Titel	**Cyber Risk Management and System Resilience (P103)**
Missie/ Topsector	Veiligheid / Topsector HTSM
Contactpersonen TNO	Ir. A.J.A. Vetjens, Director Market ICT, Dr.Ir. O.A. Niamut, VP manager Cyber
Contact Extern	Topteam ICT / Dutch Digital Delta, Erik Wijnen en Fred Boekhorst

Programma jaar 2020 - Samenvatting

Digitale veiligheid is een essentiële voorwaarde voor een welvarende samenleving en een sterke economie. Het doel van het Vraaggestuurd Programma (VP) Cyber Risk Management and System Resilience (CRM&SR) is 'Nederland digitaal veiliger en weerbaarder te maken én tegelijkertijd de economische kansen van cybersecurity te verzilveren'. Met dit VP zorgen we ervoor dat TNO samen met andere kennisinstellingen, overheidsinstellingen en (cybersecurity) bedrijven de noodzakelijke ruimte organiseren om te experimenteren, zodat innovaties een weg naar de markt vinden. Een gerichte en effectieve cybersecurity aanpak is cruciaal voor het waarborgen van de betrouwbaarheid en vertrouwelijkheid van data, en de continuïteit van ICT netwerken en systemen. Nationale veiligheidsorganisaties en beheerders van vitale processen moet beter in staat te gesteld worden om tijdig cyberdreigingen te onderkennen en te duiden, en voorzien worden van preventief versterkende, maar ook repressieve handelingsperspectieven om - in het geval van verstorende cyberincidenten of fenomenen- de continuïteit van maatschappelijke vitale functies te waarborgen. Verder willen we de impact die (cyber) ambities, (geautomatiseerde) werkwijzen en (technische) tooling van cybersecurity organisaties hebben op cyber professionals vastleggen in een cyber workforce framework om het tekort aan gekwalificeerd cyberpersoneel beheersbaar te maken.

Het is de ambitie van TNO om te voorkomen dat onze opdrachtgevers schade ondervinden als gevolg van misbruik, manipulatie, of diefstal van hun informatietechnologiesystemen en data; om nationale veiligheidsorganisaties en beheerders van vitale processen in staat te stellen de risico's en gevolgen van cyberdreigingen te minimaliseren in de context van een snel digitaliserende samenleving; en om cybersecurity organisaties te faciliteren een personeelsbestand van cyber professionals te beschrijven, te bouwen en te behouden; passend bij veranderende ambities, werkzaamheden en tooling. We adresseren daarbij de volgende behoeftes van onze partners en klanten, en beogen de volgende resultaten voor 2020.

- in onze digitale samenleving zijn ICT netwerken, systemen en de informatie-uitwisseling die zich daarbinnen afspeelt voortdurend kwetsbaar voor externe invloeden zoals misbruik, manipulatie, spionage en diefstal. Voor een betrouwbare en veilige samenleving is een gedegen aanpak voor informatie- en netwerkbeveiliging van cruciaal belang. Onze partners vragen om betrouwbare ICT (***trusted ICT***) oplossingen. In 2020 realiseren we geautomatiseerde analyse, respons en modeltransformatie methodieken, analyses en use cases voor gebruik van geavanceerde cryptografische protocollen op basis van lattices, een verbeterde en verbrede opzet van het bestaande samenwerkingsverband met de Nederlandse grootbanken, en nieuwe anomalie detectie en risico kwantificeringsmethodieken.
- Het ontwikkelen van kennis en innovatie voor zowel overheid als bedrijfsleven, primair beheerders van vitale processen, om adequaat te kunnen (blijven) anticiperen en reageren op de belangrijkste cyberuitdagingen is van belang om onze maatschappij beter weerbaar te maken (***national cyber resilience***). In 2020 realiseren we Een consortium, onderzoeksplan en toolbox ter bevordering van cybersecurityinformatiedeling en Cyber Secure Behaviour; een dataset en analyse tools voor phishing data; een forecasting gids en horizon scanning toolbox; en de ingebruikname van Security Technology Assessment Methodology (STAM).
- Onderzoek en ontwikkeling van specifieke capaciteiten voor o.m. Defensie, de defensie industrie, EDA en NATO is nodig om de hoofdtaken van Defensie veilig te kunnen uitvoeren. Het (verder) ontwikkelen van de capaciteiten van cyber security experts (***cyber workforce development***) is één van de onderwerpen waarop Defensie voor dit doel vroeg heeft ingezet. De kennis hier opgedaan kan in andere marktsegmenten worden benut en doorontwikkeld. In 2020 realiseren we een integraal cyber workforce framework dat organisaties en onderwijsinstellingen ondersteunt in hun respectievelijk taken om te komen tot een professionele cyber workforce.

De kennisprogrammering in VP CRM&SR sluit aan bij de uitdagingen en vraagstukken die in de Nederlandse Digitaliseringsstrategie, de Nederlandse Cybersecurity Agenda (NCSA), de Nationale Cyber Security Research Agenda (NCSRA) en de Internationale Cyberstrategie zijn geformuleerd. In 2019 is nadrukkelijk aansluiting gemaakt met de Missie Cyberveiligheid van de Kennis en Investering Agenda (KIA) Veiligheid (in wording). Internationaal participeert TNO in de relevante werkgroepen, taskforces en evenementen. Het opstellen en de uitvoering van het onderzoeksprogramma VP CRM&SR vindt plaats in

nauwe afstemming met VP Veilige Maatschappij (VM), programmalijn Cyber Security & Societal Resilience, VP ICT, programmalijn Cyber Security, en de TNO onderzoeksprogramma's met het bedrijfsleven, Veiligheid en Justitie, Defensie en Politie.

Korte beschrijving

Digitale veiligheid is een essentiële voorwaarde voor een welvarende samenleving en een sterke economie. Nederland staat de komende decennia voor een aantal complexe uitdagingen op het gebied van digitale veiligheid. Het Cybersecuritybeeld Nederland 2019 schetst dat de digitale dreiging voor de nationale veiligheid inmiddels permanent is, en dat, omdat vrijwel alle vitale processen en systemen in Nederland deels of volledig gedigitaliseerd zijn, Nederland kwetsbaar is voor digitale aanvallen. De digitale weerbaarheid staat onder druk door de complexiteit en connectiviteit van de digitale infrastructuur. Digitale sabotage of verstoring kan direct leiden tot aantasting van onder meer de nationale veiligheid. Nederland beschikt over de uitgangspositie om de economische en maatschappelijke kansen van digitalisering te verzilveren. Zonder doorontwikkeling van cybersecurity als doorsnijdend vraagstuk komt de Nederlandse bedrijvigheid en daarmee onze digitale samenleving, economie en vestigingsklimaat onder druk te staan. Het vertrouwen in een digitaliserende economie en samenleving staat of valt met een effectieve aanpak van de uitdagingen en problemen, die digitalisering met zich mee brengt. Een stevige kennisbasis is een randvoorwaarde voor een langdurige en sterke internationale concurrentiepositie, en is vereist om antwoord te kunnen geven op de cybersecurityvraagstukken van de toekomst.

Het doel van het Vraaggestuurd Programma (VP) Cyber Risk Management and System Resilience (CRM&SR) is '***Nederland digitaal veiliger en weerbaarder te maken én tegelijkertijd de economische kansen van cybersecurity te verzilveren***'. Om dit doel te realiseren, hanteren we een integrale aanpak om cybersecurity uitdagingen aan te gaan waarbij techniek, mens, proces en informatie in samenhang meegenomen worden om tot innovatieve oplossingen te komen. Deze integrale aanpak voorkomt puntoplossingen en vergroot de kans op structurele verbeteringen in een digitaal veilige samenleving. We zien dat de veiligheidsketen (identify, protect, detect, respond, recover) als geheel versterkt worden moet zodat niet alleen de kans op een cybersecurity incident beperkt wordt, maar dat er ook een snelle reactie bij een incident is, en een snel herstel. Dit principe geldt binnen organisaties maar ook in organisatie-overstijgende ketens en infrastructuren. TNO bouwt innovaties met en voor partners. In nauwe samenwerking met partners leidt het onderzoek tot nieuwe concepten, methoden en toepassingen, die bijdragen aan praktische oplossingen voor actuele en toekomstige uitdagingen. TNO heeft daarbij een belangrijke rol in de (kennis)valorisatieketen tussen academische instellingen en overheid/bedrijfsleven; kennisopbouw in een Publiek Private Samenwerking maakt de meeste kans op een succesvolle kennistoepassing in de markt en voor onze maatschappij. Met dit VP organiseert TNO samen met andere kennisinstellingen, overheidsinstellingen en (cybersecurity) bedrijven de noodzakelijke ruimte om te experimenteren, zodat innovaties een weg naar de markt vinden. We adresseren daarbij specifiek de volgende behoeftes van onze partners en klanten:

- *Trusted ICT*; in onze digitale samenleving zijn ICT netwerken, systemen en de informatie-uitwisseling die zich daarbinnen afspeelt voortdurend kwetsbaar voor externe invloeden zoals misbruik, manipulatie, spionage en diefstal. Voor een betrouwbare en veilige samenleving is een gedegen aanpak voor informatie- en netwerkbeveiliging van cruciaal belang. Het ontwikkelen van betrouwbare technologie vraagt daarbij om diepgaande kennis van de verschillende schakels in de keten én van de keten als geheel.
- *Cyber resilience;* het ontwikkelen van kennis en innovatie voor zowel overheid als bedrijfsleven, primair beheerders van vitale processen, om adequaat te kunnen (blijven) anticiperen en reageren op de belangrijkste cyberuitdagingen is van belang om onze maatschappij beter weerbaar te maken; en het doen van onderzoek en ontwikkeling van specifieke capaciteiten voor o.m. Defensie, de defensie industrie, EDA en NATO om de hoofdtaken van Defensie veilig te kunnen uitvoeren. Het (verder) ontwikkelen van de capaciteiten van cyber security experts is één van de onderwerpen waarop Defensie voor dit doel vroeg heeft ingezet. De kennis hier opgedaan kan in andere marktsegmenten worden benut en doorontwikkeld.

