Anna van Buerenplein 1
2595 DA Den Haag
Postbus 96800
2509 JE Den Haag

www.tno.nl

T +31 88 866 00 00

TNO-rapport

Meerjarenprogramma 2018-2021
Thema Maatschappelijke Veiligheid

Activiteitenplan 2018
(Korte versie)

Datum	September 2017
Auteur(s)	ir. C.H. van den Berg
Aantal pagina's	12
Regievoerend departement	Ministerie van Veiligheid en Justitie
Projectnummer	

Inhoudsopgave

Samenvatting

Titel	P102 – VP Veilige Maatschappij
Maatschappelijk thema	Maatschappelijke Veiligheid
Contactpersoon TNO	Ir. C.H. van den Berg
Contactpersoon overheid	Mr. H. Hanoeman (ministerie VenJ)

Veiligheid is een primaire voorwaarde voor welzijn en economische ontwikkeling in Nederland en Europa. Veiligheid is echter geen vanzelfsprekendheid. Bedreigingen voor onze veiligheid zijn velerlei, en veranderen voortdurend. Terroristische aanvallen in Europa komen steeds vaker voor en komen dichterbij ons land, criminelen verschuiven hun activiteiten naar de online wereld, en georganiseerde misdaad lijkt een steeds grotere greep te krijgen op de Nederlandse economie.

De snelheid van ontwikkelingen is dusdanig dat het veiligheidsdomein versneld moet innoveren. Innoveren in een krachtig samenspel tussen overheid, bedrijfsleven en kennisinstellingen.

Het is de doelstelling van het Vraaggestuurd Programma Veilige Maatschappij (VPVM) om Nederland veilig en rechtvaardig te helpen houden door op geselecteerde gebieden nieuwe kennis te ontwikkelen en te faciliteren dat deze kennis wordt vertaald naar de praktijk.

TNO heeft de ambitie om met dit VPVM maximale toegevoegde waarde te hebben voor het ministerie van Veiligheid en Justitie en de uitvoeringsorganisaties, waaronder de Nationale Politie. Dat vraagt focus en massa op díe onderwerpen die voor het veiligheids- en justitiedomein het belangrijkste zijn. Door programmatisch samen te werken bereiken we die focus en massa en zijn we in staat om goed te prioriteren.

TNO zet in op een bundeling van haar onderzoek binnen VPVM in een zestal programmalijnen: Terrorismebestrijding, Het Nieuwe Melden, Opsporing 2.0, Nationale Veiligheid, Cyber Security & Societal Resilience, en Intelligence. Deze bundeling is gekozen met het oog op de beoogde programmatische samenwerking. De programmering is nadrukkelijk dynamisch van aard.

Naast de huidige compacte beschrijving van VPVM is ook een meer uitgebreide versie voorhanden.

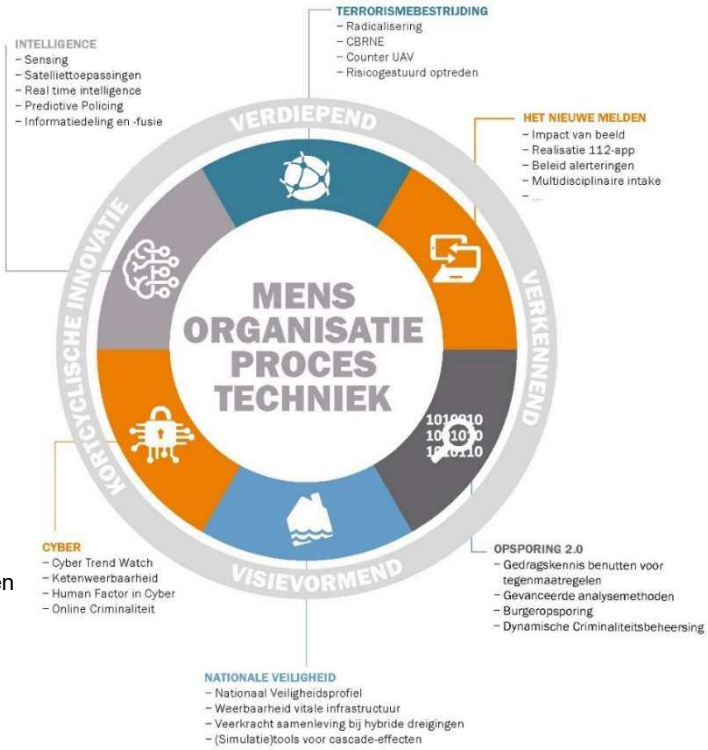
1 Omschrijving

Het is de doelstelling van het Vraaggestuurde Programma Veilige Maatschappij (VPVM) om Nederland veilig en rechtvaardig te helpen houden door op geselecteerde gebieden nieuwe kennis te ontwikkelen en te faciliteren dat deze kennis wordt vertaald naar de praktijk.

