**Integrale 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
infodesk@tno.nl

**TNO-rapport**

**TNO-DV 2011 C293**

# Thema Integrale Veiligheid Vraaggestuurd Programma 2011-2014 VP Veilige Maatschappij Bijstelling 2012

| | |
|---|---|
| Datum | september 2011 |
| Auteur(s) | Dr. ir. J.A. Don |
| Regievoereend departement | Ministerie van Veiligheid en Justitie |
| Projectnummer | 032.32799/01.05 |

Authorisatie door drs. H.G. Geveke, directeur TNO thema Integrale Veiligheid:

# Samenvatting

In het Strategisch Plan 2011-2014 van TNO is het Thema Integrale Veiligheid gericht op een veiliger samenleving. De twee innovatiegebieden binnen dit Thema zijn:

1. Defensie Research
2. Veilige Maatschappij

Voor de ontwikkeling van de strategie en de programmering van het Vraaggestuurde onderzoek voor het Innovatiegebied Defensie Research vindt de afstemming tussen de overheid en TNO plaats onder regie van het Ministerie van Defensie. In dit Meerjarenprogramma 2011-2014 voor het Thema Integrale Veiligheid wordt alleen het Innovatiegebied Veilige Maatschappij verder uitgewerkt.

Veiligheid heeft zich ontwikkeld van een verzameling ad-hoc reacties op incidenten tot een samenhangend complex van maatregelen en effecten. De potentiële impact en het domino-effect van incidenten, maar ook de maatschappelijke kosten/baten van veiligheidsmaatregelen vereisen een integrale op risico en effect gebaseerde aanpak en regie. Perceptie en acceptatie spelen een grote rol in de keuze van oplossingen.
TNO gaat deze uitdagingen aan door te focussen op de volgende proposities:

1. Nationale en grootstedelijke veiligheid
2. Crises en rampen als een grieppandemie, terroristische aanslag, overstroming of elektriciteitsuitval kunnen de maatschappij ontwrichten. TNO ondersteunt overheid en bedrijfsleven om de risico's in kaart te brengen en helpt met oplossingsrichtingen, zoals betere bescherming van vitale infrastructuren met inbegrip van cybersecurity, of grotere zelfredzaamheid van burgers. Op het gebied van grootstedelijke en sociale veiligheid onderzoeken wij met behulp van field labs bovendien de effectiviteit van (voorgenomen) veiligheidsinterventies.
3. Effectieve veiligheidsoperaties
4. Veiligheid heeft zich ontwikkeld van ad-hoc reacties op incidenten tot een samenhangend geheel van maatregelen en effecten. TNO ontwerpt innovatieve toezichtconcepten. Een betere informatiepositie voor iedereen die bij veiligheid is betrokken vereist slim gestructureerde systemen met gebruiksvriendelijke interfaces. TNO helpt om de informatie van burgers optimaal te benutten. Sociale media zijn daarvoor niet meer weg te denken, maar tegelijk een nieuw fenomeen bij crises waarop zorgvuldig ingespeeld moet worden.

Onder regie van Ministerie Veiligheid en Justitie zijn in nauw overleg met behoeftestellers de volgende prioritaire kennis-topics gekozen voor het Vraaggestuurd Programma Veilige Maatschappij 2011-2014:

1. Herkennen afwijkend gedrag,
2. Activering burgers,
3. Slimmer inzetten informatiestromen,
4. Delen informatiestromen/samenwerking,
5. Cybersecurity.

Elk van deze kennistopics is van belang voor meerdere proposities.

In het kader van dit VP zullen er ook verkenningen worden uitgevoerd met als doel de portfolio van kennistopics optimaal matchend met nieuwe ontwikkelingen in de technologie en in het veiligheidsdomein te houden.

In april 2011 heeft het ministerie VenJ per brief aan TNO gevraagd ook in 2012 te focussen op de eerder geselecteerde vijf kennistopics. Het voorliggende plan bevat de samen met stakeholders ontwikkelde focus voor de onderzoeksvragen in de jaren 2011-2014, een tussentijdse voortgangsrapportage over het eerste halfjaar van 2011 en de hoofdlijnen voor 2012 per topic. De topic-plannen voor 2012 zullen voor 1 november 2011 worden uitgewerkt.

**Begin september 2011 werd duidelijk dat in verband met het Topsectorenbeleid van de overheid het budget voor 2012 met 2,7 M€ wordt verminderd. Als consequentie hiervan is een nadere prioriteitsstelling nodig binnen het hier omschreven programma. Het daarvoor benodigde overleg is opgestart.**

# Inhoudsopgave

# 1 Inleiding thema Integrale Veiligheid

## 1.1 Plaats van het Meerjarenprogramma 2011-2014

De TNO-wet 2005 positioneert TNO als een zelfstandige en onafhankelijke organisatie, met als doelstelling het dienstbaar maken van toegepast onderzoek aan algemeen belang en daarbinnen te onderscheiden deelbelangen (artikel 4). De middelen die de wet noemt om deze doelstelling te bereiken zijn (a) het zelf verrichten van onderzoek, (b) het overdragen van resultaten, (c) de samenwerking met andere onderzoeksinstellingen, (d) bijdragen aan de coördinatie van onderzoek en internationale samenwerking en (e) het uitvoeren van opgedragen werkzaamheden (artikel 5).

De wet noemt een Strategisch Plan dat TNO eens in de vier jaar moet maken (artikel 19), rekening houdend met het overheidsbeleid ter zake. Dit plan geeft een uitwerking van de algemene doelstelling op (middel)lange termijn en de voorwaarden die daartoe vervuld moeten worden. Een van die voorwaarden is het uitvoeren van een Meerjarenprogramma.

Jaarlijks wordt daartoe aan TNO van rijkswege een subsidie verstrekt, waarbij nadere regels omtrent de aanvrage kunnen worden bepaald (artikel 21). Als zodanig functioneert de Procedurebeschrijving Overheidsfinanciering TNO (1996). Deze Procedurebeschrijving spreekt over op te stellen en goed te keuren vierjaarlijkse Meerjarenprogramma's, gebaseerd op de hoofdlijnen uit het Strategisch Plan.

## 1.2 Beschrijving van het thema Integrale Veiligheid

In het Strategisch Plan 2011-2014 van TNO is het Thema Integrale Veiligheid gericht op een veiliger samenleving. Veiligheid èn het gevoel van veiligheid zijn meer dan ooit onderhevig aan bedreigingen die voortkomen uit de verdeling van welvaart, botsende opvattingen en toenemende schaarste aan grondstoffen. Wereldwijd zetten defensie, overheden, hulpdiensten en industrie zich in om ons te beschermen tegen steeds minder eenduidige en zichtbare bedreigingen. TNO ondersteunt innovaties om deze activiteiten slimmer, efficiënter en beter beschermd te doen.

Binnen het Thema Integrale Veiligheid heeft TNO twee innovatiegebieden gevormd:

**1. Wereldwijd inzetbare Krijgsmacht**
Defensie staat voor de uitdaging om een duurzaam, dynamisch evenwicht te vinden tussen de ambitie, capaciteiten en beschikbare financiële middelen. Binnen dit innovatiegebied focust TNO op vier samenhangende onderwerpen om Defensie bij deze uitdaging te helpen:

- Kosteneffectief Opereren Krijgsmacht
- Information Superiority
- As Safe As Reasonably Affordable
- Meer Presteren met Minder Mensen

# 2 Veilige maatschappij

Veiligheid heeft zich ontwikkeld van een verzameling ad-hoc reacties op incidenten tot een samenhangend complex van maatregelen en effecten. De potentiële impact en het domino-effect van incidenten, maar ook de maatschappelijke kosten/baten van veiligheidsmaatregelen vereisen een integrale op risico en effect gebaseerde aanpak en regie. Perceptie en acceptatie spelen een grote rol in de keuze van oplossingen.