Resultaten 2020

<u>Trusted ICT</u>

Een gerichte en effectieve cybersecurity aanpak is cruciaal voor het waarborgen van de betrouwbaarheid en vertrouwelijkheid van data, en de continuïteit van ICT netwerken en systemen. Onze ambitie is om te voorkomen dat onze opdrachtgevers

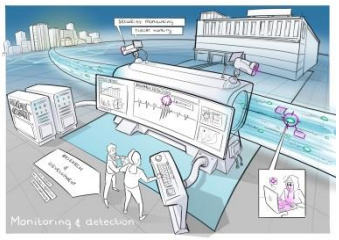
schade ondervinden als gevolg van misbruik, manipulatie, of diefstal van hun informatietechnologiesystemen en data. We verwachten resultaten voor 2020 op de volgende vier aandachtsgebieden:

Automated security; cyber aanvallen worden in toenemende mate geautomatiseerd uitgevoerd. Menselijk handelen volstaat hierdoor niet meer om aanvallen snel en effectief te beheersen. Het is voor cyber security analisten een steeds grotere uitdaging om cyber dreigingen en aanvallen tijdig te pareren. Er is tevens een structureel tekort is aan gekwalificeerde cyber security specialisten. TNO werkt aan technologieën voor geautomatiseerde analyse en mitigatie van digitale aanvallen op ICT infrastructuren, om de snelheid van detectie en response te matchen met die van een cyber aanval. Concrete resultaten voor 2020 zijn i) de uitbreiding van het Security Decision Support proof-of-concept uit 2019 met resultaten van onderzoek naar business impact modelering, modelering van extra aanvalstechnieken en kwantificering van de succesfactor van een aanvalsstap waarbij rekening gehouden wordt met aanwezige beveiligingsmaatregelen; ii) het ontwikkelen van een proof-of-concept voor het geautomatiseerd omzetten van het OSM information model van een gevirtualiseerde ICT infrastructuur naar een model voor security analyse (bijv. voor SecuriCAD of TNO's Security Decision Support tool); iii) een state-of-the-art beschrijving van Artificial Intelligence (AI) technieken voor geautomatiseerd bepalen en kwantificeren van response maatregelen (course of actions); en iv) een rapport met use cases voor geautomatiseerde analyse van en response op cyber-aanvallen en dreigingen uit een te organiseren workshop met potentiele eindgebruikers.

Quantum-safe technology; we streven naar het verminderen van de informatie- en netwerkbeveiligingsrisico's die de quantum computer oplevert voor de huidige versie van cryptografie. Onze technologie verlaagt ook nieuwe beveiligingsrisico's die ontstaan door het gebruik van quantum technologie binnen de bestaande digitale infrastructuur. In 2020 leveren we via deelname aan het H2020 project PROMETHEUS, dat gericht is op het ontwikkelen van geavanceerde cryptografische protocollen op basis van lattices; i) een analyse van de weerbaarheid van lattice based cryptografie tegen quantum computers; en ii) een eerste uitwerking van de cyber threat intelligence use case waarin lattice based cryptografie wordt toegepast.

Resilience engineering; we ontwikkelen concepten, methoden en technieken voor het ontwerp van ICT-systemen en -netwerken die veilig en betrouwbaar zijn. Denk hierbij aan een effect-gestuurde risicomanagement methodiek die verschillende bedrijfsdoelstellingen en individuele belangen bij elkaar brengt. Dit stelt organisaties beter in staat een verantwoorde afweging te maken over het geheel aan risico's binnen de complexe, dynamische omgeving waarin zij opereren. In 2020 realiseren wij de verbeterde en verbrede opzet van het bestaande samenwerkingsverband met de Nederlandse grootbanken (Shared Research Program Cybersecurity) waarin de opgebouwde kennis binnen een aantal onderzoekslijnen en -projecten wordt toegepast.

Security monitoring and detection; Het tijdig kunnen herkennen van cyberaanvallen is voor overheid en bedrijfsleven een kerncapaciteit. In de afgelopen jaren heeft TNO detectie-technologie ontwikkeld die o.a. door Defensie, Telecom, en Financiele instellingen wordt toegepast. Daarbij richt TNO zich op niches die niet door bestaande detectieoplossingen worden ingevuld: we ontwikkelen nieuwe detectiemethoden, vaak ook voor specifieke typen IT-systemen. Onze technologie draagt direct bij aan de cyberveiligheid van Nederlandse organisaties. Door de technologie samen met de Nederlandse cybersecurity-industrie te ontwikkelen en te vermarkten worden bovendien economische kansen gecreëerd. In 2020 realiseren we i) een autoencoder om abnormale hosts in gecombineerde DNS- en Netflow-gegevens te detecteren; ii) een experimentele onderzoekstoepassing voor het zoeken naar (cyber)dreigingen; en iii) een anomalie detectie en risico kwantificeringsmethodiek voor bedrijven op basis van dark web informatie, gewone web informatie, business proces informatie en virtueel geld (bijv. bitcoin) activiteiten (ITEA project DEFRAUDIFY).



National Cyber Resilience

Onze ambitie is om nationale veiligheidsorganisaties en beheerders van vitale processen in staat te stellen de risico's en gevolgen van cyberdreigingen te minimaliseren in de context van een snel digitaliserende samenleving. Dit doen we door hen

beter in staat te stellen tijdig cyberdreigingen te onderkennen en te duiden; en door in het geval van verstorende cyberincidenten of -fenomenen de continuïteit van maatschappelijke vitale functies te waarborgen door preventief versterkende, maar ook repressieve handelingsperspectieven te helpen ontwikkelen. Om deze ambitie te realiseren, richten we ons op de volgende vier focusgebieden.

Maatschappelijke digitale weerbaarheid; het cyberdreigingsbeeld is continu in verandering. Dit betekent dat de Nederlandse cybersecurity capaciteiten moeten mee ontwikkelen met het dreigingsbeeld, zodat niet alleen de problemen van vandaag maar ook die van morgen kunnen worden aangepakt. Dit vergt diepgaande kennis van risico's, informatie infrastructuren en systemen, en het organiseren van cybersecurity capaciteiten, zodat bestaande capaciteiten en nieuwe concepten kunnen worden (door)ontwikkeld en gelanceerd. Binnen dit thema onderzoekt TNO risicomanagement, informatiedeling en samenwerking in het digitale domein. TNO draagt hiermee bij de aan de ambitie 'Digitale slagkracht op orde' van de Nederlandse Cybersecurity Agenda (NCSA) om o.a. te komen tot een landelijke dekkend stelsel van cybersecurity samenwerkingsverbanden ter bevordering van de slagkracht van publieke en private partijen. Aanvullend wordt in deze programmalijn kennis bij elkaar gebracht om het TNO cybersecurity onderzoek te sturen en te laten zien hoe cybersecurity innovaties helpen om maatschappelijke uitdagingen aan te gaan. Dit focusgebied sluit aan op het Deelprogramma 5 van de KIA Veiligheid/Missie Cyberveiligheid: ketenweerbaarheid en governance. Concrete beoogde resultaten voor 2020 omvatten; i) een eerste consortium rond het thema Cyber Secure Behaviour en een concept meerjarenplan op basis van de KIA Veiligheid/Cyber; een verdere vulling van de cybersecurity informatiedeling toolbox met samenwerkingsverbanden en kennisopbouw voor alle betrokken in het landelijk dekkend stelsel (overheid, publiek en privaat) en bevordering van cybersecurityinformatiedeling.

Bestrijden Cybercrime en gedigitaliseerde criminaliteit; het ontwikkelen van tools en methoden om het actuele beeld van cybercrime fenomenen te kunnen volgen, de effectiviteit van interventies te kunnen meten en interventies te ondersteunen en hiermee het handelingsperspectief van politie, OM en bedrijfsleven ter bestrijding van cybercrime en gedigitaliseerde criminaliteit te vergroten. Dit focusgebied sluit aan op het Deelprogramma 1 van de KIA Veiligheid/Missie Cyberveiligheid: Bestrijden cybercrime. Concrete beoogde resultaten voor 2020 zijn het genereren van een dataset en analyse tools voor phishing data in samenwerking met het Electronic Crimes Task Force (ECTF) gereed. Het ECTF is een samenwerkingsverband bestaande uit vertegenwoordigers van aangesloten banken, het Openbaar Ministerie en de Politie.

Foresight and horizon scanning; het opbouwen van een TNO brede foresight and horizon scanning capaciteit, bestaande uit beschikbare expertise, afgestemd proces en dedicated toolbox voor toepassing in het digitale domein, ten behoeve van nationale veiligheidsorganisaties en hun directe partners in het bedrijfsleven in het opbouwen van anticiperend vermogen, beleidsopbouw en handelingsperspectief. Deze capaciteit draagt bij aan bestaande en zich ontwikkelende 'foresight' activiteiten bij overheidsinstanties en partners in het bedrijfsleven zoals innovatieradars, dreigingsbeeldanalyses en impact assessments. De instrumenten die hierbij ingezet worden zijn methodisch van aard, maar er worden ook technische instrumenten ontwikkeld, zoals automatische bron-scanners, systeem analyse tools en scenario development tools. Dit focusgebied is van belang voor TNO om te investeren in structurele capaciteiten die essentieel zijn om haar rol als innovatie-motor voor overheid en bedrijfsleven te kunnen spelen. Zo wordt bepaald welke cybersecurity dreigingen, technologische ontwikkelingen en trends de komende jaren onze aandacht verdienen. Concrete resultaten voor 2020 zijn i) een 'good practice' gids van forecasting methoden en technieken; en ii) een eerste versie van een 'horizon scanning' toolbox, met bron-scanners, analyse tools en de TNO Innovatieradar .

High end assurance; dit betreft het ontwikkelen van high end assurance technologie voor high end security gebruikersorganisaties in Nederland, met name voor de bescherming van laag en hoog gerubriceerde informatie (van Departementaal vertrouwelijk t/m stg Zeer Geheim). Bijvoorbeeld de toepassing van quantum safe technologie, monitoring en detectie beschreven in hoofdstuk 2.1, toegepast in het gerubriceerd domein of (andere) cryptotoepassingen. Dit focusgebied sluit aan op het Deelprogramma 3 van de KIA Veiligheid/Missie Cyberveiligheid: Defensieve cybertechnologie, met specifieke aandacht voor het ontwikkelen van cryptotechnologie. Concrete doelen voor 2020 zijn i) de ingebruikname van Security Technology Assessment Methodology (STAM) door minstens twee cybersecurity bedrijven; en ii) de vorming van de eerste nationale cryptostrategie in publiek-privaat samenwerkingsverband op één onderwerp, óf de start van een eerste onderzoek naar laag TRL technologie voor gerubriceerde informatie.

