze transitie. Het collectief ontwikkelen van oplossingen middels een centrale en proactieve (ipv reactieve) probleem-gedreven vraagarticulatie zal dit faciliteren.

Hiervoor is het belangrijk dat veiligheidsprofessionals zich digitaal wapenen. Daarvoor zal allereerst worden onderzocht waaruit de cruciale *skill*-set (onder andere ten behoeve van mentale weerbaarheid) van veiligheidsprofessional moet bestaan. Daarnaast zullen innovatieve leermethodes worden ontwikkeld om effectieve, schaalbare en betaalbare ondersteuning te bieden voor de ontwikkeling van deze *skill*-set. (*Deelprogramma 1 - Qualified-Self, Digitaal wapenen middels nieuwe (leer)methodes)*

[18] Een uitgebreide beschrijving van de missies is te vinden op https://www.rijksoverheid.nl/documenten/publicaties/2019/04/26/missies

Door prestatie en vitaliteit van veiligheidsprofessional meetbaar te maken kan de persoonlijke inzetbaarheid en mentale weerbaarheid beter gemonitord worden. Door actief onderzoek te doen naar effectieve methoden en technologie voor persoonlijke ontwikkeling en interventies op basis van individuele datasets zullen veiligheidsprofessional beter getraind en duurzamer ingezet kunnen worden. Met als doel dat medewerkers tot het einde van hun loopbaan inzetbaar blijven en met plezier naar hun werk gaan. *(Deelprogramma 2 - Quantified-Self, Meetbare prestatie en vitaliteit van veiligheidsprofessionals)*

Onderdeel van moderne inzetbaarheid is ook de ontwikkeling van nieuwe waarnemingssystemen, wearables (spraak- en vertaalapps) en non-wearable (*virtual agents/chatbots*) oplossingen ter versterking van de communicatie. (*Deelprogramma 3 - Digitaal uitgerust - Waarneming en communicatie*)

Voor een veilig Nederland in 2030 is het belangrijk om veiligheid doorlopend te blijven duiden. Wat vinden wij als maatschappij belangrijk, hoe definiëren we veiligheid en biedt dit duurzame zingeving voor alle individuele veiligheidsprofessionals. *(Deelprogramma 4 - Reframing Veiligheid)*

3.8.1 MMIP: Gekwalificeerde en gekwantificeerde veiligheidsprofessionals

Dit MMIP heeft als doel veiligheidsprofessionals via nieuwe leermethoden te wapenen voor de uitdagingen van de (toekomstige) digitale ontwikkelingen, de prestaties en vitaliteit te kunnen meten en de professionals te ondersteunen met krachtige digitale technologie. Daarnaast is een doel het bieden van zingeving binnen het vak van veiligheidsprofessionals.

Met de uitvoering van dit MMIP wordt bereikt dat veiligheidsprofessionals zijn voorbereid op de toekomst, betere prestaties leveren en weerbaarder zijn en goed zijn uitgerust met digitale middelen.

Deelprogramma 1: Qualified-self, Digitaal wapenen middels nieuwe (leer)methodes

Digitale ondersteuning en bekwaamheid staan centraal in dit deelprogramma. Hiervoor zal onderzoek worden gedaan naar wat de *'21st century skillset'* van de veiligheidsprofessional moet zijn om voldoende gekwalificeerd te zijn, te blijven en te worden. Om deze *skillset* effectief, betaalbaar, schaalbaar en doorlopend te trainen zal veldonderzoek worden gedaan naar de meest effectieve nieuwe digitale leermethodes (AI, AR, VR, *Serious gaming, 360 graden simulaties*) op de lange termijn, ter voorbereiding van veiligheidsprofessional op emotionele impact in de operatie, stress en risicovolle situaties. En rekening houdend mat individuele leerstijlen. Deze inzichten zullen worden vertaald naar prototypes voor 1.) het meetbaar maken van prestaties in digitale simulaties en 2.) realistische en doorlopende trainingsprogramma's die veiligheidsprofessionals echt voorbereiden op de toekomst.

Deelprogramma 2: Quantified-self, Meetbare prestatie en vitaliteit van veiligheidsprofessionals

Vanuit een individuele dataset kan persoonlijke mentale kracht en prestatie worden gemeten ten behoeve van het verhogen van de prestatie en psychische gezondheidsbescherming. Om dit maatwerk te bereiken zal worden onderzocht welke data (en voorspellers van psychische gezondheid) en bijpassende technologie er nodig is om doorlopend te kunnen leren en persoonlijke competenties te kunnen ontwikkelen vanuit de operatie (soortgelijke systemen worden nu al ingezet

door SpecOps in de VS en Formule 1 teams). Voor effectieve monitoring van veiligheidsprofessionals zal onderzoek naar benodigd materieel en uitrusting worden gedaan ten behoeve van nieuw te ontwikkelen en toe te passen technologie (bijvoorbeeld sensoren, slimme pakken). Voor de behandeling en preventie van traumatische stoornissen zal integraal geïnventariseerd worden welke instrumenten er al bestaan en welke ook daadwerkelijk effectief zijn en wanneer (preventie, gouden uur na incidenten (ABCDE methodiek), monitoring, behandeling).

Deelprogramma 3 - Digitaal uitgerust - Waarneming en communicatie

Ook in het veld zal de veiligheidsprofessional (moeten) worden ondersteund door krachtige digitale technologie. Onderdeel van dit deelprogramma zijn oplossingen die de communicatie bevorderen en daarmee het waarnemingsvermogen verbeteren. In het veld zal een sterke verschuiving van tekst naar spraak plaats vinden. Hiervoor zal onderzoek gedaan moeten worden naar de ontwikkeling van faciliterende en zelflerende AI-systemen voor: een *speech-to-text engine* voor de Nederlandse taal, chatbots (op basis van verbale communicatie), *virtual agents* (op basis van non-verbale communicatie om emoties bij menselijke gebruikers in uitdrukking en spraak te herkennen).