TNO gaat deze uitdagingen aan door te focussen op de volgende onderwerpen:

*Nationale en grootstedelijke veiligheid*
Crises en rampen als een grieppandemie, terroristische aanslag, overstroming of elektriciteitsuitval kunnen de maatschappij ontwrichten. TNO ondersteunt overheid en bedrijfsleven om de risico's in kaart te brengen en helpt met oplossingsrichtingen, zoals betere bescherming van vitale infrastructuren met inbegrip van cybersecurity, of grotere zelfredzaamheid van burgers. Op het gebied van grootstedelijke en sociale veiligheid onderzoeken wij met behulp van field labs bovendien de effectiviteit van (voorgenomen) veiligheidsinterventies.

*Effectieve veiligheidsoperaties*
Veiligheid heeft zich ontwikkeld van ad-hoc reacties op incidenten tot een samenhangend geheel van maatregelen en effecten. TNO ontwerpt innovatieve toezichtconcepten. Een betere informatiepositie voor iedereen die bij veiligheid is betrokken vereist slim gestructureerde systemen met gebruiksvriendelijke interfaces. TNO helpt om de informatie van burgers optimaal te benutten. Sociale media zijn daarvoor niet meer weg te denken, maar tegelijk een nieuw fenomeen bij crises waarop zorgvuldig ingespeeld moet worden.
Voor de ontwikkeling van de strategie en de programmering van het Vraaggestuurde onderzoek voor het Innovatiegebied Defensie Research vindt de afstemming tussen de overheid en TNO plaats onder regie van het Ministerie van Defensie. In dit Meerjarenprogramma 2011-2014 voor het Thema Integrale Veiligheid wordt alleen het Innovatiegebied Veilige Maatschappij verder uitgewerkt.

## 2.1 Doelstellingen en resultaten 2011-2014 voor het Innovatiegebied Veilige Maatschappij

Binnen het Innovatiegebied Veilige Maatschappij - initieert en faciliteert TNO innovaties. De kennisinvesteringen en de contractresearch zijn gericht op impact. Het Innovatiegebied heeft goede aansluiting op de beleidsintensiveringen van het kabinet Rutte. De drie hoofddoelstellingen van dit kabinet zijn (http://www.rijksoverheid.nl/regering/doelen/grenzen-stellen-en-handhaven.html):

1. Investeren in de kracht van Nederland
2. Het huishoudboekje van Nederland op orde
3. Grenzen stellen en handhaven

Veiligheid is het zwaartepunt in de laatstgenoemde doelstelling. Vier van de zes in dit kader door het kabinet te nemen maatregelen zijn daarop gericht. Met de huidige opdrachtenportfolio sluit TNO daar direct op aan:

| Kabinetsmaatregelen | Voorbeelden van TNO-bijdragen aan innovaties (opdrachten) |
|---|---|
| De politiecapaciteit neemt toe | • Vernieuwing basisvoorzieningen Politie (BVH-BVO)<br>• Basis voor netcentrisch werken<br>• Mentale weerbaarheid |
| Stevige aanpak van overlast, agressie en geweld; niet dader maar slachtoffer centraal | • *Sociale media tbv burgerbetrokkenheid*<br>• Slim cameratoezicht (automatische detectie/ training operators voor herkennen van 196 afwijkende gedragingen/ snelle koppelingen)<br>• Buurtlab Transvaal Den Haag<br>• Living Lab Veiligheid |
| Terugdringen van overlast en criminaliteit rondom prostitutie en drugs | • Living Lab Veiligheid |
| Strenger op immigratie | • @migo-concept voor mobiel toezicht vreemdelingen<br>• Schiphol toezichtsconcepten |

Ook buiten deze maatregelen in het kader van de beleidsintensiveringen van het kabinet Rutte draagt TNO met de uitvoering van opdrachten bij aan de veiligheid in de Nederlandse Maatschappij:

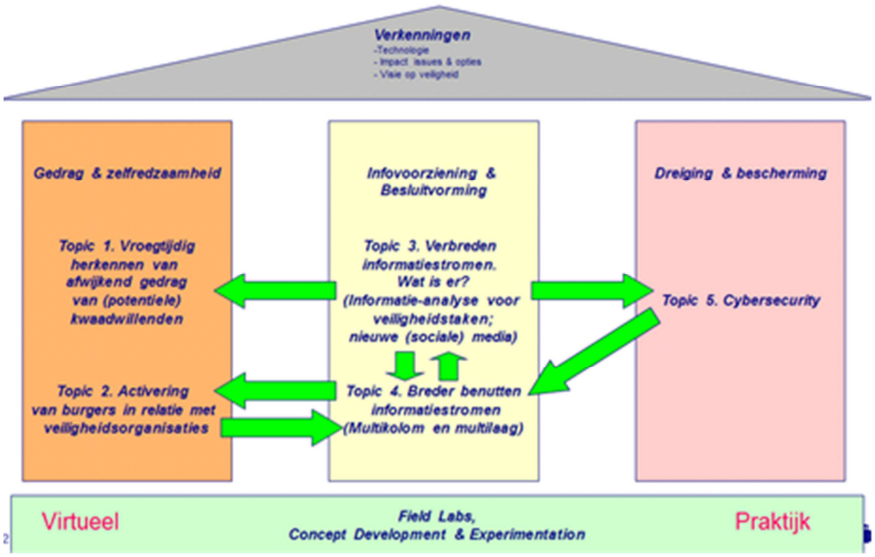
| Andere voorbeelden van TNO-bijdragen aan veiligheid in maatschappij |
|---|
| Ontwerp van inherent veilige stedelijke omgevingen (Secure Haven) |
| Inspectie en Advies: C2000, Politiemunitie, Voertuigbezetting, specifieke incidenten |
| Resilience van de vitale infrastructuur/ massatransport en airport security |
| Nationale risicobeoordeling samen met RIVM / AIVD / Clingendael / WODC |
| Evenwichtige en effectieve maatregelpakketten tegen dreiging van aanslagen met Chemische, Biologische, Radiologische, Nucleaire agentia en Explosieven |
| Crisismanagement en Rampenbestrijding, opleiding, training & oefening |
| Forensische technieken |
| Cybersecurity |
| Zelfredzaamheid van burgers en bedrijven |

TNO onderscheidt zich op het Innovatiegebied Veilige Maatschappij door:

- Hoogwaardige kennis op nieuwe technologische ontwikkelingsgebieden met gebruikmaking van de kennis bij universiteiten kennisinstellingen binnen en buiten Nederland
- Kennis van het veiligheids domein, relaties met belangrijke spelers daarbinnen en samenwerking met domein specifieke instituten (waaronder Politieacademie, NIFV en NFI)

- Onafhankelijke, gezaghebbende positie voor evaluatie van complexe afwegingen wordt met behulp van modellen en validatie van innovaties in samenwerking tussen overheid en bedrijfsleven

Om deze onderscheidende waarde te handhaven wordt via het Vraaggestuurde programma Veilige Maatschappij geïnvesteerd in kennistopics, die aansluiten bij nieuwe maatschappelijke veiligheidsvragen en technologische vooruitgang. In overleg met de stakeholders en onder regie van het ministerie VenJ is de volgende opzet voor het programma gekozen:




Naast de vijf topics wordt er geïnvesteerd in een portfolio van meerjarige EU-projecten. Deze portfolio sluit ook aan bij de kabinetsdoelstellingen:

| | |
|---|---|
| **Kabinetsdoel 3 Grenzen stellen en handhavenVeiligheid** | |
| De politiecapaciteit neemt toe | 2. Burgerbetrokkenheid<br>4. Delen informatiestromen<br>5. Cybersecurity |
| Stevige aanpak van overlast, agressie en geweld; niet dader maar slachtoffer centraal | 1. Herkennen afwijkend gedrag<br>2. Burgerbetrokkenheid<br>3. Slimmer inzetten info<br>5. Cybersecurity |
| Terugdringen van overlast en criminaliteit rondom prostitutie en drugs | pm |
| Strenger op immigratie | 1. Herkennen afwijkend gedrag<br>3. Slimmer inzetten info |
| **Kabinetsdoel 1 Investeren in de kracht van Nederland** | |
| Verminderen kwetsbaarheid economie (vitale infrastructuur, massatransport, (detail-)handel) | 1. Herkennen afwijkend gedrag (preventie)<br>4. Delen informatiestromen (crisismanagement)<br>5. Cybersecurity |
| Groei economie (met name beveiligingssector met 50 000 medewerkers en high tech sector) | 1. Herkennen afwijkend gedrag<br>3. Slimmer inzetten info |
| **Kabinetsdoel 2 Het huishoudboekje van Nederland op orde** | |
| Minder ambtenaren | 2. Burgerbetrokkenheid<br>4. Delen informatiestromen |