De kennis die we toepassen kan kennis zijn van specifieke fenomenen als hybride dreigingen of van specifieke nieuwe technologie als Unmanned Aereal Vehicles. Het kan echter ook gaan om sociologische, organisatiekundige of bedrijfskundige kennis. In ons onderzoek zoeken we altijd naar de samenhang tussen de perspectieven techniek, proces, mens en organisatie. Ook kijken we expliciet naar de werkprocessen waarin de vernieuwing moet gaan passen. Innovatie staat immers niet voor uitvinden, maar voor toepassen in de praktijk.

Ons onderzoek kan van *verkennende* aard zijn als we bijvoorbeeld in kaart brengen wat de mogelijkheden en risico's voor beleid en operaties zijn van een specifieke nieuwe technologie als nanotechnologie, robotics of 3D-printen. In *visievormend onderzoek* schetsen we een visie over een benodigde transitie, zoals die rond online criminaliteit of risicogestuurd optreden in het veiligheidsdomein. *Verdiepend onderzoek* leidt tot de ontwikkeling van mogelijke maatregelen/ methodieken tegen specifieke risico's zoals UAV's. Bij *kortcyclische innovatietrajecten* tenslotte komen de bovenstaande vormen van onderzoek samen in kleine elkaar snel opvolgende onderzoeksinterventies. Vaak zal dan sprake zijn van een 'Living Lab', waarbij dicht tegen de praktijk aan wordt geëxperimenteerd. En vaak gebeurt dat met medewerking van bedrijven en andere kennisinstellingen.

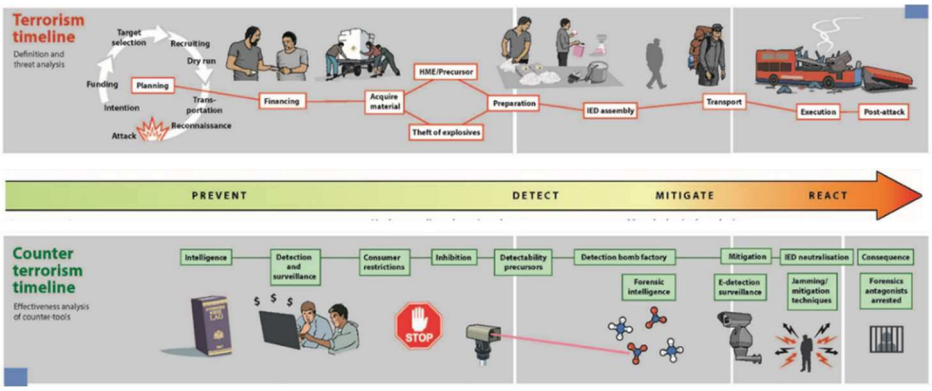
TNO zet met het VPVM in op een bundeling van haar activiteiten in zes programmalijnen: *Terrorismebestrijding, Het Nieuwe Melden, Opsporing 2.0, Nationale Veiligheid, Cyber Security & Societal Resilience* en *Intelligence.* De bundeling is gekozen met het oog op de beoogde programmatische samenwerking. De programmering is nadrukkelijk dynamisch van aard.



Figuur 1: Programmalijnen in vogelvlucht

1.1 Terrorismebestrijding

TNO zet zich in om met de programmalijn Terrorismebestrijding kennis op te bouwen (en te distribueren) over de gehele keten van terrorismebestrijding. Van het proces dat kan leiden tot de intentie een aanslag te plegen (waaronder radicalisering) tot de preventie, detectie, mitigatie van een aanslag en forensische ondersteuning na een aanslag. Door het beschouwen van de gehele keten en door samenwerking met de stakeholders kan de veiligheid van de Nederlandse maatschappij worden verhoogd. Met onze kennis ondersteunen wij de overheid en bedrijven om aanhang van radicaal gedachtengoed te beperken, aanslagen te voorkomen en/of de consequenties van een aanslag te beperken. Zo wordt het aanpassend vermogen van de Nederlandse maatschappij verbeterd bij de toenemende dreiging van terroristische aanslagen in Europa.