Het ter beschikking maken van high-end hulpmiddelen ondersteunt de professional bij zijn taakuitoefening en vakbekwaamheid. Alleen met goed gereedschap zal de professional op een (ook voor hem) bevredigende wijze zijn werk kunnen doen en daar voldoening uit putten.

Deelprogramma 4: Reframing veiligheid

Voor het bieden van zingeving binnen het vak van veiligheidsprofessionals dient het begrip veiligheid te blijven worden geduid. Hiervoor is een breed perspectief van buitenaf nodig, wat in samenwerking met verschillende betrokken bevolkingslagen zal worden geformuleerd. In samenwerking met deze stakeholders zal de duiding van veiligheid (normen, waarden, zingeving) doorlopend worden ontwikkeld, verrijkt en geïmplementeerd in bv opleidings- en trainingsprogramma's. De inzichten dienen ook als basis voor het morele weerbaarheidsdomein.

Deelprogramma	Onderzoek	Ontwikkeling	Demonstratie	Implementatie
Qualified-self, Digitaal wapenen middels nieuwe (leer)methodes	• Integraal onderzoek naar '21st century skillset' van de veiligheidsprofessional • (Veld) onderzoek naar lange termijn effectiviteit van nieuwe leertechnologie (VR/AR/Serious Gaming) t.b.v. schaalbare demonstratie en implementatie	• Doorlopende leerprogramma's in de operatie o.b.v. persoonlijke data(one-size fits all voldoet niet meer) en met zelfsturing als basis	• Prototyping van toepassingen voor het meetbaar maken van prestaties in digitale simulaties	• Betere prestaties door het aanbieden van kosteneffectieve (simulatie)trainingen die beter aansluiten bij de realiteit van de praktijk, op basis van 3 componenten: (1) individueel gepersonaliseerd (2) veilige gecontroleerde omgeving (3) gebruikmakend van Learning analytics • Digitaal platform dat instructeurs real time inzicht geeft in beleving en prestaties van professionals die

				worden getraind in een volledig immersieve leeromgeving (d.w.z. full body immersion; veel meer dan één zintuig) en dat hen in staat stelt de leerervaring bij te sturen zodat de beoogde fysieke, mentale en/of cognitieve leerdoelen behaald kunnen worden
Quantified-self, Meetbare prestatie en vitaliteit van veiligheidsprofessionals	• Onderzoek naar welke data er nodig is voor doorlopende monitoring van veiligheidsprofessionals • Integraal onderzoek naar effectiviteit van al beschikbare instrumenten voor behandeling traumatische stoornissen (o.a. PTSS)	• Draagbare monitoring technologie voor meetbaar maken van prestatie en vitaliteit van veiligheidsprofessionals	• Prototyping van geavanceerde technologie ontwikkeling ten behoeve van fysiek, cognitieve en mentale gezondheid, prestaties en inzetbaarheid. Manieren om presteren en veerkracht te verbeteren, gebruik makend van sensoren, monitors en dashboards, om fysiologische input toe te voegen t.b.v. performance en inzetbaarheid	• Een digitaal platform met wearable-, app- en dashboarding technologie, dat de veerkracht van medewerkers ondersteunt door gepersonaliseerde feedback te bieden (op basis van algoritmen voor machine learning), en die de inzetbaarheid verbetert door interventiestrategieën op basis van voorspellende algoritmen voor te stellen
Digitaal uitgerust - Waarneming en communciatie	• Onderzoek naar waarnemingssystemen die precies vertellen wat de situatie is zodat de professional actie kan nemen met minimaal aanvaardbaar risico. • Onderzoek naar communicatiebevorderende tooling.	• AI-systemen voor speech-2-text toepassingen Nederlandse taal • AI-systemen voor verbale toepassingen (chatbots) en non-verbale toepassingen (virtual agents) • AI-systemen voor herkennen van emoties bij menselijke gebruikers in uitdrukking en spraak	• …	• …
Reframing veiligheid	• ….	• Doorlopend en maatschappelijk duiden van veiligheid i.s.m. verschillende bevolkingslagen	• …	• Implementatie en communicatie van geduide normen/waarden veiligheid t.b.v. zingeving veiligheidsprofessionals

