Meerjarenprogramma 2015-2018

Thema Maatschappelijke Veiligheid

Voortgangsrapportage 2016

Algemene gegevens	
Titel	Veilige Maatschappij
~~ERP/Topsector/~~Maatschappelijk Thema	Maatschappelijke Veiligheid
TNO referent, programmaleider	Ir. H.F. Bousché, Ir. C.H. van den Berg
Contactpersoon overheid (eventueel)	Mr. H. Hanoeman/ ministerie VenJ

1. Samenvatting

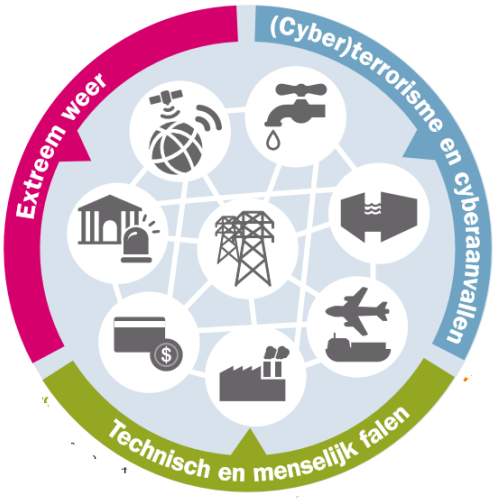
Om publieke veiligheidsorganisaties in de Nederlandse maatschappij op hun taken berekend te houden en om te beantwoorden aan de veiligheidsbehoeften van bedrijven en burgers doet TNO onderzoek in het Vraaggestuurd Programma Veilige Maatschappij. In 2016 is gewerkt aan de intensivering van de samenwerking met het regievoerend ministerie van Veiligheid en Justitie (VenJ)[1] en de publieke operationele veiligheidsorganisaties. Voor 2016 zijn de volgende onderwerpen als zwaartepunten gekozen: Informatievoorziening, Real Time Intelligence, Procesinnovatie en Cybersecurity & Societal Resilience.

De samenwerking tussen TNO, de NCTV en DG Politie van VenJ in concrete samenwerkingsprojecten en programma's is de afgelopen jaren gegroeid. Voor de DG's Rechtspleging en Rechtshandhaving (DGRR), DG Straffen en Beschermen (DGSB) en DG Vreemdelingenzaken (DGVZ) is in 2016 een aantal verkennende studies naar de meerwaarde van door TNO (te ontwikkelen) expertise uitgevoerd. Met name voor bestrijding van on-line-criminaliteit en risicogestuurd optreden bij de beveiliging van onze grenzen zijn concrete initiatieven voor vervolg opgezet. Voor 2017 voorzien we dat de samenwerking een *programmatisch* karakter krijgt. Daartoe zullen *programmalijnen* worden gevormd rond relevante onderwerpen.

Op basis van de opgebouwde kennis heeft TNO in samenwerking met haar stakeholders in het veiligheidsdomein internationaal erkende posities opgebouwd voor de volgende onderwerpen:

Resilience van de vitale infrastructuur

- In meerdere Europese projecten is TNO de coördinerende partij om modellen en analysemethoden te ontwikkelen voor het vergroten van de resilience van de vitale infrastructuur en bovendien het voorbereid zijn op benodigde respons bij onverwachte calamiteiten te versterken. Bijzondere aandacht krijgen daarbij de zgn. All Hazard Approach (figuur 1), intersectorale afhankelijkheden en ketenweerbaarheid.
- In 2016 is ook nieuwe kennis opgebouwd voor het vroegtijdig inspelen op het risico van extreem weer.
- Met de ontwikkelde basiskennis wordt o.a. het ministerie van VenJ ondersteund in het VitAp-project dat bijdraagt aan het behouden van de weerbaarheid van vitale infrastructuren. Het project levert daartoe procesbeschrijvingen en instrumenten en versterkt publiek-private samenwerkingen. Dit alles in het licht van de dreiging van het ontstaan van grootschalige maatschappelijke ontwrichting als gevolg van bijvoorbeeld extreem weer.



Figuur 1: All Hazard Approach

[1] In 2016 heeft VenJ gewerkt aan de totstandkoming van een Strategische Kennis en Innovatie Agenda. Op Kennis en Innovatiegebied wordt de samenwerking met Politie en Defensie (verder) geïntensiveerd. VenJ en daaraan gerelateerde uitvoeringsorganisaties, waaronder de Politie, werken nadrukkelijker aan de strategische samenwerking met kennisinstellingen.