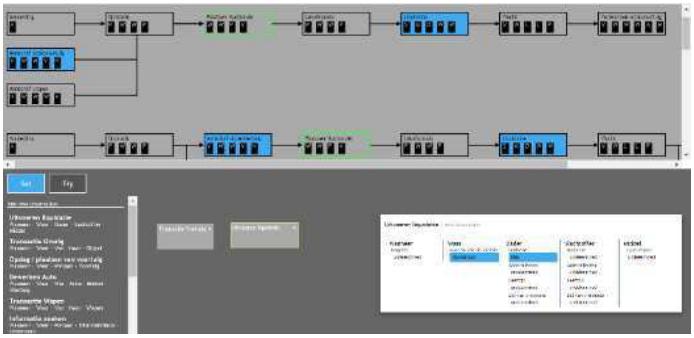
TNO's kennisbasis op het gebied van terrorismebestrijding is breed en reikt van kennis over radicalisering en CBRNE tot kennis rond de dreiging van UAV's, die kwaadwillenden kunnen inzetten om aanslagen te plegen. We vertalen dit soort kennis naar perspectieven voor beleid, detectie, mitigatie, analyse en interventie voor gemeenten, politie, grensbewaking en objectbewaking. De kennisbasis is van belang voor NCTV, crisisbestrijding en inlichtingendiensten. De snelheid van ontwikkelingen is dusdanig dat het veiligheidsdomein versneld moet innoveren. Innoveren in een krachtig samenspel tussen overheid, bedrijfsleven en kennisinstellingen.

1.2 Het Nieuwe Melden

De programmalijn 'Het Nieuwe Melden' komt voort uit een verkenning binnen VPVM waarin een visie is neergelegd ten aanzien van de benodigde transitie van de meldprocessen voor noodhulp. De programmalijn moet de vraag beantwoorden hoe de overheid zich aan de voorkant van het meldproces slimmer kan organiseren en beter gebruik kan maken van de kansen die nieuwe communicatievormen zoals sociale media voor het melden in het domein van de openbare orde, veiligheid en ambulancezorg. De programmalijn is daarmee relevant voor onder andere VenJ, LMO, Politie, brandweer, ambulancezorg en KMar.

De opgebouwde kennis heeft betrekking op de kansen en mogelijkheden van burgerparticipatie en sociale media voor het veiligheidsdomein maar ook technische kennis ten aanzien van bijvoorbeeld ‘voice over ip’. Voor een groot deel betreft het door VenJ gefinancierde kennisopbouw, gecomplementeerd met een EU-project (Media4sec) en een rijksbijdrageproject. In de programmalijn zal de komende jaren visievormend en experimenteel toegepast onderzoek worden gedaan naar een diversiteit van onderwerpen in het licht van bovenstaande doelsteling. Het betreft voor 2018 onderzoek naar de impact van beeld, multi-intake, nieuwe wijzen van alerteringen, de introductie van een app voor 112, de inzet van VOIP en standaardisatievraagstukken. Programmering van de programmalijn geschiedt in het daartoe bestemde ‘vierkantsoverleg’ aan de hand van een in een roadmap gedefinieerde set onderwerpen.

1.3 Opsporing 2.0

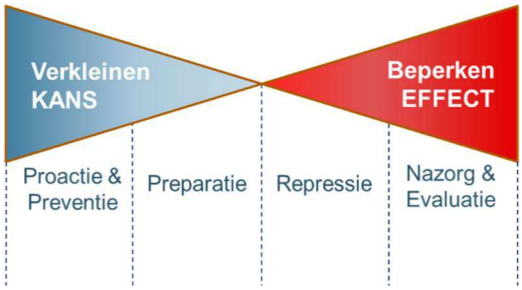


De samenleving vraagt om een politie en openbaar ministerie (OM) die burgers optimaal beschermen, hen zo nodig begrenzen en de gestelde normen bekrachtigen. Dit betekent dat op hoge snelheid op criminaliteit moet worden gereageerd (actievermogen). Daarbij moeten politie en OM tevens op maat acteren: toegespitst op aard en omvang van de criminaliteit (adaptief vermogen) met een aanpak die effectief is (lerend vermogen) en meer toegesneden is op de behoefte van burger en maatschappij. De strafrechtketen kampt met de uitdaging om oplossingspercentages en pakkans van delicten te verhogen. Daarnaast zien we dat criminaliteit verschuift én vervlecht van het fysieke domein naar en met het digitale domein. Ondermijnende criminaliteit vormt een groot en nog steeds groeiend probleem. Een verborgen omvangrijke criminele (drugs)industrie veroorzaakt maatschappelijke schade. De overheid krijgt daar nog onvoldoende grip op ondanks steeds intensievere inzet. Tegelijkertijd is er nu al een grote druk op capaciteit van recherche, OM en Rechtspraak.

