Thema Veiligheid

''Always ahead of the threat''

Ministerie van Defensie

Ministerie van Justitie en Veiligheid

Ministerie van Economische Zaken en Klimaat

Inleiding

In juli 2018 heeft het kabinet een missie gedreven innovatiebeleid voor het nieuwe topsectorenbeleid vastgesteld. Daarin staan vijf maatschappelijke thema's centraal waaronder het thema Veiligheid. Binnen dit thema worden concrete missies ter hand genomen die (toegepaste) innovaties stimuleren. De innovaties moeten bijdragen aan een veiliger samenleving, een weerbaarder Nederland, én economische kansen creëren. Dit document beschrijft de missies die onder het thema veiligheid vallen. De missies zijn onder leiding van het Ministerie van Defensie en het Ministerie van Justitie en Veiligheid tot stand gekomen, in nauwe samenwerking met het Ministerie van Economische Zaken en Klimaat, de topsectoren, kennisinstellingen en het bedrijfsleven. Deze missies worden in 2019 door hetzelfde samenwerkingsverband uitgewerkt in de Kennis en Innovatie Agenda Veiligheid. Hierbij hebben de betrokken topsectoren (HTSM, Creatieve Industrie, ICT, Logistiek, Life Sciences, en Water en Maritiem) het voortouw.

Dreigingen

De ministeries van Defensie en Justitie en Veiligheid (JenV) voeren kerntaken uit voor de veiligheid van de Nederlandse samenleving.. Het tegengaan van dreigingen neemt daarin een centrale plaats in. De Strategie Nationale Veiligheid (SNV)[1], de Geïntegreerde Buitenland- en Veiligheidsstrategie (GBVS)[2] en de Defensienota[3] onderscheiden diverse dreigingen.[4] Zo wordt Nederland rechtstreeks, en via de NAVO en de EU, geconfronteerd met militaire dreigingen. Ook de veiligheid van belangrijke handels- en transportroutes staat onder druk. Terrorisme vormt een directe bedreiging voor onze nationale veiligheid. Dat geldt ook voor de dreiging van georganiseerde criminaliteit voor de samenleving. Het hoge tempo waarmee technologie en digitalisering zich ontwikkelen biedt eveneens nieuwe uitdagingen, zoals cyberaanvallen. Buitenlandse inmenging en beïnvloeding van onze maatschappij, via desinformatie, vormen een bedreiging voor onze democratie.

Ambitie

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''.* De samenwerking stimuleert ook economische

[1] De SNV identificeert vijf vitale belangen van Nederland die moeten worden beschermd om ontwrichting van de samenleving te voorkomen: fysieke veiligheid, territoriale veiligheid, economische veiligheid, ecologische veiligheid, sociale en politieke stabiliteit.
[2] De GVBS benoemt drie pijlers voor een veilig Nederland: voorkomen, verdedigen en versterken.
[3] De Defensienota noemt drie hoofdtaken van de krijgsmacht: bescherming eigen en bondgenootschappelijke integriteit; bescherming en bevordering van de internationale rechtsorde en stabiliteit; en de ondersteuning van civiele autoriteiten bij rechtshandhaving, rampenbestrijding en humanitaire hulp, zowel nationaal als internationaal.
[4] Ministerie van Economische Zaken en Klimaat & Ministerie van Defensie. Defensie Industrie Strategie (2018)
[5] Dreigingen kunnen 'man-made' zijn ("security"), of een technische dan wel natuurlijke oorzaak hebben ("safety"). Dit missiedocument richt zich voornamelijk op security.
[6] BZK, JenV, DEF, EZK en OCW
[7] waaronder Topsectoren HTSM, ICT, Logistiek, Creatieve Industrie, Water en Maritiem.
[8] NWO, TNO, NLR, Marin, universiteiten en hogescholen

kansen voor het bedrijfsleven, in de vorm van innovaties met brede markttoepassingen in binnen- en buitenland.

Missies

Om de ambitie “always ahead of the threat” waar te maken is een aantal missies gedefinieerd op basis van succesfactoren voor het optreden van veiligheidsorganisaties:

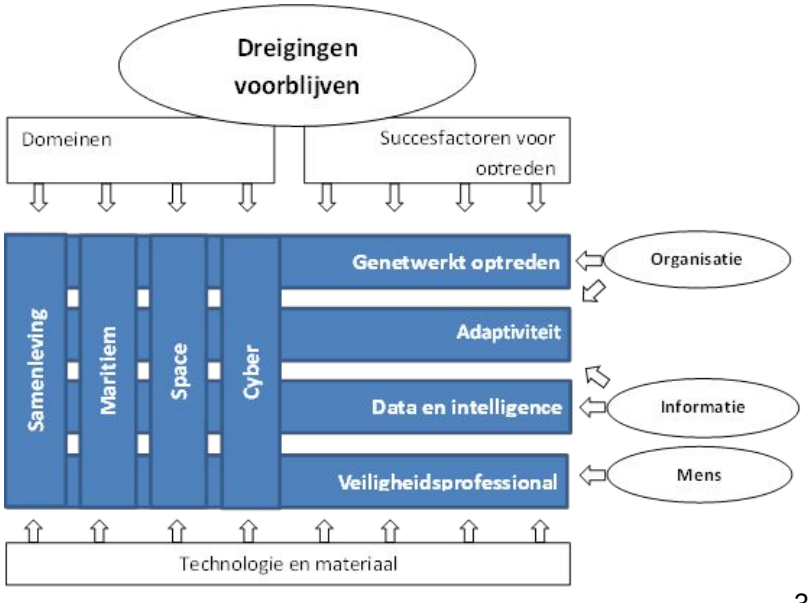
- het beschikken over een goede informatie positie,
- het snel en effectief, waar mogelijk kort-cyclisch innoveren,
- het effectief en efficiënt organiseren van veiligheidstaken, en
- het goed uitrusten van de veiligheidsprofessional in het veld of op straat.

Omdat dreigingen zich op verschillende manieren manifesteren, zijn ook missies geformuleerd op basis van toepassingsgebieden of domeinen: land, zee, lucht, space en cyber. Bij al deze missies is het van belang gebruik te maken van de nieuwste technologieën en materialen.

In een intensief consultatieproces hebben Defensie, JenV en EZK, vertegenwoordigers van de topsectoren, bedrijfsleven en kennisinstellingen vervolgens een aantal missies geformuleerd, met uitzicht op concrete innovaties voor de operationele gebruikers bij Defensie en JenV en op economische kansen voor het bedrijfsleven. Elke missie bevat combinaties van bovengenoemde aspecten, met zwaartepunten die per missie anders liggen. De missies zijn beschreven vanuit een militair of een civiel veiligheidsperspectief (“security”), waardoor deze meer leesbaar en herkenbaar zijn voor de eindgebruiker. Uitwisseling van modellen, technologieën en concepten tussen de twee perspectieven is in veel gevallen mogelijk en wenselijk. De missies hebben betrekking op de volgende onderwerpen:

1. **Samenleving**, om georganiseerde criminaliteit minder lonend te maken
2. **Maritieme hightech**, voor een veilige zee.
3. **Space**, voor veiligheid in en vanuit de ruimte.
4. **Cyber**, om veiligheid in het digitale domein te vergroten.
5. **Genetwerkt optreden op land en vanuit de lucht**, om (militair) voordeel te behalen tijdens operaties met verschillende sensoren en actoren door informatiedeling en samenwerking.
6. **Adaptieve krijgsmacht**, samen sneller innoveren.
7. **Data en intelligence**, om de met veiligheid belaste diensten te voorzien van adequate data en analyses.
8. De **veiligheidsprofessional**, wiens prestaties worden verhoogd door goede opleidingen en moderne (training) technologieën.