Cyber Workforce Development; één van de breed erkende internationale bottlenecks is het tekort aan gekwalificeerd cyberpersoneel, zowel technisch als multidisciplinair, om de vereiste activiteiten uit te kunnen voeren om aan ambities en

verplichtingen te voldoen. Het vinden en binden van goed cyberpersoneel is in de internationale competitieve cybersecurity arbeidsmarkt op zijn minst problematisch en het tekort lijkt duurzaam. Daarbij neemt de werklast van het aanwezige cyberpersoneel toe, terwijl de effectiviteit van de organisatie om haar diensten en taken uit te voeren potentieel risico loopt. We zien steeds meer digitale componenten om te beschermen, een toenemende complexiteit van cyberaanvallen, steeds meer informatie om te verwerken om die aanvallen te herkennen en te weerstaan, en toenemende risico's voor 'gewone' medewerkers/mensen die tot extra (complexiteit bij) incidenten leiden. Aangezien het huidige personeelstekort niet alleen is op te lossen met het opleiden van meer personeel, moeten bedrijven breder kijken naar mogelijke oplossingen. Over de jaren heen zijn er wel verschillende manieren ontwikkeld om werkzaamheden uit te voeren; denk aan automatisering, uitbesteding, sharing resources, afwegen van prioriteiten, etc. TNO heeft op diverse van deze onderwerpen veel ervaring opgedaan, maar niet noodzakelijk vanuit het perspectief om personeelstekorten op te vangen. Dat zou een extra dimensie vormen bij het combineren van deze oplossingen. Beoogd eindproduct is een multidisciplinaire aanpak die leidt tot concreet advies en plan van aanpak via welke weg organisaties hun tekort aan cyberpersoneel het best kunnen aanlopen. Dit start met een visie voor een multidisciplinaire aanpak met onderbouwing vanuit (reeds bestaand) TNO onderzoek van bijv. TNO Leiden, focusgebied automated security en ander (wetenschappelijk) onderzoek.

<u>Externe aansluiting en stakeholder management</u>

Het TNO meerjarenprogramma VP CRM&SR bouwt voort op bestaande beleids- en visie documenten, cyberstrategieën en cyber innovatie agenda's in de Nederlandse, Europese en internationale context. Zo is in 2019 nadrukkelijk aansluiting gemaakt met de Missie Cyberveiligheid van de Kennis en Investering Agenda (KIA) Veiligheid (in wording) . De inhoudelijke onderwerpen uit deze missie zijn herkenbaar terug te leiden naar de onderwerpen en beoogde resultaten zoals eerder beschreven in dit hoofdstuk. In de in 2019 herziene Nederlandse Digitaliseringsstrategie wordt de digitale weerbaarheid van burgers en bedrijven als prioriteit benoemd. In de Nederlandse Cyber Security Agenda (NCSA) , de Nationale Cyber Security Research Agenda (NCSRA III) en de Internationale Cyberstrategie uit 2017 komen de TNO focusgebieden on onderzoeksonderwerpen herkenbaar terug. TNO neemt samen met de Ministeries van Defensie, Veiligheid en Justitie, Onderwijs Cultuur en Wetenschap, Economische Zaken, Binnenlandse Zaken en de Nederlandse Organisatie voor Wetenschap Onderzoek deel aan de werkgroep 'Veilige Samenleving', die gestart is met het opstellen van de Publiek Private Kennis- en Innovatie Agenda 'Veilige Samenleving'. Het TNO meerjarenprogramma VP CRM&SR is in de geest van de inhoudelijke ambitie van deze maatschappelijke uitdaging opgesteld. Internationaal participeert TNO in de relevante werkgroepen, taskforces en evenementen. Voor 2020 beogen we deelname aan de World Economic Forum working group Energy; de jaarlijkse Meridian conferentie, betreffende critical information infrastructure protection; de European Cyber Security Organisation bijeenkomsten; de permanent stakeholder group van ENISA; de European SCADA and Control Systems Information Exchange; de CEPS Task Force: AI & Cybersecurity; het expertteam voor de NWA-call rondom Cybersecurity; de ronde tafel dcypher en Cyberveilig NL; en Cybersafety Noord Nederland.

Het opstellen en de uitvoering van het onderzoeksprogramma VP CRM&SR vindt plaats in nauwe afstemming met VP Veilige Maatschappij (VM), programmalijn Cyber Security & Societal Resilience, VP ICT, programmalijn Cyber Security, en de TNO onderzoeksprogramma's met het bedrijfsleven, Veiligheid en Justitie, Defensie en Politie. De onderzoeksprogramma's versterken elkaar. Innovaties in het VP CRM&SR richten zich daarbij primair op de cyberveiligheid van organisaties/sectoren, en op het versterken van de nationale IT- en cybersecurity-industrie. De focus van het VP VM ligt primair op de maatschappelijke veiligheid en weerbaarheid van de samenleving als geheel. VP ICT richt zich primair op de inzet van digitale sleuteltechnologieën, zoals de ontwikkeling van AI- en netwerkdata-gebaseerde aanvalsdetectie algoritmes, en de integratie van dergelijke algoritmes in een geautomatiseerd ICT platform voor mitigatie van cyber aanvallen en ondersteuning van security analisten.

Links naar externe rapporten en beleidsstukken:
https://www.hollandhightech.nl/nationaal/innovatie/kennis-en-innovatie-agenda/veiligheid
https://www.rijksoverheid.nl/documenten/rapporten/2019/07/05/nederlandse-digitaliseringsstrategie-2.0
https://www.nctv.nl/ncsa/index.aspx
https://www.dcypher.nl/en/research-agendas
https://www.rijksoverheid.nl/documenten/rapporten/2017/02/12/internationale-cyberstrategie-naar-een-geintegreerd-internationaal-cyberbeleid-getitield-digitaal-bruggen-slaan

Dynamiek

Het belang van cybersecurity kennisontwikkeling wordt onderstreept in de Nederlandse Cyber Security Agenda. In een brief aan de Tweede Kamer op 26 juni 2018 is dit nogmaals bevestigd:

'Het versterken van voldoende en hoogwaardige ontwikkeling van zowel fundamenteel als toegepast cybersecurity onderzoek is cruciaal. Gericht multidisciplinair onderzoek over de gehele kennisketen heen dat zowel naar oplossingen voor de langere of kortere termijn kijkt, is van het grootste belang, zo vindt het kabinet. […] Vanwege het huidige versnipperde landschap van organisaties die zich bezighouden met cybersecurity kennisontwikkeling, wordt vanuit het kabinet een verkenning gestart naar de mogelijkheden voor versterking van de kennis en innovatieketen voor cybersecurity, de opzet van een Kennis- en Innovatie Agenda daartoe en hoe een langjarige samenwerking, tussen publieke en private partijen, over de hele kennis- en innovatieketen heen kan worden georganiseerd. […] De verkenner wordt gevraagd om ten behoeve van zijn advies alle relevante actoren te consulteren, bestaande financieringsstructuren in kaart te brengen en de mogelijkheden voor verbetering van technologie overdracht te signaleren.'

TNO is een sleutelspeler in de Nederlandse cybersecurity kennisontwikkeling gezien de positie in de valorisatieketen tussen (universitair) fundamenteel onderzoek en de toepassing in de samenleving. TNO is een aanjager voor publiek-private samenwerking om de digitale weerbaarheid van Nederland te versterken en economische kansen in cybersecurity te verzilveren. Voor kennisopbouw en innovatie focust TNO zich op die cybersecurity problemen en onderliggende mechanismen waarvoor een Nederlandse kennisbasis en producten gewenst zijn (bijvoorbeeld voor veiligheidsorganisaties); en TNO draagt bij aan het oplossen van grote uitdagingen in cybersecurity en niet vanzelf door marktpartijen worden opgepakt. Vanuit deze rol heeft TNO een aanzienlijke bijdrage gegeven (en doet dat nog steeds) aan de Kennis- en Innovatie Agenda (concept-status). In deze rapportage zijn de laatste inzichten meegenomen uit de samenstelling van de KIA. De onderwerpen uit het VP zijn daarmee inhoudelijk afgestemd met de deelprogramma's uit de desbetreffende Missie Cyberveiligheid.

In 2019 is het proces rondom de programmering van VP CRM&SR grondig herzien. Focus is aangebracht op de belangrijkste maatschappelijke uitdagingen en behoeften van onze partners en sponsoren. En de investeringen in kennis en technologie zijn afgestemd met deze focus. Een stevige kennisbasis is een randvoorwaarde voor een langdurige en sterke internationale concurrentiepositie. Alleen dan kunnen we antwoord geven op de cybersecurityvraagstukken van de toekomst. Met dit vraaggestuurd programma organiseert TNO samen met andere kennisinstellingen, overheidsinstellingen en (cybersecurity) bedrijven de noodzakelijke ruimte om te experimenteren, zodat innovaties een weg naar de markt vinden. De units Defensie en Veiligheid en ICT van TNO werken intensief samen op cybersecurity, zowel vanuit het perspectief van Nationale Veiligheid, als het perspectief van bedrijfscontinuïteit en het verdienvermogen. De inhoudelijke coördinatie van dit vraaggestuurd programma is sinds 2019 verdeeld over TNO Unit ICT en de TNO Unit Defensie en Veiligheid.

Titel	**Radar and Sensor Systems (P104)**
Missie/ Topsector	Veiligheid / HTSM
Contactpersonen TNO	Director Market ISS: K. Agovic, VP Manager: F.L.M. van den Bogaart
Contact extern	J. Troost – Thales Nederland B.V., HTSM Roadmap Security H. Naus – NXP, HTSM Roadmap Electronics A. Venema – Ministry of Defence HDB J.C. Dicke – Ministry of Economic Affairs and Climate Policy, Commissariaat Militaire Productie

Programma jaar 2020 - Samenvatting

The *Roadmap Radar and Integrated Sensor Suites* focusses until 2030 on the development of the next integrated sensor suite for the future frigates of the Royal Netherlands Navy (RNLN). A major goal is to demonstrate a functional prototype of an integrated radar and EW sensor suite (EDM) and its building blocks. Essential towards 2023 is exploratory research within D-ART of the KIA Sleuteltechnologieën to establish a robust fundamental and scientific technology basis in sensor signal processing and in very advanced RF technologies. Custom design and realization of various active MMIC and passive RF components (a.o. PHAENICS) that cannot be bought on the market will be demonstrated. DAISY2 demonstrates miniaturized RF building blocks that show a cost reduction of a factor of 10 compared to the current state-of-the-art and a reduction of the volume of a radar sensor by a factor of 25, resulting in a thickness of the antenna face of only 2 cm. A step comparable with

the transition from the bulky 'classical' television set to a flat panel LCD TV screen. Complementary, full implementation of a short-distance range sensor in an SiGe MMIC, including RF front-end, control and time reference will be completed.