Investeringen in mensen én middelen moeten de spanning tussen de huidige en gewenste situatie in de strafrechtketen verminderen. TNO wil bijdragen aan deze uitdaging door innovatieve werkwijzen en ondersteunende middelen te ontwikkelen om daarmee de effectiviteit van de strafrechtsketen te verbeteren. Voor de strafrechtketen heeft TNO zich de afgelopen jaren gericht op het ontwikkelen van geavanceerde analysemethoden om recherche te ondersteunen. Daarnaast is gedragskennis ingezet voor het beter doorgronden van criminele netwerken en het ontwikkelen van effectieve interventies op individuen daarbinnen (kopstukken, slachtoffers, informanten). Tenslotte is TNO een van de drijvende krachten op het gebied van burgeropsporing. TNO streeft ernaar om elk van deze drie pijlers in zeer nauwe samenwerking met het operationele veld (minimaal politie en OM) verder te ontwikkelen. Toetsing van methoden en vaststellen van relevantie kan alleen maar in verbinding met de praktijk gebeuren.

Voor de wat langere termijn zien we de aandacht verschuiven van opsporing sec naar dynamische criminaliteitsbeheersing vanuit een integrale benadering. Inzicht in de dynamiek en complexiteit van zowel criminele netwerken als criminele fenomenen zijn noodzakelijk om het voorspellend vermogen te kunnen vergroten en effectief pro-actiever handelen mogelijk te maken.

1.4 Nationale Veiligheid



Doelstelling van de programmalijn Nationale Veiligheid is de kennis te ontwikkelen die nodig is om Nederland te beschermen tegen bedreigingen die de maatschappij (op grote schaal) kunnen ontwrichten. Met beschermen wordt in dit verband zowel de voorkant bedoeld ─ het verkleinen van de kans op een maatschappij ontwrichtend incident ─ als de achterkant ─ het beperken van de effecten daarvan. Een incident kan een overstroming zijn als gevolg van klimaatverandering, of een terroristische aanslag op de vitale infrastructuur, of een sterk toenemende migratiestroom, of bijvoorbeeld een reeks van samenhangende incidenten die op een hybride aanval duidt. Aan de zijde van de kans kiezen we voor een all hazard benadering. Aan de effectkant ligt onze focus op het maximaal beperken van de effecten op de zogenaamde vitale processen en op het minimaliseren van menselijk leed en kosten voor herstel.

Het onderzoek ondersteunt de beleidsvorming en behoeftestelling gericht op de noodzakelijke capaciteiten binnen de gehele veiligheidsketen. Een capaciteit kan wetgeving zijn of een campagne (zelfredzaamheid), maar ook zoiets fysieks als olievoorraden of een ICT-systeem. Capaciteiten zijn niet per definitie een (centrale, regionale of lokale) overheidsverantwoordelijkheid, maar in veel gevallen ook een verantwoordelijkheid van het bedrijfsleven of van de burger. De kennisontwikkeling en -toepassing betreffen weerbaarheid van de vitale infrastructuur, de samenwerking, informatievoorziening en besluitvormingsondersteuning in samenwerkingsketens, alsmede op de weerbaarheid van de burger. Daarmee is de kennisbasis relevant voor VenJ (met name NCTV), de ministeries van Infrastructuur en Milieu en Economische Zaken, politie, gemeenten en veiligheidsregio's.

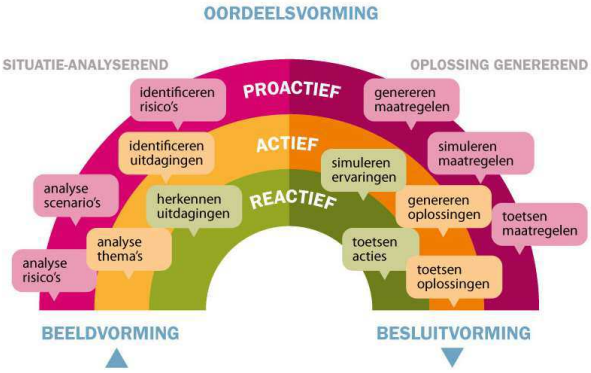
1.5 Cyber Security & Societal Resilience

De programmalijn Cyber Security & Societal Resilience heeft als doel bij te dragen aan het veilig en weerbaar maken van Nederland en richt zich op het verminderen van zowel cyberdreigingen als maatschappelijke ontwrichting door mogelijke cyberverstoringen. Cybersecurity onderzoek wordt vertaald naar voorbeelden van praktische concepten en experimentele oplossingen voor overheid en bedrijfsleven. Daarbij benaderen we de vraagstukken met een integrale aanpak, waarbij we ook de menselijke factor, de organisatie en de informatie(stromen) beschouwen. De ontwikkelde kennis is van belang voor de Ministeries van VenJ, Economische Zaken, Buitenlandse zaken, Defensie, Politie, AIVD, en via het Nationaal Cyber Security Centrum ook voor de beheerorganisaties van vitale infrastructuur. Het NCSC is voor deze programmalijn TNO's belangrijkste stakeholder. Intensieve samenwerking heeft in 2017 geresulteerd in een complementair cybersecurity onderzoeksprogramma onder VenJ-doelfinanciering.