Crisisbeheersing

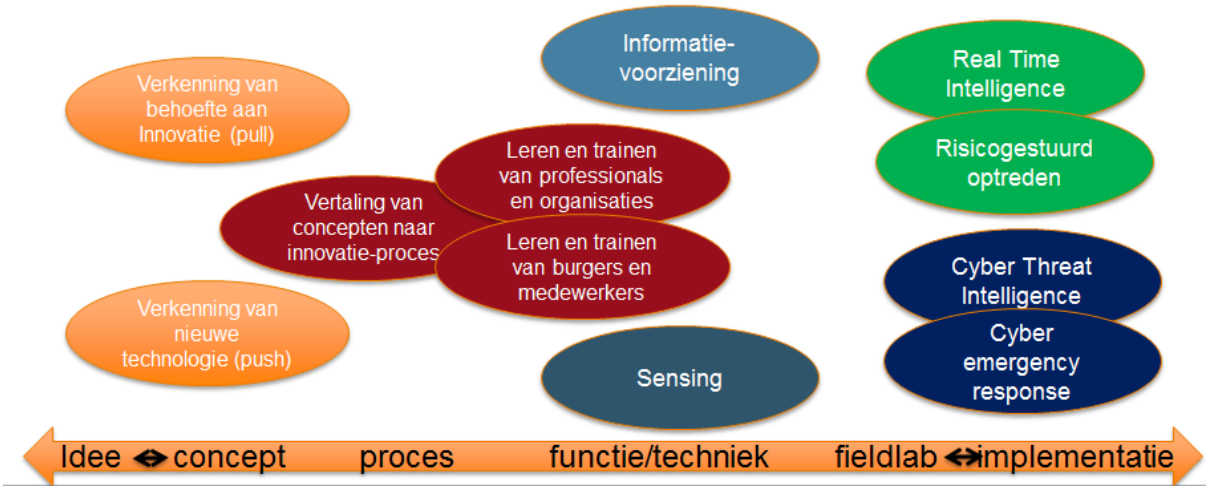
- Bij grote crises en rampen zijn vele overheden, operationele veiligheidsorganisaties, bedrijven en burgers betrokken. Voor informatie-gestuurde operationele activiteiten is de informatievoorziening en de besluitvorming van groot belang voor efficiency en slagkracht; daarnaast is de communicatie tussen betrokken instanties en naar het publiek cruciaal. TNO leidt verschillende ontwikkelingstrajecten van nieuwe crisisbeheersingstools en de standaardisatie en harmonisatie van benaderingen voor multidisciplinaire samenwerking. In 2016 is ingespeeld op nieuwe uitdagingen: het opvangen van vluchtelingen en adequaat grensmanagement.

Intelligence voor bestrijding van criminaliteit en terrorisme

- In een complexe wereld met veel actoren en steeds meer informatie is het essentieel tot inzichten en onderbouwde keuzes te komen door met nieuwe tools en methoden zo veel mogelijk automatisch ondersteund informatie te selecteren, te interpreteren en te combineren tot intelligence. Dit biedt de basis voor proactief optreden, snelle intercepties en effectieve opsporing. In 2016 is bijzondere aandacht gegeven aan nieuwe misdaadvormen in de digitale ruimte en automatische interpretatie van fysiek en digitaal gedrag.

2. Korte Omschrijving

De kern van Vraaggestuurd Programma Veilige Maatschappij (VPVM) betreft ontwikkeling van basiskennis voor innovatie van processen en functies/technieken, zoals gevisualiseerd in de middelste categorieën in figuur 2 hieronder.



Figuur 2: Karakterisering van verschillende onderdelen VPVM

De focus ligt op ontwikkelingen voor de publieke veiligheidstaken waarbij vele organisaties en stakeholders betrokken zijn. De volgende onderzoeksprojecten staan centraal:

- *Informatievoorziening:* selectief verzamelen en benutten van 'big data'.
- *Procesinnovatie:* ontwikkelen van competenties van organisaties, professionals en burgers voor multi-stakeholdersamenwerking met ad hoc partners voor actuele problematieken.
- *Real-Time Intelligence:* werkwijzen en technologieën om relevante kennis en informatie snel in bruikbare vorm aan te bieden aan veiligheidsprofessionals.
- *Cybersecurity & Societal Resilience:* door nieuwe data-analyseprocessen en data-sensing grip krijgen op cyberrisico's in vitale infrastructuren en procesketens.
- *Sensing en systemen voor security:* methodieken voor koppelen van waarnemingen uit vele bronnen in de tijd en in de relevante geografische dimensie (NB gezien de meerwaarde van samenwerking in de driehoek bedrijven-publieke veiligheidsorganisaties- kennisinstellingen wordt dit project uitgevoerd onder regie van de topsector HTSM).

Voor de voortdurende vernieuwing in de ontwikkeling van basiskennis worden in het VPVM elk jaar een aantal verkenningen uitgevoerd om voor nieuwe behoeften van het veiligheidsveld en nieuwe ideeën en concepten te ontwikkelen (links in bovenstaand schema). Hierbij is aansluiting bij de beleidsontwikkeling binnen betrokken overheden een noodzakelijke voorwaarde.

Implementatie van ontwikkelde basiskennis met betrekking tot *proces* en *functies/techniek* is complex en afhankelijk van praktijkcondities: versnelling van toepassing door experimenten in (gesimuleerde) praktijkomgevingen/fieldlabs vindt plaats in gezamenlijke ontwikkelingsprogramma's met de operationele veiligheidsorganisaties (rechts in bovenstaand schema).

3. Highlights

3.1 Informatievoorziening

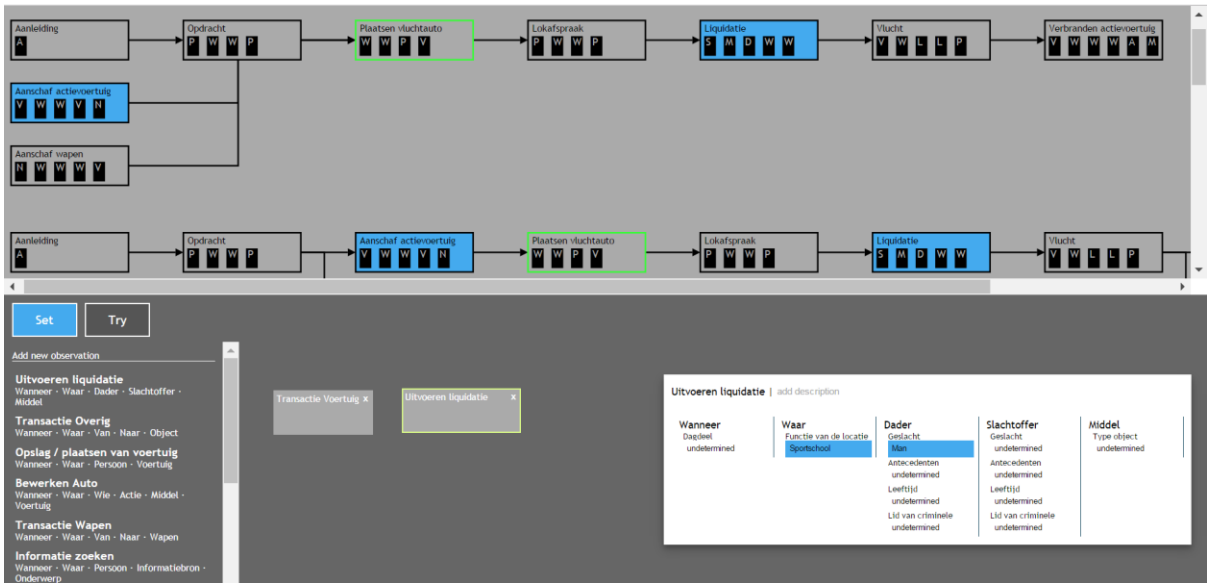
Methodiek voor spotten van online illegale transacties