4 Uitvoering van de agenda

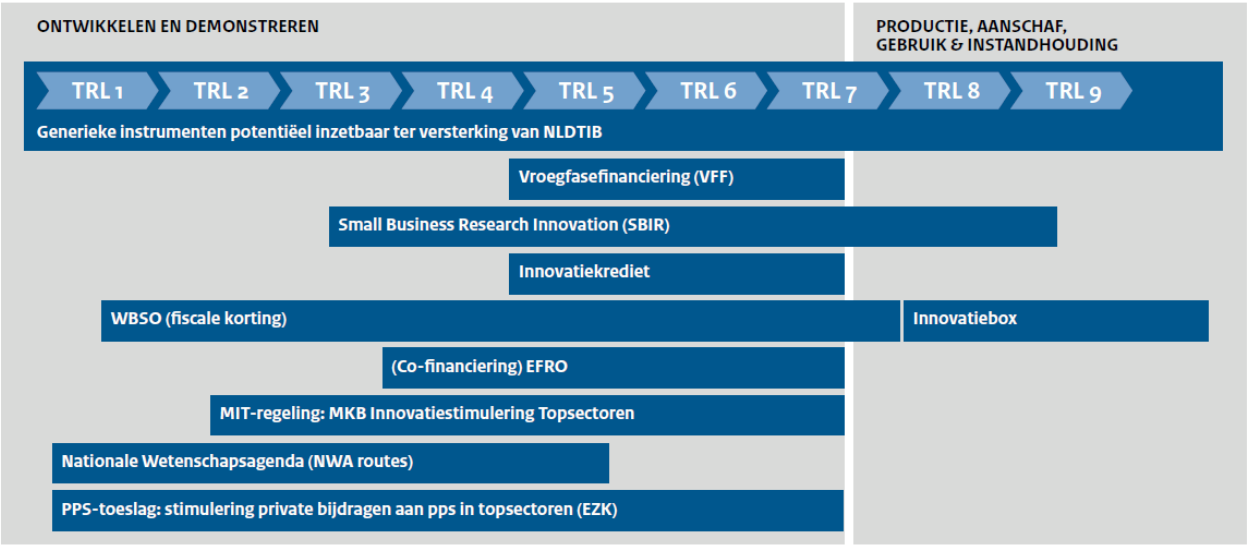
4.1 Instrumenten

Voor de uitvoering van de KIA Veiligheid zijn instrumenten nodig om de in het Kennis- en Innovatiecontract (KIC) gecommitteerde financiële middelen in te zetten. Dat zijn onder andere instrumenten die de overheid in staat stellen om als *launching customer* op te treden na een succesvol innovatietraject, maar ook instrumenten gericht op de ontwikkeling, demonstratie en exploitatie van technologie. We benoemen hieronder enkele voorbeelden van bestaande instrumenten die voor de KIA Veiligheid relevant zijn.[19]

Hoewel er een breed palet aan instrumenten beschikbaar is, onderkent de Nota Defensie Industrie Strategie (DIS) (2018) dat niet elk van deze instrumenten (eenvoudig) toe te passen is binnen de defensie- en veiligheidgerelateerde industrie. Bij de uitvoer van de KIA Veiligheid zal dus in de praktijk moeten worden bekeken of met de bestaande regelingen de gecommitteerde middelen daadwerkelijk voor de projecten beschikbaar kunnen worden gemaakt.

Instrumenten gericht op technologieontwikkeling en innovatie

De overheid biedt diverse instrumenten aan die de opbouw van kennis, en de ontwikkeling en exploitatie van technologie stimuleren. Figuur 3.1 biedt een (niet uitputtend) overzicht van beschikbare generieke instrumenten waar mogelijk een beroep op kan worden gedaan. Daarnaast beschikt Defensie ook over specifieke innovatie-instrumenten, zoals de Defensie Innovatie Competitie en Nationale en Internationale Technologie Projecten (ITP/NTP), om technologie ontwikkeling en exploitatie te stimuleren.



Figuur 4.1: Overzicht van beschikbaar generiek instrumentarium (Figuur 4.1 in DIS 2018)

De overheid als 'launching customer'

Overheden zijn in veel gevallen de operationeel eindgebruiker van de producten en diensten van de defensie- en veiligheidgerelateerde industrie. Het optreden van de Nederlandse overheid als eerste

[19] We benadrukken dat dit slechts voorbeelden zijn en op geen wijze moet worden geïnterpreteerd als een volledige opsomming van het beschikbare en (mogelijk) relevante instrumentarium.

afnemer *('launching customer'*) van een nieuw product kan daarom een belangrijke bijdrage leveren aan het succesvol naar de markt brengen én internationaal positioneren van nieuwe producten en diensten. In de eerste plaats als afnemer van het product of de dienst, wat bijdraagt aan de valorisatie. Daarnaast kan het vertrouwen in Nederlandse producten bij buitenlandse overheden en leveranciers worden vergroot als aangetoond is dat de Nederlandse overheid het product operationeel toepast. Voor exportdoeleinden, zeker in de defensie- en veiligheidsmarkt, is dergelijk vertrouwen van groot belang. Daarmee kunnen nieuwe, innovatieve producten sneller bij een groter publiek terecht komen, wat de valorisatie vergroot.

Uit de Defensie Industrie Strategie (2018) blijkt dat er momenteel geen instrument is die Defensie in staat stelt om effectief op te treden als *launching customer*. De CODEMO-regeling van Defensie, opgezet als een revolverend fonds, biedt daarvoor de meeste mogelijkheden, maar richt zich vanwege de huidige financiële omvang vooral op het mkb. Daarom hebben EZK en Defensie samen toegezegd dat de regeling zal worden doorontwikkeld, zodat het ook voor grotere bedrijven mogelijk zal worden om gebruik te maken van de CODEMO-regeling.[20] Gezien het belang van de overheid als *launching customer* beschouwen wij de doorontwikkeling én toepassing van CODEMO als een goede kans om de valorisatie van de ontwikkeling tot stand te brengen.

Instrumenten als SBIR en Innovatiepartnerschap worden ingezet waar van toepassing.

Europese onderzoeks- en ontwikkelingsprogramma's

In het toekomstige (9e) kaderprogramma Horizon Europe is het thema veiligheid opgenomen. Voor Horizon Europe is een missiegedreven aanpak gekozen om aansluiting bij de marktbehoeftes verder te verbeteren. De geschatte totale omvang van dit programma is naar verwachting 100 miljard Euro voor de hele looptijd. Vanaf 2021 zal tevens defensieonderzoek *en* ontwikkeling vanuit de Europese Commissie financieel worden ondersteund via het European Defence Fund (EDF) met een verwacht budget van circa 10,5 miljard Euro. Bijzonder is dat het EDF niet alleen onderzoek financieel ondersteunt maar ook de ontwikkelingen van capaciteiten. Beide programma's, Horizon Europe en het EDF, moeten gezien worden in het licht van de EU Global Strategy. Daarin zijn verschillende initiatieven en acties geformuleerd die moeten bijdragen aan een grotere zelfstandigheid en onafhankelijkheid van de EU ten opzichte van de Verenigde Staten van Amerika, China en Rusland.