TNO's kennisopbouw binnen VPVM heeft zich de afgelopen jaren toegespitst op monitoring en detectie van cyberdreigingen, het meetbaar maken van cyber security trends en ontwikkelingen, het versterken van ketenweerbaarheid en de response-capaciteit, verbeterde security van het Internet of Things (IoT) en de Human Factor in Cybersecurity.

Daar waar de cybersecurity kennisopbouw binnen VPVM zich kenmerkt door een maatschappelijk brede relevantie en de weerbaarheid van de vitale sectoren en de maatschappij als geheel, bouwt TNO onder het Topsectorenbeleid met en voor private partijen ook cybersecurity kennis op via het VP Cyber Risk Management & System Resilience (CRM&SR). Waar vergelijkbare onderzoeksthema's in beide programma's bestaan, wordt een nadrukkelijke keuze gemaakt in de toepassing (maatschappelijk belang of specifiek sector). In deze keuze worden ook de betrokken stakeholders geraadpleegd om synergie in de vraagsturing te creëren en zo de impact van de uitkomsten te maximaliseren.

1.6 Intelligence



Intelligence betreft het vergaren, verwerken, interpreteren en beschikbaar stellen van informatie en kennis ten behoeve van de primaire processen in het veiligheidsveld: preventie, onderschepping, handhaving en opsporing. Intelligence wordt ingezet ten behoeve van beeldvorming, oordeelsvorming en besluitvorming. Door veiligheidspartijen zoals de Nationale Politie, de NCTV, VenJ, de AIVD, de Marechaussee en particuliere bedrijven worden steeds meer data gegenereerd en verzameld. Niet alleen de hoeveelheid van de data groeit, maar ook de manier waarop deze informatie verzameld wordt verandert. Hoe kunnen deze data zo snel mogelijk omgezet worden tot de juiste intelligence, die bruikbaar is voor de ondersteuning van personen en organisatie-onderdelen in hun handelen ten behoeve van het opsporen of tegengaan van criminaliteit en terrorisme? Hoe zorgen we er voor dat intelligence optimaal aansluit bij besluitvormingsprocessen en bijdraagt aan de preventie, slag-, interventie-, heterdaadkracht?

TNO zet zich al jaren in om met nieuwe werkwijzen, technieken en inzichten de intelligenceprocessen te verbeteren, bij bovengenoemde veiligheidspartijen en voor Defensie. Drie vragen staan daarbij centraal:

- Hoe kunnen veiligheids- en opsporingsdiensten en actoren in de strafrechtketen optimaal informatie vergaren, analyseren en combineren t.b.v. intelligence en de bestrijding van criminaliteit en terrorisme?
- Hoe kan inzicht worden verkregen uit de beschikbare informatie uit vele bronnen en hoe kan deze optimaal worden aangeboden met het oog op het daadwerkelijk bereiken van meerwaarde in werkprocessen?
- Aan welk type intelligence-producten is behoefte in primaire processen en wat is er nodig om hier invulling aan te geven? Hoe kan intelligence vraag en aanbod optimaal afgestemd worden?

De programmalijn Intelligence is van waarde voor de breedte van het veiligheidsdomein: van brandweer tot politie en gemeenten. Bij de afweging of inzet van nieuwe technieken in de rede ligt, zal 'privacy by design' in de overwegingen worden betrokken.

De programmering van het Vraaggestuurd Programma als geheel is dynamisch. Gedurende een jaar kunnen zich altijd nieuwe onderwerpen aandienen. Verkenningen in de vorm van bijvoorbeeld een 'Challenge' zijn dan een geijkt middel om uit te vinden of er een toegevoegde waarde is van TNO.

