Defensie & Veiligheid
Kampweg 5
3769 DE Soesterberg
Postbus 23
3769 ZG Soesterberg

www.tno.nl

T +31 88 866 15 00
F +31 34 635 39 77

TNO-rapport

TNO 2015 R11219

Meerjarenprogramma 2015-2018

Thema Maatschappelijke Veiligheid

Bijstelling 2016

Datum	30 september 2015
Auteur(s)	Dr. Ir. J.A. Don
Aantal pagina's	31
Regievoerend departement	Ministerie van Veiligheid en Justitie
Projectnummer	060.12703

Samenvatting

Om de diverse veiligheidsorganisaties in de Nederlandse maatschappij op al hun taken berekend te houden is, en om te beantwoorden aan de veiligheidsbehoeften van bedrijven en burgers doet TNO onderzoek gericht op de gevraagde transities in defensie en veiligheid. In het Vraaggestuurd Programma in het Speurwerkthema Maatschappelijke Veiligheid wordt geïnvesteerd in verkennend onderzoek om in de toekomst als TNO optimaal aan te kunnen sluiten bij de vraag van publieke veiligheidsorganisaties naar contractresearch.

In nauwe afstemming met het regievoerend ministerie van Veiligheid en Justitie is bij de start van dit programma de focus gelegd op een drietal VP-kennisprojecten voor inhoudelijke kennisvernieuwing, terwijl deze inhoudelijke kennisvernieuwing in een vijftal clusters wordt doorvertaald naar innovatiebehoeften van publieke en private stakeholders. Hierbij krijgt ook de synergie met het Vraaggestuurd programma Security in de topsector HTSM aandacht. Onderstaande tabel vat dit samen:

VP-onderdelen / Innovatie-Clusters	VP-Veilige Maatschappij			VP Security		
	Informatievoorziening	Proces innovatie voor performance-verbetering	Cybersecurity & Societal resilience	Systems of systems	Sensoren	Cyber risk management & System resilience
Crisismanagement & resilience vitale infra	+	++	+	++		
Real Time Operations support	++	+			++	
Intelligence Terrorisme en criminaliteit	++			++		
Bewaken en beveiligen		++	+		++	+
Cybersecurity	+		++			++

In 2015 is de basis gelegd voor het uitbouwen van de relatie van VenJ en TNO. Daarbij wordt inspiratie geput uit de strategische samenwerking tussen het ministerie van Defensie en TNO. Als onderdeel van dit versterken van de samenwerking tussen het ministerie VenJ en TNO zal het opzetten van een experimenteeromgeving voor Real Time Intelligence in 2016 in dit VP verder worden ontwikkeld. Het toenemend belang van informatiesturing binnen de veiligheidsketen werd in 2013 in het Vraaggestuurd Programma Security voor de topsector High Tech Systems & Materials als uitdaging voor publiek-private samenwerking opgepakt. Door de intensieve interactie met politie en andere

operationele veiligheidsorganisaties ontstond daarbij draagvlak voor een Real Time Intelligence Lab, waar met name geëxperimenteerd kan worden met nieuwe benaderingen en tools voor de ondersteuning van veiligheidsoperaties.
De ontwikkeling voor specifieke probleemstellingen in publiek-private consortia zullen in het VP Security een vervolg krijgen.

In 2016 zal ook worden verkend hoe de Directoraten-Generaal Rechtspleging en Rechtshandhaving (DGRR), Straffen en Beschermen (DGSB) en Vreemdelingenzaken een meerwaarde kunnen ontlenen aan een nauwere betrokkenheid bij dit vraaggestuurde programma en de kennisportfolio van TNO.

Inhoudsopgave

1 Inleiding TNO Thema Maatschappelijke Veiligheid

1.1 Veiligheid in onze maatschappij

Veiligheid is een primaire voorwaarde voor welzijn en economische ontwikkeling. In de open economie van ons land maakt de veelheid van risico's kwetsbaar. En daar waar de fysieke veiligheid in Nederland is toegenomen, hebben veel vormen van onveiligheid zich verplaatst naar of vermengd met het cyberdomein. De tegelijkertijd optredende schaalvergroting van economische systemen èn van de bedreigingen voor onze veiligheid vereist een toenemende samenwerking. Politie, veiligheidsregio's en andere diensten (veiligheidsdiensten, operationele diensten, parate diensten, hulpverleningsdiensten) zetten daarom in op een regie op een grotere schaal. Tussen overheid, bedrijfsleven en burgers ontstaat een nieuw samenspel. De balans tussen privacy en veiligheid is daarbij actueel.
Ook interne of maatschappelijke veiligheid en externe veiligheid ofwel defensie raken onderling steeds meer verweven. Dit uit zich onder meer in versterking van civiel-militaire samenwerking en inzet van dual use-technologie.

1.2 TNO-strategie 2015-2018

Om bij te dragen aan het beheersen van de risico's voor de veiligheid in onze maatschappij heeft TNO kennis van en faciliteiten voor:
- Optreden, operaties en crisisbeheersing;
- Informatie en communicatie;
- Bescherming, wapens en uitrusting;
- Mensen en organisaties;
- Systemen en systems of systems.

Om de diverse veiligheidsorganisaties op al hun taken berekend te houden is, en om te beantwoorden aan de veiligheidsbehoeften van bedrijven en burgers doet TNO onderzoek gericht op de gevraagde transities in defensie en veiligheid. Hierbij ligt de nadruk op effectiviteit, bescherming, flexibiliteit en betaalbaarheid, waarbij we gebruik maken van concept development and experimentation (CD&E). TNO zoekt in het maatschappelijke veiligheidsdomein een strategisch partnerschap met haar stakeholders bij de overheid – het ministerie van Veiligheid en Justitie, de nieuwe nationale politie, de veiligheidsregio's en andere. Deze ambitie ligt in het verlengde van de al decennialange relatie met het Ministerie van Defensie.

1.3 Organisatorische inbedding van het TNO-speurwerkthema Maatschappelijke Veiligheid

Als doelstelling voor de TNO-organisatie geldt in de Strategie 2015-2018 het bereiken van impact op vijf transities. Eén daarvan betreft *Defensie en Veiligheid*. De verantwoordelijke directeur stuurt zes programma's met elk een programma-directeur aan. Voor het Speurwerkthema Maatschappelijke Veiligheid zijn twee van deze programma's dominant van belang:
- Het programma National Security & crisismanagement (directeur: drs. L.C. van Duijn).
- Het programma Cybersecurity and resilience (directeur: mw. A Zielstra).

Binnen het TNO-speurwerkthema is één Vraaggestuurd programma met Dr.ir. J.A. Don als manager.

2 Visie op programma 2015-2018

2.1 Algemeen

De visie van belangrijke stakeholders bij politie en veiligheidsregio's is dat innovatie meer vergt dan de ontwikkeling van sociaal wetenschappelijke dieptekennis en van geavanceerde technologieën. Het gaat ook om multidisciplinaire innovaties van samenwerking en van organisatorische en maatschappelijke processen en systemen. Het innovatieteam van het regievoerende ministerie Veiligheid en Justitie helpt met het versterken van de aansluiting van het programma bij de onderzoekbehoeften van de operationele organisaties en het beleid. Voor de ontwikkeling van strategische ambities bepalen de Nationale Innovatie-agenda Veiligheid en de Innovatie- Agenda's voor het ministerie van VenJ, de Nationale Politie en de Veiligheidsregio's in belangrijke mate de richting.

2.2 Focus van ontwikkelingen in VP-onderdelen

Bij de start van het vraaggestuurde programma Veilige Maatschappij zijn er drie VP-kennisprojecten gedefinieerd met ontwikkeling van fundamentelere, breder van belang zijnde kennis. Daarnaast is in 2015 binnen het VP Security een samenwerking met publieke en private partijen op het gebied van Real Time Intelligence opgebouwd. Als vervolg daarop wordt in 2016 een nieuw programma-onderdeel in dit VP VM geïnitieerd. Ook is in het kader van de uitbouw van de relatie van het ministerie VenJ en TNO besloten een onderdeel in het VP VM op te nemen voor het ontwikkelen van een kennisbasis die aansluit op het domein van de Directoraten-Generaal Rechtspleging en Rechtshandhaving (DG RR), Straffen en Beschermen (DG SB) en Vreemdelingenzaken. Dit resulteert in een VP met vijf specifieke onderdelen:

VP-onderdelen
1. Informatievoorziening (selectieve info-verzameling, -analyse, -validatie en -deling)
2. Procesinnovatie voor performanceverbetering (samenwerking binnen en tussen organisaties, insourcing capaciteiten, effectiviteit in praktijk, ontwikkeling competenties, oefenen, (virtuele) training)
3. Cybersecurity & Societal resilience (monitoring voor detectie misbruik internet, resilience cross sector info-uitwisseling, keteneffecten infra)
4. Real Time Intelligence
5. Ontwikkelen initiatieven voor versterking kennisbasis DG's RR, SB en VZ

Er zijn daarnaast nog twee programma-brede elementen. Dat zijn civiel-militaire samenwerking en de continue behoefte aan het toepasbaar maken van nieuwe technologieën voor het veiligheidsveld.