Nederland is een hub in de internationale online drugshandel. Dit betreft een miljardenmarkt die sinds 2011 is ontstaan. Voor het inzicht krijgen in online illegale transacties en de aard en de omvang van illegale online handel op het dark web zijn nieuwe technologieën ontwikkeld, gericht op het verzamelen van gestructureerde en ongestructureerde data op het dark web. Vervolgens is het door toepassing van nieuwe analyse-methodieken gelukt individuele illegale transacties op te sporen. We zijn met deze kennis nu in staat om een beeld te krijgen van de aard en omvang van illegale online handel op het dark web. De resultaten zijn goed ontvangen door de Nationale Politie, de Landelijke Recherche, de NCTV, EUROPOL en Interpol.

Tooling voor het criminele opsporingsproces

Voor het criminele opsporingsproces komt steeds meer data uit meerdere informatiebronnen beschikbaar. Om optimaal gebruik daarvan te maken is een nieuwe benadering in ontwikkeling: 'crimescripting'. De essentie is dat een misdaad wordt gemodelleerd als een filmscenario met scenes en rollen; door expertkennis en historische data in een informatiebase toegankelijk te maken kan de kan de taak van informatie-analisten behapbaar worden gemaakt. TNO heeft QUIN als

ondersteunende tooling ontwikkeld voor het proces van ‘crimescripting’ en het toetsen van concurrerende hypothesen middels algoritmen in een intuïtieve gebruikersinterface. Zowel operationele begeleiders uit de eenheid Amsterdam van de Nationale Politie als de Politieacademie zijn enthousiast om hier vervolg aan te geven; ook NCTV, DGPOL en DGRR zijn hierbij betrokken.



Figuur 3: De QUIN interface toont bovenin de mogelijke scenario’s, en onderin een ruimte om bewijzen toe te voegen. De groen gehighlighte scenes wijzen de analisten op logische vervolgvragen

Het Nieuwe Melden

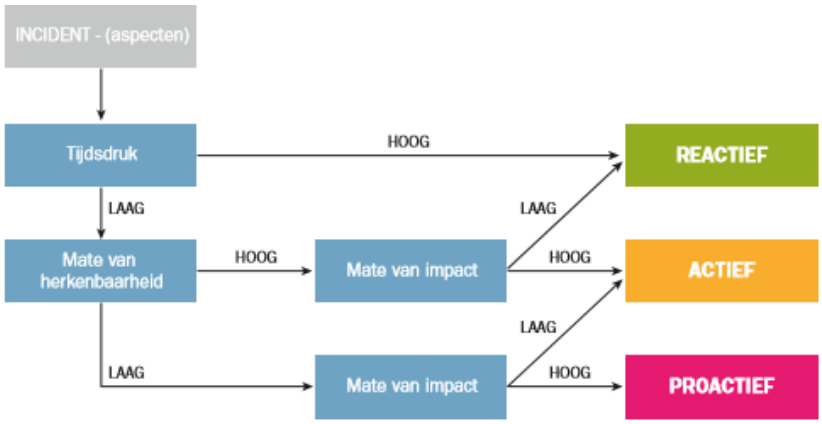
Figuur 4: Publicatie 'Wie belt er nog?'

In het VP Veilige Maatschappij is de basis gelegd voor het ontwikkelen van een visie en roadmap voor “Het Nieuwe Melden” (figuur 4). Als kernvraag is genomen: het slimmer organiseren en benutten van de capaciteiten en informatie van burgers en bedrijven voor het adequaat inspelen op veiligheidsincidenten. In 2016 is gefocust op de haalbaarheid van een 112 app in het meldkamerdomein. Daarbij speelt de noodzaak processen en organisaties te veranderen om samenwerking van burgers en professionals en mogelijk ook andere bedrijven te faciliteren. Het TNO-rapport heeft veel aandacht gekregen. Zo heeft de minister VenJ in een Algemeen Overleg met de Tweede Kamer in november een vervolg hierop aangekondigd.