Bij iedere missie is uiteengezet wat het doel is en op welke termijn dat moet zijn behaald. Ook kennis en innovatievragen zijn vermeld. In de bijlage zijn de relevante kennis- en technologiegebieden opgenomen. Hiervoor is multidisciplinair wetenschappelijk onderzoek van belang



1. Missie: Integrale aanpak van georganiseerde criminaliteit

Omschrijving missie

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

Toelichting missie

Georganiseerde ondermijnende criminaliteit is ontwrichtend voor de samenleving. Het gaat dan veelal om stelselmatig gepleegde criminaliteit, die onwettige vermogens genereert en leidt tot economische machtsposities met corruptie, marktverstoring en verwevenheid tussen onder- en bovenwereld. Deze criminaliteit is vaak onzichtbaar, maar kan zich ook manifesteren in de publieke ruimte door intimidatie en geweld. Waar daders vaak bovenregionaal of internationaal opereren, heeft ondermijnende criminaliteit tegelijkertijd op lokaal niveau veel uitingsvormen en verbindingen. De bestrijding van ondermijning en meer in het algemeen de georganiseerde criminaliteit wordt effectiever als overheid, bedrijfsleven en burgers intensiever en gerichter samenwerken. En als de gehele keten (preventie, anticipatie, repressie, vervolging, zorg, lokaal jeugdbeleid, etc.) achter een gezamenlijke aanpak staat. De aanpak van georganiseerde criminaliteit vraagt dus om een brede maatschappelijke aanpak en gedeelde verantwoordelijkheid. Op basis hiervan kunnen innovatieve interventiemodellen ontstaan. Bij de integrale aanpak van georganiseerde criminaliteit is de inzet van data-onderzoek om misdaadfenomenen en concrete criminele activiteiten in beeld te brengen noodzakelijk. De uitdagingen daarbij zijn:

- de mogelijkheden en beperkingen om bestaande data van publiek en private instanties te gebruiken om misdaadfenomenen en concrete criminele activiteiten in beeld te brengen;
- het binnen bestaande juridische kaders gebruiken en toepassen van deze data bij preventie, opsporing en vervolging.

Verbeteringen zijn nodig op drie terreinen:

1. Zicht : “Alle ogen verbonden”
   Er is specifiek behoefte aan instrumentaria om criminele activiteiten waar te nemen en ontwikkelingen te herkennen zoals het ontstaan van criminele samenwerkingsverbanden en werkwijzen. Nieuwe, slimme sensoren (bijvoorbeeld uit de chemische industrie) kunnen ongebruikelijke activiteiten detecteren en gedragswetenschappelijke inzichten kunnen patronen herkennen en analyses versterken. Het waarnemend vermogen kan verhoogd worden door gebruik te maken van detectiemiddelen van andere publieke en private partijen.

   Onderzoek met betrekking tot bescherming en versterking van relevante instituties in een democratische rechtsstaat is daarbij van belang, evenals organisatiekundige kennis die het verantwoordelijkheidsdomein van enkele overheidsorganisaties overstijgen.
2. Inzicht : “Voorspellende kracht”
   Omdat veel illegale activiteiten zich ‘ondergronds’ manifesteren, is het van belang om toekomstige ontwikkelingen goed te voorspellen. Dat is nodig om de schaarse interventie mogelijkheden effectiever te benutten. Omdat er uiteindelijk (heel) veel geld mee in omgaat, bieden ook financiële analyses nuttige inzichten. Gedragswetenschappelijke inzichten dragen bij aan het voorspellen van reacties van criminelen op interventies van de overheid. Daarmee proberen we ze één stap voor te zijn.
3. Interventie : “Nieuwe modellen ”
   Hoe komt vertrouwen tot stand tussen burgers, getuigen en opsporingsinstanties (en hoe kan technologie daarbij een rol spelen)? Omdat een publiek-private aanpak goed kan werken, vragen

interventie modellen om nieuwe, creatieve manieren van ingrijpen. Die kunnen technisch, procesmatig of sociaal van aard zijn. En met gebruik van nieuwe partners of tactieken uit andere domeinen.

Kennis- en innovatievragen

1. Zicht : "Alle ogen verbonden"
   - In aanvulling op de gangbare observatietechnieken, gaat het hier om specialistische, technische monitoring en ontwikkeling van nieuwe (Chemisch, Biologisch, Radiologisch, Nucleair) detectietechnieken: kijken, horen, ruiken, signaal interceptie, digital sensing; al dan niet heimelijk, met hoog onderscheidend vermogen. Het gaat om het ontdekken van verbanden door waarnemingen van verschillende spelers te combineren, en technieken gezamenlijk uit te voeren in forensic engineering platforms.
     - Kijken: heimelijke observatiemiddelen en technieken, transponders, bakens, camera's in het infrarode spectrum of multi spectraal;
     - Horen : geluidscamera's, microphone arrays;
     - Ruiken: geavanceerde sensoren om chemicaliën / verdovende middelen te detecteren en traceren, zoals 'e-noses';
     - Digital sensing: in kaart brengen van zwart geld stromen / zwarte markten / illegale activiteiten op dark web.

2. Inzicht : "Voorspellende kracht"
   - Voorspellen van toekomstige ontwikkelingen:
     - Van een 'real time' naar 'pre time' informatiepositie;
     - Van descriptieve - naar predictieve modellen die plaats en tijd van gebeurtenissen zo goed mogelijk inschatten;
     - Verklarende modellen voor effecten van interventies en reacties van criminele samenwerkingsverbanden daarop ;
     - Inzicht in beïnvloedingsmogelijkheden.
   - Het gebruik van privacy bestendige 'multi party computation' technologie en AI om op basis van verschillende databronnen criminele samenwerkingsverbanden in kaart te brengen.
   - Psychologische gedragskunde toepassen bij geavanceerde beeldanalyses.

3. Interventie : "Nieuwe modellen "
   - Methoden om de medewerkingsbereidheid, verklaringsbereidheid, aangiftebereidheid en waarheidsvinding te verhogen:
     - Technologie en gedragsinzichten om de kwaliteit van verhoren te verhogen, bijvoorbeeld 3D reconstructies of VR/AR;
     - Methoden en technieken die drempel verlagend werken zoals gebruik maken van sociale media en burgerparticipatie;
     - Gebruik van nudging technieken;
     - Computational game theory, teneinde het intelligent, adaptief vermogen van de tegenstander te modelleren ('graphical models for security' en quantum technologieën).

2. Missie: Maritieme hightech voor een veilige zee

Omschrijving missie

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.

Toelichting missie

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 toekomstbestendige en concurrerend ecosysteem van overheid, kennisinstellingen en (maritieme) industrie is hiervoor essentieel.