2.3 Focus van multi-stakeholder-innovaties in innovatieclusters

In het civiele domein van het TNO thema Defensie en Veiligheid heeft TNO vijf innovatieclusters gespecificeerd, waarbinnen strategische samenwerking voor multi-stakeholderinnovaties gestalte krijgt. Voor elk van deze innovatieclusters is binnen TNO een team gevormd dat verantwoordelijk is voor de strategische positionering van TNO, de relaties met trendsettende stakeholders, de samenwerking met partners en de ontwikkeling van de opdrachtenportefeuille. Vanuit deze clusters wordt ook bijgedragen aan de programmering van de kennisontwikkeling binnen de VP's en de toepassing van de onderzoeksresultaten. TNO-breed is - mede op aangeven van het voor innovatie coördinerende ministerie EZ - een ontwikkeling van strategische researchprogramma's op gang gebracht; kenmerk daarvan is dat TNO en de betreffende stakeholders meer gezamenlijk gaan investeren en zo de investeringsrisico's in innovatietrajecten gaan delen om een beter toepasbaar resultaat te krijgen.
In de innovatieclusters zal ook de benutting van de resultaten van EU-projecten aandacht krijgen. Met een acceptabele inspanning kunnen zo de resultaten toegankelijk gemaakt worden voor belanghebbenden buiten de directe projectpartners. Verder kunnen vanuit deze innovatieclusters initiatieven voor nieuwe EU-samenwerkingsprojecten worden ontwikkeld.

De civiele innovatieclusters in het TNO-thema Defensie en Veiligheid zijn nagenoeg synchroon aan de Security-innovatiegebieden voor multi-stakeholdersamenwerking in het Europese programma Horizon 2020 (zie onderstaande tabel). Dit synchroon lopen is van belang voor het verwerven van additionele financiering en voor het versterken van de betrokkenheid van potentiële gebruikers van de onderzoeksresultaten.

<table>
<tr><th>Civiele innovatieclusters
in TNO-thema Defensie en Veiligheid</th><th>EU-Security H2020</th></tr>
<tr><td>Crisismanagement en Resilience vitale infra</td><td rowspan="2">Disaster Reduction and Resilience</td></tr>
<tr><td>Real Time Operations support</td></tr>
<tr><td>Intelligence Terrorisme en Criminaliteit</td><td rowspan="2">Fight against Crime and terrorism</td></tr>
<tr><td rowspan="2">Bewaken en beveiligen</td></tr>
<tr><td>Bordersecurity</td></tr>
<tr><td>Cybersecurity</td><td>Cybersecurity</td></tr>
</table>

2.4 Internationale samenwerking

Een aantal nationale onderzoeksbehoeften op het gebied van Maatschappelijke Veiligheid zijn in de EU actueel. Voor deze onderzoeksbehoeften kan het nationale budget uit het VP VM van een multiplyer worden voorzien door participatie in EU-projecten. Deze multiplyer betreft zowel een budget-vergroting voor de door TNO te ontwikkelen kennis en toegang tot de kennis van de internationale partners in het EU-project. TNO zet zich ervoor inzetten om Nederlandse stakeholders bij de uitvoering van zulke projecten te betrekken ter bevordering van de benutting van de

resultaten. De betrokkenheid van de nationale veiligheidsorganisaties zal ook via de innovatieclusters worden geoptimaliseerd.

TNO zal de ontwikkeling van de Nederlandse positie in de Europese innovatie-arena helpen uitbouwen. Essentieel daarvoor is de verankering van de innovatieclusters in het Nederlandse veiligheidsveld. Dit biedt dan een vertrekpunt voor initiatie, monitoring en benutting van de resultaten van de projectenportfolio per innovatiecluster. Een kritische selectie van Nederlandse deelnames is daarbij vereist.

Ontwikkelingen in de Europese samenwerking in de komende jaren zijn:

- Uitbouw van het in 2014 gestarte EU-project DRIVER tot een nationaal en internationaal centrum voor het valideren en harmoniseren van crisismanagement bij grootschalige rampen. Dit mega-project met 38 consortiumpartners en een budget van 43 M€ is gericht op “common understanding of crisis management and increased willingness to share capabilities and collaboration in crisis management innovation”. Nationaal zijn met steun van NCTV-directie Weerbaarheid al meerdere partijen aangesloten (o.a. de veiligheidsregio’s Haaglanden en Twente, Landelijke Operationele Staf en de bedrijven HKV en Ecorys). Nationale verankering in het innovatiecluster crisismanagement in samenwerking met HSD biedt grote meerwaarde.
- Het ontwikkelen van een vergelijkbaar initiatief voor het innovatiecluster “Surveillance and protection” in samenwerking met politie en KMar. De al lopende projecten voor luchthavenbeveiliging bieden hiervoor al een goede basis.
- Het bijdragen aan civiel militaire ontwikkelingsinitiatieven in de EU. Internationaal groeit het draagvlak voor civiel militaire samenwerking, niet in de laatste plaats omdat bij expeditionair optreden in conflictgebieden ook de civiele veiligheidstaken steeds vaker integraal aandacht gegeven worden. In de eerste calls van het Security-onderdeel van Horizon 2020 zijn ook enkele topics opgenomen met civiel militaire vraagstellingen. Zowel de EU als EDA zijn voorstander van het verder uitbouwen.

3 Ambitie en doelstellingen

3.1 Ambitie VP 2015-2018

Het nieuwe VP 2015-2018 bestaat uit twee soorten onderdelen:

- Kennisprojecten voor inhoudelijke kennisvernieuwing, die 100% uit SMO-middelen voor VP's gefinancierd worden:
  - Wetenschappelijke vernieuwing zo mogelijk in samenwerking met universiteiten.
  - Aansluiting bij toepassingsbehoefte door betrokkenheid/begeleiding inhoudelijk specialisten van veiligheidsorganisaties.
  - Periodieke rapportage aan de relevante innovatieclusters.
- Clusters voor gezamenlijk innovatie-initiatieven die met in natura en cash-bijdragen aanvullend worden gefinancierd:
  - Ontwikkelen van gebruikerscommunities.
  - Optimale benutting en samenwerking met andere kennisinstellingen, waaronder TO2-instituten.
  - Portfolio van EU-projecten.
  - Verankeren in Strategische Research Programma's.
  - Parallel aansturing van (PPS-)projecten in kader van VP Security.

Het ministerie van EZ stelt voor haar financiering van VP's aan TNO de voorwaarde dat er commitment is van potentiële gebruikers van de onderzoeksresultaten. TNO heeft mede als gevolg daarvan aan de TNO-themadirecteuren de eis gesteld, dat VP's een groeiend financieel commitment van stakeholders zullen realiseren.
De overheidsfinanciering voor VP's moet leiden tot Strategische Research Programma's met medefinanciering uit belanghebbende stakeholders en spin off naar een opdrachtenportefeuille voor TNO. Om deze ambitie waar te maken is de samenhang tussen de ontwikkelingen in de kennisprojecten en de innovatieclusters essentieel. In paragraaf 3.2 wordt gespecificeerd wat de innovatiespeerpunten zijn in de kennisprojecten en welk belang deze hebben voor de innovatieclusters. Vervolgens worden in paragraaf 3.3 de innovatieclusters gespecificeerd.

3.2 Focus van de kennisprojecten van het VP Veilige Maatschappij voor inhoudelijke kennisvernieuwing

VP-kennisprojecten	Innovatiespeerpunt	Mogelijke onderwerpen in de innovatieclusters
Informatie-voorziening	• Informatie-analyse voor real-time intelligence door informatie uit crowds/ burgers en overige ongestructureerde bronnen. • Duiding van informatie op netwerkknooppunten (o.a. LMO). • Tools en concepten voor intelligencetaken.	• Interactieve crowdsourcing via o.a. sociale media. • Informatieverwerking en duiding (Big data). • Predictive policing. • Dark web research.
Proces-innovatie voor performance-verbetering	• Harmonisering optreden binnen en tussen organisaties. • Intermenselijke samenwerking multi-organisatie-optreden. • Stimuleren en ondersteunen burgerparticipatie. • Simulatie, gaming en oefenen.	• Civ-mil samenwerking bij groot-schalig geïntegreerd optreden. • Benutten burgercapaciteiten bij crises. • Planmatig ontwikkelen performance van multi-organisatie-samenwerking. • Community policing.
Cybersecurity & societal resilience	• Modellen en tools met betrekking tot cyber resilience van maatschappij. • Privacy and security bij design voor internetdiensten aan burgers en bedrijven. • Nieuwe vormen van opleiden, trainen en oefenen van cybersecurity personeel. • Detectie internetmisbruik.	• Effectief vergroten maat-schappelijke cyber resilience (oa Smart modularisering van vitale infrastructuur). • Gedragsbeïnvloeding ter beperking van cybergerelateerde schade. • Effectievere middelen om cybersecurity personeel te trainen. • Monitoring en opsporing internet-misbruik.
Real Time Intelligence	• RTI-lab voor beproeving en ontwikkeling nieuwe concepten • Real-time intelligence door combinatie van info uit systemen van Veiligheidspartners. • Preparatie info-uitwisseling bij calamiteiten. • Ontwikkelen Thematisch Quadruple Helix netwerk voor thought-leadership, roadmapping, kruisbestuiving en voedings-bodem voor nieuwe ideeën	• Infosystemen en multi-user interfaces. • Control room technologie (bv. toepassing Touch-table in Operationeel Centrum) • Expert-systems voor beslisondersteuning • Head-up displays voor agenten • Interfaces naar burgers
Kennisbasis voor DG's RR, SB en VZ	• Verkennen behoeften waar TNO-expertise toegevoegde waarde kan hebben • Ontwikkelen samenwerking met andere nationale en internationale kennispartners	

3.3 Focus van de innovatieclusters

De ambitie van TNO is om met het VP Veilige Maatschappij en het VP Security bij te dragen aan krachtenbundeling voor innovatietrajecten en uitwisseling van best practices in het operationele veld van de professionele veiligheidsorganisaties. Om dit te bereiken zullen naast de in 3.2 omschreven VP-kennisprojecten voor kennisontwikkeling vijf innovatieclusters van stakeholders worden gevormd (zie paragraaf 2.3). In onderstaande subparagrafen is voor elk van de vijf clusters een omschrijving uitgewerkt.