3.2 Procesinnovatie voor risico- en crisismanagement

Besluitvorming in crisissituaties is complex. In de praktijk van crisismanagement blijkt bijvoorbeeld de uitwisseling van informatie een uitdaging, net als het gezamenlijk komen tot een oordeel en een besluit. Ook de coördinatie tussen verschillende organisaties - vaak met tegengestelde belangen -is vraagt om structurele versterking. Daarbij gaat het om versnelling en effectiviteit van het drie-fase-proces Beeldvorming-Oordeelsvorming-Besluitvorming (het BOB-proces) en dan met name om de laatste twee fasen. In 2016 hebben de ontwikkelde inzichten geleid tot de publicatie van een model voor oordeelsvorming met als essentiële onderdelen:

1. Het snel kunnen selecteren van de optimale modus voor oordeelsvorming: reactief, actief of proactief (zie figuur 5 hieronder)



Figuur 5: Schematische weergave van de optimale modus voor oordeelsvorming

2. Het binnen de gekozen modus van oordeelsvorming kunnen focussen op de prioriteiten wat betreft situatieanalyse en oplossing. Zie figuur 6 hieronder:

Figuur 6: Oordeelsvorming, beeldvorming en besluitvorming

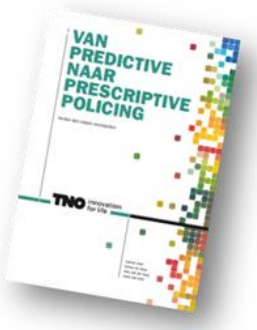
Naast de ontwikkelde kennis over oordeelsvorming is ook onderzoek gedaan naar versterking van de interactie van veiligheidsprofessionals en burgers. De resultaten worden ingebracht in onder andere:

- Een initiatief voor versterking van lokale veerkracht voor de opvang van vluchtelingen op gemeentelijk niveau. Bij de ontwikkeling van een gezamenlijke aanpak door co-creatie zijn o.a. betrokken COA, het Rode Kruis, de Veiligheidsregio's, DG Vreemdelingen Zaken en de VNG.
- Een initiatief voor verbetering van de risicobeheersing bij evenementen in samenwerking met Politie Haaglanden, veiligheidsregio's en ketenpartners.
- Een initiatief voor versterken van de weerbaarheid van de vitale infrastructuur met behulp van tools voor de analyse van gezamenlijke kwetsbaarheden en weerbaarheidsindicatoren op netwerk/ ketenniveau. Hierin participeren NCTV en vertegenwoordigers van vitale sectoren.

3.3 Real Time Intelligence

Bij tal van publieke veiligheidstaken wordt de effectiviteit van het operationele optreden in belangrijke mate bepaald door het beschikbaar hebben van de juiste informatie op de juiste plaats en op het juiste moment. Dat betekent concreet bijvoorbeeld dat bij een overval de meest waarschijnlijke vluchtroutes zijn afgezet en dat surveillerende politiemensen de bruikbare intelligence over bijvoorbeeld een jeugdgroep in de buurt op het juiste moment krijgen aangeleverd, zodat ze optimaal kunnen handhaven.

In samenwerking met de politie en 'the Hague Security Delta' (HSD) heeft TNO het Real Time Intelligence lab opgezet. Het initiatief staat voor een experimenteeromgeving en thematisch netwerk waar bedrijfsleven, wetenschap, veiligheidspartners en maatschappelijke organisaties deel van uitmaken (een zogenaamd 'Thematisch Quadruple Helix netwerk'). Het samenwerkingsverband wordt stap-voor-stap opgebouwd tot een in de praktijk verankerd gremium dat waarde toevoegt doordat daar eenvoudig en eenduidig de waarde van nieuwe producten, diensten of concepten op het gebied van RTI kan worden aangetoond. In 2016 zijn experimenten uitgevoerd voor een Staf Grootschalig en Bijzonder Optreden (SGBO) in Den Haag en voor een vervolg op het project Burger Alert Real Time (BART!).

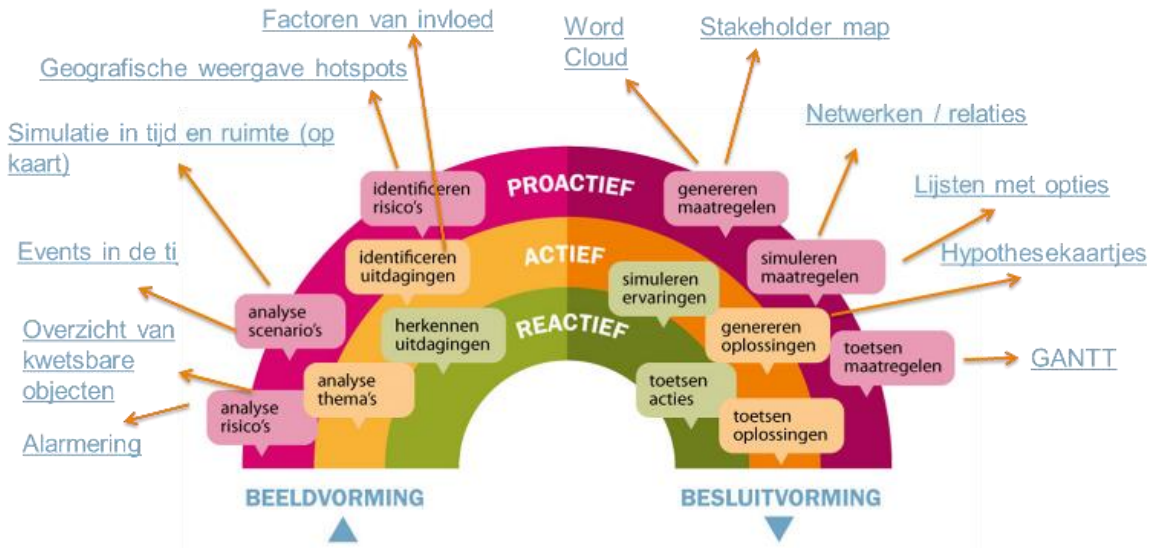


Figuur 7: Publicatie 'van Predictive naar Presecriptive Policing'

Voor het kunnen voorspellen van de plaats en de tijd van veelvoorkomende criminaliteit zijn methoden ontwikkeld met gebruikmaking van machine learning op basis van historische data. Uitdaging daarbij is het vertalen van voorspellingen naar adviezen voor effectieve interventies (bijvoorbeeld zichtbare patrouilles). Op 26 april 2016 is aan de Secretaris Generaal van het Ministerie VenJ een boekje aangeboden met een beschrijving van een voorspellend effectmodel van interventies (figuur 7).