Kennis- en innovatievragen:

Maritieme hightech gaat de volgende gebieden versterken:

- Smart Operations
  Inzet van onbemande en autonome middelen in stand-off/swarming operaties , met gezamenlijk te ontwikkelen procedures, doctrines en tactieken.
- Smart Kill-chains
  De meest moderne sensoren, missie management systemen en effectoren, boven en onder water, bijvoorbeeld in de Roadmap Nederland Radarland.
- Smart Manning & Automation
  Autonomisering, AI en robotisering, in een geïntegreerde flexibele en missiegerichte architectuur van adaptieve systemen in de Roadmap Manning & Automation.
- Smart Survivability
  Stealth-eigenschappen en incasseringsvermogen van de schepen, nieuwe materialen. Gedistribueerde intelligente distributiesystemen en signatuur management systemen.
- Zero Emission Warships
  Alternatieve brandstoffen, batterij-technologie, brandstofcellen, hydrodynamica, voortstuwers, onderwater geluid en hydro-system integration in een roadmap Zero Emission Warships.
- Smart Maintenance
  Remote asset management, robotisering, nanotechnologie en 3D-printing.
- Smart Design
  Concept development en experimenten in VR en AR omgevingen, SARC4 aan de wal, flexibiliteit en adaptiviteit voor de future toolbox, -and submarine design with very low hydrodynamic drag, a high shock resistance and a very low noise signatureweerbaar scheeps-en onderzeeboot ontwerp, met zeer lage hydrodynamische weerstand, schokbestendigheid en een zeer lag geluidssignatuur.
- Smart Concepts
  Ontwikkeling van volledig nieuwe concepten en operaties voor de ‘navy after next’ op basis van Risicodragend Verkennend Onderzoek.
- Het ontwikkelen van mitigatie-strategieën voor maritieme CBRNe bedreigingen.
- Het ontwikkelen van safety-design technieken.

3. Missie: Veiligheid in en vanuit de ruimte

Omschrijving missie

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.

Toelichting missie

Met een operationele ruimtevaartcapaciteit kunnen we een essentiële bijdrage aan de veiligheid leveren door:

a. het beschermen van de kritische ruimtevaart- infrastructuur;
b. het optimaal benutten van satelliettoepassingen voor het volgen van bewegende objecten, detectie van emissie, illegale gedragingen op het aardoppervlak, veranderingen, vegetatiedroogte, observatie, en veilige communicatie;
c. het beschermen tegen dreigingen uit de ruimte (objecten, zonnestormen, spectrum verstoringen, ongewenste observatie, etc.).

Handelen, of het juist niet handelen op basis van ontbrekende of verkeerde informatie kan ernstige gevolgen hebben voor onze veiligheid. Satellietinformatie vervult bij het borgen van nationale en internationale veiligheid een belangrijke rol door het tijdig identificeren van mogelijke risico's. 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 al deze satellietinformatie op tijd de juiste conclusies te kunnen trekken, dient ook het informatieverwerkingsproces (downstream) goed ontwikkeld te worden. Hierbij worden vanzelfsprekend ook de nieuwe mogelijkheden vanuit (onder meer) kunstmatige intelligentie, Big Data en Cyber betrokken. Tevens dient de infrastructuur robuust genoeg zijn tegen natuurlijke en vijandelijke dreigingen.

Kennis- en innovatievragen

- Ondervangen van afhankelijkheden van plaatsbepaling- en tijdsynchronisatiesystemen (GNSS systemen als GPS en Galileo);
- Inrichten van een grondgebonden Situational Awareness, Surveillance & Tracking dienst om snel te kunnen reageren op dreigingen vanuit de ruimte (Near earth objects, Space Weather). De dienst neemt natuurlijke en man made activiteiten waar in de ruimte en detecteert eventuele dreigingen, maar mitigeert ze niet;
- Inrichten van een grondgebonden Situational Awareness dienst om vanuit een constellatie van satellieten en grondstations gebeurtenissen (bijvoorbeeld bosbranden, olievervuiling, etc) aan het aardoppervlak te detecteren;
- Inzet van laser communicatie voor beveiligde satelliet communicatie;
- Inrichten van een operationeel systeem voor informatieverwerking en datafusie;
- Realisatie van een (gedeeltelijk) eigen ruimte infrastructuur met waarborgen voor een tijdige en veilige toegang.

4. Missie: Cyberveiligheid

Omschrijving missie

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 Global Cybersecurity Index als de National Cyber Security Index te staan.

Toelichting missie

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 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;
- 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.

5. Missie: Genetwerkt optreden op land en vanuit de lucht

Omschrijving missie

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.

Toelichting missie

Kennisontwikkeling en innovatie op het gebied van Genetwerkt Optreden is nodig om de hoofdtaken van onze Krijgsmacht te kunnen blijven invullen. 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.

Ook de tegenstanders werken steeds meer in netwerken met nieuwe technologieën. 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 onze *decision loop* (van herkennen naar handelen) sneller en beter blijft dan die van onze tegenstander.

De belangrijkste Nederlandse uitdagingen op het gebied van genetwerkt optreden worden uiteengezet in de Strategische Kennis- en Innovatieagenda 2016-2020 en in de toekomstvisie Commando Landstrijdkrachten (CLAS), Veiligheid is vooruitzien. Net als het CLAS moet ook Commando Luchtstrijdkrachten (CLSK) in staat zijn om sneller en beter informatie te vergaren, te analyseren, samen te brengen en te delen dan onze tegenstanders en hierbij gebruik maken van onbemande systemen.

Genetwerkt optreden vraagt om het integreren van nieuwe technologieën in het optreden. Het integreren van nieuwe technologieën verandert het informatiegestuurd optreden. 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.

Daarnaast vraagt Genetwerkt optreden om andere wijzen van optreden; nieuwe operatieconcepten. Er zijn nog niet veel operatieconcepten die vorm geven aan genetwerkt optreden. Genetwerkt optreden wordt vaak geassocieerd met operatieconcepten als *swarming* en *dispersed operations*. Het is noodzakelijk om operatieconcepten voor genetwerkt optreden te ontwikkelen en zo de mogelijkheden van nieuwe technologieën te benutten. Experimenteren, trainen en oefenen in diverse oefenomgevingen en operationele domeinen (fysiek, menselijk en informatie) is nodig om de ontwikkeling van nieuwe operatieconcepten te versterken. Oefenomgevingen (in fysieke landschap) moeten worden voorzien van representatieve menselijke en informatielandschappen (bijvoorbeeld social media, realistische cyber incidenten etc.).

Experimenteren, trainen en oefenen vergt wel een zo realistisch mogelijk fysiek landschap zoals bijv. een gesloten luchtruim, menselijk landschap (combinatie van ideologie, overtuiging en ervaringen die het gedrag ‘drijft’) en informatielandschap. Het vereist derhalve een netwerk om deze innovatieomgeving te creëren.

Naast de operationele meerwaarde draagt deze missie bij aan het versterken van een hoogwaardige, autonome kennispositie in Nederland waardoor Nederland enerzijds minder afhankelijk zal zijn van het buitenland en anderzijds haar handelspositie kan verbeteren. De norm bij deze ontwikkelingen is een vergaande samenwerking met kennisinstituten, onderwijsinstellingen en het bedrijfsleven.