3.3.1 Crisismanagement en resilience vitale infrastructuur

Het cluster Crisismanagement en resilience vitale infrastructuur richt zich op:

- wat een maatschappij kan ontwrichten (*all hazard*),
- wat we daaraan kunnen doen ter voorkoming,
- hoe we er achter komen dat het fout gaat,
- wat we kunnen doen als dat het geval is,
- en als het fout is gegaan, wat we kunnen doen om tot maatschappelijk herstel te komen en de rust terug te brengen.

Deze vraagstukken zijn actueel zowel binnen Nederland, grensoverschrijdend met onze buurlanden, als in de buitenlanden waar Nederland actief is om de maatschappelijke weerbaarheid te verhogen, crisis en conflicten te beheersen, of de maatschappij er weer bovenop te brengen.

Een belangrijke basis voor het versterken van crisismanagement en de weerbaarheid van de vitale infrastructuur ligt in een goed begrip van de toenemende onderlinge afhankelijkheden en de complexiteit binnen de maatschappij, alsook van de ontwrichtende domino-effecten die als gevolg van een (zelfs kleine) verstoring kunnen optreden. In het kader van het EU-programma ISF wordt voor de vitale infrastructuursectoren in onze maatschappij een grootschalig initiatief ontwikkeld, waar ook TNO een substantiële bijdrage aan levert op basis van de in Europees verband ontwikkelde databestanden, modellen en overige kennis in EU-projecten en –netwerken.

In het kader van het EU-project DRIVER heeft al de basis gelegd voor samenwerking met een aantal Nederlandse partners en aansluiting bij de Strategische Agenda voor Versterking van de Veiligheidsregio's. In de komende maanden zal dit verder worden uitgebouwd.

De aan dit cluster gelieerde kennisopbouw richt zich op het vinden van mogelijkheden om het vermogen tot acteren en samenwerken te vergroten, op individueel, team, organisatie en inter-organisatie niveau. Zodat alle spelers (overheden, burgers, bedrijfsleven, NGO´s, etc.) tot actie komen en die hun acties zodanig (kunnen) kiezen dat de effecten daarvan elkaar maximaal versterken. Het vermogen tot acteren en samenwerken wordt bepaald door de mate waarin alle spelers beschikken over de juiste competenties, informatie en middelen en de mate waarin sprake is van de juiste voorbereiding. Het vergroten van het vermogen betekent ook het sneller kunnen doorlopen van de loop *informatievergaring en -uitwisseling* > *duiding* > *beeldvorming (komend tot een gedeeld beeld)* > *oordeelsvorming* > *besluitvorming* > *leiding & coördinatie* > *actie* > *actie evaluatie* (en vergelijkbare loops als Plan Do Check Act en Observe Orient Decide Act).

Huidige en potentiële gebruikers van de opgebouwde kennis behorende bij dit cluster zijn bijvoorbeeld de ministeries van VenJ, Defensie, EZ, BZ, IenM (RWS), de Veiligheidsregio's, hun ketenpartners zoals de Waterschappen en de vitale sectoren, Brandweer Nederland, de Nationale Politie, de Landelijke Meldkamerorganisatie, de grote gemeenten, en internationaal partijen als de VN (UNISDR), UNICRI, de Wereldbank en vanzelfsprekend de EC.

De portfolio van lopende EU-projecten bestaat nu uit (alfabetische volgorde):

- COBACORE
  www.cobacore.eu
  COmmunity-BAsed COmprehensive Recovery.
- CIPRNET
  www.ciprnet.eu
  Critical Infrastructure Preparedness and Resilience Research Network.
- DRIVER
  http://cordis.europa.eu/project/rcn/188608_en.html
  DRiving InnoVation in crisis management for European Resilience.
- IMPACT Europe
  impacteurope.eu
  Innovative Method and Procedure to Assess Counter-violent-radicalisation Techniques in Europe.
- INTACT
  http://cordis.europa.eu/project/rcn/185476_en.html
  On the Impact of Extreme Weather on Critical Infrastructures.
- PREDICT
  www.predict-project.eu
  PREparing for the Domino effect in Crisis siTuations.
- SOURCE
  www.societalsecurity.net
  Virtual centre of excellence for research support and coordination on societal security.

Verder is het defensie-doelfinancieringsprogramma *V1227 vervolg: gedragsbeïnvloeding in civ-mil operaties* van belang voor dit cluster.

3.3.2 Real Time Operations support

Dit innovatiecluster zal met name inzoomen op een samenwerkingsverband met politie, veiligheidsregio's en LMO. Nadere uitwerking van een gezamenlijk investeringsprogramma zal de komende maanden plaatsvinden.

3.3.3 Cluster Intelligence, terrorisme en criminaliteit

Intelligence betreft het vergaren, verwerken, interpreteren en beschikbaar stellen van informatie t.b.v. de overige processen in het veiligheidsveld. Intelligence betreft in wezen informatie die geschikt is voor vroegtijdige onderschepping, handhaving en opsporing (besluitvorming, sturing, ondersteuning etc.).

Door veiligheidspartijen zoals de Nationale Politie, de NCTV, V&J, de AIVD, de Marechaussee en particuliere bedrijven, wordt 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 kan 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? Twee vragen staan centraal bij de focus van het Cluster Intelligence, Terrorism & Organised Crime namelijk:

- Hoe kunnen veiligheids- en opsporingsdiensten en de actoren in de strafrechtketen optimaal informatie vergaren en analyseren t.b.v. intelligence en de bestrijding van criminaliteit en terrorisme.
- Hoe kan inzicht worden verkregen uit de beschikbare informatie uit vele bronnen en kan deze optimaal worden benut voor sturing en support van het handelen van veiligheids- en opsporingsdiensten op diverse niveaus (strategisch, tactisch, operationeel).

Specifieke onderwerpen die onder het cluster vallen:

- Continue verbetering van bijzondere observatiemethoden die specifiek t.b.v. intelligence worden benut.
- Grip krijgen de radicalisering van groepen en individuen in de maatschappij.
- Ontwikkelen en verbeteren van analyse- en sturingsmethoden teneinde effectiviteit en efficiency te vergroten Voorbeelden zijn: Analysemethoden (MARVEL, SNA, near real time analysis) Sturingsmethoden (predictive policing, hypothesemanagement, selectie van informanten, slim kiezen, handelingsperspectieven voor interventies).
- Meer inzicht in dreiging en fenomenen door slim gebruik en combineren van (diverse) bronnen: Internetrecherche, Social media monitoring, Bijzondere contentdetectie (bijvoorbeeld radicale content), Gedragdetectie en interventie op digitaal medium, multimediamining/textmining /big data analyse, Dark web.
- Verhogen van voorspellend vermogen door interpreteren van zwakke signalen en ontwikkelen en verbeteren van methodieken voor predictive policing.
- Betere ondersteuning en sturing van operationele processen d.m.v. real-time intelligence .

Er loopt nu één EU-project:

- VOXPOL
  http://www.cmcs.ceu.hu/vox-pol-virtual-center-excellence-research-violent-online-political-extremism
  Virtual Center of Excellence for Research in Violent Online Political Extremism (VOX-POL).

3.3.4 Bewaken en beveiligen

Mainports, bedrijventerreinen, stedelijke gebieden, paleizen, internationale instellingen (ICC, Eurojust..), internationale zone, gesloten opvanglocaties (gevangenissen, asielzoekersopvang), ambassades en evenementen. Allemaal locaties waar veel mensen komen, of die om andere specifieke redenen een hoger veiligheidsrisico met zich mee brengen. Bij deze locaties kunnen verschillende partijen verantwoordelijk zijn voor het waarborgen van de veiligheid: NCTV, V&J, BiZa, BuZa, I&M, Defensie, Politie, Marechaussee, Gemeente, internationale organisaties, (lucht)havenautoriteiten en particuliere beveiligingsbedrijven.
Zij werken samen om op korte en lange termijn deze veiligheid te borgen.
De private markt ontwikkelt op zijn beurt diensten en technologieën om deze partijen te ondersteunen met deze uitdagingen.

Het cluster Bewaken en beveiligen helpt de partijen met het ontwikkelen van kennis, diensten en producten die bijdragen aan optimale integrale security concepten. Integraliteit betekent in dit geval dat de mogelijkheden voor het gehele spectrum aan organisatorische, technische, informatie en mens-gerelateerde innovaties in samenhang onderzocht en ontwikkeld worden. Met de veiligheidsdiensten, en met de commerciële leveranciers.

Binnen dit cluster is speciale aandacht voor:
- Security by design in mainports, stedelijke ontwikkeling en bij evenementen.
- Ontwikkelen van een beveiligingsconcept (KMAR, internationale zone, kindvriendelijke opvang asielzoekers).
- (Mobiele) sensoren en sensorfusie (incl. UAV's en onderwaterbeveiliging).
- Toegangscontrole
- Fysieke bescherming van gebouwen/locaties.
- Publiek private samenwerkingsconcepten voor bewaking en beveiliging.
- Definiëren van en reageren op afwijkend gedrag, door mens en machine.