Voor snelle vooruitgang op dit gebied is er behoefte aan het intensiever vastleggen van interventies in de praktijk en de daarmee bereikte effecten op de frequentie van incidenten. Ook kenmerken van de omgeving (zoals uitvalswegen) en sociaal-demografische factoren zijn van belang.

In 2016 is een analyse uitgevoerd van de taken van de (wijk)agent, hoofdagent, brigadier, centralist en functionaris in de Real Time Intelligence Centres van de politie. Dit heeft geresulteerd in een *framework* voor 'intelligence modules'. Ook is verkend hoe dit soort modules vorm gegeven kan worden en welke toegevoegde waarde te verwachten is voor specifieke activiteiten binnen de *BOB-cyclus (beeldvorming, oordeelsvorming en besluitvorming)*. Een conceptuele uitwerking ziet er als volgt uit (figuur 8):



Figuur 8: Verschijningsvormen van Intelligence modules aan de hand van de BOB-cyclus

Een eerste visie op een realisatieplan en systeemarchitectuur is ontwikkeld na een aantal interviews bij bedrijven en politie (IV-organisatie). Eind 2016 / begin 2017 worden acties uitgevoerd om de opgebouwde inzichten te verspreiden en het breder benutten van binnen veiligheidsorganisaties al gebruikte instrumenten *voor specifieke toepassingen* te initiëren. De roep om méér voorspellende modellen die richting kunnen geven aan interventies voor méér gebruikssituaties is sterk bij m.n. politie en in het meldkamerdomein. Met de komst van Cloud-based en Big Data infrastructuren ontstaan nieuwe mogelijkheden: meer dynamisch brongebruik wordt mogelijk, meer data is beschikbaar en complexe databewerkingsacties worden gemakkelijker. Dit gaat mogelijk maken dat intelligence modules (op basis van *generieke bouwstenen*) gemakkelijker te realiseren zijn voor diverse gebruikersdoeleinden en op diverse elektronische apparaten (devices).

3.4 Cyber Security & Societal Resilience

Cyber Trend Watch

Voor de ontwikkeling van strategisch beleid en operationele krachtenbundeling bij de bestrijding van cyber incidenten zijn specifieke cyber security metrieken met breed bruikbare indicatoren nodig. Dit is essentieel voor het kunnen produceren van een zgn. Cyber Trend Watch met in het verlengde een meer operationeel Cyber Intelligence Platform. Door de realisatie van het Cyber Threat Intelligence (CTI)-Lab is een goede kennisbasis gevormd van de tools, protocollen en concepten die gebruikt kunnen worden door verschillende disciplines binnen een SOC, CERT en/of CTI-omgeving. De CTI-lab omgeving is een goede basis voor vervolgonderzoek op cybersecurity metrieken, analyses en visualisaties van gecombineerde data. De binnen het onderzoek gerealiseerde dashboards laten zien dat het met goede brondata mogelijk is om het aandeel van Nederland in bepaalde typen dreigingen te meten. Dit biedt mogelijkheden voor de doorontwikkeling richting sectorale dreigingsbeelden. Het ontwikkelde *kwetsbaarhedendashboard* biedt interessante mogelijkheden als operationele tool binnen het CERT werkveld.

Cyber Resilience City Scan

Cyber is een onderwerp dat steeds nadrukkelijker op de agenda van steden komt te staan, maar het is tegelijkertijd een onderwerp dat voor een stad moeilijk grijpbaar is. TNO heeft zich als kennispartner van het 100 Resilient Cities-network van de Rockefeller Foundation ingezet om de Cyber Resilience City Scan te ontwikkelen (figuur 9). Hiermee worden steden geholpen om inzicht te krijgen in wat cyber security en resilience betekent in hun context, en het biedt aanknopingspunten voor het definiëren van actiepunten voor het versterken van de digitale weerbaarheid van de stad.

Figuur 9: Cyber Resilience City Scan

3.5 Verkenningen voor DG's RR, VZ en SenB

In het eerste kwartaal van 2016 is een verkenning uitgevoerd naar de meerwaarde van TNO-expertise in vraagstukken van de drie Directoraten-Generaal (DG) Rechtspleging en Rechtshandhaving (DGRR), DG Straffen en Beschermen (DGSB) en DG Vreemdelingenzaken (DGVZ) . De verkenning heeft geresulteerd in de selectie van een viertal verkennende projecten, die medio 2016 zijn gestart en in december zijn gerapporteerd:

- Integrale Ketensturing met een casus van DGVZ,
- Risicogestuurd Optreden in het Veiligheidsdomein met een casus van DGVZ en de Koninklijke Marechaussee (KMar),
- Sharing Analysis not Data met casus van DGSB
- Strategie voor bestrijding Online Criminaliteit met een casus van het Openbaar Ministerie en politie.