2 Externe aansluiting

Het VPVM slaat de brug tussen academisch (fundamenteler) onderzoek en toepassing in de praktijk. Aan de kant van de wetenschap halen we inspiratie uit de Nationale wetenschapsagenda. Hierop sluiten TNO's Early Research Programs (ERP) en Risicovol Verkennend Onderzoek (RVO) aan. Aan de behoefte-zijde bieden de diverse decentrale en centrale kennis-, onderzoeks- en innovatieagenda's aanknopingspunten voor de programmering van het onderzoek van TNO. Ook de Strategische Kennis- en Innovatieagenda (SKIA) van Defensie is in dit kader uiteraard relevant. Het zwaartepunt van TNO's bijdrage ligt rond de gestelde 'smart' uitdaging. Van de aansluiting op de nieuwe SKIA van het ministerie van Veiligheid en Justitie[1] wordt hieronder een impressie gegeven. Met de verdere ontwikkeling van een programmatische samenwerking met de politie en andere uitvoeringsorganisaties van VenJ zullen verbindingen op specifieke onderwerpen kunnen worden gemaakt.

[1] https://www.rijksoverheid.nl/documenten/publicaties/2017/05/18/strategische-kennis-en-innovatieagenda-skia

Tabel 1: Relatie tussen uitdagingen SKIA VenJ en programmalijnen VPVM. Een donkere arcering geeft aan waar een specifieke VPVM Programmalijn grotendeels aansluit bij uitdagingen in de SKIA. Met een lichte arcering is aangegeven waar er op elementen aansluiting is.

Uitdagingen SKIA VenJ \ Programmalijnen VPVM	Terrorisme-bestrijding	Het Nieuwe Melden	Opsporing 2.0	Nationale Veiligheid	Cyber Security & Societal Resilience	Intelligence
De 'justice' uitdaging						
De 'governance' uitdaging						
De 'smart' uitdaging						
Weerbaarheid en veerkracht						
Globalisering als uitdaging						

3 Ontwikkeling

De ontwikkeling van het VP is gericht op programmatische samenwerking. Het is de ambitie van TNO om met het VPVM maximale toegevoegde waarde te hebben voor het ministerie van Veiligheid en Justitie en de daaronder ressorterende (veiligheids)organisaties, waaronder de Nationale Politie. Dat vraagt focus en massa op díe onderwerpen die voor het veiligheids- en justitiedomein het belangrijkste zijn. Door programmatisch samen te werken bereiken we die focus en massa en zijn we in staat om goed te prioriteren.

De onderwerpen voor kennisopbouw en -toepassing benaderen we met 'programmalijnen'. Daarmee wordt een bundeling beoogd van samenhangende onderzoeksprojecten met een passend begeleidings- en vraagsturingsmodel.

Binnen elke programmalijn is het streven naar een mix van korte- en lange termijn-onderzoek passend bij de verschillende niveaus van toepasbaarheid van een onderwerp: VPVM-projecten vanuit rijksbijdrage TNO, VenJ-doelfinancierings-projecten, projecten vanuit Europese fondsen en projecten met bijdragen van veiligheidsorganisaties ('klantprojecten'). Naarmate de directe toepasbaarheid hoger wordt zal de samenwerking met een of meerdere organisaties ook intensiever worden. Met deze mix wordt continue kennisvernieuwing gestimuleerd, en wordt toegewerkt naar toepassing in de praktijk.

Veel van de uitdagingen waar TNO zich op richt vragen om een keten-brede benadering, waarbij met verschillende ketenpartners van bijvoorbeeld de Rechtshandhavingsketen wordt samengewerkt. Dit uitgangspunt vertaalt zich ook in de bemensing van de begeleidingsgroep van de programmalijnen.

Een goed voorbeeld van dergelijke programmatische samenwerking is de programmalijn Het Nieuwe Melden. Deze programmalijn is ontstaan als onderzoeksproject met rijksbijdrage, en is later gecomplementeerd met een Europees project (Media4sec) en met projecten met VenJ-doelfinanciering. De programmabegeleiding vindt plaats in een zogenaamd 'vierkantsoverleg' met vertegenwoordigers van VenJ en LMO/politie. Ook rond de publieke onderzoeksactiviteiten met betrekking tot Cyber security is met het Nationaal Cyber Security Centrum een dergelijke programmalijn ontwikkeld.

4 Activiteitenplan 2018

De activiteiten en de onderzoeksvragen van het onderzoeksprogramma worden nader met de stakeholders afgestemd. Naast het opleveren van kennisdocumenten streeft TNO ook nadrukkelijk naar het opleveren van demonstrators en proof-of-concepts, inclusief een toetsing in de praktijk. Hieronder is een selectie van activiteiten per programmalijn kort beschreven.

4.1 Terrorismebestrijding

- *Radicalisering:* Vertalen van kennis en modellen tot early warning en beslisondersteuning voor interventies.
- *CBRNE:* In kaart brengen van mogelijke interventies in de gehele tijdlijn van contraterrorisme.
- *Risicogestuurd Optreden:* Toepassen van kennis over risicogestuurd optreden in het veiligheidsdomein en vertalen naar nieuwe werkwijzen.
- *Migratie- en asielketen:* Uitvoeren van een verkenning rond het asiel- en migratieproces gericht op het identificeren van personen met extremistische en potentieel gewelddadige intenties.