Mission Critical Systems aims to design software-intensive management and highly complex systems that are crucial for carrying out successful defence and security operations. Long-term focus is on naval integrated mission management and command & control (C2) in maritime support centers. A heterodyne sensing solution to detect illegal trafficking of narcotics in the Mediterranean is demonstrated in ALFA (H2020), COMPASS2020 will complement this by demonstrating the combined use and seamless coordination of manned and unmanned assets to achieve greater coverage, better quality of information and shorter response times. Effects and benefits of UXV integration in C2 systems are demonstrated (OCEAN2020). A solution will be demonstrated that performs automated reasoning over input streams such as e.g. vessel motion and contextual information (H2020 MARISA) enabling faster detection of maritime anomalies such as illegal diving activities and transfer of contraband in the North Sea for better decision making.

Passive Sensors for Defence and Security focusses on using optical sensors, associated image processing and interpretation. Technology will be demonstrated to recognise human behaviour in video streams and turbulence mitigation in video. Development of sensor packages for unmanned systems will be pursued.

Space Situational Awareness (SSA) aims at a step-by-step development towards a national SSA facility based on SMART-L radar. With SMART-L, the Netherlands has already an intrinsic SSA capacity. This will be further expanded into a unique distinctive capability in Europe which guarantees access to an information position that would otherwise never be accessible to the Netherlands. Short term goal for 2020 is the development of radar classification, radar imaging and radar behaviour analysis techniques of unknown and unidentified objects in a low-orbit.

The aim of *Quantum Sensing* is to keep pace and to lead the way with the incredible rapid developments of quantum scale physics which will undoubtedly have a dramatic impact on the architecture and potential disruptive performance of future defence and security systems. The year 2020 will be characterized by demonstrating advances in quantum radar, quantum front-end technologies, quantum navigation, quantum magnetometers and in quantum signal processing.

Korte beschrijving

The VP aims to strengthen the global leadership and the competitiveness of our national defence and security industry, technology suppliers, SME's and universities by industrially relevant R&D that excels in speed of innovation. Main challenge is how to design and develop high-tech components, subsystems and complex sensor and associated C2 systems within a triple helix together with our national defence/security industry and governmental parties to fulfil their requirements as launching customer and which are crucial for carrying out successful defence and security operations.

Activities are reported to the Roadmap Security and the Roadmap Electronics of the Topsector High Tech Systems and materials (HTSM). The VP contributes to the Societal Theme Security, in particular to the topics *Smart Kill-chains - Radar en Geïntegreerde Sensorsuites* and *Smart Manning & Automation* of the mission "*Maritieme hightech voor een veilige zee*" and to the topic Space Situational Awareness of the mission "*Veiligheid in en vanuit de Ruimte*". The multi-year project D-ART is included in the KIA *Sleuteltechnologieën* as MJP88.

The VP has links with the *Nationale Wetenschapsagenda Routes*: "Quantum- en nanorevolutie", "Smart Industry", "Tussen conflict en coöperatie" and "Waardecreatie door verantwoorde toegang tot en gebruik van big data".

Technological breakthroughs are created and in-depth knowledge is built in areas were knowledge is crucial and can't be bought anywhere else. In the following technology and knowledge areas we strive to be recognised worldwide key players.

The *Roadmap Radar and Integrated Sensor Suites* considers 3 technology and knowledge areas: 1) Radar and Suite Concepts to develop flexible, reconfigurable and multi-functional sensor suites that can cope with future threats with a better performance than 'the sum' of the performances of the individual sensors. This requires new architectural concepts that allow new processing and interfacing technologies; 2) RF Front-ends including large scale packaging to enable critical hardware realisation of above-mentioned novel concepts; and 3) Advanced AESA algorithms and processing techniques to enable reconfigurable processing and new functionalities.

The overall objective of Mission Critical Systems (MCS) is to design and develop intelligent systems for combat management, platform management, bridge management and mission management. These are systems that can autonomously reconfigure during design and runtime as to optimize available resources in the military naval/land domains and in the civil maritime domain. The basic idea is how artificial intelligence can be used to integrate model-based engineering of complex systems. MCS develops in this way answers to industrial standards and can make autonomous decisions without human intervention and hence reduce operational cost of the RNLN and development cost of industry.

A key enabler for future optical sensors is to improve image enhancement techniques for optimal system performance. While traditional image enhancement techniques show fundamental limitations, machine learning techniques in particular deep learning will allow a next generation of image enhancement.

Resultaten 2020

The 2020 results reported below will be realised in various contracts with many different partners, sponsors and funding agencies. In general we target:

- Sponsored contracts and TKI contracts with Dutch industry and SME's in defence & security;
- Contracts of the European Defence Agency (EDA) carried out together with national and EU defence industries and EU research institutes;
- Contracts within the scope of national and regional funded programs (EFRO) carried out with national industry, national universities and SME's;
- Contracts within the scope of the Security calls of Horizon2020 together with national and foreign industry and universities;
- Contracts within the scope of the Preparatory Actions on Defence Research (PADR) of the EC as preparation for participation in projects within the European Defence Fund (EDF) carried out together with national defence industry and with EU defence industries and research institutes;
- Contracts within ECSEL and PENTA initiatives of the EC with EU and national (defence related) companies and universities.

The extensive cooperation with the EDA and within PADR should be emphasized. Within these frameworks, all program lines of this VP partner together with almost all major defence sensor manufacturers (Thales, Leonardo, Hensholdt, INDRA, Rheinmetall, Elettronica, Airbus, SAAB, SAFRAN, Adimec, Photonis, Nedinsco ITS), with partners that provide critical independent defence technology (UMS, NXP) and with all relevant defence research institutes (Fraunhofer FHR and IOSB, FOI, ONERA, III-V Labs and VTT). Our activities are fully aligned with the Strategic Research Agendas of EDA and the national priorities in PADR and EDF.

<u>Roadmap Radar en Geïntegreerde Sensorsuites</u>

The national Roadmap Radar and Integrated Sensor Suites is governed by the Platform Nederland Radarland and is carried out within the Triple Helix and in an established R&D ecosystem. The end goal of the Roadmap 2030 is a new integrated sensor suite for the next generation frigates of the RNLN. All annual results contribute to this final goal, these results have been formulated in such a way that they can also be exploited in other (economic) domains. Continuing this proven concept in a similar way until 2030 implies a bundling of public and private investments and a very intense cooperation with end users. In the period 2010-2016 of the previous roadmap we worked together with 8 Dutch knowledge centres, 8 national industries, 28 national SME's, 15 European knowledge institutes and 40 non-Dutch companies. A similar number is expected and required to realize the Roadmap until 2030.

New science questions at a very early stage in signal processing and front end electronics will be answered. Cooperation with the 3 Dutch Technical Universities is therefore established.

Future naval operations will require an Integrated Air and Missile Defence capability, and the RNLN will have to operate worldwide in a congested and contested environment with increasingly advanced challenges, such as swarms or hypersonic missiles. A breakthrough in technology is necessary to develop sensors that are flexible enough to be reconfigured in near real-time

such that they can detect, track and classify a variety of objects simultaneously and in a timely manner. The development of an array antenna with the capability to perform multiple tasks in parallel and using simultaneously different parts of the array enables this flexibility.

A functional prototype of an X/S band one-radar functionally integrated with an ESM system will be demonstrated until 2023 with Thales, the RNLN and in-kind support of others. Hardware and software building blocks hereto will be realized in 2020.

The multi-year multi-partner program D-ART (D-RACE - Advanced Radar Technology) within the KIA Sleuteltechnologieën demonstrates a proof of concept of a system with digital signals becoming available closer and closer to the front-end. The main knowledge question is how to solve fundamental science problems in signal processing algorithms, RF front-end technologies and system concepts.

The innovation area front-end technology focusses on the design and realization of high-frequency active electronic circuits on GaAs, GaN and SiGe (a.o. DAISY2) semiconductor technologies and on the realisation of passive RF components on classical RF/PCB substrates or on silicon in order to further miniaturise while increasing significantly the RF performance. In 2019 a 100W S-Band GaN MMIC is realized with twice the output power than current state-of-art, leading in 2020 to 275W packaged S-Band high power amplifiers (HPAs): a world record. In addition the feasibility of a new generation architectures for HPAs will be shown to enable more functionality (CROWN, ALMA). In 2020 DAISY2 will define how an entire receiver and digitization can be added to the existing DAISY module without growing in volume. SiGe building blocks will be demonstrated with Thales and a foreign semiconductor manufacturer, to prove the availability of a supply chain for military components (HIGHEST). Robust receivers MMICs for radars that have to operate in a heavily contested and congested EM spectrum will be demonstrated (SPICE). In previous years, the feasibility is shown of a fully functional SiGe IC for distance detection for low volume products with extreme SWaP requirements (CANDID). In 2020 the full IC implementation, including analogue and digital parts will be demonstrated for short-distance range sensing applications for sensors in <1 cm3 (PROSE). To drastically improve dynamic range issues in receivers, un-integrable passive RF components such as very selective filters that allow for a substantial reduction in size will be demonstrated on a passive silicon technology of Philips Innovation Services (SFINX). Antenna elements with inherent selectivity characteristics will be demonstrated by tackling unconventional solutions based on 2-dimensional PCB stack-ups and 3-dimensional developments (PHAENICS).

The innovation area Advanced AESA Algorithms and Processing Techniques focuses on the design and development of novel waveforms, signal processing algorithms and machine learning techniques that will enable future sensors with the capability to detect and engage upcoming new threats such as hypersonic missiles. In the scope of EDA together with Thales, SAAB and FOI (MANTRA) we demonstrate robust machine learning techniques for the classification of small and slow moving objects, such as swarms of UAVs. In CROWN (PADR) we demonstrate novel system concepts for performing radar and EW functions using a single, distributed antenna aperture We do this together almost all relevant defence industries and research institutes in Europe. In H2020 (ALFA) we work together with police forces and other European organizations and demonstrate the detection and identification of small UAV's that are used for drug trafficking into the EU.