De portfolio van lopende EU-projecten bestaat nu uit:
- SUBCOP (matchende financiering ook uit andere bron)
  http://cordis.europa.eu/project/rcn/108806_en.html
  Suicide Bomber Counteraction and Prevention.
- TACTICS (matchende financiering uit VP Security).
- HECTOS (matchende financiering uit VP Security).
- XP-DITE (matchende financiering uit VP Security)

3.3.5 Cybersecurity

De maatschappij wordt steeds afhankelijker van ICT. Dat zorgt voor nieuwe kwetsbaarheden. Ook is er sprake van een toenemende dreiging in de vorm van cyberspionage, -sabotage, -crime, etc. Tegen deze dreigingen moeten we ons weren. Cyberaanvallen worden al tijden niet alleen maar uitgevoerd vanuit zolderkamertjes. Het gaat ook om georganiseerde misdaad, een zwarte economie en een concrete dreiging gericht op onze vitale infrastructuur, mogelijkerwijs zelfs door statelijke actoren. De bijzondere EU Commissie voor Georganiseerde Misdaad, Corruptie en Witwassen (CRIM) heeft eind 2013 berekend dat cybercriminaliteit wereldwijd jaarlijks zo'n 290 miljard Euro kost aan opgelopen schade. Dat is meer dan alle drugsoperaties ter wereld (240 miljard) en ook meer dan de schade door corruptie (120 miljard). TNO berekende in 2012 dat de schade door cybercrime in ons land op ongeveer 10 miljard ligt. Om deze reden heeft het kabinet in oktober 2013) een tweede versie van de Nationale Cyber Security Strategie gepubliceerd. Nederland zet samen met partners in op een veilig digitaal domein waarin kansen van digitalisering worden benut, dreigingen het hoofd worden geboden en fundamentele rechten beschermd.

Cybersecurity is niet alleen een dreiging, maar ook een kans. Het cyberdomein maakt deel uit van de Nederlandse maatschappij. Een veilige en veerkrachtige cyberspace is een randvoorwaarde voor ICT gedreven innovaties, welvaart en een duurzame economie. TNO ziet het als haar verantwoordelijkheid om bij te dragen aan een veilige en veerkrachtige digitale maatschappij.

Cyber Security richt zich op het beschermen van gevoelige informatie en kritische ICT-gebaseerde processen en infrastructuren. Met onderzoek en innovatie wordt kennis en kunde ontwikkeld ten behoeve van innovatieve oplossingen en nieuwe generaties producten en diensten die bescherming bieden tegen toekomstige cyberdreigingen:

- Security in design: ontwerp van veilige soft- en hardware, methodieken en technieken voor veilig ontwerp van (ICT) infrastructuren.
- Veilige communicatie bescherming van telemetriedata en informatiestromen, etc.
- Detectie monitoring and Situational Awareness.
- Early Detection: detectie op basis van zwakke signalen, nieuwe vormen om zogenaamde Advanced Persistent Threats (gecompliceerde spionageaanvallen) op te sporen, etc.
- Advanced Risk Management: rechtmatige verdeling van verwachtingen, verplichtingen en bijbehorende risico's in ketens en netwerken, etc.
- Resilience & Continuity: security life cycle assurance, self healing, disaster recovery, continuity as a service, company reboot, etc.

De veiligheid van cyberspace vraagt om een integrale, multidisciplinaire aanpak met betrokkenheid van publieke en private stakeholders.
Buiten de overheid (V&J) komen cyber security vraagstukken vooral uit de vitale sectoren, zoals de financiële sector (bijvoorbeeld ING, ABN, Rabobank), telecom (bijvoorbeeld KPN), en energie (bijvoorbeeld Gasunie, TenneT, Alliander).

Het innovatiecluster Cyber Security kan bijdragen aan het opbouwen van een test-, ontwikkel- en evaluatiecentrum dat zich bezig houdt met het uitvoeren van proof-of concepts (laat zien dat oplossing technisch werkt), experimenten (uitproberen in een operationele omgeving) en oefeningen (trainen alsof het echt is).

De portfolio van lopende EU-projecten bestaat nu uit:

- CYSPA (matchende financiering ook uit andere bron).
  CYSPA is an initiative set up by 17 organizations from across industry and research, aiming to create a European Alliance to protect cyberspace for industry. CYSPA's goal is to increase the capacity of industry to protect itself from cyber disruptions. While the CYSPA community is grounded in the EU, its aim is to extend its outreach at international level.
- CAPITAL
  Cyber-security And Privacy research challenges, Innovation Technologies processes and market Analysis - will deliver an integrated research and innovation agenda for Cyber security and privacy. CAPITAL is built around two pillars:
  - coordinate European R&D efforts in the cyber-security domain,
  - jointly address research and innovation within an Integrated Research & Innovation Agenda.
- COURAGE (matchende financiering uit VP Security)
  The project Cybercrime and cyberterrOrism (E)UropeanResearch AGEnda consortium will deliver a measured, comprehensive, relevant research agenda for Cyber Crime and Cyber Terrorism. Based on three pillars:
  - user centric methodology, to identify gaps, challenges and barriers based on real-world needs and experiences,
  - taxonomy to create a common understanding of the subject CC/CT,

  - market oriented approach, to foster practical implementations of countermeasures using effective test and validation solutions.
- SEGRID (matchende financiering uit VP Security)
  The project Security for smart Electricity GRIDs is co-ordinated by TNO; its main objective is to enhance the protection of smart grids against cyber-attacks. The project consortium does this by applying a risk management analysis approach to a number of smart grid use cases (the SEGRID use cases), which will define security requirements and determine gaps in current security technologies, standards and regulations. The identified gaps and the analysis itself will give input to the enhancement of risk assessment methodologies and the development of novel security measures for smart grids.

4 Vraaggestuurde interactie

4.1 Programmering

Het voorliggende programma is opgesteld met input uit vele bronnen bij de professionele veiligheidsorganisaties, de departementen Veiligheid en Justitie en Defensie en The Hague Security Delta. Verder is het programma afgestemd met de TNO-strategie voor het Thema Defensie en Veiligheid. Vervolgens zijn TNO en VenJ het eens geworden over de inhoud en de aansturing van het programma voor de indiening van het voorstel bij EZ. Inmiddels zijn voor de drie lopende kennisprojecten voor respectievelijk Informatievoorziening, Procesinnovatie voor performance-verbetering en Cybersecurity & societal resilience begeleidings-groepen opgezet.

Het ministerie VenJ geeft in het kader van haar periodieke oproep voor innovatievoorstellen de gelegenheid tot het indienen van ideeën voor nieuwe ontwikkelingen in het kader van het VP Veilige Maatschappij.
Hiermee kan de aansluiting met de toekomstige behoeften van het operationele veiligheidsveld worden versterkt. De door VenJ verzamelde ideeën worden gebruikt worden voor de formulering en de jaarlijkse bijstelling van het VP. Bij uitzondering kunnen tussentijdse voorstellen – als de actualiteit dit nodig maakt en mits het van strategisch belang is om erop in te spelen – tot aanpassing van de onderzoeksplannen leiden.

Op basis van deze programmabijstelling zullen interacties met de potentiële gebruikers plaatsvinden in de maanden oktober en november, zodat per 1 december de projectplannen voor 2015 kunnen worden vastgesteld.

4.2 Betrokkenheid van de operationele veiligheidsorganisaties bij de uitvoering

Voor de VP-kennisprojecten is aansluiting bij de behoeften van de publieke veiligheidsorganisaties essentieel. Naast individuele vertegenwoordigers van deze organisaties worden ook de bestaande netwerken zo goed mogelijk benut.
In werkbijeenkomsten worden afspraken gemaakt over de betrokkenheid van partners uit de praktijk (tijd, expertise, experimenten).

Met de afronding van het eerste jaar in het vooruitzicht zullen er afspraken worden gemaakt over de communicatie over resultaten (opties: website, infographics, nieuwsbrief, etc.).

4.3 Ontwikkeling innovatieclusters

De vorming van de innovatieclusters zal nader worden ingevuld. Aandachtspunten zijn de optimale aansluiting bij bestaande netwerken in het veiligheidsdomein en de (door-)ontwikkeling van consortia. Ook het faciliteren van harmonisatie van informatievoorziening en samenwerkingsprocessen is daarbij aan de orde.
Het uitbouwen van de samenwerking in het DRIVER-consortium is voor het innovatiecluster Crisismanagement een belangrijk issue. Onderzocht wordt of dit voor nog twee innovatieclusters kan worden geïnitieerd.

5 Programma 2016

5.1 VP-VM-onderdeel Informatievoorziening

Motivatie
In 2015 is aansluiting ontwikkeld met de volgende bij het Innovatieteam van VenJ ingediende onderzoeksbehoeften:

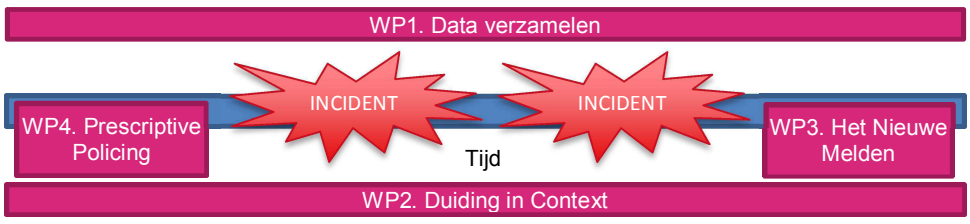
- Big data analytics voor opsporen verdachte transacties in chemicaliën-handel in relatie drugs en explosieven. (H. Hali/O.Pouw, Nat Politie / A'dam);
- Tools voor herkenning radicaliserende, haat-zaaiende, jihadistische online propaganda op internet. (K. Schoonen, Nat Politie / A'dam);
- Verminderen leeslast voor analisten - Duiden van samenhang tussen incidenten/ context (H. Hali/O.Pouw, Nat Politie /Adam);
- Ontwikkel referentiemodel voor communicatiekanalen tussen meldkamer/ professionals/ bedrijfsleven/ burgers i.r.t. noodhulpverlening (E. Beld, LMO);

In diverse workshops en bijeenkomsten is gebleken dat onze aanpak op deze onderwerpen door een veel breder publiek wordt gedragen, door o.a. DG Pol, DG RR, Inspectie SZW, Landelijk Parket, NCTV, OM, NP, Politie-academie en enkele Veiligheidsregio's.