De Commissie en de lidstaten hebben elf capaciteitsgebieden vastgesteld die richting moeten geven aan de defensieonderzoeks- en ontwikkelingsprogramma's in het EDF. Een vergelijkbaar instrument bestaat niet voor het veiligheidsonderzoek. Keuzes vanuit een technologie of toepassingsperspectief is niet de enig invalshoek. De in Nederland bestaande industriebasis, inclusief MKB, is een andere, maar eveneens relevante invalshoek. Europese financiering kan worden aangewend om de bestaande industriebasis te versterken maar ook om opkomende industrieën te ondersteunen in hun ontwikkeling. Een derde invalhoek is die van het toepassingsgebied. Diverse technologieën lenen zich voor toepassing in verschillende toepassingsgebieden.

Om maximale efficiëntie en effectiviteit te kunnen bereiken is het wenselijk projecten te volgen waarbij dezelfde technologie(-basis) wordt gebruikt maar voor verschillende toepassingen. Dit om er voor te zorgen dat zodat de (basis-) technologieën ook in andere thema's kunnen worden gebruikt bij de ontwikkeling van nieuwe toepassingen. Een dergelijk volgsysteem zou nationaal moeten worden opgezet en laagdrempelig moeten zijn om ook startups en MKB te stimuleren gebruik te maken van de verzamelde informatie.

[20] Defensie Industrie Strategie (2018)

Voor zover mogelijk zou daarbij ook rekening moeten worden gehouden met (defensie-)onderzoek wordt uitgevoerd met name binnen de NATO Science & Technology Organisation (STO). Dat onderzoek wordt voor wat betreft Nederland voor het overgrote deel gefinancierd uit de kennisopbouwmiddelen van het Ministerie van Defensie.

4.2 Valorisatie en marktcreatie

Valorisatie, de vertaalslag van (wetenschappelijke) kennis naar economische en/of maatschappelijke waarde is samen met marktcreatie een sleutelbegrip in het missiegedreven innovatiebeleid van dit kabinet en zal een van de belangrijkste doelstellingen blijven van de topsectoren. In de ideale situatie neemt valorisatie een centrale plek in binnen de onderzoeksinstellingen en zijn kennistransferprocessen en -voorwaarden gericht op het stimuleren van kennisverzilvering.

Binnen het thema Veiligheid is een bredere aanpak nodig, met name:

- Het bevorderen van deelname van (MKB-) bedrijven aan onderzoekconsortia / PPP's;:
- Het bevorderen van startups/*scale-ups*: het scouten, screenen, opwerken, begeleiden, investeringsrijp maken en financieren van kansrijke nieuwe bedrijven;
- Valorisatie via bestaande bedrijven; dat kan individueel, maar ook via allianties van bedrijven, clusters van bedrijven en bredere (thematische) ecosystemen en
- Faciliteiten die zowel nieuwe als bestaande bedrijven nodig hebben om nieuwe producten, diensten en methodieken te kunnen testen, valideren en vooral op te schalen.

Het betrekken van bedrijven in de programma's zal eerst en vooral gebaseerd moeten worden op de aansluiting van de bedrijfsactiviteiten bij specifieke programmaonderdelen. De diversiteit in de bedrijfsachterban vraagt om een diversiteit aan programmering en instrumenten om betrokkenheid van bedrijfsleven te borgen. In veel ecosystemen sluiten bedrijven (inclusief MKB) aan bij PPS-constructies met duidelijke innovatiedoelen en draagt ieder bij met expertise. Een sterk PPS kan worden opgezet door op voorhand al een sterk commitment van private partijen te hebben en programma's en projecten van begin af aan als een partnership op te zetten. Daarbij zijn de spelers grotendeels al bekend (in ieder geval de grote partijen). In andere ecosystemen is er ruimte voor open Calls waar private partijen (al dan niet meegenomen door een kennisinstellingen) met een passend voorstel op reageren. Dit past beter bij de relatief beperkte draagkracht en horizon van dat MKB.

4.3 Regionale inbedding

Regionale overheden en regionale ontwikkelingsmaatschappijen (ROM's) zijn belangrijke partners bij valorisatie en marktcreatie. Zij kunnen een stevige bijdrage leveren aan de verwezenlijking van het missiegedreven innovatiebeleid op het gebied van Veiligheid, met name in relatie tot het MKB. Regio's en ROM's weten hoe in de topsectoren succesvolle ecosystemen kunnen worden gebouwd. Zij zijn competent om nieuwe, veelbelovende bedrijven te ontwikkelen en te financieren. Het is daarom waardevol de kennis te mobiliseren die zij in dit verband hebben opgebouwd, gebruik te maken van het kapitaal dat zij in kunnen zetten voor goede bedrijven en hun netwerken te ontsluiten om de ambities van de topsectoren te realiseren.

Voor een succesvolle aanpak van de brede valorisatiebenadering is het belangrijk om te komen tot afstemming en waar mogelijk een samenhangende programmering van activiteiten en middelen tussen de topsectoren en de regio's / ROM's, inclusief regionale innovatiestructuren en vergelijkbare regionale organisaties gericht op business development en financiering in de regio's. Doel van de

samenwerking is de regio's / ROM's beter te benutten als groeiversnellers voor veelbelovende nieuwe en bestaande bedrijven in de topsectoren en daarmee de uitvoering van de KIA richting succesvolle toepassingen en brede implementaties te stimuleren. Deze samenwerking kan praktisch vorm krijgen langs vijf lijnen:

1. *Het bieden van inzicht* in het landschap van relevante voorzieningen, faciliteiten en instrumenten per thema;
2. *Makelen en schakelen*: gerichte koppelingen tussen topsectorinitiatieven en de voorzieningen, initiatieven en instrumenten in de regio's;
3. *Ontwikkeling van nieuwe producten, diensten en projecten* om witte vlekken in te vullen;
4. *Alignment en/of bundeling* van landelijke, regionale en thematische instrumenten en middelen;
5. *Het bouwen van gezamenlijke proposities rond kansrijke thema's voor een geïntegreerde aanpak* van technologieontwikkeling, innovatievermogen en talentontwikkeling.