## 2.2 Overzicht Vraaggestuurde Programma's en relatie met ETP's

In het Vraaggestuurde Programma Veilige Maatschappij zijn de investeringen gericht op kennis die direct van belang is voor aan veiligheid gerelateerde vraagstellingen. Een aantal relevante kennisontwikkelingissues is veel breder van belang. De zogenaamde Enabling Technology Programma's van TNO zijn met name gericht op fundamentelere kennisontwikkeling die de kennisbasis voor meerdere thema's essentieel versterken.
Van de zeven ETP-programma's in de periode 2011-2014 zijn er drie direct van belang voor het VP Veilige Maatschappij:

- Het ETP *Gedrag en Innovatie* gaat in op perceptie in relatie tot gedrag en beïnvloeding van actiebereidheid op micro-, meso- en macroniveau. Een uitdaging is de onderscheiding van bevolkingsgroepen met karakteristieken, die verschillende mechanismen voor effectieve beïnvloeding vergen. Dit ETP is ook van belang voor de TNO-thema's Gezond Leven en Mobiliteit.
  In het VP Veilige Maatschappij zijn de aanknopingspunten voor dit ETP: het vroegtijdig herkennen van potentieel verdacht gedrag en zelfredzaamheid en burgerparticipatie.

- Het ETP *Sensoren* betreft de ontwikkeling van adaptieve multi-sensor-netwerken, waarbij geminiaturiseerde low-cost sensoren en nieuwe inter-connecties tussen giga- hoeveelheden sensoren, netwerken en informatie leiden tot een golf van nieuwe toepassingsopties. Dit ETP is van belang voor al de zeven TNO-thema's.
  In het VP Veilige Maatschappij zijn de aanknopingspunten voor dit ETP: het vroegtijdig herkennen van potentieel verdacht gedrag en de informatievoorziening voor het gecoördineerd uitvoeren van veiligheidstaken.

- Het ETP *Modellen* betreft de ontwikkeling van methoden om giga hoeveelheden waarnemingen, data, relaties en op te werken tot beslissingsondersteuning en stuurinformatie voor actoren in beleid en operaties. Gebruikersspecifieke interfaces tot de informatie-oceaan dienen gebruikers snel en juist interpreteerbare inzichten te geven die nodig zijn voor effectieve actie, coördinatie, gezamenlijke besluitvorming en communicatie. Dit ETP is ook van belang voor de TNO-thema's Mobiliteit, Gebouwde omgeving, Energie en Informatiemaatschappij.
  In het VP Veilige Maatschappij zijn de aanknopingspunten voor dit ETP: de activering van burgers in relatie tot veiligheidsorganisaties, informatiemining, de informatievoorziening voor het gecoördineerd uitvoeren van veiligheidstaken en cybersecurity.

## 2.3 Overleg met VenJ als regievoerend Departement

VenJ heeft als regievoerend departement het initiatief genomen om het VP in de strategie-periode 2011-2014 sterker te verankeren in de kennisbehoeften van de stakeholders. Tegelijkertijd is er strak vastgehouden aan de wens om de kennisontwikkeling te focusseren op een beperkt aantal topics.

De scherpere positionering van het VP kwam mede tot stand door betrokkenheid van trendsettende stakeholders, waarmee TNO in de voorgaande strategieperiode relaties heeft opgebouwd.

In het voorjaar van 2010 zijn door het toenmalige Ministerie BZK een aantal bijeenkomsten georganiseerd, waarvoor uitgenodigd waren: Ministerie van Justitie, Ministerie van Defensie, AIVD, NCTb, NICC, ICTU, Veiligheidsregio Noordoost Gelderland, NVBR, Brandweer Amsterdam, LFR, vts-PN, KLPD, CIV, Politieacademie en CCV. In een interactief proces heeft dit geleid tot de keuze voor een vijftal topics en een overkoepelend onderdeel voor verkenningen:

1. Vroegtijdig herkennen van afwijkend gedrag van (potentiële) kwaadwillenden
2. Activering van burgers in relatie met veiligheidsorganisaties
3. Slimmer inzetten van informatiestromen voor veiligheidstaken
4. Delen en benutten van informatiestromen voor het samen uitvoeren van veiligheidstaken
5. Cybersecurity
6. Verkenningen

Voor elk van deze topics zijn een aantal onderzoeksvragen geïdentificeerd en afgestemd, terwijl er een coördinerend behoeftesteller voor de begeleiding van de verdere uitwerking en uitvoering is aangewezen. Ook is afgesproken dat er twee keer per jaar een formeel voortgangsoverleg is tussen VenJ behoefte-stellers en TNO.

De hierna te presenteren stand van zaken met betrekking tot de programma-voortgang en -ontwikkeling zijn gebaseerd op afstemming met vijf topic-begeleidingscommissies. In april heeft het ministerie VenJ per brief aangegeven zeer tevreden te zijn over de ontwikkeling van dit programma en voor 2012 te kiezen voor het doorzetten van de vijf gekozen topics. Dit is ook in voortgangsoverleg in juni nogmaals door de heer M. van der Duin en mw. S. Geerdes als vertegenwoordigers van het regievoeren departement VenJ.

# 3 Vraaggestuurd Programma Veilige Maatschappij

## 3.1 Beoogde Impact en Doelgroep

1. In het TNO-Innovatiegebied Veilige Maatschappij zijn de contractresearch en de kennisinvesteringen in de strategieperiode 2011-2014 gericht op de volgende impact: Effectiever/efficiënter optreden veiligheidsorganisaties door innovatie van informatievoorziening, meldkamers, besluitvorming, doctrines, materieel, uitrusting en competenties;
2. Meer verantwoordelijkheid en betrokkenheid van burgers en bedrijven bij het zorgen voor de eigen veiligheid en de veiligheid in de openbare ruimte;
3. Veiligheid beter verankerd in verschillende maatschappelijke sectoren (waaronder de topsectoren Hightech, Logistiek en Water) en een beter kunnen afwegen van de maatschappelijke en economische effecten van risicomaatregelen;
4. Verbetering van de resilience van de maatschappij tegen cyberrisico's en van de bestrijding van de cybermisdaad;
5. Voorkomen en beperken van schade ten gevolge van rampen/crises (overstromingen, CBRNe-incidenten, uitval vitale infrastructuren) door vergroten van de maatschappelijke resilience, snel en adequaat optreden en door kosteneffectieve proactieve maatregelen.

In het kader van dit VP zullen er ook verkenningen worden uitgevoerd met als doel de portfolio van kennistopics optimaal matchend met nieuwe ontwikkelingen in de technologie en in het veiligheidsdomein te houden.