Op basis van de rapportages van de vier verkenningen zal er in 2017 vervolg worden opgezet voor drie van deze onderwerpen:

- Risicogestuurd optreden in het veiligheidsdomein: in een publicatie (begin 2017) zal worden ingegaan op het denkkader en de randvoorwaarden voor risicogestuurd optreden en de roadmap voor vervolg. Zowel de KMar als DGVZ hebben aangegeven door te willen gaan met dit onderwerp. De H2020 call van komende zomer biedt daar ook extra kansen voor.
- Voor de verkenning Sharing Analysis not Data is belangstelling geuit door DGSenB en DGRR. Onderzocht wordt hoe dit een vervolg kan krijgen, gezien ook de prioriteit voor informatiedeling tussen partijen op de Strategische Kennis- en InnovatieAgenda van het ministerie van VenJ.
- Strategie voor bestrijding Online Criminaliteit: De resultaten van de Challenge sluiten goed aan bij de nog in te voeren nieuwe wetgeving (Computercriminaliteit III) en de oprichting van cybercrimeteams bij alle politie-eenheden. Het 'Cyber Threat Intelligence lab' van TNO in samenwerking met publieke en private partijen biedt perspectief op verbetering van de informatiepositie rond aankomende cyberdreigingen.

4. Actualisatie /dynamiek

Het plan 2015-2018 gaat uit van de uitvoering van een portfolio strategische kennisvernieuwings-projecten met betrokkenheid van de operationele veiligheidsorganisaties om de implementeerbaarheid van de ontwikkelde kennis te borgen. De relaties met de nationale politie, de KMar en de veiligheidsregio's zijn in dat kader uitgebouwd. De ambitie om TNO-kennis ook in te zetten bij beleidsontwikkeling was echter nog niet geconcretiseerd. In 2016 is door het ontwikkelen van een co-creatie-proces voor het opvangen van vluchtelingen met de landelijke beleidsgremia nauwe interactie ontstaan. Ook het bestrijding van online criminaliteit en het ontwikkelen van een cyber trend watch demonstrator leidde tot intensieve belangstelling tot op het hoogste beleidsniveau met bezoeken van minister Van der Steur en premier Rutte aan door TNO gedragen initiatieven.

In 2016 is de samenwerking met het ministerie VenJ geïntensiveerd. Samen met het Innovatieteam van het ministerie VenJ streven we naar een intensievere verankering van innovatietrajecten in het beleid van het ministerie. In een interactief Symposium "Van kennis naar Innovatie voor Veiligheid en Justitie" op 20 mei 2016 zijn door de ruim 200 aanwezigen uit het publieke veiligheidsdomein vragen en nieuwe ideeën voor onderzoek ingebracht. TNO-directeur van het Thema Defensie en Veiligheid de heer Henk Geveke benadrukte dat zijn organisatie direct bij VenJ aan de bel trekt als het nieuwe ontwikkelingen signaleert in wetenschap en technologie die voor het ministerie van belang kunnen zijn. Omgekeerd zullen zich bij Veiligheid en Justitie steeds nieuwe vragen aandienen waar TNO een antwoord op kan geven. Dat is wat hem betreft de kern van de samenwerking: elkaar doorlopend informeren en stimuleren nieuwe uitdagingen op te pakken. Ook voor de Secretaris Generaal van VenJ de heer Siebe Riedstra stond vast dat samenwerking met kennisinstituten, universiteiten en het bedrijfsleven, de sleutel is tot innovaties binnen het veiligheidsdomein. "Zo zijn we gezamenlijk in staat oplossingen te ontwikkelen die voor ons praktisch bruikbaar zijn".

Als vervolg op het symposium op 20 mei is onder regie van het Innovatieteam VenJ en de TNO roadmap National Security de programmatische samenwerking tussen het ministerie van Veiligheid en Justitie en de daaraan gerelateerde uitvoeringsorganisaties, waaronder de Nationale Politie, ingericht. Daartoe is samen met diverse organisatieonderdelen de kennisbehoefte geïnventariseerd. Die kennisbehoeften zijn en worden vertaald naar onderzoeksplannen die een plaats krijgen in zogenaamde programmalijnen. Het onderzoek in die programmalijnen wordt gefinancierd uit het VPVM (SMO), alsmede uit lopende en nog te verwerven H2020 (en andere) fondsen als ook uit VenJ. Er zijn vijf criteria met het Ministerie van Economische Zaken (EZ) vastgesteld waaraan het onderzoek binnen de programmalijnen moet voldoen. Een belangrijk element daarin is dat het moet gaan om pre-competitief onderzoek. Met EZ en VenJ is de werkwijze vastgesteld om de VenJ-bijdrage via EZ naar TNO te geleiden.

Essentieel voor de uitbouw van de nu bereikte stand van zaken is het optimaal benutten van de innovatie-krachten bij de vele partijen binnen het veiligheidsdomein; het gaat dan om zowel nationale als internationale partijen uit overheid, bedrijfsleven en kennisorganisaties. De recente honorering van het Europese project I-LEAD is in dit verband een mooi wapenfeit: met een twaalftal Europese veiligheidsorganisaties wordt in samenwerking met TNO o.a. een innovatie-roadmap ontwikkeld onder aanvoering van het European Network of Law Enforcement Technology Services (ENLETS), dat verankerd is in de Nederlandse Nationale Politie.