Op het gebied van Veiligheid kunnen regio's vanuit de missies de link leggen met kennisinstellingen en bedrijfsleven in regionale clusters zoals The Hague Security Delta, Twente Safety Campus, Businesspark Aviolanda, waar sterke netwerken van MKB binnen het Veiligheidsdomein vertegenwoordigd zijn. Samenwerking met deze regionale netwerken biedt de kans om MKB beter aan te laten haken op de missies en daarop nieuwe veiligheidsoplossingen en –producten te ontwikkelen. Daarnaast wordt de verbinding met het MKB in de regio's versterkt via regionale proeftuinen zoals Digital Trust Centers, en regionale Smart Industry Hubs, waar MKB-ers worden ondersteund bij het digitaal weerbaar maken van de maakindustrie. Ook sectorspecifieke innovatieprogramma's zoals het Cybersecurity Programma Groningen en het Innovatieprogramma Maintanance & Services (Noord-Brabant) dragen bij aan versterking van het innovatievermogen binnen het veiligheidsdomein. Daarbinnen spelen ROM's met hun beschikbare fondsen en business-development een belangrijke stimulerende rol voor verdere innovatieontwikkeling binnen de sector.

Voor de provincies en het Rijk is marktcreatie een interessante vorm om innovatie binnen het MKB en starters te bevorderen. We zoeken echter ook samenwerking met alle (semi-) overheden die grote financiers zijn in de maatschappelijke uitdagingen achter de missies. Zo ontstaat een enorm vermogen om innovaties te genereren die de missies sneller, beter en goedkoper tot een einde kunnen brengen. Dat zijn dus het Rijk, maar bijvoorbeeld ook gemeenten met een specifieke focus op veiligheid (zoals Den Haag met onder meer The Hague Security Delta) en veiligheidsregio's en de ROM's met hun netwerken, business development en financieringsopties. Voor de financiering van de projecten en de organisatie zoeken we een verdeelsleutel die recht doet aan de belangen en verantwoordelijkheden van de verschillende partijen, maar waar relevant ook aan het economisch stimuleringseffect. Waar van toepassing, wordt gebruik van de EFRO-structuurfondsen aangemoedigd.

4.4 Kennisoverdracht

Wetenschapsbrede aanpak

Het funderend onderzoek binnen deze KIA zal naar verwachting voornamelijk uitgevoerd worden door NWO in samenwerking met private partijen en met behulp van het instrumentarium voor de Kennis- en innovatieagenda. Het thema Veiligheid en de in deze KIA beschreven missies en MMIP's bieden volop kennis- en innovatievragen die voor een wetenschapsbrede aanpak pleiten, van technologie tot het menselijke gedrag. Enerzijds is de ontwikkeling van nieuwe technologie onmisbaar voor Veiligheid. Anderzijds vergen de transitie naar de inzet van deze technologie en de

daarmee verbonden implicaties voor de maatschappij onderzoek op het gebied van de sociale wetenschappen. Het menselijke gedrag is immers van enorme invloed, zowel voor de veiligheidsprofessionals als voor de maatschappij. Ook logistieke vraagstukken, beslissingsondersteuning en juridische kaders alsmede privacy kwesties zijn van belang. De verbinding tussen deze vraagstukken is essentieel voor een gerichte aanpak van dit thema.

Samenwerking in geheel ecosysteem

Voor onderzoek en innovatie op het gebied van Veiligheid is de samenwerking in het gehele ecosysteem van gebruikers/maatschappij, overheid, kennisinstellingen en bedrijfsleven vereist.

Deze aspecten voor de aanpak van het thema Veiligheid vragen om een gerichte strategie rondom kennisbenutting en –overdracht gericht op het bereiken van impact en de valorisatie van de opgebouwde kennis, bijvoorbeeld door het faciliteren van interacties tussen gebruikers en onderzoekers. Bij de voorbereiding en uitvoering van projecten, maar ook tijdens het vormen van consortia zal hierop worden gestuurd vanuit de governance.

Met oog op de internationale ontwikkelingen op dit terrein is de aansluiting bij en afstemming met internationale activiteiten hierbij onmisbaar. Ook een wisselwerking tussen de kennisopbouw voor het thema Veiligheid en voor de andere thema's en sleuteltechnologieën is noodzakelijk.

4.5 Human Capital

De gezamenlijke topsectoren werken aan een gezamenlijke *roadmap* Human Capital Topsectoren 2020 – 2023 voor geheel Nederland, met oktober 2019 als geplande tijd van oplevering, met als doel dit sectoroverstijgend te versterken. De *roadmap* wordt vorm gegeven in samenhang met lopende trajecten zoals Techniekpact (o.a. EZK, OCW, SZW, regio's, werkgevers en werknemers), MKB Actieplan, Nederlandse Digitaliseringsstrategie, Smart Industry (*skills labs*) en het Klimaatakkoord. Inzet is om dubbel werk te voorkomen en een efficiënte en effectieve samenwerking te organiseren.