<u>Mission Critical Systems</u>

In Mission Critical Systems, research focusses on how to provide systems with intelligence as to autonomously reconfigure during design time and at run time to optimize operational effectiveness. The design and development of such systems depends on autonomization of the loop "user needs - operational effect – functional system requirements – resource optimization" at different time scales, i.e. during the design and at runtime. Currently, DMO, TNO, Thales Netherlands BV, RH Marine Netherlands BV, and Damen Shipyards are researching MCS for the purpose of CMS, PMS and IBMS systems of navy vessels. In 2020-2023 this approach will be validated in a number of use cases, i.e. fusion of heterogeneous data and information for risk management in a maritime support center (MARISA use case for NL Coastguard), and integration of UXVs in a naval combat system for the RNLN (OCEAN2020 use case M-Frigate).

In MARISA a data and information fusion toolkit will be developed in 2020 in support of coastguard centers from e.g. the Netherlands, Spain and Italy. This toolkit serves as a technology demonstrator for the detection of maritime anomalies such as illegal diving activities and transfer of contraband at sea in the North Sea. From the viewpoint of technology, TNO will develop the goal function in terms of metrics and meta-metrics for an absolute comparison of various observation systems and information resources. In this way, an autonomous selection of observation resources can be made as to adapt to changes

in the environmental state while maintaining the coastguard center's operational objective. In 2020, TNO and the Netherlands coastguard will set up the 'MARISA proeftuin' in Den Helder, where MARISA innovative solutions will be demonstrated.

PADR's OCEAN2020 focuses on how to enhance situation awareness in a naval environment using unmanned systems and which additional functionalities for the command and control of unmanned systems from the Combat Management System of the RNLN ate thereto necessary. The functionalities will be trialed during the second OCEAN2020 trial in the Baltic sea in August 2020. This system-of-systems will consist of components originating from at least 8 different countries and will include underwater, surface and aerial platforms as well as combat management systems and maritime operational centers from various countries. In OCEAN2020, a multitude of partners participate, research institutes as well as industry. Moreover, PADR's OCEAN2020 is extended in H2020 which provides Mission Critical Systems with a long-term multiplier preparing for the European Defence Fund with strategic partners such as Thales, RH Marine and Damen.

Passive Sensors for Defence and Security

The ongoing activities regarding advanced image processing, camera signal conditioning and techniques for behaviour recognition together with Dutch SME's like Photonis, Grass Valley, ITS, Adimec and Nedinsco are continued from 2020 onwards. In addition it will be investigated how deep learning as well as other machine learning techniques can be applied to provide a smart region-of-interest capability. This enables full exploitation of 65 Mpixels+ high resolution high framerate (HRHFR) cameras by integrating into the camera data pre-selection. In the subsequent visualization, a standard HD output with high-resolution insets of regions of interest will be shown. The desired target is to transmit critical image information from a 65 MP/35 fps camera on a drone over a WiFi link to the ground; an estimated decrease from data to metadata of -99%. That goal can only be reached by combining advanced knowledge on embedded technology and transmission optimization (compression technology) with state of the art image processing. The resulting technology also allows direct generation of metadata to effectively use the optical sensors by MCS-like systems.

The compensation of the effects of turbulence in optical surveillance systems will be demonstrated in 2020 (TURBO). A PENTA project strives towards the development of high-performance smart imaging systems for (amongst others) security applications by using higher spatial, temporal and spectral solutions. Adimec, GrassValley and TNO will for the first time develop the complete imaging system using shared components. The software and firmware will be developed on the same platform to bring processing algorithms closer to the imaging sensor. This enables faster development and more advanced results. Trend within Dutch SME is creating 100% Netherlands built defense products. An intended initiative is to grow interest for designing and building a Dutch, expendable, low cost unmanned surface vehicle including sensor packages and payloads.

Space Situational Awareness and Tracking (SSA)

This new program line will start in 2020 and focuses on how to classify unknown objects in space with new signal processing algorithms to develop an unique distinctive capability with features that other countries do not have and cannot develop in the short term. The final ambition is to create a national SSA facility that also houses an R&D center of expertise where, as a spin-off, also economically promising projects can emerge from. With the SMART-L radar developments, the Netherlands already has an intrinsic radar SSA capacity. Through incremental steps and multi-spectral fusion with other sensors this can be further expanded. This together guarantees the Netherlands access to information from other countries that would otherwise not be accessible. Intermediate technical results for 2020 include the demonstration of the feasibility to identify objects in low space orbits and analyse its behaviour by radar classification and radar imaging algorithms; by detection and tracking tools with a very high accuracy; and by multi-static sensing and interfacing with other SSA facilities. Participation in the EDIDP and EDF is actively pursued with potential partners Thales, Airbus, NLR, S&T and others.

Quantum Sensing

Quantum technology based sensors may well in the future disrupt and transform the military battle field or even the balance of power. This very-low-TRL program line aims to co-develop our understanding of the added value in actual military use cases in parallel to the process of improving our technical understanding.

Future warfare at sea, in the air, at land or in space requires sensors that are an order of magnitude better than the current state-of-the-art. Quantum devices are extremely sensitive to its environment, this sensitivity to its environment may enable

sensing tools with enhanced and new capabilities. Quantum radar focuses on how to detect objects unseen by current systems, and quantum navigation technology answers the question how to make a better precise form of positioning systems.

The year 2020 will be characterized by demonstration of advances in quantum radar, quantum front-end technologies, quantum navigation sensors, quantum magnetometers and in quantum signal processing techniques together with the "natural" partners QuTech and TUDelft. Technical results for 2020 include the assessment study of selected quantum sensors and their consequences on military operations.

Dynamiek

Program lines are updated with respect to the program lines as reported in the plan 2019-2022. In addition, additional budget is allocated in 2020 to the VP resulting in the new program line Space Situational Awareness. The changes are indicated in the table below with an explanation of the major changes in the footnotes below the table:

Program lines in VP P104 Radar and Sensor Systems	
Reported in plan 2019-2022	*Plan 2020-2023*
Radar and Integrated Sensor Suites, *Stakeholder Platform Nederland Radarland* *~ 59% of the VP in 2020*	*Radar and Integrated Sensor Suites*, including from 2020 onwards the multi-year program D-ART of KIA Sleuteltechnologieën Stakeholders: Platform Nederland Radarland, D-RACE, HTSM and Societal Theme Security. ~ 49% of VP in 2020
Mission Critical Systems with stakeholders Dutch Maritime Defence industries and Royal Dutch Navy *~ 18% of the VP in 2020*	*Mission Critical Systems with stakeholders Dutch Maritime Defence industries, Royal Dutch Navy and Societal Theme Security* *~ 23% of the VP in 2020*
Passive Sensors for Defence and Security with stakeholders Dutch SME's in the field of Electro-optical systems. *~ 13% of the VP in 2020*	*Passive Sensors for Defence and Security with stakeholders Dutch SME's in the field of Electro-optical system, Ministry of Justice and Security* *~ 8% of the VP in 2020*
Quantum Sensing *10% of the VP in 2020*	*Quantum Sensing* *~ 8% of the VP in 2020*
D-RACE / D-ART with stakeholders Platform Nederland Radarland and D-RACE	
	Space Situational Awareness, *stakeholder Platform Nederland Radarland, partners of the mission Space in the Societal Theme Security* *~ 12% of the VP in 2020*

D-ART: In 2018 and 2019 a preliminary investigation of possible research topics, and discussions with the future D-ART partners identified the most relevant and promising techniques that are further investigated in the upcoming D-ART program leading to a significant risk reduction. D-ART is from 2020 onwards fully embedded in the Roadmap Radar and Integrated Sensor Suites.

Space Situational Awareness is new due to the involvement in the mission Space of the Societal Theme Security.

Mission Critical systems is growing due to its involvement in various H2020 and PADR contracts.

Titel	**Veilige Maatschappij (P102)**
Missie/ Topsector	Veiligheid
Contactpersonen TNO	Dr. T.W.J. van Ruijven
Contact extern	Mr. H. Hanoeman (ministerie JenV)

Programma jaar 2020 - Samenvatting

Veiligheid is een primaire voorwaarde voor welzijn en economische ontwikkeling in Nederland en Europa. Veiligheid is echter geen vanzelfsprekendheid. Bedreigingen voor onze veiligheid zijn divers en veranderen voortdurend. Terugkeerders uit Syrië zijn een bron van zorg, criminelen verschuiven hun activiteiten naar de onlinewereld, en de groeiende invloed van georganiseerde misdaad kan de samenleving ondermijnen. De snelheid van ontwikkelingen is dusdanig dat het veiligheidsdomein versneld moet innoveren. Innoveren in een krachtig samenspel tussen overheid, bedrijfs¬leven en kennisinstellingen.

Het kabinet benoemt 'veiligheid' als een wereldwijde maatschappelijke uitdaging waarvoor gerichte cross-sectorale inzet op het gebied van wetenschap, toegepast onderzoek en innovatie onontbeerlijk is . TNO verbindt zich met de grote uitdagingen van het veiligheidsdomein, door met het Vraaggestuurd Programma Veilige Maatschappij (VPVM) relevante nieuwe kennis en technologie te ontwikkelen en deze te vertalen naar innovatieve oplossingen voor de praktijk. TNO zet in op een bundeling van onderzoek binnen VPVM in een zestal programmalijnen:

1. *Terrorismebestrijding:*
   a. Meerjarendoelstelling: het verkleinen van de kans op aanslagen door de inzet van slimme technologie.
   b. Doelstelling 2020: het ontwikkelen van nieuwe bewakingsconcepten, identiteitsvaststelling, tracking en monitoring van (potentiële terroristen), en counter drones.
2. *Versterking strafrechtketen:*
   a. Meerjarendoelstelling: het vergroten van de effectiviteit van de strafrechtketen door het ontwikkelen van innovatieve werkwijzen en ondersteunende middelen.
   b. Doelstelling 2020: het versterken van capaciteiten in de strafrechtketen door systeemanalyses en kennisopbouw t.a.v. forensic intelligence.
3. *Crisisbeheersing:*
   a. Meerjarendoelstelling: het vergroten van de weerbaarheid van de samenleving door kennisopbouw en technologieontwikkeling voor crisisbeheersingsorganisaties.
   b. Doelstelling 2020: kennisopbouw t.a.v. de (cyber)dreiging voor de vitale infrastructuur, gesynchroniseerde besluitvorming en dynamisch risicomanagement.
4. *Cyber security & societal resilience:*
   a. Meerjarendoelstelling: een weerbaar en digitaal veilig Nederland door het vertalen van cybersecurityonderzoek naar praktische concepten voor overheid en bedrijfsleven.
   b. Doelstelling 2020: ontwikkeling model voor het kwantificeren van cyberrisico's, methoden voor identificatie vitale ketens (supply chain cybersecurity), herstelvermogen bij cyberincidenten en forecasting in het cyberdomein.
5. *Intelligence*
   a. Meerjarendoelstelling: het versterken van de inlichtingenpositie van gemeenten en veiligheidsorganisaties door het ontwikkelen van innovatieve werkwijzen en ondersteunende analysetechnologie voor hun inlichtingencapaciteit.
   b. Doelstelling 2020: ontwikkeling meerjarenplan gemeentelijke intelligence, validatie van het gemeentelijk intelligence raamwerk en ontwikkeling van technologieën om analysecapaciteit en voorspellend vermogen van gemeenten te vergroten.