De gemene deler onder de genoemde stakeholders is dat de juiste informatie beschikbaar moet zijn op het juiste moment in het juiste format bij de juiste persoon met de juiste actie tot gevolg, zonder dat er informatie-overload ontstaat. De eerste stap met betrekking tot "de juiste informatie" is direct één van de meest lastige stappen in het kader van doorgaans ongestructureerde data binnen diverse externe bronnen, zoals web-content, sociale media, en meldingen van burgers. Het belang van deze bronnen neemt ogenschijnlijk even snel toe als de complexiteit van deze bronnen. Deze complexiteit uit zich in toename van omvang van (online) bericht-gevingen, potentiële samenhang tussen deze berichtgevingen, en onduidelijkheid in betekenisgeving van deze berichtgevingen.

In dit kader richt het project Informatievoorziening zich op het duiden van deze doorgaans ongestructureerde data ten behoeve van het verkrijgen van actiegerichte informatie. De inhoud van dit VP-onderdeel wordt afgestemd op onder andere het defensie doelfinancieringsprogramma "Big data & Intelligence".

Inhoud
De overall focus van het project Informatievoorziening ligt op informatieverwerking en duiding (Big data), ofwel: hoe kan inzicht worden verkregen uit de beschikbare informatie uit vele bronnen en kan deze optimaal worden benut voor sturing en support van het handelen van veiligheids- en opsporingsdiensten op diverse niveaus.
Voor 2016 zijn er diverse mogelijkheden ter verdieping en/of verbreding van de vier in 2015 gedefinieerde werkpakketten (zoals weergegeven in onderstaande figuur).



WP1. Data verzamelen
In 2015 is de basis gelegd voor het ontwikkelen van een platform om gericht data te verzamelen uit complexe (open)bronnen. Op dit platform is reeds een “Proof of Principle” ontwikkeld voor een data-analyse-methodiek gericht op online detectie van nieuwe vormen van drugs. Last but not least is een aanzet tot een MoU gemaakt m.b.t. juridische en ethische afwegingen als onderdeel van een richtlijn t.a.v. “hoe om te gaan met data uit open bronnen”.

- Verdieping:
  - Verschillende methodieken om de omvang van online drugs-handel te bepalen;
    - Hoe substantieel is die handel eigenlijk?
    - Legitimiteit voor het opsporen;
- Verbreding:
  - Ontwikkelen roadmap voor Dark Web Research ;

Voor beide invullingen geldt dat ook in 2016 deze dataverzameling (aan de voorzijde van de informatieketen) een cruciaal onderwerp voor meerdere organisaties in de veiligheidsketen zal zijn.

WP2. Duiding in context
In 2015 is de basis gelegd voor het ontwikkelen van een Prototype/ Proof of Principle t.a.v. het gebruik van scenario/ scripting methodiek om context zowel qua netwerk als sequentie van gebeurtenissen te duiden; gekozen is voor ontwikkeling aan de hand van een praktijkprobleem.

- Verdieping:
  - Toewerken naar “Proof of concept"
  - Dieper in het praktijkprobleem duiken, met echte data, daadwerkelijk model van expertkennis tot het duiden ervan, meerdere malen beproefd, en potentiële koppeling met bestaande systemen;
- Verbreding:
  - Proof of principle van de scenario/ scripting methode uitwerken voor andere domeinen

Voor beide invullingen geldt dat ook in 2016 deze duiding van context een cruciaal onderwerp voor meerdere veiligheidsorganisaties zal zijn. Reeds nu is het OM geïnteresseerd in de verdiepingsslag, en zien Inspectie SZW en het NCTV toegevoegde waarde om het huidige principe in hun domein te toetsen.

WP3. Het Nieuwe Melden
In 2015 is de basis gelegd voor het ontwikkelen van een visie en roadmap voor “Het Nieuwe Melden”. Als kernvraag is genomen: het slimmer organiseren en benutten van de capaciteiten en informatie van burgers en bedrijven voor het adequaat inspelen op veiligheidsincidenten. De onderscheiden aanknopingspunten voor verdere kennisontwikkeling zullen medio november worden besproken met meerdere stakeholders.
Feiten zijn dat 112 een vitale infrastructuur is, dat de groei aan data binnen dit domein zal toenemen, en dat dilemma’s op het gebied van publieke-private samenwerking vragen om heldere afwegingen.

WP4. Prescriptive Policing
Onderzoek naar Prescriptive policing, lees: een handleiding/ roadmap voor het gebruik van predictive policing, was in 2015 niet direct gekoppeld aan een ingediende onderzoeksbehoefte. Desalniettemin bleek gedurende het jaar dat er op dit vlak diverse vraagstukken bij meerdere veiligheidsorganisaties spelen:

- Welk type technologische ontwikkelingen spelen er zo al?
- Welke impact/ meerwaarde heeft het mogelijk voor mijn organisatie?
- Welke impact heeft het mogelijk op welke processen?
- Welke verdere verwachtingen en eisen zijn er zo al?

In 2015 wordt daarom verkend wat de meerwaarde kan zijn van predictive policing voor politie doeleinden en voor bewaken en beveiligen doeleinden. Naar verwachting zal dit onderwerp op dit domein en ook op andere domeinen (zoals voorspellen van de volgende brand) via andere wegen dan het project Informatievoorziening verder worden onderzocht. Indien noodzakelijk/ gewenst kunnen onderdelen mogelijk alsnog worden ondergebracht bij het project Informatievoorziening.

Doelgroepen en beoogde impact
De volgende veiligheidssectoren hebben potentieel belang en zijn al betrokken bij het project Informatievoorziening:

- Politie; Dreigings- en risico analyses, vroeg-signalering, inlichtingen, opsporing: slechts enkele aspecten waar diverse onderdelen van de KLPD mee te maken hebben.
- LMO; de LMO fungeert dadelijk als een centraal informatieknooppunt waar een reeks aan burgermeldingen via diverse (multimodale) kanalen binnenkomt, waar potentiële interactie met deze burger(s) plaatsvindt, en waar een eerste aansturing van professionals uitgaat.
- Veiligheidsregio's; diverse VRs proeven momenteel aan het gebruik van digitale informatievoorziening voor een stukje Business Intelligence: op basis van het combineren van databronnen achterhalen waar potentiële (brand)haarden zich het meest waarschijnlijk voordoen, en op basis van deze informatie de eigen organisatie aanpassen.

Daarnaast zijn de resultaten ook relevant voor;

- KMAR.
- NCTV-VenJ.
- Defensie.

In 2016 zal verder worden onderzocht hoe de aansluiting bij de stakeholders van de DG's RR, SB en VZ van het ministerie VenJ kan worden versterkt. Daarbij zullen ook instellingen als het OM en het landelijk parket betrokken worden.

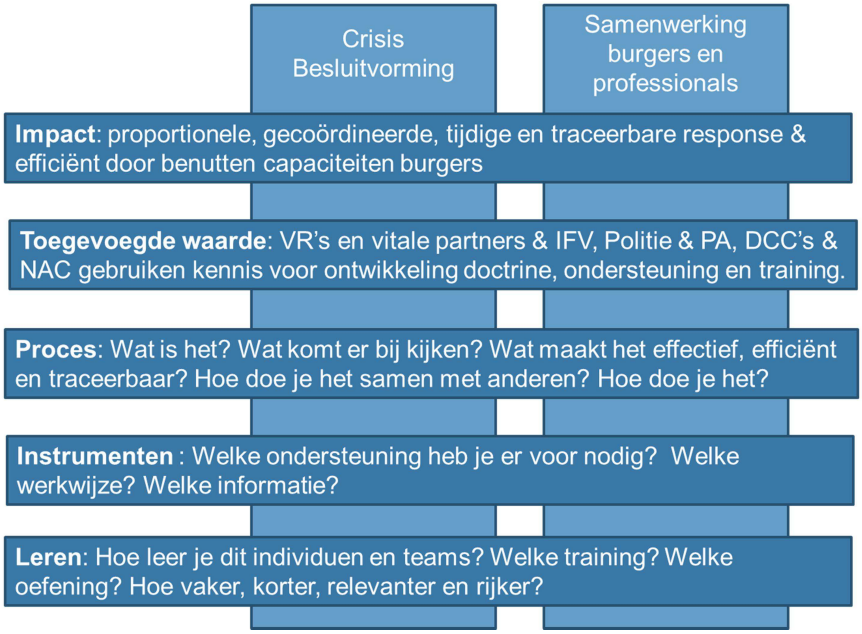
5.2 VP-VM-onderdeel Procesinnovatie voor performance-verbetering

Motivatie
Het VP onderdeel Procesinnovatie voor performance-verbetering richt zich op de ontwikkeling van breed toepasbare kennis en innovaties voor crisisbesluitvorming en samenwerking binnen en tussen organisaties en met burgers en laat dit landen met stakeholders in gezamenlijke innovatieprogramma's.