Kennis- en innovatievragen

- Het commanderen en coördineren van informatiegestuurd en genetwerkt optreden, oftewel Command & Control. Hiervoor is nodig:
  - Hoogwaardig interoperabel communicatienetwerk;
  - C2-ondersteunende systemen in drie landschappen om informatie te verwerken, te representeren en te ondersteunen bij besluitvorming. NetForce commandC2 in genetwerkt optreden voor *multi domain battles*: zowel coordinatie van militaire effectoren als effectoren op gebied van politiek, informatie als economie;
- Kunnen ontwikkelen van begrip van een complexe omgeving om waarnemingen te kunnen interpreteren;
- Hoe groepeer en koppel je – gegeven een bepaalde taak – activiteiten en hoe ontwerp je regelkringen om qua besturing dit geheel aan te sturen?
- Ten behoeve van integratie met het luchtoptreden het inrichten van een operationeel systeem voor informatieverwerking en datafusie en de ontwikkeling van een genetwerkte omgeving en integratie van huidige en toekomstige wapen- en informatiesystemen;
- Het genetwerkt optreden van bemande en onbemande systemen. De landmacht heeft hiervoor een Remotely Autonomous Systems (RAS) eenheid opgericht om hiervoor te experimenteren. Van belang hiervoor is de mens-machine interactie, autonomie/AI van de platformen en snelheid en precisie van informatie. De integratie van bemande en onbemande systemen ten behoeve van het luchtoptreden, evenals het integreren van onbemande vliegende systemen in het civiele en militaire luchtruim vereist onder meer ontwikkeling van capabilities van onbemande systemen;
- Het genetwerkt optreden met “Informatie als Wapen”. Naast letale middelen zijn er ook niet-letale capaciteiten om de tegenstander via het internet (*cyber warfare*), het elektromagnetisch spectrum en via gesprekken en social media te beïnvloeden. Hiervoor is het essentieel om goede informatie en inlichtingen te verkrijgen, te verwerken en toe te passen. Dit vereist o.a. *Big data* analyse en AI;
- Het genetwerkt optreden tegen *Rockets, Artillery of Mortars* (RAM) en vijandelijke vliegtuigen en drones. Ook hier spelen sensoren, elektromagnetisch spectrum en het communicatie netwerk een belangrijke rol;
- Het garanderen van de human-in-the-loop principe om te voorkomen dat machines zelf beslissingen omtrent kill-missies gaan nemen;
- Het genetwerkt optreden met een slimme en robuuste logistiek waarbij de logistiek o.a. middels onbemande/semi-autonome middelen, track & trace voorraden incl. *blockchain* technologie en verbruiks/energiebesparende technologieën effectief ingericht kan worden.
- Het vergroten van de genetwerkte slagkracht door het integreren van verschillende sensor- en sensoranalysemogelijkheden in een enkel concept/platform, waarbij met een snelle *decision loop* slagkracht ingezet kan worden, nieuwe sensortechnologie, technologie voor camouflage om eigen capaciteiten te beschermen tegen dreiging. Het doel is commandanten te voorzien van tijdige en relevante informatie;
- Ontwikkelen Smart Kill-chains: moderne sensoren, missie management systemen en effectoren om onder alle operationele omstandigheden een diversiteit aan letale en niet-letale (precisie-)wapens in te kunnen zetten. Het ontwikkelen van operatieconcepten in een *Joint Interagency Multinational and Public (JIMP)* omgeving;
- Onderzoek naar Explainable AI en privacy preserving computing ten behoeve van autonome systemen. Steeds meer van belang als de loop herkennen-handelen steeds sneller wordt;
- Network science en agent-based simulations. Hiermee kunnen relaties worden gelegd tussen C2 factoren en onderwerpen uit de network science.

6. Missie: Samen sneller innoveren voor een adaptieve krijgsmacht

Omschrijving missie

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.

Toelichting missie

Om adaptiviteit te bereiken is er een langdurig stabiel fijnmazig innovatienetwerk nodig om vraag en aanbod bij elkaar te brengen, aandacht voor ketenontwikkeling, sustainment en service logistiek, met stevige verbindingen tussen de operationele eindgebruikers (bij o.a. de landmacht en luchtmacht), de topsectoren (in het bijzonder HTSM, logistiek en Creatief/ICT) en kennisinstituten (in het bijzonder Marin, NLR en TNO). Daarnaast moet er ook 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. Daarnaast vraagt innovatie en adaptiviteit om inzicht in het organiseren van het innovatieproces en onderzoek naar organisatiekundige vragen in verband met adaptiviteit veelal vanuit een integraal perspectief.

Het scheppen van de juiste voorwaarden en/of juridische kaders voor kort-cyclische innovaties is van belang. Het huidige innovatie instrumentarium van het ministerie van Economische Zaken en Klimaat is bijvoorbeeld generiek van aard. Maatwerk is nodig om met dit instrumentarium binnen het thema veiligheid uit de voeten te kunnen. Daarbij kan worden gedacht worden aan het toepasbaar maken van de SBIR-regeling binnen het veiligheidsdomein om Defensie te faciliteren op te kunnen treden als launching customer in het veiligheidsdomein.

Defensie biedt in het kader van *Concept Development & Experimentation* (CD&E) ruimte voor experimenteren op allerlei vlakken en disciplines. Gezien de vele toepassingen van civiele technologie voor Defensie met de verscheidenheid aan taken en capaciteiten is er bij de Landmacht een grote behoefte aan samen sneller innoveren. Innovatiegericht inkopen met een passende set van instrumenten, waaronder *launching customership*, als startmotor speelt hierin een belangrijke rol.

Kennis- en innovatievragen

- Robotica en autonome (onbemande) systemen, bijvoorbeeld voor risicovolle en repetitieve taken; mens-machine teaming;
- Nieuw energievoorziening en voortstuwingtechnologie;
- Toepassingen van verklaarbare kunstmatige intelligentie (AI); big data en analyse technieken ; snellere besluitvorming/snelheid van handelen: van herkennen tot handelen (OODA Loop), maar ook het verkrijgen van inzicht in de doelgroepen met intenties en gedrag en het behoud van human-in-the loop
- Dataverwerking en algoritmes ten behoeve van decentrale netwerken;
- Toepassingen biotech (bijvoorbeeld biometrie) voor bijvoorbeeld het vergroten van het eigen menselijk presteren, of juist het identificeren van irreguliere strijdkrachten en terroristen;
- Nieuwe technologieën v.w.b. sensoren en communicatie;
- Nieuwe technieken voor effectieve informatie disseminatie in het kader van informatiegestuurd optreden;
- Additive Manufacturing, 3D-printing; nieuwe materialen (composieten)/nanotechnologie, waarmee gewicht bespaard kan worden en waar bijv. nieuwe functionaliteiten uit volgen;