6. *Weerbare professional:*
    a. Meerjarendoelstelling: het vergroten van de weerbaarheid en duurzame inzetbaarheid van Nederlandse veiligheidsprofessionals.
    b. Doelstelling 2020: kennisopbouw t.a.v. toekomstgerichte ontwikkelpaden en psychotrauma bij veiligheids-professionals.

Deze onderwerpen staan voor gebieden met hoge innovatiebehoefte, passend bij de kennisbasis van TNO. Daarnaast kent VPVM een in omvang toenemend onderdeel Verkenningen waarbinnen de relevantie van nieuwe technologie voor het brede veiligheidsdomein wordt verkend. In 2020 zullen de verkenningen worden uitgevoerd t.a.v.:

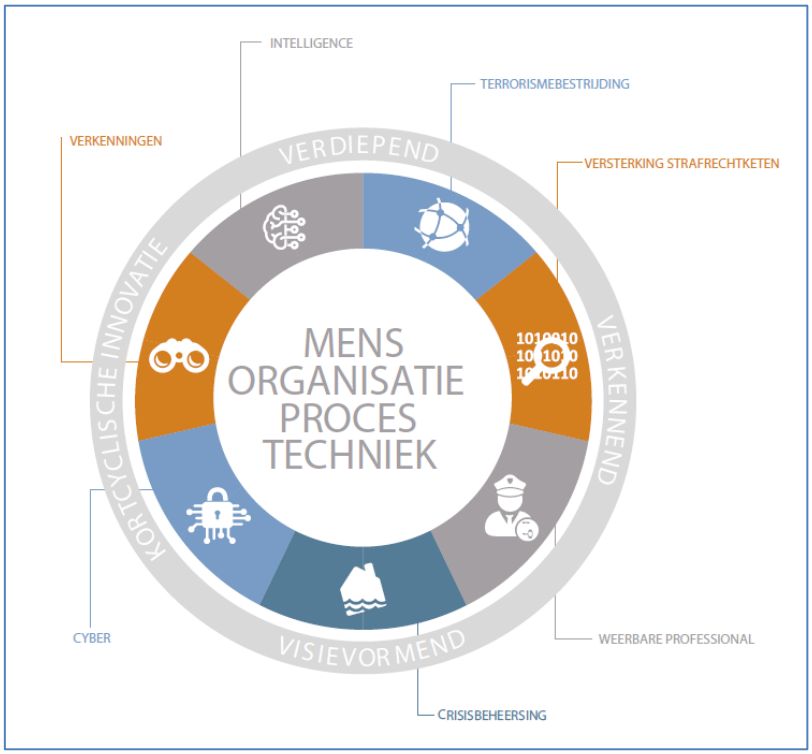
- Robotica
- Profiling
- Forensisch gebruik van data
- Identiteitsmanagement
- Privacy Enhancing Technologies

Om verschil te maken is focus en massa nodig op díe onderwerpen die voor het veiligheids- en justitiedomein het belangrijkst zijn. Het kiezen en invullen van de prioriteiten vindt plaats in een zich ontwikkelende programmatische samenwerking met het ministerie van JenV en de uitvoeringsorganisaties.

Korte beschrijving

De kennis die wordt opgebouwd en toepasbaar wordt gemaakt binnen VPVM betreft kennis van fenomenen zoals ondermijnende criminaliteit of van nieuwe technologie zoals robotica. Het kan ook gaan om sociaalwetenschappelijke of organisatiekundige kennis zoals gedragsbeïnvloeding of forecasting methoden. In het onderzoek wordt altijd gezocht naar samenhang tussen techniek, processen, mens en organisatie. Ook wordt expliciet gekeken naar de praktijk waarin kennis en technologie moeten worden toegepast. Innovatie staat immers niet voor uitvinden, maar voor toepassen in de praktijk.

TNO zet in op een bundeling van het onderzoek binnen VPVM in een zestal programmalijnen (Figuur 1): intelligence, terrorismebestrijding, versterking strafrechtketen, weerbare professional, crisisbeheersing en cyber security & societal resilience. Deze onderwerpen staan voor gebieden met hoge innovatiebehoefte, passend bij de positionering van TNO. Daarnaast wordt onder de noemer Verkenningen de waarde van nieuwe technologieën voor het bredere veiligheidsdomein verkend.



Figuur 1 - Programmalijnen VPVM

Bij de keuze voor onderwerpen voor kennisopbouw binnen VPVM wordt gezocht naar gebruik van kennis en technologie die is ontwikkeld voor Defensie of binnen de Early Research Programma's. Daarnaast wordt voorrang gegeven aan kennisopbouw die aansluit bij de Kennis en Investering Agenda (KIA) Veiligheid.

Resultaten 2020

<u>Terrorismebestrijding</u>

Met de programmalijn Terrorismebestrijding wordt kennis opgebouwd over de gehele keten van terrorismebestrijding; van vatbaarheid voor extremisme en radicalisering en de voorbereiding van aanslagen tot de preventie, detectie, mitigatie van aanslagen en forensische ondersteuning na afloop.

De meerjarendoelstelling voor Terrorismebestrijding is gericht op het vergroten van capaciteiten door de slimme inzet van technologie voor de gehele keten. Hiervoor zijn in het verleden een samen¬hangend kader voor gerichte kennis- en techno-logieontwikkeling voor en met veiligheidsorganisaties, een vraag¬sturingsmodel met de NCTV en een technologie-agenda ontwikkeld. De samenwerking binnen de keten wordt in 2020 bestendigd in een meerjarige programmatische samenwerking met de NCTV. De kennisopbouw voor Terrorismebestrijding is in 2020 gericht op het vergroten van capaciteiten ten behoeve van terrorismebestrijding waaronder:

- Ontwikkeling van nieuwe bewakingsconcepten
- Tracking & monitoring van (potentiële) terroristen waarbij een koppelvlak wordt gemaakt tussen zorg en veiligheid
- Nieuwe concepten ten behoeve van ID-vaststelling
- Counter Drones

Voor het onderzoek rond Terrorismebestrijding wordt naast de NCTV samengewerkt met Europese partners, FIOD, NFI, DEC-CIED, Koninklijke Marechaussee, Politie, AIVD, Schiphol en beveiligingsorganisaties als Securitas.

<u>Versterking strafrechtketen</u>

De strafrechtketen kampt met de uitdaging om oplossingspercentages en pakkans van delicten te verhogen. Daarnaast zien we dat criminaliteit verschuift van het fysieke domein naar en met het digitale domein én vervlecht tussen boven- en onderwereld. Ondermijnende criminaliteit vormt een groot en nog steeds groeiend probleem.

De meerjarendoelstelling van TNO is om bij te dragen aan deze uitdagingen door innovatieve werkwijzen en ondersteunende middelen te ontwikkelen om daarmee de effectiviteit van de strafrechtsketen te verbeteren. Kennisopbouw op dit onderwerp heeft reeds geleid tot samenwerking met RIECS in het Ondermijningslab. In 2020 wordt toegewerkt naar een programmatische samenwerking met het Openbaar Ministerie.

In 2020 wordt ingezet op kennisopbouw ten aanzien van:

- Versterking van de analysekracht (systeemanalyses, gedragsanalyse, intelligente tooling)
- Forensic Intellingence
- Verkenning van nieuwe technologieën voor de strafrechtketen

Bij de onderzoeksactiviteiten rond Versterking strafrechtketen wordt, naast Europese partners, samengewerkt met Politie, NFI, CJIB, DJI, en het Ministerie van Justitie en Veiligheid.

Crisisbeheersing

De programmalijn Crisisbeheersing is gericht op het ontwikkelen van kennis die nodig is om Nederland te beschermen tegen gebeurtenissen die de maatschappij (op grote schaal) kunnen ontwrichten. Het onderzoek ondersteunt beleidsvorming en capaciteitenontwikkeling binnen de veiligheidsketen; van proactie tot en met de nazorg. De opgebouwde kennis wordt onder andere toegepast ten behoeve van het Analistennetwerk Nationale Veiligheid en de bescherming van vitale infrastructuur. De kennis-ontwikkeling is in 2020 gericht op:

- De ontwikkeling van (cyber)dreigingen en de bescherming van de vitale infrastructuur in het kader van de nationale veiligheidsstrategie.
- Doorontwikkeling van kennis ten aanzien van netcentrisch werken in relatie tot gesynchroniseerde besluitvorming, alsmede van de ondersteunende technologie.
- Dynamisch risicomanagement.

Bij de onderzoeksactiviteiten rond Crisisbeheersing wordt, naast met Europese partners, samengewerkt met de NCTV, de ministeries van Infrastructuur en Waterstaat en Economische Zaken en Klimaat, vitale aanbieders, Politie, gemeenten en veiligheidsregio's.

Cyber Security & Societal Resilience

De programmalijn Cyber Security & Societal Resilience heeft als doel bij te dragen aan een veilig en weer¬baar Nederland in het cyber domein. Onderzoek en kennisopbouw zijn gericht op het verminderen van zowel cyberdreigingen als maatschappe¬lijke ontwrichting door mogelijke cyberverstoringen. Cybersecurityonderzoek wordt vertaald naar praktische concepten en experimentele oplossingen voor overheid en bedrijfsleven. Het grootste deel van het onderzoek vindt plaats in een meerjarige programmatische samenwerking met het Nationaal Cyber Security Centrum (NCSC).

Deze meerjarige samenwerking kent een onderzoeksplan voor de periode 2020-2023, waarin onderwerpen zijn opgenomen (herstelvermogen, supply chain risico, kwantificering van cyberrisico's en schade, forecasting, eindgebruikers) in lijn met het NCSC-onderzoeksplan, de TNO ambitie op cyberonderzoek en de missie Cyberveiligheid van de KIA Veiligheid.