Uit de bij het Innovatieteam van VenJ door publieke veiligheidsorganisaties ingediende onderzoekbehoeften zijn belangrijke aanknopingspunten geïdentificeerd voor het programma in 2015:

- Ketensamenwerking voor handhaving van veiligheid in verschillende domeinen, met flexibel infodelings-systeem voor snelle interventies.
- Infovoorziening voor crisismanagement bij overstromingen.
- Voorbereiding van burgers op overstromingen.
- Flexibele, realistische, deels mobiele trainingsobjecten voor beeldvorming en besluitvorming onder tijdsdruk.
- Doorontwikkeling van Risk Based Security Model en daarbij passende state-of-the-art maatregelen en informatieprocessen.

In diverse workshops en bijeenkomsten zijn voor het onderzoek in dit VP-onderdeel twee centrale vraagstukken gedefinieerd:



1. <u>Samenwerking: professionals & burgers</u>
   In de Strategische Agenda voor Versterking van de veiligheidsregio's (Veiligheidsberaad, 16 mei 2014) is "samenwerking in de regio: versterking interdisciplinaire en intersectorale samenwerking" als belangrijk item onderkend. Naast multidisciplinaire samenwerking tussen hulpdiensten wordt het steeds belangrijker om capaciteiten van andere sectoren en burgers te kunnen benutten. Dat geldt zowel tijdens een crisis als ook daarvoor en erna. Daarom maken we samenwerking tussen professionals en burgers inzichtelijk. Wanneer is samenwerken nuttig? Welke samenwerkingsvormen zijn er? Hoe samenwerking te organiseren? Hoe ervaring op te doen en hoe leren? Inzicht hierin gebruiken we voor de ontwikkeling van ondersteunende instrumenten en nieuwe trainingsconcepten.

2. Gezamenlijke besluitvorming
   Crisisorganisaties werken continu aan het verbeteren van crisisbeheersing. Het vergroten van het besluitvormend vermogen betekent het sneller kunnen doorlopen van de loop informatie verzamelen > beeldvorming, oordeelsvorming, beslissen > leiding & coördinatie > actie > actie evaluatie. De focus lag de afgelopen jaren bij de gezamenlijke beeldvorming. Als resultaat daarvan wordt informatie over incidenten steeds beter gedeeld tussen operationele partijen en ook worden er stappen gezet om de beeldvorming met bedrijven en burgers beter te delen.
   Een gedeeld beeld van een incident is echter niet voldoende om te komen tot een goed afgestemd plan van aanpak voor een crisis, ramp of incident. Hiervoor is meer grip op oordeelsvorming nodig met een objectieve afweging van opties voor inzet van capaciteiten, te betrekken partijen, te bereiken doelen en te verdelen taken. Hoewel het beoogde effect van de inzet vaak helder is (beperken van schade, slachtoffers en ontwrichting), is de manier waarop dat kan, en met wie, divers. Diversiteit en creativiteit zijn dan ook van belang bij oordeelsvorming, net als snelheid. Om crisisbesluitvorming te innoveren maken we wij het oordeelsvormingsproces inzichtelijk. Wat is het? Waar gaat het over? Hoe verloopt het? Wat betekent het voor beeldvorming en beslissen? Hoe doe je het samen met anderen? Wat maakt het flexibel, effectief, efficiënt en traceerbaar? Deze inzichten gebruiken we voor de ontwikkeling van ondersteunende instrumenten en trainingsconcepten.

De inhoud van dit VP-onderdeel is afgestemd op het parallel in uitvoering zijnde doelfinancieringsprogramma van Defensie: “Informatievoorziening als operationele capaciteit (V1517)”. Hierin loopt het project Federatief Digitaal SamenWerken (FDSW) dat zich richt op het versnellen van informatie-uitwisseling tussen defensie en civiele partijen in uitzendgebied en nationaal. Dit defensieprogramma richt zich meer op het technische vlak terwijl het VP-onderdeel Procesinnovatie voor prestatie-verbetering zich meer richt op de mens en het proces in de samenwerking.

Inhoud
Van de gedefinieerde vraagstukken zijn de onderstaande onderzoeksvragen afgeleid:

- Wat is een effectief en efficiënt oordeelsvormingsproces, waarbij samenwerking tussen partners en dynamische belangenafweging centraal staan?
- Welke nieuwe trainingsconcepten (methode en tools) ondersteunen het individu en de samenwerking in een team, alsmede het snel implementeren van het oordeelsvormingsproces?
- Wat zijn effectieve vormen van samenwerking tussen professionals en burgers?
- Hoe ziet een leer en experimenteer omgeving er uit waarin samenwerkende partijen vaker, een korte, relevante en rijke ervaring krijgen.

De werkpakketten zijn:

1. Gezamenlijke oordeelsvorming
   Er wordt een nieuw model ontwikkeld voor een gecoördineerd, effectief, efficiënt, traceerbaar oordeelsvormingsproces bij de besluitvorming tijdens crises. Met het eind dit jaar op te leveren boekje “Innovatie van oordeelsvorming bij crisismanagement” zullen operationele veiligheidsorganisaties handvaten

krijgen om initiatieven te nemen voor het ontwikkelen van doctrines, operatie-ondersteunende tools en het helder krijgen van trainingsbehoeften.
De concretisering en ondersteuning daarvan staat centraal voor 2016.
Het zwaartepunt van de nu betrokken doelgroepen ligt bij de veiligheidsregio's en het Instituut voor Fysieke Veiligheid; in 2016 zal aandacht gegeven worden aan de vertaling naar meerwaarde voor de Politie en de Politie-academie en voor de Departementale CoördinatieCentra voor crisisbeheersing en de Nationale Academie Crisisbeheersing.

2. Training modules oordeelsvorming
   In dit werkpakket worden modules ontwikkeld om individuen en teams te trainen in oordeelsvorming en een analyse instrument om het effect te meten. Op de in 2015 ontwikkelde aanzet met casussen met de veiligheidsregio's Groningen, Friesland en Drenthe zal in 2016 een proces voor het op maat maken van trainingen aandacht krijgen. Dit zal ook worden ingebracht in het EU-project DRIVER, waar een testbed voor crisismanagementtools op Europees niveau ontwikkeld wordt.

3. Samenwerking professionals en burgers
   In dit werkpakket richt zich op het grip krijgen op het samenwerkingsproces van burgers en professionals / burgerparticipatie inclusief het voorzien in de informatie behoefte voor verhogen van de weerbaarheid van en burgers en werkwijzen voor het benutten van de capaciteiten van burgers voor veiligheidstaken. Hierbij wordt samengewerkt met de veiligheidsregio's IJsselland en Haaglanden.
   In 2016 wordt een methode ontwikkeld voor het maken van samenredzaamheids-oplossingen op maat. Hiermee zal worden geëxperimenteerd in casussen met samenwerking van veiligheidsregio, politie en burgers. Onderdeel daarvan zal het ontwikkelen van een impact dashboard zijn en een werkwijze daarvoor. Samenredzaamheid- concepten zullen in de aanpalende EU-projecten (COBACORE/DRIVER en INSPECT/BART) doorontwikkeld worden.

4. Leer & ervaringsomgeving (LEE): benutten elkaars capaciteiten
   Dit werkpakket richt zich op het ontwikkelen van een visie op een gezamenlijke leer & ervaringsomgeving (LEE) waarin crisisorganisaties vaker een korte, relevante en rijke ervaring op kunnen doen m.b.t. benutten van elkaars capaciteiten (bijvoorbeeld civiel-militaire samenwerking).

Doelgroepen en beoogde impact
De volgende veiligheidssectoren hebben belang bij de ontwikkelingen in dit VP onderdeel Proces Innovatie:

- Veiligheidsregio's, moeten met steeds meer partijen samenwerken in dynamische settings. Met nieuwe manieren van samenwerken verhogen zij hun effectiviteit door de betrokken (onbekende) partners op de juiste manier te betrekken en in te zetten.
- NCTV-VenJ. Steeds vaker vinden er incidenten plaats die een groot deel van Nederland raken. Het betreft a-typische incidenten (denk aan MH17) waarbij ook naar het rijk gekeken wordt. Bij de voorgestelde samenwerking is natuurlijk ook ruimte voor VenJ, zonder van het rijk direct overal voor verantwoordelijk wordt als dat niet noodzakelijk is.

- Politie. Crisisbeheersing is vooral een kerntaak van de brandweer. De samenwerking met de politie is in de laatste jaren belangrijker geworden, terwijl ook de politie enkele malen geconfronteerd werd met een situatie met grootschalige maatschappelijke onrust. Het slim delen van informatie en capaciteiten is breed van belang.
- Koninklijke Marechaussee zoekt naar nieuwe samenwerkingsmogelijkheden bij grensbewaking en mainports. Daarbij zijn het bedrijfsleven en reizigers (burgers) belangrijke doelgroepen.
- Bedrijfsleven. Het bedrijfsleven is door haar betrokkenheid bij incidenten steeds vaker een partner voor de hulpdiensten; (denk aan Chemiepack). Zij kunnen (lang niet altijd) mee-oefenen met de hulpdiensten. Toch moet deze groep bewust worden van de risico's en hun handelingsperspectief, mocht het fout gaan. Tijdsefficiëntie is daarbij van groot belang, zowel voor het bedrijfsleven als voor de partijen in de veiligheidssectoren. Daarnaast kan het bedrijfsleven natuurlijk ondersteunen als leverancier van ondersteuningsmiddelen.