De belangrijkste doelgroepen waarop TNO zich richt met dit VP en hun aansluiting bij proposities en topics zijn:

| Doelgroep | Belangrijke sectoren |
|---|---|
| Nationale overheid | - Veiligheid (VenJ Defensie)<br>- Economie (EZ)<br>- Infrastructuur (EZ, V&W, VROM) |
| Decentrale overheid | - Veiligheidsregio's (brandweer, GHOR, meldkamers)<br>- Gemeenten |
| Bedrijfsleven | - Veiligheidsbranche (industrie en diensten)<br>- Vitale infrastructuur<br>- Mainports |
| Veiligheid gerelateerde Instituten | - Onderzoek (NFI, CCV, Verweij-Jonker e.a.)<br>- Opleiding (Politieacademie, NIFV e.a.) |
| Internationaal | - Overheden (EU, EU-lidstaten, DHS in VS)<br>- Bedrijfsleven (Multinationals)<br>- Complementaire kennisinstituten |
| Consortia voor publiek-private samenwerking | - Veiligheid op luchthavens<br>- Vitale infrastructuur<br>- e.a. |

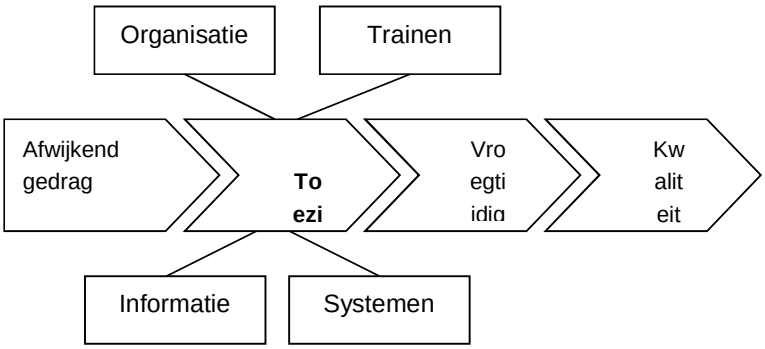
## 3.2 Focus van onderzoeksvragen en roadmap

Voor de vijf geselecteerde specifieke topics zijn de focus en de te beantwoorden onderzoeksvragen onderstaand uitgewerkt.

### *3.2.1 Vroegtijdig herkennen afwijkend gedrag*

#### *3.2.1.1 Omschrijving van het topic*

Bij toezicht op de veiligheid in de (openbare) ruimte is het vroegtijdig herkennen van afwijkend gedrag een belangrijke sleutel om te komen tot verbetering van kwaliteit, efficiency en veiligheidsbeleving.




Deze verbeteringen zijn gericht op:

- hogere kwaliteit: effectief voorkómen van terrorisme, criminaliteit en veiligheidsincidenten, beperken van de gevolgen daarvan en opsporen van daders;
- betere efficiency: richten van de professionele capaciteit op de juiste prioriteiten en met minder inspanning effectief handhaven;
- optimale veiligheidsbeleving: burgers die zich veilig voelen, veilig handelen en mogelijk in de waarneming participeren.

Ontwikkelingen zijn tot nog toe overwegend geweest in het investeren van technische middelen:

- Vooral meer camera's, meer toezichtcentrales en als gevolg daarvan meer operators, geen heldere prestatie indicatoren;
- Het ontwikkelen van slimme uitkijksoftware, automatisch herkennen van bepaalde (afwijkende) gedragingen;
- Slimmer werken door netwerkverbinding te leggen tussen meldkamers en centrale.

Het onderwerp herkennen van afwijkend gedrag van potentieel kwaadwillenden staat nog in de kinderschoenen.

In het VP wordt basiskennis ontwikkeld voor innovatieve integrale concepten voor toezicht van (openbare) ruimte in (camera)toezichtcentrales of genetwerkt (virtuele) toezichtorganisaties waarin alle relevante professionals (Multi party) en burgers gezamenlijk tot betere kwaliteit, efficiency en een verhoogde veiligheidsbeleving komen. De focus is onderstaand uitgewerkt en afgestemd met de door VenJ gecoördineerde begeleidingsgroep. Als vervolg op de kennisontwikkeling is

doorontwikkeling in nationale en internationale innovatieprogramma's voorzien gevolgd door vanuit stakeholders gefinancierde innovatietrajecten.

#### *3.2.1.2 Focus van het topic*

| | |
|---|---|
| Waar gaat het precies over? | Vroegtijdig waarnemen en beïnvloeden van (potentieel) kwaadwillenden (niet corrigeren en handhaven) om terrorisme en criminaliteit te voorkomen |
| Wie betreft het? | Alle partijen met toezichttaken en eigenaars van locaties waar toezicht nodig is; partijen die daarvoor de (beleids)kaders opstellen:<br>- VenJ (NCTb, DJI)<br>- Gemeenten<br>- Politie KLPD, Marechaussee<br>- Openbaar Vervoer, mainports<br>- Winkeliers, detailhandel, bedrijfsterreinen<br>- Beveiligingsbedrijven |
| Waarom is het onderzoek van belang? | - Veiligheid in het openbaar vervoer (issues groepsgedrag jeugd, gedragsbeïnvloeding reizigers/bestuurders, crowd management evenementen)<br>- Veiligheid in gevangenissen (monitoren gevangenen en bezoekers0<br>- Toezicht in winkels en winkelcentra (preventie diefstal, vandalisme)<br>- Toegangscontrole (Schiphol, rechtbanken, voetbalstadions) |
| Waarmee kunnen we dit doen? (Focus) | - Met een ontwerp- en evaluatie-instrument voor de ontwikkeling en toets van effectieve en efficiënte toezichtorganisaties<br>- Waarnemen, vroeg interpreteren en beïnvloeden van afwijkend gedrag (weak signals, prikkelen individuen/groepen)<br>- Optimale samenwerking tussen toezichthouders, gebruikmakend van alle beschikbare bronnen en informatie die afwijkend gedrag kunnen signaleren en duiden<br>- Intelligente sensornetwerken (spot, track & trace, intelligente camera's)<br>- Ontwikkeling van in de surveillancepraktijk bruikbare risicoprofielen van een gebied, groepen en personen op basis van tijd, plaats, omgevingskenmerken, eigenschappen; randvoorwaarde: privacywetgeving<br>- Concept development & experimentation faciliteit, Living lab in stedelijke omgeving/ Fieldlab in winkelcentrum |
| Wie begeleidt? | Desiree Geerts (VenJ/NCTV; NB tijdelijk vervangen door Marian Luursema/Irene Doll), J. Lavèn(Subarena Geïntegreerde Systemen /CIV), AIVD |
| TNO-team | Maaike Lousberg (trekker), Gert-Jan Burghouts e.a. |

#### *3.2.1.3 Met VenJ en stakeholders afgestemde onderzoeksvragen*

**Vraag 1: Basismodel voor toezichtorganisatie in openbare ruimte**
Hoe leidt het vroegtijdig herkennen van verdachte gedragingen afhankelijk van de context in verschillende (openbare) ruimten (openbaar vervoer, wijk, winkelcentra, luchthaven, enzovoort) tot een verhoogde kwaliteit, efficiency en veiligheidsbeleving bij het voorkomen van overlast en verloedering, kleine en grote criminaliteit en terrorisme en wat is het effect op het toezichtproces, de organisatie en de ondersteuning daarvan?

Focus op:

- Herkennen van verdacht gedrag
- Relatie tussen gedragingen, omgeving, toezichtproces en prestatie-eisen
- Professionalisering van toezicht in de (openbare) ruimte
- Model waaruit men eisen kan afleiden voor het toezichtproces afhankelijk van het te herkennen verdacht gedrag, omgeving en prestatie-indicatoren

**Vraag 2: Door professionals herkennen van (potentieel) verdacht gedrag**
Welke gedragingen, contextinformatie en andere relevante (intelligence) informatie hebben voorspellende waarde (profiling) voor het voorkomen van overlast, kleine en grote criminaliteit en terrorisme?

Focus op:

- Breed perspectief gedragingen: personen in de ruimte maar ook informatie over personen in gegevensbestanden en andere informatiebronnen
- Relatie met opsporing en proactief voorkomen van criminaliteit en terrorisme
- Profiling: op basis van kenmerken extrapoleren van informatie om verdacht gedrag vroegtijdig te herkennen

**Vraag 3: Prikkelen**
Welke proactieve handelingen kunnen professionals toepassen om afwijkend gedrag beter te interpreteren en potentieel verdacht gedrag eerder te kunnen waarnemen (prikkelen)?