systemen voor non destructieve inspectie en onderhoud van deze nieuwe materialen; smart structures die aangeven hoe groot of kritiek battle damage is;
- Swarming drones en counter drones, inclusief (non) cooperatieve sense and avoid systemen. Integratie van drones/RPAS in civiel en militair luchtruim;
- Ontwikkelen van zelfbeschermingsmiddelen om te anticiperen op bedreigingen van wapensystemen en (satelliet-)communicatieplatforms. (bijvoorbeeld Stealth, Electronic warfare, Cyber);
- Verbeterde anti-ballistische bescherming en integratie van anti-ballistische en structurele functies;
- Ontwikkelen van nieuwe materieel logistieke technieken, zoals remote asset management, robotisering, nanotechnologie en 3D-printing, block chain technologie, concept development en experimenten in VR en AR omgevingen, reductie logistiek footprint, alternatieve energievoorziening, emissie reductie;
- Verdere verduurzaming (CO2, Geluid, NOX) van de militaire luchtvaart;
- Nieuwe materialen, materiaalconcepten, productiemethodieken, ontwerpmethodieken, sensoren en systemen voor de volgende generatie fixe dan rotary wing wapensystemen;
- Internet of Things, digitale ketens, servitization;
- Het ontwikkelen van instrumentarium voor beoordelingskaders voor het accepteren van innovaties;
- Het ontwikkelen van gemeenschappelijke (informatie) protocollen voor het matchen van vraag en aanbod in de lifecycle van innovatieprocessen (comptabiliteit);
- Het ontwikkelen van Ecosystemen voor innovaties.

7. Missie: Data en intelligence

Omschrijving missie

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

Toelichting missie

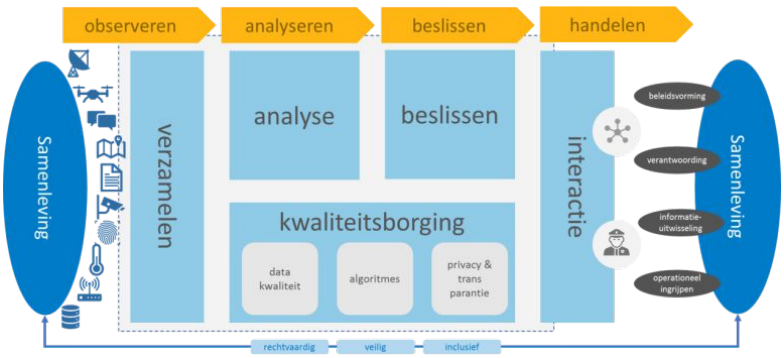
Om onveilige situaties te voorkomen, of adequaat op te treden in crisis of conflict situaties en bij rampenbestrijding en migratievraagstukken, moeten veiligheidsprofessionals beschikken over tijdige, juiste en op maat geselecteerde informatie. Voor het delen van data zijn institutionele kaders nodig om een juiste balans te houden tussen operationele/logistieke effectiviteit en maatschappelijke spelregels.

Observeren: soms blijft relevante, in de samenleving beschikbare informatie, onbenut. Bijvoorbeeld uit social media, van burgers, of uit sensoren van andere maatschappelijke organisaties dan de betrokken veiligheidsinstanties. Ook kan moderne technologie nieuwe informatiebronnen aanboren die relevant zijn voor de uitvoering van veiligheidstaken. Verhoogde observatiecapaciteit leidt tot verruiming van het waarnemingsvermogen en een versterking van de informatiepositie.

Analyseren: De hoeveelheid data groeit, de verwerkingscapaciteit voor de analyse daarvan dient mee te groeien. Een hogere analyse-capaciteit is ook nodig om real-time informatie te kunnen verwerken en delen. Koppeling van data uit verschillende bronnen kan leiden tot extra informatie en inzichten. Al die data wordt verwerkt en veredeld tot bruikbare ‘intelligence’. Moderne technologie kan dit proces versnellen en verbeteren.

Beslissen: Vervolgens wordt duiding gegeven aan deze analyses en ontstaat ‘intelligence’ die de basis vormt voor beslissingen om acties uit te voeren. Moderne technologie en gedragswetenschappelijke inzichten dragen bij aan een hogere kwaliteit van die besluitvorming. Ook is er behoefte aan modules die de gebruiker automatisch informatie op maat aanreiken, afhankelijk van de situatie waarin deze zich op dat moment bevindt.

Handelen, feedback, en kwaliteitsborging: De beslissingen worden geëffectueerd door het uitvoeren van een interventie door de veiligheidsprofessional, of door een technisch middel. De uitvoering en de effecten daarvan worden vervolgens gemonitord. Dit 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. Dat betekent dat de data van goede kwaliteit zijn (geen vervuiling), dat algoritmen de juiste analyses doen, en dat er gehandeld wordt binnen de ethische, morele waarden en wettelijke kaders. Dit moet betrouwbare, reproduceerbare en evidence-based beslissingen en voorspellingen opleveren.



Kennis- en innovatievragen

1. Observeren
   - Ontwikkelen van nieuwe sensoren, beter gebruik maken van bestaande sensoren en andere databronnen, zoals social media, met oog voor de betrouwbaarheid van deze gegevens (verificatie);
   - Betrouwbare en privacy vriendelijke data-uitwisseling vormgeven tussen veiligheidsorganisaties;
   - Multi-use[9] data- en sensortechnologie ontwikkelen;
   - Databronnen gebaseerd op burgerparticipatie toepassen;
   - Privacy bestendige informatiedeling realiseren, bijvoorbeeld met secure multiparty computation, of gebruik van blockchain en homomorfe encryptie.

2. Analyseren
   - Gebruik van big data analyse methodes en voorspellende modellen;
   - Gebruik van Artifical Intelligence voor veiligheidstaken, bijvoorbeeld bij spraak- en beeld herkenning;
   - Oplossingen voor multi stakeholder sensor- en data-integratie realiseren;
   - Analyse methodieken zoals sense making en projectie naar de toekomst.

3. Beslissen
   - Verbeteren van datavisualisatie – in de dynamiek van verschillende abstractieniveaus, parameters en tijd;
   - Beslissingsondersteunende modellen en algoritmen ontwikkelen, onder andere met Artificial Intelligence;
   - Simulaties en visualisatie van scenario's.

4. Handelen / Kwaliteitsborging
   - Methoden ontwikkelen voor het bevorderen van de kwaliteit van data, de betrouwbaarheid van interpretaties daarvan, de besluitvorming daarover, en de reproduceerbaarheid daarvan;
   - Toetsing van de effectiviteit (monitoring, feedbackloop) van handelingen door middel van evidence-based prototyping;
   - Adversarial Learning: wat als de tegenstander een offensief op social media opent waardoor de beslissing wordt beïnvloed?

[9] Bijvoorbeeld veiligheidsdomein overstijgend.

8. Missie: De veiligheidsprofessional

Omschrijving missie

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

Toelichting missie

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 crisis situaties. Het kan gaan om militairen in het veld, om 'first responders' op straat (politie, brandweer, ambulance), hulpverleners, beveiligers, marechaussee en (grens) bewakers en crisismanagers/-bestuurders.

De veiligheidsprofessional wordt opgeleid als 'reflective practitioner' die in staat is om om te gaan met complex samenhangende problematiek en organisatiesystemen die adaptief moeten zijn. Vanuit een integrale benadering kan veel gedaan worden aan de verbetering van de toerusting van de veiligheidsprofessional. De institutionele setting van de veiligheidsprofessional is van grote invloed op zijn handelen. Veiligheidsprofessionals moeten werken in complexe organisaties en coördinatie-arrangementen die de effectiviteit van het handelen van deze veiligheidsprofessionals verminderen. Dat vraagt om bestuurskundige en bedrijfskundige inzichten alsmede kennis vanuit organisatiewetenschappen die helpen bij het versterken van de effectiviteit van de veiligheidsprofessional.