Universiteiten en hogescholen dragen bij aan de ontwikkeling van *human capital* door opleiding van nieuwe talenten en onderzoek naar de manier waarop een antwoord gegeven kan worden op de vraag naar de kennis en vaardigheden die nodig zijn voor de 21ste eeuw. In de periode 2020-2023 hebben hogescholen de ambitie om in elk geval op de volgende aspecten een significante bijdrage aan de missie Veiligheid te leveren door opleidingen en praktijkgericht onderzoek op het gebied van bescherming van mkb tegen cyberaanvallen (bijv. het lectoraat 'Cyberveiligheid in het mkb' aan de Haagse Hogeschool), de beleving van veiligheid door burgers (bijv. de onderzoekslijn 'Publiek vertrouwen in veiligheid' van Hogeschool Inholland, het lectoraat 'Maatschappelijke Veiligheid' aan Saxion), het versterken van de rechtskundige weerbaarheid van professionals (bijv. het 'Expertisecentrum Veiligheid' van Avans Hogeschool), en sociale veiligheid (bijv. het lectoraat 'Kennisanalyse Sociale Veiligheid' aan de Hogeschool Utrecht).

4.6 Internationalisering

Vanwege de relatief kleine binnenlandse markt heeft een groot deel van de Nederlandse industrie een sterke internationale focus. Dit openbaart zich in topsectorverband bij voorbeeld door een actieve deelname aan een grote reeks internationale beurzen en handels missies zoals de Hannover Messe, de Paris Airshow, JEC World, Semicon Japan.

Voor specifiek defensie- en veiligheidsproducten is export voor het stimuleren en in stand houden van de Nederlandse basis defensiegerelateerde bedrijven essentieel. Tegelijk is export aan strenge regels onderhevig. Een consistent en voorspelbaar overheidsbeleid is van essentie voor de industrie om geïdentificeerde kansen te kunnen verzilveren.

4.7 Relatie met sleuteltechnologieën en andere agenda's

In deze KIA worden relaties met diverse sleuteltechnologieën benoemd. Zowel de nieuwste ontwikkelingen op het gebied van Artificial Intelligence en Robotics als Augmented Reality en Serious Gaming, maar ook Digital Twinning, Big Data, Cybersecurity, Photonics en Quantum Technology. Ook energievraagstukken, circulariteit, sensor systemen en een veilige communicatie-infrastructuur alsmede veilig data delen zijn essentieel.

Juist de KIA Veiligheid heeft sterke behoefte aan een breed palet aan meerjarenprogramma's in de KIA Sleuteltechnologieën. Specifiek vanuit het perspectief van het Ministerie van Defensie is in tabel 3.1 een focus set aan meerjarenprogramma's gedefinieerd, essentieel voor het (op termijn) realiseren van de missies rondom thema Veiligheid.

Meerjarenprogramma (MJP)	**Onder andere van essentie voor**
Nationale Agenda Quantumtechnologie	Toekomstige computerkracht en communicatie methodes
Atomically controlled magnetic meta-materials	Sensoren
Duurzame geavanceerde materialen	Voer-, vaar- en vliegtuigen
Maritieme Sleuteltechnologieën	Vaartuigen
Nationaal Artificiële Intelligentie (AI) Onderzoekscentrum	Data mining en cyber security
Artificial Intelligence 4 Engineering Lab – Towards Intelligence Machines	Data mining en cyber security
AI enabled Electronic Components & Systems addressing Societal Solutions	Data mining en cyber security
Commit2Data	Data mining
D-ART: D-RACE Advanced Radar Technology	Radaroplossingen

Tabel 4.1: Relatie met meerjarenprogramma's in de KIA Sleuteltechnologieën

Naarmate sleuteltechnologieën resultaten opleveren, worden deze opgenomen in MMIP's en doorontwikkeld naar specifieke oplossingen. Een continue aanwas is cruciaal voor een hightech domein als thema Veiligheid.

Relatie met andere agenda's

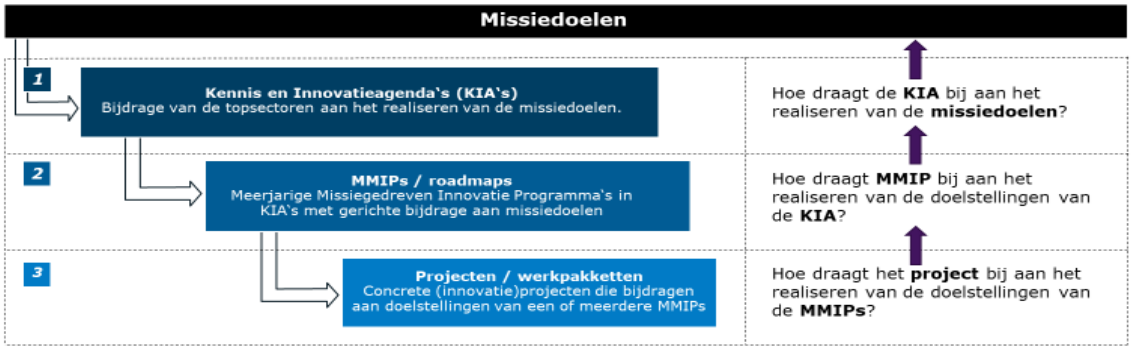
Op het gebied van Veiligheid zijn er verschillende specifieke kennis- en innovatieagenda's, bijvoorbeeld rond Cyberveiligheid. Er is de noodzaak en belang die agenda's gezamenlijk te beheren en op elkaar af te stemmen, zodat kennisontwikkeling en innovatie optimaal bijdraagt aan het oplossen van maatschappelijke uitdagingen op het gebied van Veiligheid, zoals aangegeven door de missies.

4.8 Organisatie en governance

Voorstellen voor governance zijn in bespreking en worden uitgewerkt in het najaar van 2019. Het principe wordt gevolgd dat budgethouders aan tafel komen om in afstemming de innovatieprogramma's voor thema Veiligheid te optimaliseren. Topsector HTSM neemt het voortouw voor afstemming op het niveau van boegbeelden/DG's en voorbereiding van deze regiegroep door een sherpa-groep.