Focus op:

- Afwijkende gedragingen snel interpreteren
- Bieden van handelingsperspectief aan professionals

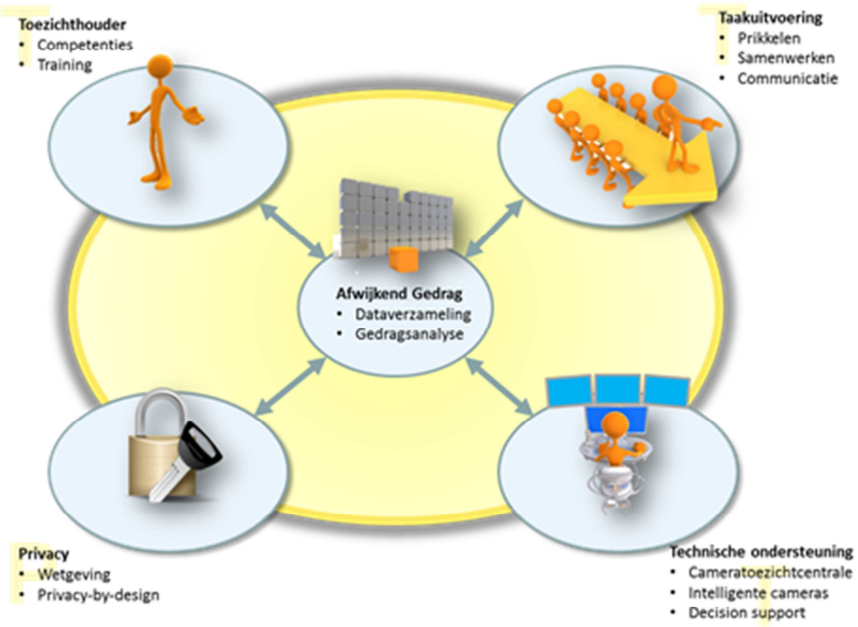
**Vraag 4: Intelligente systemen**
Welke verdachte / afwijkende gedragingen zijn met intelligente systemen beter te signaleren, en welke door mensen? Welke technologische ondersteuning kan worden ingezet om tot een beter en vroeger oordeel te komen? Hoe is een signalering door intelligente systemen zó te representeren dat een operator snel een juiste interventie kan doen?

Focus op:

- Systemen en automatisering van herkenning van verdachte gedragingen
- Evaluatie in praktijk met professionals
- Optimaliseren van rendement door optimale mens-systeem interactie

#### *3.2.1.4 Voortgang in 2011*

In 2011 is het onderzoek naar afwijkend gedrag binnen het VP Maatschappelijke Veiligheid gericht op het ontwikkelen, en invullen van een basismodel van afwijkend gedrag in toezichtsituaties. Het basismodel geeft aan welke kennis er nodig is om toezichtorganisaties optimaal te ontwerpen, in te richten en te evalueren. Het streven is naar toezicht op maat: voor elke toezichtsituatie de optimale mix van organisatie, mensen en middelen, informatiebronnen, werkwijzen en competenties. Met als resultaat veiligheid, minder overlast en verloedering, criminaliteit en het kunnen voorkomen van terrorisme.




Figuur: Basismodel “Toezicht op afwijkend gedrag”

In 2011 is het bovenstaande model met de bijbehorende visie ontwikkeld. Onderdelen van deze visie zijn gepubliceerd en gepresenteerd tijdens een tweetal internationale wetenschappelijke conferenties. De visie in zijn geheel en het model staan beschreven in een basisdocument dat in de toekomst zal dienen voor het adviseren, inrichten en evalueren bij toezichtlocaties. Binnen (en buiten) het vraaggestuurde programma (VP) richt TNO zich op het ontwikkelen van kennis over de verschillende onderdelen van het model “Toezicht op Afwijkend Gedrag”. Zo doet TNO bijvoorbeeld via een TNO EL&I Cofinancieringsproject, i.s.m. het Rijksmuseum en het Van Gogh museum onderzoek naar competenties die nodig zijn voor het goed kunnen herkennen van, en reageren op afwijkend gedrag.

De activiteiten binnen het VP worden hier onder beschreven.

**Fundamenten van afwijkend gedrag**
Door middel van een literatuuronderzoek en een experiment probeert TNO inzicht te krijgen in waarom mensen die iets verbergen zich anders gedragen dan anderen. Er is een theoretisch model opgesteld gebaseerd op studies naar het gedrag van mensen met verborgen stigmata (zoals HIV positief zijn) in omgevingen waarin het uitkomen van deze verborgen stigmata een negatief effect heeft op een gewenst einddoel. Dit theoretische model wordt eind van dit jaar getoetst door middel van een experiment. We onderzoeken of deze kennis ook toe te passen is op mensen die iets slechts in de zin hebben in toezichtlocaties. Indien duidelijk wordt waarom mensen die iets slechts in de zin hebben, of iets willen verbergen zich anders gedragen, kan ook meer inzicht worden gekregen in hoe dit er uit ziet, en hoe men hier op zou kunnen reageren.

In dit onderdeel van het onderzoek neemt TNO ook deel aan het FP7-EU Project SAFIRE. TNO is coördinator van dit project waarin samen met nationale en internationale partners een non-lineair model gemaakt wordt van het proces van radicalisering. Dit project geeft inzicht in de fundamenten van het gedrag van mensen die kunnen komen tot criminele delicten of terroristische activiteiten.

**Dataverzameling en gedragsanalyse**
Om het voorspellend vermogen van beveiligingsmedewerkers met betrekking tot afwijkend gedrag te verhogen is er een conceptmethodiek opgesteld. Deze methodiek bestaat uit een database met videobeelden van incidenten (zoals zakkenrollen, rip deals, dealen, terroristische aanslagen, overvallen) en van situaties waarin niets gebeurt op verschillende toezichtlocaties. Verschillende externe partijen hebben bijgedragen aan de opbouw van deze database, of hebben intenties daartoe (Politieacademie, NS, Kmar). Indien er voldoende data verzameld zijn kunnen de data geanalyseerd worden met behulp van de hypothesemanager. Deze hypothesemanager geeft de kans aan dat indien men bepaald gedrag ziet, men te maken zou kunnen hebben met een bepaald type delictpleger.
Aangezien het verzamelen van videobeelden niet altijd even makkelijk is wegens privacywetgeving, ontwikkelen en testen we een tool bij de toezichtcentrale van de Kmar op Schiphol waarmee operators zelf beelden van delicten kunnen annoteren, zonder dat de beelden gedeeld hoeven worden. We onderzoeken in hoeverre de annotaties toegevoegd kunnen worden aan de videodatabase, en daarmee gebruikt kunnen worden in de analyse.

**Interpretatie van afwijkend gedrag**
Het definiëren van wat afwijkt en wat niet is zeer complex. Er spelen verschillende aspecten een rol, zoals tijd, locatie, cultuur, type delict, het combineren van gedragingen en het definiëren van normaal gedrag. In dit onderzoek is een overzicht gemaakt van de stappen die er nodig zijn om te kunnen bepalen wanneer iets afwijkend is of niet. Dit stappenmodel zal gebruikt worden voor de hypothesemanager, maar dit overzicht kan echter ook gebruikt worden om toezichtlocaties te adviseren over afwijkend gedrag toegespitst op een specifieke locatie.

**Reageren op afwijkend gedrag: “Prikkelen”**
Als afwijkend gedrag gedetecteerd wordt, betekent dit niet automatisch dat iemand verdacht is. Het gaat slechts om een vermoeden van een beveiligingsmedewerker op basis van een bepaalde gedraging. Om dit vermoeden te toetsen kunnen proactieve handelingen toegepast worden. Deze handelingen worden “prikkels” genoemd. In 2011 wordt onderzocht in hoeverre en hoe mensen met slechte intenties anders reageren op prikkels dan mensen zonder slechte intenties. Een van de grootste uitdagingen tijdens het experiment behorende bij dit onderzoek is het manipuleren van “slechte intenties”. Het experiment zal in het laatste gedeelte van het jaar plaatsvinden.