Veiligheidsprofessionals werken in complexe organisaties en coördinatie-arrangementen die nodig zijn, maar ook de effectiviteit van het handelen van deze veiligheidsprofessionals kunnen verminderen. Bestuurskundige en bedrijfskundige inzichten alsmede 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 van de veiligheidsprofessional verhogen. Ook kunnen ze bijdragen aan een betere opleiding en selectie procedure. Dat moet leiden tot een aantrekkelijker opleidingstraject en betere prestaties.

Veiligheidsprofessionals kunnen bloot staan aan hoge risico's, heftige situaties of schokkende gebeurtenissen. Dat kan op straat of in het veld zijn, of in het digitale domein. De fysieke en digitale omgeving raken steeds meer verweven, waardoor hun werkveld complexer en uitdagender wordt. Het onderscheid tussen 'werk' en 'privé' wordt door social media aandacht moeilijker te beschermen. Het doel van hun werk (veiligheid 'brengen'), brengt veel verantwoordelijkheid mee. Dat heeft invloed op het functioneren en impact op de weerbaarheid van veiligheidsprofessionals.

Technologische ontwikkelingen zoals wearables, exoskeletten en detectieapparatuur zullen een verschuiving teweeg brengen in de aard van het werk van veiligheidsprofessionals. Permanente opleiding en training is daarom van belang.

Verbeteringen zijn nodig op drie terreinen:

1. Werving, selectie, opleiding en training: De opleiding en training van veiligheidsprofessionals is gebaseerd op zowel de fysieke als mentale 'fitness' voor de moeilijke omstandigheden en de informatie overload waaronder ze werken. Gedragswetenschappelijke inzichten kunnen de

kwaliteit hiervan verhogen en dit kan ondersteund worden door een reeks aan moderne technologieën.

2. Persoonlijke prestatie: Veiligheidsprofessionals kunnen met moderne technologie beter waarnemen en communiceren. Hun fysieke inspanningen kunnen worden versterkt, en geavanceerde materialen kunnen hen beter beschermen tegen extreme omstandigheden.

3. Weerbaarheid: Veiligheidsprofessionals moeten in goede gezondheid en conditie zijn en blijven. Omdat de fysieke prestaties en biologische condities met elkaar verbonden zijn en variëren in de tijd, kunnen de prestaties worden verhoogd als de persoonlijke fitheid real time gemonitord wordt. Hetzelfde geldt voor de mentale conditie.

Kennis- en innovatievragen

1. Opleiding en training:
   - Bij opleiding, oefenen en trainen wordt gebruik gemaakt van nieuwe instrumenten zoals simulatie, *virtual reality* en/of *serious gaming.* Die kunnen ook ontwikkeld worden voor complexe systemen en specifieke toestellen. Digitale leermiddelen zoals een 'VR Escaperoom', AR toepassingen en 'Micro learnings' worden ontwikkeld om zelfstandig te kunnen leren. Privacy bestendige informatiedeling helpt om te focussen op de persoonlijke condities in relatie tot de prestaties in een team.
   - Bij selectie, opleiding en training is naast de (traditionele) aandacht voor de fysieke component, ook de mentale conditie van belang. Hierbij is ondersteuning vanuit gedragswetenschappen, met name psychologie, essentieel. Ook samenwerking tussen de verschillende kolommen, de aansturing vanuit de meldkamer en omgang met de informatie overload zijn van belang.

2. Persoonlijke prestatie:
   - Tijdens veiligheidsoperaties is het 'situationeel bewustzijn' van cruciaal belang. Het waarnemingsvermogen wordt verhoogd door gebruik te maken van technologieën als augmented reality en identificatie technologie (sensoren/scanners).
   - De communicatie wordt versterkt door draagbare apparatuur zoals spraak- en vertaal apps.
   - De bescherming en ondersteuning wordt opgevoerd door betere kleding, bewapening, exoskeletten, en bepantsering. De initiatieven op het gebied van 'soft advanced materials' en ook 'composieten' zijn hier relevant.
   - Fysieke inzet kan vervangen worden door, of aangevuld met robots, onbemande systemen, virtuele agents zoals chatbots en AI-systemen.

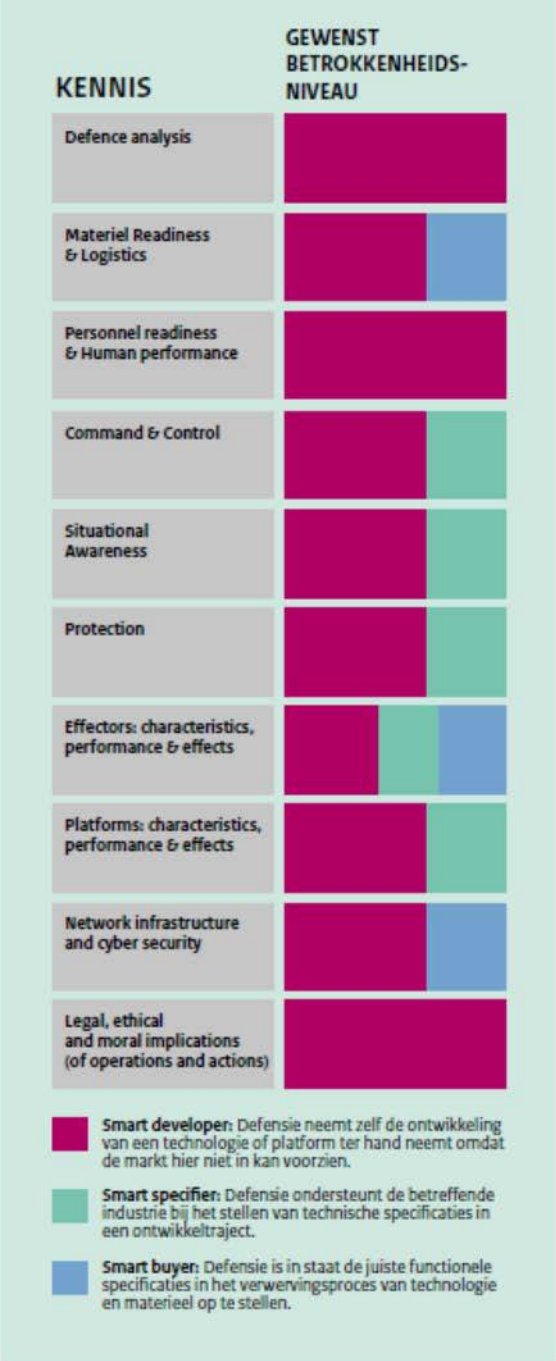
3. Weerbaarheid:
   - Onderzoek naar aard en achtergronden van traumatische stoornissen, en de ontwikkeling van programma's om werkgerelateerde klachten te voorkomen.