4.9 Monitoring en effectmeting

Om inzichtelijk te maken welke bijdrage de uitvoering van de KIA Veiligheid levert aan het realiseren van de missiedoelen, en wat daarop de voortgang is, kunnen we onderscheid maken tussen drie niveaus (zie figuur 3.2). Op het hoogste niveau gaat het om de gehele bijdrage van de KIA Veiligheid aan het realiseren van de opgestelde missiedoelen. Daaronder gaat het om het de bijdrage van de verschillende MMIP's aan specifieke missies. Een niveau daaronder beschouwen we de bijdrage van concrete projecten aan deze MMIP's.



Figuur 4.2: Gecomprimeerd overzicht van de samenhangende monitor- en evaluatieniveaus

Omgekeerd kan dan ook worden geredeneerd dat van elk PPP en/of PPS-project duidelijk moet zijn wat het bijdraagt aan het realiseren van het MMIP, het MMIP helder moet bijdragen aan het realiseren van de KIA('s), en de opeenvolgende KIA's (nu en in de toekomst) inzichtelijk moeten maken wat de volgende stappen zijn op weg naar het realiseren van de missiedoelen van de maatschappelijke thema's, en wat daarvan het resultaat is. Zo wordt duidelijk waar het proces op koers ligt en waar meer aandacht naartoe moet.

Monitoring en effectmeting (M&E) van het missiegedreven innovatiebeleid zal daarom voor de KIA Veiligheid ook plaatsvinden op de diverse niveaus. Dataverzameling wordt zoveel als mogelijk op projectniveau gedaan. Door op projectniveau data te verzamelen, kan door het combineren van data ook op een hoger abstractieniveau worden gemonitord. Wanneer de te meten parameters goed gekozen worden, wordt interactie versterkt tussen de vele verschillende partijen die samen bouwen aan de missie. Zij kunnen leren van elkaars successen en tegenslagen, elkaar inspireren en dwarsverbanden leggen waardoor synergie ontstaat.

Bij het uitwerken van de MMIP's in de komende periode zal deze systematiek van monitoring ingebracht worden. Ook zullen we vanuit de KIA Veiligheid in de aankomende periode werken aan een *monitoring framework*, waarin we een systematiek zullen ontwikkelen om zowel korte als lange termijn resultaat – en waar mogelijk impact – van de KIA Veiligheid in kaart te brengen. De systematiek zal aan de hand van bewezen M&E-technieken worden vormgegeven, waarbij expliciet

zal worden stilgestaan welke (type) activiteiten er binnen de KIA Veiligheid zullen worden uitgevoerd en hoe deze (uiteindelijk) tot respectievelijk output, *outcome* en impact leiden. Vervolgens zal voor elk van deze niveaus gekeken worden hoe – en óf - ze meetbaar kunnen worden gemaakt.

Bij de uitwerking van het monitoring framework zal rekening worden gehouden met een set generieke indicatoren ("core KPI's") die voor elk thema van het missiegedreven innovatiebeleid relevant is. Deze generieke indicatoren zullen in nader overleg met betrokken partijen worden vastgesteld. Een eerste aanzet voor meetbare indicatoren is weergegeven in tabel 3.1. De impact van activiteiten uitgevoerd binnen deze KIA op de missiedoelen laat zich lastig kwantificeren. We verwachten daarom dat deze vooral kwalitatief zal worden gerapporteerd.

Ten slotte zal in het monitoring framework worden bezien of er specifiek rondom veiligheid indicatoren kunnen worden geformuleerd die inzicht geven in de bijdrage van de KIA Veiligheid aan de missiedoelen van het thema.

i. Input	**ii. (tussen)Resultaat**	**iii. Impact**
i.1: Financiële inbreng (totaal; EUR) i.2: Publiek/private inbreng (%) i.3: Aantal partners (per "type")	ii.1: ΔTRL (gerealiseerd) ii.2: Aantal (succesvol) afgeronde projecten ii.3: Aantal publicaties ii.4: Aantal patenten ii.5: Aantal ontwikkelde prototypes ii.6: Aantal ontwikkelde demonstrators ii.7: Aantal spin-offs / spin-outs ii.8: Aantal nieuwe of verbeterde producten/ processen/diensten geïntroduceerd op de markt	*Succesverhalen (anekdotisch en inspirerend; wat is er binnen projecten gedaan en waar heeft dat toe geleid?)*

Tabel 4.2: Potentiële generieke indicatoren om de inzet, voortgang en impact van de KIA te meten op de missiedoelen (core KPI's; indicatief)

5 Vervolgstappen

Deze KIA Veiligheid beschrijft de kennisontwikkelings- en innovatieonderwerpen waarop de vijf betrokken topsectoren de komende jaren gezamenlijk willen inzetten. Dit met als doel een essentiële bijdrage te leveren aan de realisatie van de onder leiding van het Ministerie van Defensie en het Ministerie van Justitie en Veiligheid gedefinieerde missies op het gebied van Veiligheid.

De meerjarige missiegedreven innovatieprogramma's (MMIP's) van deze KIA Veiligheid zijn de basis voor het kennis- en innovatiecontract (KIC). Daarin worden afspraken over de inzet en verdeling van publieke en private middelen voor onderzoek en over valorisatie en marktcreatie gemaakt tussen overheden, bedrijfsleven en kennisinstellingen.

Voor de uitvoering van de agenda zijn sectoroverschrijdende samenwerking en instrumenten ter ondersteuning benodigd.

5.1 Meerjarige missiegedreven innovatieprogramma's

Deze KIA Veiligheid stelt acht meerjarige missiegedreven innovatieprogramma's voor, die bijdragen aan de realisatie van de missies. Onderstaande tabel geeft een overzicht van de doelstellingen en beoogde resultaten van de MMIP's.