**Communicatie, samenwerking en besluitvorming**
Op Koninginnedag is er een online vragenlijstonderzoek gedaan bij de politiemensen die voor de jaarlijkse Koninginnedagviering door de Politieacademie getraind zijn in het herkennen van afwijkend gedrag. De resultaten van het onderzoek

zijn gedeeld met de NCTV en het politiekorps Limburg Noord en worden meegenomen in de organisatie van komende nationale evenementen.

**Intelligente Camera's**
In 2010 heeft TNO op A'dam CS laten zien dat er potentie is voor intelligente camera's bij het signaleren van afwijkingen. In 2011 wordt dit een stap concreter: is er uit een afwijkende gedraging af te leiden dat het gaat om een intentionele afwijking? Daartoe hebben is er samen met het KLPD en DKDB beeldmateriaal opgenomen. Aanvallen door een solistische dreiger(s) op een individu werden gesimuleerd. Acht individuen hebben een aanval voorbereid en uitgevoerd. Het beeldmateriaal laat duidelijk zien dat er een intentie van de dreiger uitgaat: zijn looppatroon is anders dan van normale voorbijgangers. Deze eigenschap is vastgelegd in een patroon (patentverzoek voor deze methode is ingediend), waarnaar de software op zoek kan gaan bij het analyseren van nieuwe beelden.

In het kader van dit onderzoek is ook deelgenomen aan het Pijler 2 project: "het observeren van het gedrag van mensen" waarin samen met andere partners onderzoek gedaan wordt naar hoe men het herkennen van afwijkend gedrag technisch kan ondersteunen.

#### *3.2.1.5 Voorgestelde zwaartepunten voor voortzetting in 2012*

Om de wetenschappelijke analyses rondom van afwijkend gedrag te verbeteren is het nodig om meer te weten over de fundamenten van afwijkend gedrag. Daarbij is onder andere kennis over van lichamelijke reacties en hersenprocessen een belangrijke toevoeging ten opzichte van vorig jaar. Dit speelt ook een belangrijke rol bij het onderzoek naar de reacties op verschillende interventies of prikkels. Daarnaast is het nodig om de in 2011 opgebouwde filmdatabase kwantitatief en kwalitatief uit te breiden.

De visie van TNO op het gebied van afwijkend gedrag moet getoetst en verfijnd worden met behulp van veldexperimenten, daar waar mogelijk in fieldlabs (hoeveel effectiever en efficiënter, sneller, goedkoper is de voorgestelde aanpak/verbeteringen daadwerkelijk?).

De verdere ontwikkeling van intelligente camera's en de mens-machine interactie is nodig. Experimenten met andere vormen van afwijkend gedrag, of het automatisch herkennen van relevante reacties op interventies of prikkels dragen bij aan de technische ondersteuning van de beveiligingsmedewerker in het herkennen van en reageren op afwijkend gedrag.

In 2012 wordt ook deelgenomen in het FP7 project TACTICS. TNO is coördinator van dit project waarin samen met nationale en internationale partners een decision support tool gemaakt wordt. Deze decision support tool ondersteunt in het creëren van optimale detectie omstandigheden (door juiste afstemming van bestaande kennis, mens en techniek) op het moment dat er sprake is van een acute terroristische dreiging is in stedelijk gebied. De NCTV zit in de advisory board van dit project.

### *3.2.2 Activering burger in relatie met veiligheidsorganisaties*

#### *3.2.2.1 Omschrijving van het topic*

De professionele veiligheidsorganisaties zien als belangrijke uitdaging het betrekken van de burger bij het zorgen voor de veiligheid in de maatschappij. Daarbij gaat het om:

- Het invullen van de verantwoordelijkheid van burgers en bedrijven om te zorgen voor hun eigen veiligheid en bij te dragen aan de veiligheid van hun omgeving.
- Het gaat dan om preventieve maatregelen (rookdetectoren, inbraakpreventie etc.), voorbereiding op eventuele noodsituaties (bekendheid met vluchtmogelijkheden, vorming emergente groepen), zelfredzaamheid bij veiligheidsincidenten en rampen, en hulp aan medeburgers vóór de professionele veiligheidsorganisaties ter plekke zijn.
- Het benutten van de competenties van burgers en in de omgeving aanwezige professionals (buschauffeurs, verpleegkundigen, winkeliers, etc. etc.) voor het effectief en efficiënt realiseren van veiligheidsdoelstellingen.
- Dit is bv van belang voor toezicht op de openbare ruimte, opsporing van daders na incidenten, eerste acties na brandmelding, bijstand bij veiligheidsoperaties.

Rond burgerbetrokkenheid bij veiligheid zijn er vele initiatieven. In het kader van dit topic zal basiskennis ontwikkeld worden die bijdraagt aan:

- Het bevorderen van veiligheidsbewustzijn en actiebereidheid door nieuwe communicatieconcepten (bv inzet van sociale media, gaming);
- Effectievere inzet van burgers door informatievoorziening en communicatie gebaseerd op in zicht in de plaatsvindende psychologische processen;
- Methoden om groepen burgers als vrijwilliger te mobiliseren en hun competenties te vergroten door instructie, training en opleiding.

### *3.2.2.2 Focus van het topic*

| | |
|---|---|
| Waar gaat het precies over? | Zelfredzaamheid (betere preventie en preparatie van burgers en bedrijven op fysieke en sociale veiligheidsincidenten) en burgerparticipatie (benutting van competenties van burgers en bedrijven voor uitvoeren van veiligheidstaken) |
| Wie betreft het? | - Burgers<br>- Politie, brandweer en GHOR<br>- Veiligheidsregio's<br>- Gemeenten<br>- Bedrijven, waar veiligheid bijzondere aandacht krijgt i.v.m. risico's en/of hoeveelheid mensen |
| Waarom is het onderzoek van belang? | Beïnvloeden veiligheidsbewustzijn<br>Verankeren van verantwoordelijkheid t.a.v. eigen veiligheid bij burgers en bedrijven<br>Handelingsperspectief en handelingsbereidheid van burgers en bedrijven<br>Terugtredende overheid<br>Opbouwen community resilience |
| Waarmee kunnen we dit doen? (Focus) | Communicatie voor beïnvloeding van perceptie en gedrag (incl. sociale netwerken)<br>Leren en instructie van burgers en professionals voor optimale samenwerking (serious gaming)<br>Stimuleren en belonen om motivatie voor participatie te bewerkstelligen<br>Organisatie van en infrastructuur voor burgerinzet |
| Wie begeleidt? | Marjan Heijman (Coördinator; NVBR), Paul Verlaan (veiligheidsregio Brabant Noord)VenJ/programma dreigingen en capaciteiten, VTSPN, NCTV |
| TNO-team | Gerard Veldhuis (trekker), Jose Kerstholt, Hester Stubbé, Inge Trijssenaar |

### *3.2.2.3 Met VenJ en stakeholders afgestemde onderzoeksvragen*

**Vraag 1: Informatie keuze en vorm t.b.v. handelingsperspectief en -bereidheid**
Welke informatie kan op welke manier beschikbaar worden gesteld aan burgers, bedrijven en organisaties; om het eigen handelingsperspectief en –bereidheid te vergroten? Welke incidenten, noodsituatie of rampen zijn te identificeren? Welke informatiebehoefte hebben burgers en bedrijven? Welke scenario's zijn er en hoe kunnen deze worden gemodelleerd?