Bij de onderzoeksactiviteiten rond terrorismebestrijding wordt samengewerkt met VenJ, NFI, DEC-CIED, KMar en Schiphol.

4.2 Het Nieuwe Melden

- *Impact van beeld:* Experimenteren om (na de visie en roadmap in 2017) te onderzoeken hoe beeld (video en foto) in het meldproces benut kan worden.
- *Realisatie 112 app:* Bijdragen aan de specificaties (met blik op EU/standaardisatie), visie en roadmap voor localisatie en 112 app, en beproeven van de app.
- *112 VOIP beleid:* In kaart brengen van de impact op 112 van zogenaamde 'Over The Top'-diensten als Skype.
- *Beleid alerteringen:* Opstellen van een toekomstvisie en roadmap voor het ontwikkelen van beleid met betrekking tot de familie van alerteringen (o.a. NL Alert, burgernet, amber alert, WAS).

- *Het Nieuwe Melden Pop-Up Lab*: Leren en experimenteren samen met stakeholders op diverse locaties in het land.

In de programmalijn wordt samengewerkt met projecten op het gebied van het Nieuwe Melden van de Landelijke MeldkamerOrganisatie (LMO). Informatie wordt uitgewisseld met EU-projecten, ook projecten waarin TNO niet actief participeert). Samenwerking met private partijen is voorzien waar het aanvullende expertise en faciliteiten betreft, bijvoorbeeld binnen de context van de HSD (Hague Security Delta). Ook interacties met andere projecten binnen VPVM worden nagestreefd, met name die binnen Intelligence zoals het RTI Lab en het BART-project (met TU Delft, CGI als partners naast TNO). Tenslotte krijgt samenwerking met diverse universiteiten gestalte middels onder andere het hoogleraarschap van José Kerstholt (expertise burgerparticipatie - Universiteit Twente).

4.3 Opsporing 2.0

- *Big Data:* Experimenteren met en deels ontwikkelen van Big Data analysetools (afkomstig van o.a. EU en ander onderzoek) en toepassingen van kunstmatige intelligentie.
- *Psycho-sociale modellering:* Ten behoeve van risicoanalyses voor persoons-gebonden benaderingen.
- *Burgeropsporing:* Ontwikkelen van een visie en instrumenten voor het structureel samenwerken met burgers bij de opsporing.
- *Dynamische CriminaliteitsBeheersing:* Ontwikkelen van modellen voor criminaliteitsbeheersing op basis van gedragskennis en kennis over complexiteit.

In de programmalijn wordt samengewerkt met de Politieacademie, de Taskforce Ondermijning (Openbaar Ministerie, politie, gemeenten), het programma Herijking Opsporing, DGPOL, DGRR; NSCR, UvA Institute of Advances Studies, RIECs en de Veiligheidshuizen.

4.4 Nationale Veiligheid

- *Nationaal Veiligheidsprofiel:* Verdiepen (cyber, vitale infrastructuur) zowel als verbreden (hybride dreigingen) van de kennisbasis.
- *Weerbaarheid vitale infrastructuur:* Ontwikkelen van methodes om inzicht te krijgen in de weerbaarheid op netwerkniveau van meerdere samenhangende vitale processen.
- *(Simulatie)tools beslisondersteuning:* Ontwikkelen van een ‘test-bed’ voor modellen van risico’s voor vitale infrastructuren en voorspellende modellen voor keteneffecten.

TNO is sterk verankerd in het netwerk van Nationale Veiligheid, onder andere als kernorganisatie van het Analistennetwerk Nationale Veiligheid (TNO, RIVM, AIVD, WODC, Clingendael en de Erasmus Universiteit). Rond Vitale infrastructuur-bescherming werken we samen met NCTV en de Commissie Vitale Infrastructuur van VNO-NCW binnen en buiten het project VitAp, alsmede met de vitale infra-structuurbeheerders. Andere samenwerkingen lopen met Fraunhofer, ENEA en CEA.

4.5 Cyber Security & Societal Resilience

- *Security and resilience concepts:* Ontwikkelen van een besturingsconcept van Critical Information Infrastructure (CII).
- *Security, Monitoring & Detection*: Ontwikkelen van een visie op Threat Hunting Support (werkwijze en tooling), en toetsen aan de praktijk.
- *Automated Security:* Ontwikkelen van (deels) geautomatiseerde Security Decision Support, gebruikmakend van de Cyber Threat Intelligence omgeving.
- *Secure Behaviour*: Ontwikkelen en testen van gedragsinterventies ten behoeve van veilig internetgebruik.
- *Cyber Forecasting Tournament*: Uitvoeren van een Cyber Forecasting competitie.