Tabel 4.1: Doelstellingen en beoogde resultaten meerjarige missiegedreven innovatieprogramma's

MMIP	**Doelstelling**	**Resultaat**
MMIP 1: Integrale aanpak, digitaal gedragen, van interventies, tools en data	De integrale aanpak van georganiseerde criminaliteit versterken door de zichtbaarheid van normafwijkend gedrag te en het reactieve én proactieve vermogen te vergroten	Bestrijders van criminaliteit beter in staat zicht en inzicht te hebben op georganiseerde criminaliteit en effectiever te kunnen interveniëren
MMIP 2: Maritime security	Invulling geven aan de Defensie Industrie Strategie middels het opbouwen van een sterke basis van Nederlandse kennis en innovatie	Middelen voor de KM en de Kustwacht om op alle huidige en toekomstige veiligheidsuitdagingen een antwoord te kunnen geven
MMIP 3: Voor veiligheid in en vanuit de ruimte	Ontwikkelen van systemen voor observatie ten behoeve van grotere *situational awareness,* robuuste plaatsbepaling- en tijdsynchroni-satiesystemen *(PNT)* en veilige communicatie via satellieten	Dat Nederland beschikt over faciliteiten voor observatie en communicatie vanuit de ruimte ten behoeve van defensie en veiligheid en over een Robuuste Nationale PNT Oplossing
MMIP 4: Cyberveiligheid	Kennisontwikkeling en innovatie voor een digitaal weerbaar Nederland; draagt bij aan de uitvoering van onderzoeksagenda NCSRA-III, de Nederlandse Cybersecurity Agenda , Nederlandse Digitaliseringsstrategie en de Defensie Cyber Strategie 2018	Nederlandse cybersecurity innovatie ecosysteem heeft in 2030 een duidelijke vorm, en laat het zien dat Nederland in staat is om urgente uitdagingen effectief het hoofd te bieden en ook doelgericht aan fundamentele vraagstukken te kunnen werken
MMIP 5: Informatiegestuurd en genetwerkt optreden	De krijgsmacht en andere veiligheidsorganisaties effectief te laten functioneren in genetwerkte omgevingen, mat als uiteindelijkdoel de slagkracht te vergroten	Defensieonderdelen en andere veiligheidsorganisaties zijn in 2030 in staat voor een willekeurige operatie, alsmede voor de *going concern* activiteiten, snel een acceptabel niveau van netwerk integratie te behalen en te behouden

MMIP 6: Innovaties voor een adaptieve krijgsmacht	Adaptiviteit van de krijgsmacht te verhogen door concrete innovaties te realiseren, ook bijdragend aan bijgedragen aan het samen kort-cyclisch tot succesvolle innovaties komen	De adaptiviteit van de krijgsmacht wordt vergroot door innovaties die bijdragen aan het versnellen en wendbaarder maken van operaties
MMIP 7: Data en intelligence	Realiseren van oplossingen voor privacy-bestendige informatiedeling tussen verschillende partijen en oplossingen om op basis van data en intelligence de juiste beslissingen te kunnen nemen	Op basis van informatie voorkomen en ondervangen van incidenten, juist inschatten van situaties, geheel conform de werkelijkheid en zodanig doorgegeven aan de professional dat die de optimale interventie uitvoert
MMIP 8: Gekwalificeerde en gekwantificeerde veiligheidsprofessionals	Veiligheidsprofessionals via nieuwe leermethoden wapenen voor (toekomstige) uitdagingen, meten van prestaties en ondersteunen met krachtige digitale technologie	Veiligheidsprofessionals zijn voorbereid op de toekomst, leveren betere prestaties en zijn weerbaarder

5.2 Uitvoering van de agenda

De uitvoering van de kennis- en innovatieagenda vraagt om het gezamenlijk organiseren en uitvoeren van innovatie vanuit de bij de missies behorende doelstellingen.

Voor de uitvoering van de KIA zijn instrumenten nodig, onder andere om als overheid als *launching customer* op te treden en instrumenten gericht op de ontwikkeling, demonstratie en exploitatie van technologie. Naast nationale instrumenten zijn dat ook de Europese onderzoeksprogramma's (Horizon Europe) en het European Defence Fund (EDF).

Valorisatie en marktcreatie vraagt vanwege de diverse typen bedrijven om een diversiteit aan programmering en instrumenten om betrokkenheid van bedrijfsleven te borgen: zowel via PPS-constructies als open Calls. Regionale overheden en ontwikkelingsmaatschappijen (ROM's) zijn belangrijke partners bij valorisatie en marktcreatie.

De MMIP's bieden volop kennis- en innovatievragen die voor een wetenschapsbrede aanpak pleiten, van technologie tot het menselijke gedrag. Daarvoor is samenwerking in het gehele ecosysteem van gebruikers/maatschappij, overheid, kennisinstellingen en bedrijfsleven vereist. Voor de verdere ontwikkeling en instandhouding van Human Capital werken de gezamenlijke topsectoren aan een gezamenlijke *roadmap* Human Capital Topsectoren 2020 – 2023, met als doel dit sectoroverstijgend te versterken.

Een consistente en voorspelbare regelgeving rond export is van belang aangezien voor een groot deel van de Nederlandse defensiegerelateerde bedrijven export essentieel is.

Relaties met sleuteltechnologieën, waaronder Artificial Intelligence, Robotics, Augmented Reality, Serious Gaming, Digital Twinning, Big Data, Cybersecurity, Photonics en Quantum Technology zijn wezenlijk. Het is van belang de verschillende specifieke agenda's op het gebied van Veiligheid gezamenlijk te beheren en op elkaar af te stemmen.

Met de uitvoering van de KIA Veiligheid willen de topsectoren blijven investeren in het gezamenlijk realiseren van de missies: samen organiseren, samen innoveren, één doel. Voor het inzichtelijk maken van de bijdrage die uitvoering van de KIA Veiligheid levert aan het realiseren van de missiedoelen zal de komende periode een systematiek worden ontwikkeld.