In 2020 richt het onderzoek in VPVM zich op de eerste fase van dit onderzoeksplan:

- Aanvullingen op het herstelmanagement van vitale processen door onderzoek naar het (collectief) herstelvermogen van organisaties in de vitale infrastructuur na cyberincidenten;
- Specificeren van methoden om supply chain netwerken van de vitale processen in kaart te brengen;
- Ontwikkelen van een model voor het kwantificeren van cyberrisico's ter aanvulling van integrale risicomethodieken toegepast op vitale processen;

- Ontwikkelen van een Good Practice van gebruikte forecasting methoden en technieken gespecificeerd voor het cyberdomein.

De genoemde onderzoekvoorstellen sluiten aan op de deelprogramma's (2) Bevorderen ontwikkeling cybercompetenties, (3) Defensieve cybertechnologie en (5) Ketenweerbaarheid en governance van de KIA (cyber)Veiligheid.

Bij de onderzoeksactiviteiten rond cyber security & societal resilience wordt met name samengewerkt met het NCSC. Daarnaast zijn vitale aanbieders zoals de mainports Schiphol en de Rotterdamse Haven betrokken.

Intelligence

Intelligence betreft het vergaren, verwerken, interpreteren en beschikbaar stellen van infor¬matie en kennis ten behoeve van de primaire processen in het veiligheidsveld: preventie, onderschepping, handhaving en opsporing. Intelligence wordt ingezet ten behoeve van beeldvorming (wat is er aan de hand?), oordeelsvorming (wat vinden we hiervan?) en besluit¬vorming (wat te doen?).

De meerjarendoelstelling van de programmalijn Intelligence is de ontwikkeling van een raamwerk voor de inlichtingenpositie van organisaties en de bijbehorende analysetechnologie en kennis. Het onderzoek voor 2020 is gericht op:

- Ontwikkelen van een meerjarenplan gemeentelijke intelligence
- Validatie van het capaciteitenraamwerk gemeentelijke intelligence zoals ontwikkeld in 2019
- Ontwikkeling van methodieken om de ontwikkeling van gemeentelijke intelligence organisaties te stimuleren
- Ontwikkeling van technologieën om analysecapaciteit van gemeenten te vergroten.

Bij de onderzoeksactiviteiten rond Intelligence wordt, naast Europese partners, samengewerkt met Politie, OM, bijzondere opsporingsdiensten, het Ministerie van Justitie en Veiligheid en gemeenten.

Weerbare professional

Veiligheidsprofessionals moeten dagelijks presteren onder risicovolle omstandigheden en worden blootgesteld aan (zeer) schokkende gebeurtenissen. Dat heeft invloed op het functioneren; fysiek als mentaal welzijn staan onder druk. Tegelijk verandert de context waarin veiligheidsprofessio¬nals werken sterk: het digitale domein wordt belangrijker, 21st century skills worden gevraagd en talentonwikkeling is een must.

Voor een structurele 'fitness' is permanent leren nodig. Tenslotte vereist een dynamische, onvoorspelbare wereld ook op organisatieniveau adaptiviteit en wendbaarheid, van de organisatie: een uitdaging voor de cultuur, het leiderschap en de individuele werknemers. Voor het onderzoek naar de weerbare professional werkt TNO in een meerjarige programmatische samenwerking met de Politie en de Dienst Justitiële Inrichtingen.

In 2020 is de kennisopbouw binnen VPVM voor de weerbare professional gericht op:

- Nieuwe vaardigheden en toekomstgerichte ontwikkelpaden voor veiligheidsprofessionals
- Psychotrauma bij veiligheidsprofessionals

De huidige kennisbasis rond de weerbare professional is voornamelijk gebaseerd op defensieonderzoek. In 2020 blijft het doel om deze kennis toepasbaar te maken bij civiele veiligheidsorganisaties. Daarnaast wordt aansluiting gezocht bij de programma's die voortvloeien uit de KIA Veiligheid.

Verkenningen

De verkenningen in VPVM zijn erop gericht de potentiele toepassingen en toegevoegde waarde van nieuwe technologieën voor het brede veiligheidsdomein te onderzoeken. De meerjarendoelstelling van de verkenningen is vanuit TNO een actuele, omvattende en onderbouwende visie (kansen, dreigingen, ethische, juridische en maatschappelijke aspecten) op nieuwe kennis en technologie voor het veiligheidsdomein te ontwikkelen en te onderhouden.

In 2020 zal in ieder geval voor de volgende onderwerpen een verkenning worden voortgezet of opgestart:

- Robotica
- Profiling
- Forensisch gebruik van data
- Identiteitsmanagement
- Privacy Enhancing Technologies

De programmering van het Vraaggestuurd Programma is dynamisch, gedurende het jaar kunnen zich nieuwe onderwerpen aandienen. In deze gevallen kan een kleine verkenning worden opgestart.

Dynamiek

Het onderzoek en de kennisopbouw binnen VPVM worden gestuurd door middel van een meerjarige programmering. De structuur van zes programmalijnen en verkenningen die in 2020 wordt gehanteerd, is gelijk aan de programmering van VPVM in 2019. De wijzigingen in de kennisopbouw in de zes programmalijnen en de verkenningen is hierboven toegelicht. Op hoofdlijnen worden, ten opzichte van de programmering uit voorgaande jaren, de volgende wijzigingen in de programmering doorgevoerd:

- Het aandeel van de verkenningen in de totale programmering neemt toe met als doel de inbreng van nieuwe technologie in de onderzoeksprogrammering te vergroten.
- Kennisopbouw en onderzoek vindt buiten de verkenningen zoveel mogelijk plaats binnen meerjarige onderzoeksprogramma's met veiligheidsorganisaties.
- De naam van de programmalijn Nationale Veiligheid is veranderd in Crisisbeheersing omdat nationale veiligheid een bredere betekenis heeft dan het onderzoek dat in deze programmalijn plaats vindt.
- Het programma Avatar XPRIZE wordt onderdeel van VPVM.
- - Waar mogelijk wordt kennisopbouw gericht op de samenwerking met het bedrijfsleven in het kader van de KIA Veiligheid en de Meerjarige Missiegedreven Innovatie Programma's.

Titel	**Kennisopbouw Politie (P106)**
Missie/ Topsector	Veiligheid
Contactpersonen TNO	Tjarda Krabbendam MSc
Contact extern	Drs. S.C. Hamelink (Politie)

Programma jaar 2020 - Samenvatting

Veiligheid is een essentiële voorwaarde voor welzijn van de samenleving en economische ontwikkeling. Nederland staat voor complexe uitdagingen op het gebied van veiligheid, waaronder internationale instabiliteit, terrorisme, voortschrijdende digitalisering en de overheersende rol van informatie, en georganiseerde en ondermijnende criminaliteit. Om hiertegen opgewassen te zijn moet de politie voortdurend innoveren en daarvoor is het nodig om in toenemende mate te investeren in toegepast onderzoek ter versterking van de kennisbasis. Naast de gelden van EZK investeert de politie zelf ook in deze kennisopbouw.

De programmering 'Kennisopbouw Politie' heeft als voornaamste doel om de politie proactief aan te sluiten op de nieuwste (technologische) mogelijkheden voor zowel opsporingsmiddelen als de weerbaarheid van de politie professional.

Activiteiten binnen het programma richten zich op:

- inrichten van een gestructureerde kennisbasis ten behoeve van innovatie voor de politie;
- meerjarige kennisopbouw programma's met uitwerking op de korte, middellange en lange termijn;
- inrichten van een innovatie-ecosysteem (samenwerkingsmodel) voor de politie, bestaande uit kennisinstituten, wetenschappelijke instellingen, bedrijven en overheid.

In 2018 zijn binnen de programmering 'Kennisopbouw Politie' de volgende programma's gestart: *Programmakompas, Gestructureerde kennisbasis t.b.v. innovatie, Politiewerk in het cyberdomein, Operationele slagkracht (in specifieke zin versterken*

van het informatieproces), Politie in verbinding, en Ontwikkeling professional. Deze onderwerpen staan voor gebieden met hoge innovatiebehoefte, passend bij de kennisbasis van TNO.

De resultaten van de kennisopbouw programma's helpen de politie met de aanschaf en ingebruikname van een geïnnoveerde (technische) uitrusting, opsporingsmiddelen; en vergroten de weerbaarheid van de politie professional in nauw contact met haar omgeving. Middels kennisopbouw en innovatie wordt de operationele slagkracht van de politie vergroot.

Korte beschrijving

De politie is de grootste uitvoeringsorganisatie van het ministerie van Justitie en Veiligheid.

"De vraag is niet of de politie wil innoveren, we moeten innoveren!" (Korpschef Erik Akerboom op het Innovatiecongres 2016 'Tomorrow is Today'). Het werken met state of the art intelligence en technologie is een van de strategische prioriteiten van de politie.

De programmering 'Kennisopbouw Politie' heeft als voornaamste doel om de politie proactief te laten inspelen op nieuwe technologieën en maatschappelijke ontwikkelingen. Activiteiten binnen het programma richten zich op:

- inrichten van een gestructureerde kennisbasis ten behoeve van innovatie voor de politie;
- meerjarige kennisopbouwprogramma's met uitwerking op de korte, middellange en lange termijn;
- inrichten van een innovatie-ecosysteem (samenwerkingsmodel) voor de politie, bestaande uit kennisinstituten, wetenschappelijke instellingen, bedrijven en overheid.

TNO en politie zetten in op bundeling van het onderzoek binnen zes programma's: *Programmakompas, Gestructureerde kennisbasis t.b.v. Innovatie, Politiewerk in het cyberdomein, Operationele slagkracht (in specifieke zin versterken informatieproces), Politie in verbinding, en Ontwikkeling professional*. De eerste twee programma's geven structuur en richting aan het onderzoek, de laatste vier staan voor gebieden met hoge innovatiebehoefte, passend bij de kennisbasis van TNO.

Het kiezen en invullen van deze en onderliggende prioriteiten vinden plaats binnen de programmatische samenwerking tussen TNO en politie.

Resultaten 2020

<u>Programmakompas</u>

Belangrijkste doelstelling van het Programmakompas is het vormgeven van de strategische samenwerking politie-TNO.

In specifieke zin kent dit programma de volgende resultaten:

- Bepalen van (nieuwe) thema's en inrichten van programma's.
- Monitoren en bijsturen van de programma-uitvoering.
- Inrichten van het innovatie-ecosysteem (nationaal en internatio-naal) voor het politiedomein.
- Communiceren en dissemineren van de onderzoeksresultaten en de strategische samenwerking.