Voor het Cyberonderzoek wordt nauw samengewerkt met het NCSC. Dit helpt TNO bij het vinden van de juiste vitale infrastructuurbeheerders die meehelpen en/of meedenken bij de uitvoering van het cybersecurity onderzoek en de toetsing in praktische situaties. Daarnaast wordt samengewerkt met OM en politie rond Cyber Threat Intelligence en met de TUDelft rond Dark Web. Internationaal is sprake van samenwerking in H2020-projecten en met het Global Forum on Cyber Expertise, met Singapore (Dark Web onderzoek en IoT security) en Aruba (Publiek-Private Samenwerking en cyber security strategieontwikkeling). Tenslotte is er afstemming met lopend Defensie-onderzoek (programma V1622) op aanpalende cyber operations onderwerpen.

4.6 Intelligence

- *Sensing:* Onderzoeken van rijpheid en toegevoegde waarde van nieuwe sensing-technologieën als Wide Area Motion Imagery.
- *Satellietoepassingen:* Ontwikkelen van kennis van technologie/technieken/ middelen in relatie tot satellieten waarmee veiligheidstaken als monitoren, opsporen en vervolgen beter, efficiënter en sneller zijn uit te voeren.
- *Real Time Intelligence:* Doorontwikkelen van het RTI-lab, ontwikkelen en uitvoeren van diverse experimenten.
- *Prescriptive Policing:* Onderzoeken van de haalbaarheid van prescriptive policing via prototypes en experimenten, in samenwerking met de politie.
- *Informatiedeling en informatiefusie:* Onderzoeken van haalbaarheid en toegevoegde waarde van nieuwe technologieën als homomorfe encryptie.

Voor de kennisontwikkeling wordt samengewerkt met diverse universiteiten zoals de TUDelft en de Universiteit van Amsterdam, evenals met Europese onderzoeks-partners. Voor kennistoepassing is sprake van samenwerking met innovatieclusters zoals the Hague Security Delta en natuurlijk met de diverse Veiligheidspartners. Rond Amsterdam ArenA wordt gewerkt aan de opzet van een experimenteer-programma met diverse partijen, waaronder politie, gemeente en de verschillende podia en stadions. In deze context kunnen vraagstukken als publiek-private samenwerking rond gebiedsbeveiliging worden onderzocht.

4.7 Voorstel bij aanvullende overheidsfinanciering

Tijdens het opstellen van dit meerjarenplan 2018-2021 was er nog geen duidelijkheid over eventueel nieuw onderzoek- en innovatiebeleid van het nieuwe kabinet. Als er binnen dit beleid ruimte is voor additionele financiering voor toegepast onderzoek, ziet TNO kansen om de kennisontwikkeling zoals beschreven in dit rapport te versnellen en te intensiveren (bijvoorbeeld, maar zeker niet uitsluitend, waar het de bestrijding van cybercrime en terrorisme betreft).

In het TNO Strategisch Plan 2018-2021 “Vliegwiel voor innovatie in Nederland” wordt beschreven hoe de gekozen domeinen, speerpunten en technologische vernieuwing aansluiten bij c.q. bijdragen aan de externe uitdagingen en agenda’s: ‘Sustainable Development Goals’ van de VN, ‘Grand Societal Challenges’, ‘Key Enabling Technologies’ en ‘Leadership in Enabling Industrial Technologies’ van de EU, de Nationale Wetenschapsagenda, en agenda’s/roadmaps van Ministeries en Topsectoren. Voor VPVM zijn in het bijzonder de Secure Societies challenge van de EU en de Strategische Kennis- en Innovatieagenda van VenJ van groot belang. Van de recent geformuleerde Maatschappelijke Uitdagingen (MU) en Sleuteltechnologieën (ST) ligt met name de MU Veilige Samenleving in het hart van dit VPVM.

Indien het nieuwe kabinet in de komende jaren additionele financiële ruimte creëert voor het toegepast onderzoek, zal TNO het programma actualiseren en aangeven welke onderwerpen, met inachtneming van de aanwijzingen van de overheid, zullen worden versterkt.

5 Ondertekening

Den Haag, September 2017

Ir. C.H. van den Berg
VP Manager
Veilige Maatschappij

Drs. H.G. Geveke
Directeur
TNO Defensie & Veiligheid