Focus op:

- Type incident, ramp noodsituatie
- De eigen veiligheid, de veiligheid van de omgeving en de ondersteuning van veiligheidsorganisaties
- Type informatie en wijze beschikbaar stellen
- Typen omgeving (o.a. woon-, werk-, recreëer-omgeving)
- Juridische consequenties
- Verschillen tussen groepen (burgers: sociaal zwakkeren, sociaal sterkeren, semiprofessionals; bedrijven: bedrijfshulpverlening, bedrijfsbewakers)

**Vraag 2: Ondersteuning veiligheidsorganisaties**
Hoe kunnen veiligheidsorganisaties worden ondersteund bij de uitvoering van hun taken door inzet van burgers en bedrijven? Wat zijn effectieve wijze van samenwerking en afstemming tussen burgers, bedrijven en veiligheidsorganisaties? Welke blokkades en knelpunten zijn er voor effectieve samenwerking? Hoe kunnen

bevindingen worden verpakt zodat betrokkenen ervaren en leren hoe samenwerking effectief kan verlopen?

Focus op:

- Verkrijgen betrouwbare informatie en beoordeling ervan
- Voorbereiden op en tijdens incident, ramp noodsituatie
- Anticiperen op actiebereidheid ‘mentaliteit’
- Informatie voor taken m.b.t. toezicht en opsporing
- Communicatie naar directe omgeving bij incident, ramp noodsituatie
- Fysieke inzet van burgers en bedrijven bij incident, ramp noodsituatie
- Blijvende motivatie van burgers en bedrijfsleven ‘terugmelden’ communicatie

**Vraag 3: Ingrepen gebouwen en gebouwde omgeving (in relatie tot gedrag van burgers)**
Wat is het effect van ingrepen gericht op veiligheid en zelfredzaamheid in gebouwen en de gebouwde omgeving op het gedrag van burgers? Welke maatregelen zijn er in gebouwde omgeving en in gebouwen te nemen en welk effect is er te verwachten op het vergroten van de zelfredzaamheid? Wat is de relatie tussen maatregelen in de gebouwde omgeving en gebouwen en het optreden veiligheidsorganisatie Hoe kunnen deze relaties worden gevat in een kwalitatief relatiemodel?

Focus op:

- Veilig bouwen
- Afhankelijkheid inzet professionele veiligheidsorganisaties
- Decentrale middelen voor hulpverlening en organisatievormen
- Mogelijke interventies en hun werking: actuele informatievoorziening bij incidenten, rampen noodsituaties voor vergroting zelfredzaamheid
- Kwalitatief relatiemodel voor effectiviteit van verschillende ingrepen op eigen resilience

**Vraag 4: Optimale samenwerking burgers en professionals**
Op welke manier kunnen burgers en professionals bij incidenten en crises en rond sociale veiligheid samenwerken? Welke reële scenario’s, gericht op samenwerking van burgers en professionals, zijn er? Hoe kan disseminatie van samenwerkingsconcepten vorm krijgen?

Focus op:

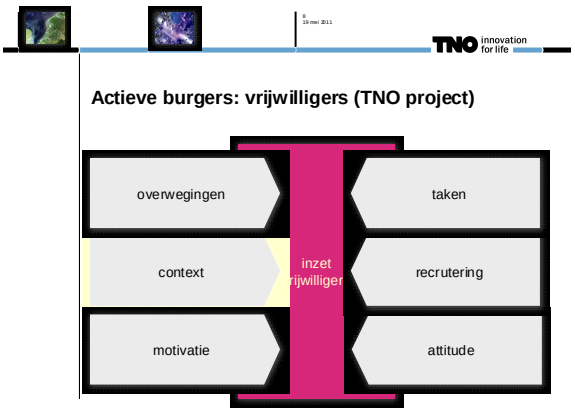
- Vertrouwen en gezamenlijke verantwoordelijkheid
- Type incident, ramp noodsituatie
- Verhoging veiligheidsbeleving
- Disseminatie, oefenen, gaming, middelen

#### *3.2.2.4 Voortgang in 2011*

**Informatiekeuze en vorm t.b.v. handelingsperspectief en -bereidheid**
Er is verkend op welke wijze informatie wordt geproduceerd en gedeeld tussen melder (burger) en hulpverlenersorganisaties. Met name tijdens de na de incidentfase zijn mogelijkheden voor verbetering. De bevindingen kunnen ook

implicaties hebben voor de voor de incident fase. Er wordt niet gekeken naar de tijdens de incidentfase, omdat al veel projecten zich hierop richten. De verwachte meerwaarde zit vooral in de nafase. Er is een experiment voorbereid, in samenwerking met. Topic 3, waarbij op een alternatieve wijze informatie wordt gedeeld tussen hulpverlener en burgers. Dit experiment (verwachte uitvoering najaar 2011) zal meer inzicht verschaffen in de informatie-uitwisselcyclus. Het kan tevens een stap zijn in verandering van de positie die burgers innemen in een netcentrische crisisorganisatie (relatie topic 4).

**Basismodel voor met burgerbetrokkenheid te bereiken effecten op de veiligheid**




Er is een vragenlijst voorbereid en uitgezet bij vrijwilligers betrokken bij diverse organisaties. De vragen zijn erop gericht om te achterhalen welke intenties mensen hebben om als vrijwilliger te werken bij betreffende organisatie. De uitkomsten moeten leiden tot een overzicht van verschillende beweegredenen van mensen om een taak op te pakken. Daarnaast wordt er gekeken binnen organisaties die vrijwilligers inzetten welke taken zij laten uitvoeren, hoe de matching tot stand komt en welke ondersteuning wordt geboden. Van belang hierbij is te achterhalen of er verschillen zijn tussen organisaties en het type profielen van vrijwilligers. De bevindingen worden opgenomen in een model, met factoren die aan de kant van de vrijwilliger en aan de kant van de professionele hulpverlenersorganisaties in kaart zijn gebracht. Met de uitkomst kunnen organisaties worden vergeleken om mogelijke verbeterpunten aan te geven ten aanzien van de effectiviteit van de inzet van hun vrijwilligers.

**Ingrepen gebouwen en gebouwde omgeving (in relatie tot gedrag van burgers)**

Er is een conceptmodel voorbereid waarmee veiligheidsmaatregelen/ -interventies worden geïndexeerd op hun effect op veiligheid en daardoor verbeterde zelfredzaamheid. Voor verschillende ramptypen worden maatregelen gekoppeld aan de kans op overlijden of verwonding. Het ligt voor de hand dat maatregelen elkaar bij verschillende ramptypen kunnen tegenwerken. Bijv. .beter beveiligd tegen ongewenst gebouw betreden kan de snelle evacuatie tegenwerken. Door in het uiteindelijke model meerdere rampscenario's te laten draaien kan inzicht worden verkregen op welke wijze maatregelen effect hebben op een bepaald gebied/gebouw. Inzicht in de uitkomsten geeft gerichte input aan advies over een gebouw of gebied. Momenteel worden de maatregelen geïnventariseerd en geïndexeerd. De modelvorming volgt in een latere fase van het project (2012).

**Optimale samenwerking tussen burgers en professionals**
Er is als eerste stap een verkenning gedaan naar de ontwikkelingen op het gebied van de sociale veiligheid in relatie tot sociale media. Het blijkt uit de eerste resultaten dat het nog niet mogelijk is om de effectiviteit van sociale media te koppelen aan beoogde effecten. Er is nog geen wetenschappelijke evidentie. Daarbij zijn er nog geen geschikte meetmethoden om initiatieven en situaties met elkaar te vergelijken. Dit overzicht zal leiden tot een aantal niches waar vervolgonderzoek op kan worden geënt. Daarbij is een verkenning gedaan naar mogelijkheden van burgerpanels. Er zijn verschillende verschijningsvormen van burgerpanels. Gekeken wordt op welke wijze burgerpanels als instrument effectief kan worden ingezet.