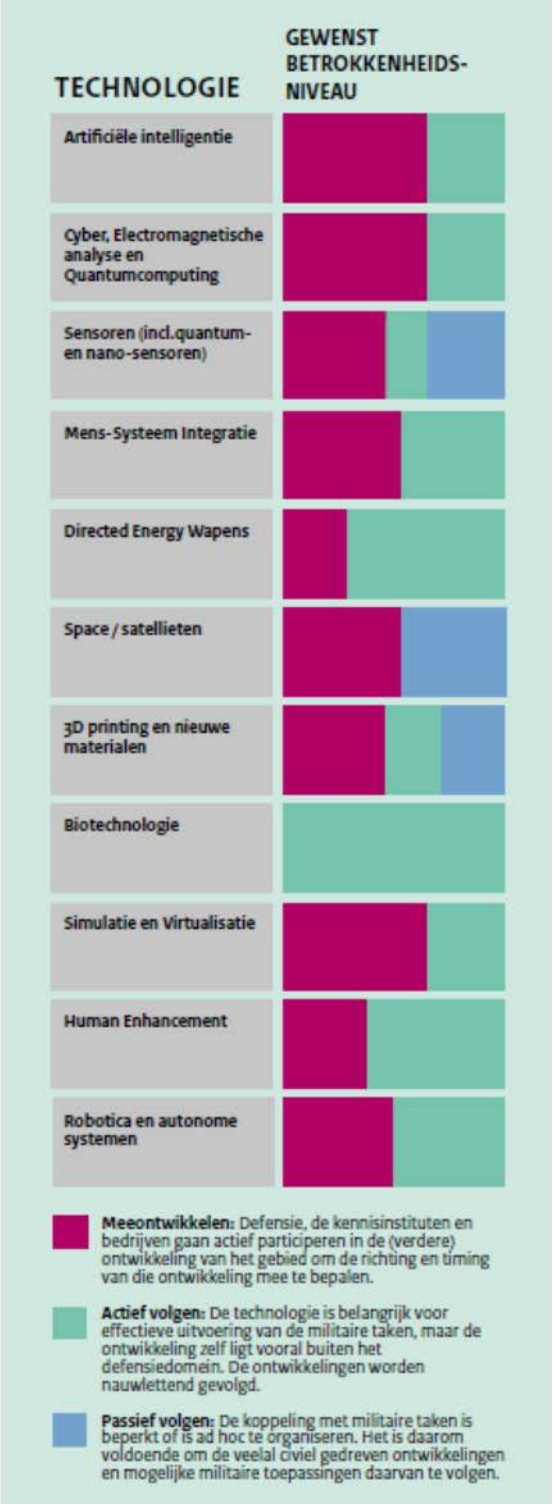
De fysieke prestaties, de gezondheid en de weerbaarheid worden doorlopend gemeten, geanalyseerd en voorspeld voor een efficiënt optreden in stressvolle en moeilijke situaties. Daarbij kan gebruik gemaakt worden van wearables en biofeedback. Het hoeft hierbij niet alleen te gaan om de veiligheidsprofessional zelf, maar kan bijvoorbeeld ook gaan om verdachten en gedetineerden.

Bijlage A. Overzicht Kennis- en Technologiegebieden per missie

Missie	Kennisgebied	Technologiegebied
Veiligheid in en vanuit de ruimte	Command & control Situational Awareness Protection (platform and infrastructure) Network infrastructure and cyber security	Artificiële intelligentie Cyber, elektromagnetische analyse (EMA) en quantumcomputing Sensoren (incl. quantum en nanosensoren) Mens-Systeem integratie Space/satellieten 3D printing en nieuwe materialen
Genetwerkt optreden op land en vanuit de lucht	Command & control Situational Awareness Effectors: characteristicsperformance & effects (info ops and strategic campaigning) Network infrastructure and cyber security	Artificiële intelligentie Cyber, elektromagnetische analyse (EMA) en quantumcomputing Sensoren (incl. quantum en nanosensoren) Mens-Systeem integratie Simulatie en virtualisatie Human Enhancement Robotica en autonome systemen
Cyberveiligheid	Network infrastructure and cyber security Effectors: characteristicsperformance & effects (cyber operations)	Artificiële intelligentie Cyber, electromagnetische analyse (EMA) en quantumcomputing
Maritieme hightech voor een veilige zee	Materiel readiness and logistics Command & control Situational Awareness Platforms: characteristics, performance & effects Network infrastructure and cyber security	Artificiële intelligentie Cyber, electromagnetische analyse (EMA) en quantumcomputing Sensoren (incl. quantum en nanosensoren) Mens-Systeem integratie Directed Energy wapens 3D printing en nieuwe materialen Simulatie en virtualisatie
Adaptieve krijgsmacht	Material Readiness and logistics Personnel readiness and human performance Command and control Network infrastructure	Artificiële intelligentie Sensoren Mens-systeem integratie 3D printing en nieuwe materialen Robotica en autonome systemen

Bijlage B. Overzicht gewenst betrokkenheidsniveau Kennis en Technologie (Defensie Industrie Strategie, 2018)





Bijlage C. Tabel Sleuteltechnologieën voor overige missies

Onderstaande tabel geeft aan welke ST-en o.i. bijdragen aan de kennis –en innovatievragen behorende bij de verschillende JenV missies. Ze zijn gemarkeerd met in groen, voor een grote bijdrage, en geel, voor een gemiddelde bijdrage.

Naast het bieden van kansen leveren (sleutel)technologieën ook risico's op waarmee wij rekening dienen te houden. Er zitten grote vraagstukken, voor wat betreft veiligheid, c.q. privacy en ethiek, op het terrein van life sciences, quantum technologies, digital technologies, een aantal engineering and fabrication technologies en nanotechnology.

Missie	*Onderzoeks- en Innovatievragen*	*Sleuteltechnologieën*
Data- en Intelligence gestuurd werken	<u>Observeren</u> • Ontwikkelen van nieuwe sensoren, beter gebruik maken van bestaande sensoren en andere databronnen, zoals social media, met oog voor de betrouwbaarheid van deze gegevens (verificatie); • Betrouwbare en privacy vriendelijke data-uitwisseling vormgeven tussen veiligheidsorganisaties; • Multi-use[10] data- en sensortechnologie ontwikkelen; • Databronnen gebaseerd op burgerparticipatie toepassen; • Privacy bestendige informatiedeling realiseren, bijvoorbeeld met secure multiparty computation, of gebruik van blockchain en homomorfe encryptie. <u>Analyseren</u> • Gebruik van big data analyse methodes en voorspellende modellen; • Gebruik van Artifical Intelligence voor veiligheidstaken, bijvoorbeeld bij spraak- en beeld herkenning; • Oplossingen voor multi stakeholder sensor- en data-integratie realiseren; • Analyse methodieken zoals sense making en projectie naar de toekomst. <u>Beslissen</u> • Verbeteren van datavisualisatie – in de dynamiek van verschillende abstractieniveaus, parameters en tijd; • Beslissingsondersteunende modellen en algoritmen ontwikkelen, onder andere	• *Artificial intelligence (incl. machine and deep learning)* • *Big data and data analytics* • *Block chain* • *Encryption technologies/ digital security* • *High Performance Computing Grid Computing and Cloud Technologies/Computing* • *(Opto)mechatronics* • *Cyberphysical systems* • *High frequency and mixed signal technologies* • *Imaging technologies* • *Robotics* • *Sensors and actuators* • *Biochips and biosensors* • *Integrated photonics* • *Photon generation technologies* • *Photonic detection* • *Quantum communication*