<u>Gestructureerde kennisbasis ten behoeve van Innovatie</u>

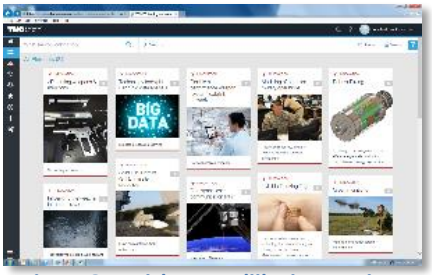


Fig. 1: Overzicht mogelijke innovaties

Een belangrijke stap om als politie slagkracht en legitimiteit te behouden in een veranderde wereld is een continu kennis- en innovatieproces. Belangrijk onderdeel daarvan is het opbouwen en gebruiken van een gestructureerde kennisbasis ten behoeve van innovatie.

Deze heeft tot doel:

- Inzicht geven in de kennis- en innovatiepositie van de politie, door enerzijds relevante innovaties, (sleutel)technologieën en trends in kaart te brengen en door anderzijds ontwikkelingen en behoeften binnen de politie met deze externe kennis- en technologieontwikkelingen in verband te brengen.
- Op basis daarvan de kennisopbouw en innovatie van en voor de politie opbouwen en uitbouwen.

Het resultaat bestaat uit:

- Gestructureerde kennisbasis met ondersteunende infrastructuur om deze te ontsluiten, deels gevuld met beschikbare informatie (technologieën, technologische ontwikkelingen en trends).
- Innovatieradars en bijbehorende roadmaps ten behoeve van de inhoudelijke programma's binnen de samenwerking Politie – TNO en op aanvraag van onderdelen van de politie.
- Verkenning hoe een samenwerkingsverband met relevante part-ners kan bijdragen aan een actuele gestructureerde kennisbasis.
- Advies over het kennis- en innovatieproces bij de politie en de aansluiting daarvan op de gestructureerde kennisbasis.
- Begeleiding en ondersteuning van AIO's of postdocs op sleuteltechnologieën

In latere jaren moeten de gestructureerde kennisbasis en de infrastructuur onderhouden worden en beschikbaar zijn voor gebruik door de relevante doelgroepen binnen de politie en TNO.

Politiewerk in het cyberdomein

Het programma politiewerk in het cyberdomein kent drie doelstellingen:

- Vergroten van het inzicht in en de kennis van trends en ontwikkelingen van cybercriminaliteit en gedigitaliseerde criminaliteit.
- Meetbaar maken van politie-interventies in het digitale domein om daarmee toe te werken naar evidence-based policing.
- Vergroten van de handelingsperspectieven ten aanzien van het omgaan met cybercriminaliteit en gedigitaliseerde criminaliteit.

Fig. 2: Dark web monitor

De complexiteit van het fenomeen vraagt erom dat nauwe afstemming plaatsvindt met stakeholders en vraagstellingen uit de praktijk. Hiervoor wordt gewerkt aan uitbreiding van de contacten met de verschillende politieonderdelen die actief zijn in het cyberdomein, en worden deze contacten benut voor het aanscherpen van de vraagsturing. De kennisontwikkeling is met name gericht op:

- Overzicht van trends en ontwikkelingen in het digitale domein en analyse van hun impact voor cybercriminaliteit en gedigitaliseerde criminaliteit.
- Beeld van de effecten en de effectiviteit van interventies, allereerst gericht op de wereld van het dark web, en uitbreiding naar andere fenomenen zoals phishing.
- Vertaling van de twee vorige punten naar handelingsperspectieven voor politiemedewerkers bij de aanpak van criminaliteit in het digitale domein.

Versterken informatieproces

Een sterke informatiepositie in de operatie is voor de politie essentieel om effectief uitvoering te kunnen geven aan politiewerk. Inzet van moderne technologie maakt een goede informatiepositie steeds beter mogelijk. Deze technologie wordt pas inzetbaar indien deze goed bijdraagt aan de behoeften van de politiemedewerker in de operatie.

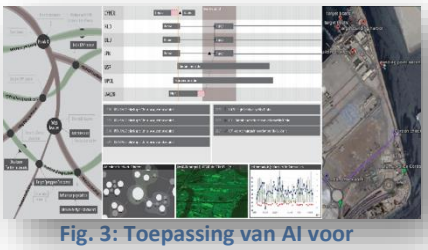


Fig. 3: Toepassing van AI voor besluitvormingsondersteuning

Het hoofddoel van het programma is als volgt:

Het vergroten van de operationele slagkracht door opbouw van kennis en ontwikkeling van methodieken en technieken die nu en in de toekomst ondersteunen dat de politie met de juiste informatie, op de juiste plek, bij de juiste persoon, op het juiste moment, op de juiste wijze beschikbaar, het juiste veiligheidsprobleem met de juiste interventie, beide juist onderbouwd, juist afhandelt.

Alle activiteiten binnen de projecten in dit programma dragen bij aan dit hoofddoel. Dit programma werkt waar mogelijk aan prioritaire onderwerpen op de veiligheidsagenda, zoals:

- Ondermijning
- CTER (contra terrorisme)
- PGA (persoonsgerichte aanpak)

Eerste resultaten komen beschikbaar in de vorm van:

- *Prototypes en demonstrators* (o.a. van een dynamisch draaiboek), bepaling toegevoegde waarde, visievorming sensing, concept tools en algoritmen, en een ontwerprichtlijn, toetsingskaders en beleidsadvies voor real time risicotaxatie.

In 2020 wordt er toegewerkt naar de volgende resultaten:

- een implementatie van het Dynamisch Draaiboek bij en samen met de politie voor ondersteuning van SGBO's
- het opstellen van een methode om met (zoek)profielen om de effectiviteit van politie inzet te vergroten binnen de ethische en juridische kaders
- ontwikkeling van algoritmes/indicatoren voor ondermijning rol, taak en visualisatie concepten voor de visualisatie regisseur die in het 'gouden uur' een overzicht moet geven aan de HoVD's.

Politie in verbinding

Het programma 'Politie in Verbinding' heeft als doel het ontwikkelen en beproeven van robuuste werkwijzen, inzichten en tools betreffende het samenwerken van de politie met burgers, bedrijfsleven en samen¬leving. Dit alles opdat de politie haar taken ook in de toekomst op een optimale manier kan uitvoeren.

Fig. 4: Applicaties voor gebruik door zowel burger als politie

Het onderzoek kent de volgende elementen:

- Bepalen van nieuw kader voor samenwerken met burgers, bedrijven en ketenpartners in een veranderende samenleving.
- Ontwikkelen, uitproberen en beoordelen van technologische oplossingen.
- Ontwikkelen, uitproberen en beoordelen van sociale, sociaal-technologische en procesinnovaties.
- Meten en voorspellen van de effectiviteit van samenwerken.

Onder de beoogde resultaten zijn:

- Raamwerk en werkwijzen voor samenwerking met burgers, bedrijven en keten¬partners,
- Prototypes van instrumenten en tools voor waarmee burgers en politie kunnen samenwerken,
- Effecten van nieuwe manieren van samenwerken of van samenwerken met nieuwe middelen.

Ontwikkeling professional

Veiligheidsprofessionals staan voort¬durend bloot aan risico's en (zeer) schokkende gebeurtenissen. Zij moeten weerbaar zijn om goed te kunnen blijven functioneren en gezond te blijven. Daarnaast vragen technolo¬gische innovaties veel van hun ver¬mogen om te leren en zich aan te passen. Binnen het programma wordt onderzocht wat technologische en intelligence-ontwikkelingen in combinatie met maatschappelijke veranderingen vragen van vakmanschap, weerbaarheid en adaptief vermogen van de professional.

Het programma bestaat uit twee onderdelen:

Weerbaar en wendbaar

Hierin wordt onderzocht hoe professionals omgaan met de opbouw van mentale, morele en fysieke belasting, waarbij kennis wordt ontwikkeld over hoe innovatieve technieken als personal sensing, Virtual Reality en HR analytics weerbaarheid van individuen en in teams kan versterken. Daarnaast wordt onderzocht hoe het adaptief vermogen van professionals kan worden

versterkt, waarbij kennis wordt opgebouwd over de wisselwerking tussen de adaptieve vermogens van medewerkers en leidinggevenden en organisatie-factoren zoals bestaande procedures en werkwijzen.

Figuur 5: weerbaarheidsdashboard voor leidinggevenden

Flexibilisering van leerprocessen

Dit betreft een samenwerking met Defensie onderzoek. Het onderzoek richt zich op de ontwikkeling van innovatieve trainingsmethodieken en interventies waarin flexibilisering, leren op maat en werkplekleren centraal staan. Hierbij wordt onderzocht hoe technologieën als learning analytics kunnen worden gebruikt om gepersonaliseerd leren te ondersteunen.

Beoogde resultaten zijn o.a.

- Prototype voor een 'weerbaarheidsdashboard' voor leiding-gevenden dat monitoring en analytics combineert om inzicht te geven in de weerbaarheid van het team en bovendien risico-signalering doet op basis van voorspellende algoritmes (zie figuur 5);
- Inzicht in effectiviteit van Virtual Reality Training in voorbereiding evenementen voor prestatie en stress tijdens optreden;
- Een diagnose tool voor adaptief leiderschap;
- (Raamwerk voor) leerinterventies op de werkplek.

Dynamiek

Na de realisatie van samenwerking tussen JenV en TNO is de politie, na besluit daartoe in november 2017 van de Korpsleiding politie (KL) en de Raad van Bestuur TNO, is in 2018 gestart met de programmering 'Kennisopbouw Politie'.

Als eerste zijn de twee inrichtingsprogramma's Programmakompas en Gestructureerde kennisbasis t.b.v. innovatie van start gegaan. In de zomer van 2018 begon vervolgens de definitiefase van de vier technologische programma's Politiewerk in het cyberdomein, Operationele slagkracht (in specifieke zin Versterken informatie-proces), Politie in verbinding en Ontwikkeling professional. Deze fase diende om in nauw overleg met de specifieke betrokken politie-geledingen de bestedingsplannen nader uit te werken en vorm te geven.

De aanpak binnen de programma's beoogt een bundeling van samenhangende onderzoeksprojecten met een passend begeleidings- en vraagsturingsmodel. Onderdelen en projecten binnen programma's die voldoende zijn afgestemd zijn inmiddels gestart.

In 2020 zal de kennisopbouw (nog) meer in lijn worden gebracht met de strategische onderzoekslijnen van politie en worden naar verwachting enkele nieuwe programmalijnen opgestart.