5.3 VP-VM-onderdeel Cybersecurity en societal resilience

Motivatie
Het belang van ICT voor vrijwel alle processen en diensten in onze moderne samenleving maakt het onderwerp cybersecurity van groot belang voor vrijwel iedere organisatie en elk bedrijf. Hierbij geldt dat het regelen van een goed niveau van cybersecurity allereerst een verantwoordelijkheid is van de afzonderlijke organisaties ; innovatief onderzoek op dit gebied voor het bedrijfsleven vindt plaats in het kader van het VP onderdeel Cyber risk management & technical resilience van het VP Security.
Er zijn echter ook belangen die de verantwoordelijkheid van de afzonderlijke organisaties te boven gaat, wanneer cyber verstoringen kunnen leiden tot een veel bredere impact in de maatschappij. In het VP-onderdeel Cybersecurity en societal resilience wordt daarom aandacht besteed aan:

- Grootschalige maatschappelijke ontwrichting door cyberverstoringen in de vitale infrastructuur en de daarbij optredende keteneffecten. Om ondersteuning te kunnen bieden voor de gehele OODA loop dient er een inzicht te worden verkregen in de cybersecurity status van de verschillende vitale sectoren, de mogelijke maatschappelijke impact van cyberverstoringen, de effectiviteit van mogelijke maatregelen en het handelingsperspectief van personeel.
- De kwetsbaarheid van burgers en kwetsbare groepen door blootstelling aan cyberrisico’s.
- De aangrijpingspunten en impact van cyberdreigingen op procesketens (security of the supply chain) en genetwerkte organisaties.

De inhoud van dit VP-onderdeel wordt afgestemd op het defensie doelfinancieringsprogrammma dat zich richt cybersecurity in het militaire domein.

Inhoud en onderzoeksvragen
In dit VP-onderdeel worden tools en modellen ontwikkeld voor het beter kunnen analyseren en handelen bij grootschalige verstoringen in complexe omgevingen door cyberincidenten met een kans op substantiële maatschappelijke ontwrichting.

Het onderzoek richt zich op de volgende elementen:

- Situational awareness: Om snel en goed te kunnen reageren is het van belang om een gezamenlijk beeld van de stand van zaken te hebben. De ontwikkelingen in 2015 zijn hierop gericht. Het gaat hierbij niet alleen om de status op technisch niveau, maar vooral het analyseren en inschatten van de potentiële impact van verstoringen op sector- en cross-sector niveau. Naast het belang tijdens crisismanagement zou dit ook in de voorbereidende fase kunnen door het ontwikkelen van een cyber risico of infrakaart voor strategisch-tactisch niveau. De onderzoeksvraag voor 2016 wordt voor dit element nog geformuleerd. Mogelijke focus is het in kaart brengen van de (nationale en internationale) internetknooppunten en hun importantie voor de Nederlandse infrastructuur zodat effecten en prioriteitstelling in geval van verstoringen efficiënter en effectiever te bepalen is. Een andere en bredere vraagstelling kan zijn wat de cyber-vitale infrastructuur in Nederland is en in hoeverre het beheer en eigendom van buitenlandse organisaties een risico vormt voor de weerbaarheid van de Nederlandse samenleving.
- Kwantitatieve modellen: voor effectief beleid is het van belang om te beschikken over de juiste uitgangspunten en getallen. In het cyber domein zijn dit soort schattingen tot op heden niet betrouwbaar gebleken voor het kunnen maken van afwegingen over de te nemen maatregelen. In 2016 zal de bruikbaarheid van de resultaten van het onderzoek in de jaren 2014/2015 worden getoetst aan de hand van een onderwerp uit het komende, binnenkort te publiceren Cybersecuritybeeld Nederland (CSBN-5) te nemen en dit te onderbouwen met trends en data afkomstig van kwantitatieve modellen en analyses.
- Opleiden, trainen en oefenen: Naast het hebben van de juiste techniek en uitvoeren van een passend proces is het van groot belang cybersecurity professionals in organisaties bekwaam te laten handelen in het geval van voorzienbare cyberdreigingen en cyberincidenten. Veel organisaties worstelen echter hoe dit voor hun personeel op een juiste wijze vorm te geven, om over een uniforme standaard en eenzelfde palet aan opleidingen nog maar te zwijgen. De onderzoeksvraag is of een Software Defined O&T ontwikkelfaciliteit dat dynamisch configureerbaar is aan een specifieke vraag van een (netwerk van) organisatie(s) hiertoe een belangrijke bijdrage kan leveren.
- In 2015 is een onderzoek naar de haalbaarheid van een Nederlandse Civil Cyber Watch uitgevoerd. Daarbij is vooral gekeken naar een situatie van grootschalige incidenten die in Nederland (gelukkig) relatief weinig voorkomen. Wel zijn kleinere cyber-incidenten aan de orde van de dag, maar het ontbreekt (bijvoorbeeld) de politie om hier met voldoende mankracht, kennis en kunde adequate opvolging aan te kunnen geven. Hierdoor worden de mogelijkheden tot onderzoek en eventuele vervolging beperkt en krijgt de maatschappij de indruk dat er niets mee gedaan wordt. Een passende onderzoeksvraag hierbij is of een vrijwillige cyber-politie hierbij een oplossing kan bieden.
- Attributie - inclusief daderidentificering - van cyberincidenten is vaak moeilijk, terwijl er wel veel belang aan wordt gehecht. Een analyse van good-practices naar methoden en technieken van attributiebepaling kan cyber security professionals helpen in een betere attributiebepaling.
- Praktijkgericht onderzoek naar specifieke en gedeelde trends bij de stakeholders van het NCSC (nader af te stemmen wat deze zijn). Een voorbeeld is security van de supply chain in de Rotterdamse haven.
- Daarnaast richt dit VP-onderdeel zich op de bescherming van burgers en kwetsbare groepen in cyberspace. Zo laten recente onderzoeken zien dat

jongeren veelvuldig bloot staan aan “grooming” in digitale omgevingen. Handhaving op internet, waar veel ongewenst en onveilig gedrag plaatsvindt, ontbreekt, en is bovendien lastig omdat er geen gedeelde normen, waarden of regels zijn voor online gedrag. In deze onderzoekslijn worden methoden onderzocht om ongewenst en onveilig gedrag op internet te herkennen en te bestrijden.

In de maanden september/oktober 2015 zal in overleg met de stakeholders de focus opnieuw tegen het licht worden gehouden; indien daar aanleiding toe is kunnen ook nog andere onderwerpen dan de bovenstaande in overweging worden genomen. .

Samenwerking met publieke en private stakeholders

Bij het verder vorm geven van de inhoud van het VP zal samenwerking worden gezocht met een aantal publieke en private stakeholders. Deze brede community van stakeholders bestaat uit een primaire (geconsulteerde) en secundaire (geïnformeerde) groep belanghebbenden:

Primair

- NCSC, o.a. in samenwerking met het CSBN en het programma “kritieke cyber belangen”.
- NENCyS, het Nationaal Expertise Netwerk Cyber-Security (in oprichting). Een netwerk dat Nederland veiliger maakt door deelnemers met verschillende achtergronden uit uiteenlopende organisaties de mogelijkheid te bieden om onderling informatie uit te wisselen in een veilige en vertrouwde omgeving. De plek waar experts mede-experts met gelijke interesses en belangen (virtueel) ontmoeten om eigen ideeën te toetsen of aan te vullen en maximaal gebruik te maken van elkaars expertise.
- De stakeholders van het NCSC; waarin in het geval van het beheer van de vitale infrastructuur in Nederland specifiek wordt gekeken naar de deelnemers van de Information Sharing and Analysis Centers (ISACs). Zij vormen de uiteindelijke doelgroep die onze maatschappij op directe wijze meer cyber resilient kan maken.
- Nationale Politie (onder andere Team High Tech Crime) en Politieacademie. Zij beschikken over de kennis en ervaring uit de praktijk van veel voorkomende en/of impactvolle cybercrime incidenten.
- Defensie Cyber Commando en het Defensie Cyber Expertise Centrum. Defensie heeft belang bij het weerbaarder maken van Nederland om het tegenstanders in het digitale domein lastiger te maken succesvolle aanvallen uit te voeren. Defensie werkt daarom nauw samen met o.a. het NCSC.

Secundair

- Samenwerking met universiteiten binnen de TNO Cyber Security Cooperation, met name samenwerking met de Universiteit Twente, en de TU Delft,
- Cyber Security Raad (CSR), de cyber security raad zal zich meer en meer gaan richten op toekomstige vragen, die voorbij de horizon van NCSS II liggen. TNO kan hierbij fungeren als belangrijke gesprekspartner.
- Samenwerking met NIS platform (EU).
- Samenwerking in internationale consortia binnen verschillende EU projecten (CYSPA, COURAGE, CAPITAL).

5.4 VP-VM-onderdeel Real Time Intelligence

Motivatie
High Reliability Organisaties belast met de uitvoering van veiligheidstaken, zoals politie, veiligheidsregio's en het meldkamerdomein, staan voor de uitdaging om meer veiligheid te leveren in een toenemend complexe maatschappij. En in tijden waarin er eerder minder dan meer geld beschikbaar is -voor hun taken- betekent dat ook: met minder mensen meer moeten doen.

In antwoord op deze maatschappelijke uitdaging, zien we de rol van informatiesturing toenemen binnen de veiligheidsketen. Informatiesturing binnen bijvoorbeeld politie, brandweer en GHOR in het veiligheidsveld, maar ook met gemeenten en beveiligingsbedrijven. En vooral ook in de *samenwerking* tussen de partijen. In een netcentrisch samenspel tussen systemen, organisaties en mensen. Veiligheid is al lang niet alleen meer iets van de fysieke wereld. Ook de virtuele wereld van internet en social media speelt een steeds belangrijker rol. En daarmee komt de burger als onderdeel van het 'systeem' ook in beeld.