Ondertekening

Rijswijk,

Henk Geveke

Algemeen Directeur

Defensie & Veiligheid

Christiaan van den Berg

Programmamanager VPVM

Publicaties

Informatievoorziening

- Sappelli, M., de Boer, M., en van Wegberg, R.S., Objectiveren van criminele winsten op het Dark Web, Secondant (ingediend)
- Sappelli, M., de Boer, M., van Wegberg, R.S., en Young, H., VP VM Informatievoorziening – WP1 Databronnen, TNO-rapport 2016.
- Smit, S., Van der Vecht, B., Van Wermeskerken, F. & Streefkerk, J.W. (2016). QUIN: Providing Integrated Analysis Support to Crime Investigators. Proceedings of the European Intelligence and Security Informatics Conference (EISIC 2016), Uppsala, Sweden.
- De Vries, A., Menkhorst, M., cs*, Wie belt er nog? Het nieuwe melden. Een toekomstverkenning*, TNO-Rapport, www.tno.nl/hetnieuwemelden, januari 2016; o.a verstuurd als bijlage van officiële 2e Kamerstukken: https://www.rijksoverheid.nl/documenten/rapporten/2016/03/14/tk-bijlage-tno-rapport-het-nieuwe-melden.
- Presentatie CULTNET conferentie, 25 Mei 2016
- De Landmeter, R. (2016), *3D Delta: Informatierotonde watercrisisbeheersing*, Waterschap, Tijdschrift voor Waterschappen en waterbeheersing, Nr. 11, Nov 2016.
- Poster 3D-Delta: connecting applications for joint insight into (impacts of) flooding, Video & Website: http://3ddelta.nl/

Procesinnovatie voor performanceverbetering

- Huis in 't Veld, M.A.A., Koning, L., Schraagen, J.M.C, Stolk, D.J, *Ondersteuning van oordeelsvorming*. TNO rapport komt in april 2017 gereed.
- Van Rijk, R, Van den Bosch, K & Veldhuis, G (maart). *Interventies ter versterking van oordeelsvorming en adaptieve vaardigheden*, TNO rapport komt in april 2017 gereed.
- Van Rijk, R, Van den Bosch, K, Oomen, T, van Sassen-van Meer, J & Veldhuis, G., *Procesinnovatie: trainingsconcept oordeelsvorming. Train de trainer document*, TNO rapport komt in april 2017 gereed.
- Kerstholt, J., Duijnhoven, H., Paton, D., *Flooding preparedness in The Netherlands: Integrating factors at individual, social and institutional level,* submitted for publication in International Journal of Disaster Risk Reduction.
- Bakker, M., Kerstholt, J. & Giebels, E., *Deciding to Help: Effects of Risk and Crisis Communication* (in press), Journal of Contingencies and Crisis Management.
- Davis, S., Duijnhoven, H., Dinesen, C., Kerstholt, J. (2016). Strengthening community resilience: a toolkit. Paper presented at 6th Conference on Building Resilience. Auckland New Zealand, 7-9 September 2016.
- Duijnhoven, H., Neef, M., Davis, S., Dinesen, C. & Kerstholt, J. (2016). Resilient communities: implications for professionals. Paper presented at 6th Conference on Building Resilience. Auckland New Zealand, 7-9 September 2016.
- Paton, D., Kerstholt, J. & Skinner, I., *Hazard Readiness and Resilience* (in press), In D. Paton and D.M. Johnston (Eds). Disaster Resilience: An integrated approach (2nd Ed). Springfield, Ill., Charles C. Thomas.
- Schraagen, J.M., Van Buul-Besseling, K., Ruijven, T.W.J. van, Koning, L. de, *Oordeelsvorming: elk oordeel heeft zijn aandeel*, TNO-publicatie, mei 2016
- Brinck, P. van de, Duijnhoven, H., Kerstholt, J., Neef, M., *Samenredzaamheid in crisismanagement,* TNO-publicatie, mei 2016
- Duijnhoven, H., Nieuwenhuijs, A., Van den Brink, P., & Stolk, D. (submitted) *Critical Infrastructure Resilience: Bridging the Gap Between Measuring and Governance.* Submitted to the 7th Symposium on Resilience Engineering Association, 26-29 June 2017, Liège, Belgium

Real Time Intelligence

- Smit, S., Vries, A. de, Kleij, R. van der, Vliet, H. van *Van Predictive naar prescriptive policing*, TNO-boekje, Den Haag (2016), gepubliceerd op internet, zie www.tno.nl/
- Smit, S., Vries, A. de., *Is met Predictive Policing de heilige graal gevonden?*, artikel in Secondant (mei 2016)
- Smit, S. *Hoe big data het aantal inbraken in Amsterdam verlaagt*, artikel in TNO Time(2016)
- 'Vries, A. de, Steen. M., *BART rapport fase 2c*, TNO-rapport, Den Haag (2016).
- Hengst, M. den, Vriesde, R., Rouwenhorst, E., Vries, A. de, Berg, R. van den, Arnold, H., *Met BART werken aan een veilige buurt*, artikel in Secondant,(november 2016).
- BART film (momenteel alleen nog voor intern gebruik politie en gemeente)
- Workshop BART op Innovatiedag Nationale politie(3 november 2016)
- Workshop BART op CCR Summit (5, 6 oktober 2016)
- RTI-lab film: https://vimeo.com/161504721/c7b7af403a
- Berg, C.H. van den et al (2016), Memorandum 'Spelregels voor Innoveren in het RTI-lab', TNO en politie, Den Haag

Cyber Security & Societal Resilience

- Roos, B., Toelichting Cyber Trend Watch project 2016 (TNO notitie RWP-ELSS-2017-0100303151).
- Smulders A. et al (2016).*Veilig omgaan met het Internet of Things. Een handreiking voor informatiebeveiligers* (TNO 2016 R11648). Den Haag: TNO.