[10] Bijvoorbeeld veiligheidsdomein overstijgend.

	met Artificial Intelligence; • Simulaties en visualisatie van scenario's beschikbaar maken. <u>Handelen / Kwaliteitsborging</u> • Methoden ontwikkelen voor het bevorderen van de kwaliteit van data, de betrouwbaarheid van interpretaties daarvan, de besluitvorming daarover, en de reproduceerbaarheid daarvan; • Toetsing van de effectiviteit van handelingen door middel van evidence-based prototyping.	*GROEN : van groot belang* *GEEL : van gemiddeld belang*
De Veiligheidsprofessional	<u>Opleiding en training</u>: • Bij opleiding, oefenen en trainen wordt gebruik gemaakt van nieuwe instrumenten zoals simulatie, *virtual reality* en/of *serious gaming.* Die kunnen ook ontwikkeld worden voor complexe systemen en specifieke toestellen. Digitale leermiddelen zoals een 'VR Escaperoom' en 'Micro learnings' worden ontwikkeld om zelfstandig te kunnen leren. Privacy bestendige informatiedeling helpt om te focussen op de persoonlijke condities in relatie tot de prestaties in een team. • Bij selectie, opleiding en training is naast de (traditionele) aandacht voor de fysieke component, ook de mentale conditie van belang. Hierbij is ondersteuning vanuit gedragswetenschappen, met name psychologie, van belang. <u>Persoonlijke prestatie</u>: • Tijdens veiligheidsoperaties is het 'situationeel bewustzijn' van cruciaal belang. Het waarnemingsvermogen wordt verhoogd door gebruik te maken van technologieën als augmented reality en identificatie technologie (sensoren/scanners). • De communicatie wordt versterkt door draagbare apparatuur zoals spraak- en vertaal apps. • De bescherming en ondersteuning wordt opgevoerd door betere kleding, bewapening, exoskeletten, en bepantsering. De initiatieven op het gebied van 'soft advanced materials' en ook 'composieten' zijn hier relevant. • Fysieke inzet kan vervangen worden door, of aangevuld met robots, onbemande	• *Bio (related) materials and soft material* • *Composite and ceramics* • *Energy storage materials* • *Smart/self healing/self-organising materials* • *Artificial intelligence (incl. machine and deep learning)* • *Big data and data analytics* • *Encryption technologies/ digital security* • *(Opto)mechatronics* • *Additive manufacturing/3D printing* • *Cyberphysical systems* • *High frequency and mixed signal technologies* • *Imaging technologies* • *Robotics* • *Sensors and actuators* • *Biochips and biosensors* • *Genomics* • *Nanomaterials* • *Integrated photonics* • *Photonic detection*

	systemen, virtuele agents zoals chatbots en AI-systemen. Weerbaarheid: • Onderzoek naar aard en achtergronden van traumatische stoornissen, en de ontwikkeling van programma's om werkgerelateerde klachten te voorkomen. De fysieke prestaties, de gezondheid en de weerbaarheid worden doorlopend gemeten, geanalyseerd en voorspeld voor een efficiënt optreden in stressvolle en moeilijke situaties. Daarbij kan gebruik gemaakt worden van wearables en biofeedback. Het hoeft hierbij niet alleen te gaan om de veiligheidsprofessional zelf, maar kan bijvoorbeeld ook gaan om verdachten en gedetineerden.	
Integrale aanpak van georganiseerde criminaliteit	Zicht : "Alle ogen verbonden" • In aanvulling op de gangbare observatietechnieken, gaat het hier om specialistische, technische monitoring : kijken, horen, ruiken, signaal interceptie, digital sensing; al dan niet heimelijk, met hoog onderscheidend vermogen. Voorbeelden hiervan zijn: o Kijken: heimelijke observatiemiddelen en technieken, transponders, bakens, camera's in het infrarode spectrum of multi spectraal. o Horen : geluidscamera's, microphone arrays. o Ruiken: geavanceerde sensoren om chemicaliën / verdovende middelen te detecteren en traceren, zoals 'e-noses'. o Digital sensing: in kaart brengen van zwart geld stromen / zwarte markten / illegale activiteiten op dark web. Inzicht : "Voorspellende kracht" • Voorspellen van toekomstige ontwikkelingen: o Van een 'real time' naar 'pre time' informatiepositie o Verklarende modellen voor effecten van interventies en reacties van criminele samenwerkingsverbanden daarop o Inzicht in beïnvloedingsmogelijkheden • Het gebruik van privacy bestendige 'multi party computation' technologie en AI om op basis van verschillende databronnen criminele samenwerkingsverbanden	- *Analytic technologies* - *Artificial intelligence (incl. machine and deep learning)* - *Big data and data analytics* - *Block chain* - *Encryption technologies/ digital security* - *High Performance Computing Grid Computing and Cloud Technologies/Computing* - *(Opto)mechatronics* - *Additive manufacturing/3D printing* - *Cyberphysical systems* - *High frequency and mixed signal technologies* - *Imaging technologies* - *Robotics* - *Sensors and actuators* - *Industrial biotechnology* - *Integrated photonics* - *Photon generation technologies* - *Photonic detection*

	in kaart te brengen. • Psychologische gedragskunde toepassen bij geavanceerde beeldanalyses <u>Interventie : "Nieuwe modellen "</u> - Methoden om de medewerkingsbereidheid, verklaringsbereidheid, aangiftebereidheid en waarheidsvinding te verhogen: o Technologie en gedragsinzichten om de kwaliteit van verhoren verhogen, bijvoorbeeld 3D reconstructies. o Methoden en technieken die drempel verlagend werken zoals gebruik maken van sociale media en burgerparticipatie. o Gebruik van nudging technieken.	
Voor meerdere missies is onderzoek en ontwikkeling op Artificial Intelligence van belang. In deze kolom wordt deze specifieke ST uitgewerkt.	EXPLAINABLE AI: KOPPELING KENNIS EN DATA IN DE ARTIFICIËLE INTELLIGENTIE - Hoe kan data-gedreven AI (zoals machine leren) gekoppeld worden aan kennis-gebaseerde AI (zoals regelgebaseerde expertsystemen). - Hoe kunnen statistische/kwantitatieve en logische/kwalitatieve analysetechnieken (respectievelijk de grondslag voor data-gedreven en kennis-gebaseerde AI) elkaar kunnen versterken. RESPONSIBLE AI: NORMATIEVE STURING IN DE ARTIFICIËLE INTELLIGENTIE - Onderzoek naar de risico's van artificiële Intelligentie: Privacy, autonome wapens en surveillance societies, juridische normering van AI-systemen en `human-in-the-loop' controlesystemen of het inbouwen van normatieve sturing in AI-systemen. SOCIAL AI: INTERACTIEVE, WEDERZIJDS VERSTERKENDE SYSTEMEN - Onderzoek naar mens-machine interactie (hybride systemen) multi-agentsimulaties en robotica. - Onderzoek naar Social cognition en theory of mind (modellen van de ander) zijn relevante onderzoeksthema's die bijvoorbeeld bijdragen aan win-win onderhandelen.	-