In het Vraaggestuurd Programma Security voor het roadmapteam Security in de topsector High Tech Systems & Materials is bovenstaande uitdaging in publiek-private samenwerking opgepakt. Door de intensieve interactie met politie en andere operationele veiligheidsorganisaties is er daarbij draagvlak gegroeid voor een Real Time Intelligence Lab, waar met name geëxperimenteerd kan worden met nieuwe benaderingen en tools voor de ondersteuning van veiligheidsoperaties. Dit zgn. RTI-lab zal als spin off van de ontwikkelingen in het VP Security worden doorontwikkeld in het VP Veilige Maatschappij. In het VP-Security zal de focus blijven liggen op innovatietrajecten voor vraagstukken met perspectief op substantiële betrokkenheid van private stakeholders naast de overheidspartijen; zonodig zal ook validatie van in het VP Security te ontwikkelen concepten voor specifieke consortia in het RTI-lab kunnen plaatsvinden.

Real Time Intelligence:
Onder de noemer 'Real Time Intelligence' zijn politie, maar ook andere spelers uit de veiligheidsketen informatiesturing gestalte aan het geven in het meldkamer-domein. En door (real time) informatie te combineren met kennis, wordt voorspellend vermogen verkregen, zodat betere besluiten voor de aansturing van operationele taken kunnen worden genomen. Naast organisatorische veranderingen gaat de interesse uit naar het slim combineren van data uit verschillende open en gesloten bronnen. Dat kan sensordata zijn in de vorm van bijvoorbeeld videofeeds, maar ook locatiegegevens van telefoons, informatie uit basisadministraties,
of bronnen als websites en Twitter. In het real time combineren van deze bronnen schuilt de kracht met als beoogd resultaat: 'first time right'.

Inhoud
Dit VP-onderdeel richt zich op de ontwikkeling van een *Thematisch Quadruple Helix Netwerk en experimenteeromgeving* onder de noemer 'RTI-lab'. In dit gremium worden vanuit een Thought-leadership positie experimenten geprogrammeerd met een toegepast karakter. Tevens worden projecten gedefinieerd die nog niet gelijk toe zijn aan beproeving, maar die wel binnen 1-2 jaar zover kunnen zijn. Inhoudelijk richten de projecten en het RTI-lab zich op de volgende inhoudelijke pijlers:

- *RTI door informatie te delen tussen organisaties.* Bijvoorbeeld datafusie van bronnen rond de Internationale Zone, of voor Overstromingsdreiging.
- *RTI door samen te werken met burgers.* Bijvoorbeeld inrichten dialoog via sociale media.
- *RTI aan het eindpunt*: effectief en efficiënt intelligence beschikbaar maken bij de professional op straat. Bijvoorbeeld head-up displays voor first-responders.
- *RTI bij het coördinatiepunt*: effectief en efficiënt intelligence beschikbaar maken in het Operations Centre (of meldkamer). Bijvoorbeeld expert-systems voor vermissingen, of toepassing Multitouch-table.

Samenwerking met publieke en private stakeholders – RTI-lab:
TNO vormt samen met de politie, The Hague Security Delta en de Landelijke Meldkamer Organisatie (LMO) de 'Initiatiefgroep RTI-lab', die werkt aan de doorontwikkeling van het RTI-lab:

- Het RTI-lab voorziet in de behoefte om evidence based te werken aan de ontwikkeling van RTI binnen het Openbare Orde en Veiligheidsdomein. Het doel van het RTI-lab is om de toegevoegde waarde te bepalen van nieuwe concepten, technologie en processen. Het lab is dus (ook) een fysieke plek, waar alternatieve opties aan de werkelijkheid worden getoetst.
- Het RTI-lab als netwerk: Het RTI-lab bestaat ook uit een netwerk van professionals uit kennisinstituten, industrie en politie. Ook burgers of wijkbewoners worden betrokken. Vragen uit de politiepraktijk, succesvolle concepten uit andere toepassingsdomeinen, nieuwe technologieën uit bedrijfsleven en ideeën van burgers moeten elkaar zo gaan 'kruisbestuiven'. Leidend tot een vruchtbare grond voor vernieuwing.
- Waarde aantonen: Wat levert een nieuwe werkwijze, product of dienst op? Voor Operationele efficiëntie en effectiviteit. In hoeverre matcht het met de beoogde informatiearchitectuur? Wat heeft de man/vrouw op straat hieraan? En de burger? En wat is uiteindelijk het effect op het veiligheidsbeeld? Zo gaan we toe naar evidence based policy (beleid gebaseerd op bewezen waarde)
- Programmatisch experimenteren: De kruisbestuiving in het netwerk leidt tot programmering van experimenten rond Real Time Intelligence, waarbij aandacht is voor het operationele, het technische en het menselijke perspectief. Als onderdeel van de initiatieffase van het lab zijn of worden experimenten uitgevoerd, zoals de RTI-Challenge (een toetsingskader voor nieuwe experimenten voor 'Go''No Go'), de RTI-Radar (eerste zicht op de state-of-the-art van RTI wereldwijd voor het richten van de RTI-onderzoeksagenda) en de RTI-experience (bedoeld om publiek RTI te laten ervaren). In het najaar van 2015 worden nieuwe experimenten voorbereid en uitgevoerd rond grootschalig politieoptreden in (Den Haag) en CAS (Amsterdam predictive policing).
- The Hague Security Delta heeft belangrijke voordelen als locatie voor het RTI-lab. Er kan daar een verbinding opgebouwd worden met de HSD-programmalijnen en de initiatieven in het kader van de Nationale Innovatie Agenda Veiligheid.

Een belangrijke kennispartner voor het RTI-lab is de Politieacademie (lectoraat Intelligence). Daarnaast wordt voor specifieke onderzoeksvragen samengewerkt met:

- VR Hollands Midden, VR Zuid-Holland Zuid, HKV en Centric in het kader van *Informatiepreparatie.*
- Politieacademie, TUDelft, CGI en politie in het kader van *BART.*

- Politieacademie, politie en diverse bedrijven in het kader van *Predictive Policing.*
- Security Officers van Europol, Eurojust, OPCW & ICTY, Thales, Siemens, Gemeente Den Haag en politie in het kader van de *Internationale Zone (project in VP Security).*

5.5 VP-VM-onderdeel verkenning voor de DG's RR, SB en VZ

In de achterliggende jaren is de relatie van TNO met de DG's NCTV en Politie in concrete samenwerkingsprojecten en programma's sterk gegroeid. De interactie met de DG's RR, SB en VZ beperkte zich tot een aantal actuele onderwerpen; voorbeelden daarvan zijn:

- De ontwikkeling van het grensbewakingssysteem Mobiel Informatiegestuurd Optreden (@migo-Boras) voor versterking van het oezicht op vreemdelingenverkeer en drugssmokkel.
- Intelligence voor de aanpak van Mobiel banditisme door versterking van de samenwerking in de handhavings- en rechtsketen (zie blz 32 van rapport op https://www.tno.nl/media/3971/p102.pdf en blz 33 van rapport op https://www.tno.nl/media/5024/thema_maatschappelijke_veiligheid_2014.pdf).
- Dark Web monitoring (lopend onderzoek,zie https://www.tno.nl/media/4016/thema_maatschappelijke_veiligheid_program_2015.pdf)
- Bewaken en beveiligen voor DJI en PI's.
- Radicalisering onderkennen en beïnvloeden om te deradicaliseren.
- Bescherming jeugd tegen 'grooming' en andere risico's op het gebied van cybersafety.

Deze contacten betroffen advisering voor actuele beleidsvragen en operationele behoeften. De visie van het ministerie VenJ is dat een structurele benadering van innovaties departementsbreed meer aandacht behoeft. Dat is ook de reden dat op topniveau is uitgesproken dat de relatie van het departement en haar veiligheidspartners met TNO een strategischer karakter zou moeten krijgen.

In dit VP zal een verkenning plaatsvinden van de meerwaarde van TNO-expertise voor de DG's RR, SB en VZ. Ook zal voor enkele actuele vraagstukken een verdieping plaatsvinden. In de Memorie van Toelichting op de begroting van het ministerie VenJ zijn onder andere de volgende opties te vinden:

- Samenwerking en informatiedeling voor de aanpak van fraude;
- Verbetering samenspel Politie, OM en GGZ-sector met betrekking tot de omgang met verwarde personen (naar aanleiding zaak Van U. en rapport van Commissie Hoekstra;
- Bestrijding en opsporing cybercrime.

De meest relevante terreinen van TNO-expertise zijn:

- *Waarnemen*: vergaren van informatie met steeds meer, ook mobiele sensoren en duiding van waarnemingen voor operationele acties;
- *Data analyseren*: verwerken van data uit meerdere gesloten en open bronenn tot nuttige informatie en visualisatie van analyseresultaten;
- *Identificeren*: achterhalen van de identiteit in de digitale en de fysieke wereld én beschermen van de privacy;

- *Gedragsanalyse en -beïnvloeding*: inzicht verkrijgen in menselijk(e) gedrag(ingen) en vertalen naar vergroten van de effectiviteit bij toezicht en opsporing;
- *Aansturen*: risk based en informatiegestuurde uitvoering operationele taken;
- *Opvolgen*: interacteren met machines voor informatie(uitwisseling);
- *Informatie-uitwisseling beveiligen*: beveiligen van cyberspace en protocollen voor trusted info-uitwisseling;
- *Acteren in slimme omgeving*: inzetten van intelligente platformen en Infrastructuren;
- *Samenwerking bij complexe taken*: multidisciplinaire besluitvorming en optimaliseren van informatievoorziening in procesketens;
- *Training van nieuwe uitvoeringswijzen*.

6 Ondertekening

Soesterberg, September 2015

Dr. Ir. J.A. Don
Manager Speurwerkprogramma
Maatschappelijke Veiligheid

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