- Ruijven, T. van, Keijzer B., Whitepaper: *Sterke schakels, zwakke ketens? Good practices voor het vergroten van ketenweerbaarheid tegen cyberdreigingen*, Den Haag: gezamenlijke TNO | NCSC publicatie [in 2017 beschikbaar via www.tno.nl]
- Ruijven, T. van, Keijzer B., (2017) *Sterke schakels, zwakke ketens?*, Magazine Nationale Veiligheid en Crisisbeheersing [nog te plaatsen in 2017]
- Smulders A. et al (2016).*Veilig omgaan met het Internet of Things. Een handreiking voor informatiebeveiligers* (TNO 2016 R11648). Den Haag: TNO.
- Smulders, A., Ham, J. van der (2016), *Security voor Internet of Things*, Informatiebeveiliging Magazine (IB-5 2016)
- Wegberg, R.S. van, A.J. Klievink, M.J.G. van Eeten, (2016, in print). *'Bitcoin Money Laundering: Mixed Results? An explorative study on money laundering of cybercrime proceeds using Bitcoin'*, Journal of Financial Crime, (http://dx.doi.org/10.1108/JFC-11-2016-0067)
- Wegberg, R.S. van, A.J. Klievink, M.J.G. van Eeten (2016, under review). *'Value Chains in Financial Malware, On the economic incentives and business models in current-day financial malware schemes'* (European Journal on Criminal Policy and Research)
- Wegberg, R.S. van (2016, under review). *'Experimenteren op het Dark Web? Methodologische kansen en uitdagingen in criminologisch onderzoek naar technologisch gedreven cybercrime'* (Tijdschrift voor Criminologie)
- Kernkamp A. (2016, 19 mei), *Internet of Things and Risk Management* op de Risk 2016 conference "Risk & Opportunity in a State of Development [Online video presentatie], Sydney, Australië
- Roos, B. Polen, M. van (2016, 21 december), *Threat Intelligence Lab Demonstration* [break-out sessie TNO CTI Event], Den Haag
- Ruijven, T. van (2016, 11 november), *Presentatie Cyber City Resilience Scan* tijdens de Rockfeller 100RC Cyber Resilience Workshop, New York, USA

Verkenning voor de DG's RR, SB en VZ

- Van der Kleij, R., Van den Brink, P., *Integrale ketensturing: Toepassing op de vreemdelingenketen,* TNO-rapport 2016 R11624.
- De Groen, L., van Slingerland, P., & van Vliet P.J., (2017) *Share Analysis, Not Data: Informatiedeling zonder twijfels*. TNO-rapport komt gereed in Q1 2017
- Workshop Coördinatievormen, dd. 13 december, 2016. T.b.v. leden van de leerkring ketensamenwerking: een interdepartementaal kennisuitwisselingsplatform.
- Eindpresentatie Ketensturing, dd. 15 december, 2016. T.b.v. medewerkers van het directoraat-generaal Vreemdelingenzaken van het ministerie van Veiligheid en Justitie.
- Workshop 'Crisisbeheersing' op de State of the art conferentie, dd. 9 december, 2016, door Rick van der Kleij & Joeri Kapteijns (DGVZ).
- Workshop 'Share analysis, not data' dd 11 december, 2016, tbv vertegenwoordigers van de stakeholders in het domein Verwarde Personen.
- Workshop 'Governance: Grenzen' op de State of the art conferentie,dd 9 december 2016, door Jeroen van Rest, Ingrid Weima, Sander Luijsterburg (DGVZ) en Prof. Thomas Spijkerboer (VU).
- Van Rest, J.H.C., Weima, I.; (2017) *Risicosturing - Een verkenning in het veiligheidsdomein - Bekeken vanuit het grensproces op luchthavens*, TNO Rapport komt gereed in Q1 2017

Websites van EU-projecten, waarin basiskennis van het VP Veilige Maatschappij wordt toegepast

Crisis management
- ResiStand: Increasing disaster Resilience by establishing a sustainable process to support Standardisation of technologies and services, http://resistand.eu/
- ISITEP: Inter System Interoperability for TETRA-TETRAPOL Networks, http://isitep.eu/
- PREDICT: PREparing for the Domino effect In Crisis siTuations, https://www.predict-project.eu/home
- COBACORE: COmmunity-BAsed COmprehensive REcovery, http://www.cobacore.eu/
- DRIVER: DRiving InnoVation in crisis management for European Resilience, http://driver-project.eu/

Critical Infrastructure Protection
- CIPRnet: Critical Infrastructure Preparedness and Resilience Research Network, https://www.ciprnet.eu/home.html
- INTACT: On the Impact of Extreme Weather on Critical Infrastructures, http://www.intact-project.eu/index.cfm
- SEGRID: Security for Smart Electricity GRIDs , https://segrid.eu/

Intelligence Terrorisme en criminaliteit
- ASGARD: Tools and infrastructure for the fusion, exchange and analysis of big data including cyber-offense generated data for forensic investigation, http://asgardproject.eu/
- VOX-Pol: Virtual Centre of Excellence for Research in Violent Online Political Extremism, http://www.voxpol.eu/
- SOURCE: Virtual centre of excellence for research support and coordination on societal security, http://societalsecurity.net/about-source
- IMPACT Europe - Innovative Method and Procedure to Assess Counter-violent-radicalisation Techniques in Europe, http://impacteurope.eu/
- SubCop: Suicide Bomber Counteraction and Prevention , http://www.subcop.eu/

Bewaken en beveiligen
- Media4Sec: Better understanding the role of new social media networks and their use for public security purposes, http://media4sec.eu/
- INSPEC2T: Inspiring citizeNS Participation for Enhanced Community poliCing acTions, http://inspec2t-project.eu/nl/
- XP-DITE: Accelerated Checkpoint Design Integration Test and Evaluation, http://www.xp-dite.eu/

Cybersecurity

- CAPITAL: Cybersecurity research Agenda for PrIvacy and Technology chALlenges, http://www.capital-agenda.eu//?Page=home
- COURAGE: Cybercrime and cyberterrOrism (E)Uropean Research AGEnda, https://www.courage-project.eu/