**Interactie met stakeholders**
Naast de discussies met de topicbegeleidingsgroep is interactie met stakeholders gezocht door bijdragen aan:

- Discussiebijeenkomst Zelfredzaamheid bij het CCV op 11 april 2011, Utrecht
- Workshop Activeren van burgers, bedrijven en instellingen bij veiligheid tijdens Seminar Veiligheid en Geïntegreerde Systemen op 15 juni 2011 in Utrecht
- Projectteam voor het opstellen van een visie Burgers als Bondgenoten in opdracht van het POC, 2011 en het opstellen van een actieplan
- Presentatie/deelname aan NUWCReN consortium
- Voorbereiden en inmiddels goedgekeurd KP7-voorstel BESECURE

#### *3.2.2.5 Voorgestelde zwaartepunten voor voortzetting in 2012*

**Informatiekeuze en vorm t.b.v. handelingsperspectief en -bereidheid**
In 2012 zal de kennis informatie-uitwisselingcyclus verder worden uitgediept. Doel is om te achterhalen wat het delen van informatie oplevert voor burgers en hulpverleners na incidenten. Is van belang voor topic 4 en levert kennis op om een eerste aanzet te geven voor nieuwe wijze van samenwerking (hulpverlenersorganisaties en burgers) en onderlinge interactie.

**Ondersteuning veiligheidsorganisaties**
In 2012 zullen de resultaten van 2011 worden doorontwikkeld tot een concept model voor analyse en advisering van voor professionele hulpverlenersorganisaties inzichtelijk te maken welke slagen te maken zijn om het proces van taken, matching en begeleiding vrijwilligers te optimaliseren. Vervolgens zal een game worden voorbereid waarbij hulpverleners kunnen leren van burgers welke taken er veilig kunnen worden uitgevoerd (hulp bij cultuuromslag). Vrijwilliger kunnen meer te weten komen over mogelijkheden die organisaties hebben voor vrijwilligers en het werk dat wordt uitgevoerd. Doel is om meer expliciet te maken welke taken er zoal zijn, hoe betreffende organisaties optreden en om door middel van de gameomgeving vraag en aanbod met elkaar te brengen. Het onderzoek zal zich richten op de wijze waarop deze game het meest effectief zal zijn. Als de ontwikkeling van de game voorspoedig verloopt, zal een eerste try out worden gedaan met het prototype.

**Ingrepen gebouwen en gebouwde omgeving (in relatie tot gedrag van burgers)**
In 2012 zal de modelvorming verder worden geïntensiveerd. Dit model zal als basis dienen voor een tool voor analyse en advisering van veiligheidsregio's, gemeenten, projectontwikkelaars, woningcorporaties. Er is vraag naar om structuur aan te brengen in dit complexe vraagstuk. Naast de verdere invulling en concretisering van de modelvorming zal met het landelijk netwerk risicobeheersing en andere betrokkenen worden afgestemd.

**Optimale samenwerking burgers en professionals**
In 2012 zal, wanneer de resultaten van de analyse dit ondersteunen, een eerste concept meetaanpak worden voorbereid en in een experiment te toetsen om de effectiviteit van sociale media en beoogd effect tijdens de inzet kan worden bepaald.

### *3.2.3 Slimmer inzetten van informatiestromen voor veiligheidstaken (Verbreden van informatiestromen. Wat is er nodig? En wat kunnen we ermee?)*

#### *3.2.3.1 Omschrijving van het topic*
Informatie en informatie gestuurd werken zijn van grote waarde binnen het veiligheidsdomein (lees: instanties verantwoordelijk voor toezicht, handhaving en opsporing). Zonder tijdige en juiste informatie op de juiste plaats kunnen de operationele taken niet goed worden uitgevoerd.
Er is een enorme hoeveelheid informatie beschikbaar op basis waarvan uitvoerende en sturende instanties hun activiteiten en beslissingen kunnen baseren. In de praktijk blijkt er echter vele malen meer informatie en informatiebronnen beschikbaar dan die door de mensen werkzaam in het domein tijdig en juist ontsloten kunnen worden. De hoeveelheid beschikbare informatie neemt ook exponentieel toe. Dit leidt ertoe dat relevante informatie niet tijdig kan worden onderkend en verwerkt om mede input te vormen voor acties en besluitvorming bij operationele inzet. Een neveneffect hiervan is onrust bij de medewerkers en besluitvormers die achteraf verwijten krijgen als bepaalde beslissingen onjuist blijken te zijn. Zo van, "als jullie wat beter hadden gezocht in de beschikbare informatie hadden jullie vooraf kunnen weten dat …."

De vraag rijst hoe hier op een goede wijze mee om te gaan? Zijn er technologische, organisatorische of procesmatige innovatieve oplossingen te bedenken die het mogelijk maken om meer informatie op goede wijze te ontsluiten ter ondersteuning van de operationele taken? Zijn er effectieve manieren van werken te bedenken waarbij het niet beschikken over volledige informatie niet als belemmerend wordt ervaren? Hoe kan de relevante informatie worden ontsloten terwijl alle niet relevante informatie buiten beeld blijft? Wat is de rol van de nieuwe media in het tijdig kunnen beschikken over de benodigde informatie?

Dit is de kern waar dit onderzoek om draait. Omdat er al veel gebeurt aan onderzoek op dit gebied zowel nationaal als internationaal zal worden gezocht naar additionele benaderingen en/of het verbinden van onderkende best practices tot bruikbare methoden of werkprocessen.

### *3.2.3.2 Focus van het topic*

| | |
|---|---|
| Waar gaat het precies over? | Slimmer inzetten van breed beschikbare informatie en nieuwe (sociale) media voor operationele veiligheidstaken. Verwerking van grote hoeveelheden aanwezige informatie, waarnemingen en meldingen tot direct bruikbare informatie. |
| Wie betreft het? | Operationele diensten in veiligheidsregio's en politieregio's (hulpverlening, toezicht, handhaving)<br>Justitie/NFI/politie (opsporing)<br>KLPD, NCTb, AIVD (intelligence) |
| Waarom is het onderzoek van belang? | De beschikbaarheid van (openbare) bronnen en informatie neemt exponentieel toe. Nieuwe sociale media (twitter, discussiefora) en andere bronnen (SMSalert, youtube) kunnen zinvolle informatie leveren waarmee risicovolle situaties en dreigingen vroegtijdig kunnen worden onderkend en op basis waarvan de-escalerend kan worden opgetreden. In al bestaande, geëscaleerde dreigingen of crisis kan de informatie worden gebruikt voor een snelle en eenduidige opsporing en/of afhandeling. |
| Waarmee kunnen we dit doen? (Focus) | **Technologische innovatie gericht op informatie-ontsluiting**: datamining, koppelen van informatiebronnen, videocontentanalyse, realtime vs. offline<br>**Procesinnovatie gericht op informatiegestuurd optreden**: risicoprofilering voor analyse van grote informatiestromen en koppeling van bronnen (kredietregistratie, kenteken, onroerend goed, …), burgerparticipatie<br>**Kwalitatieve en kwantitatieve analyse** van multimodale (burger-) meldingen op eigen initiatief c.q. n.a.v. oproepen (meldkamer, twitter, website voor registratie van meldingen etc.), analyse van sociale media |
| Wie begeleidt? | Bart Custers (Coordinator/VenJ) AIVD, NCTb, VTSPN, NICC |
| TNO-team | Karin de Jong (trekker) |

### *3.2.3.3 Met VenJ en stakeholders afgestemde onderzoeksvragen*

**Vraag 1: Ontwikkelingen, methoden en technieken voor ontsluiting van nieuwe media (en wat kunnen we ermee?)**
Bij deze onderzoeksvraag ligt de focus op de technologie voor mining van informatie uit nieuwe en bestaande bronnen. Invalshoeken zijn:

- Welke informatiebronnen leveren (de meeste) zinvolle informatie? Hoe verhouden de kosten en baten zich hiervan? Welke kwaliteit hebben ze (betrouwbaarheid, actualiteit, juistheid)? ***(Beschrijvend/vergelijkend)***
- Hoe kunnen verschillende soorten informatiebronnen optimaal bij elkaar worden gebracht? (beeld, spraak, data, video,…) Tbv analysedoeleinden en operationele inzet? ***(Probleemoplossend)***
- Te veel informatie is zowel voor de privacy als voor het veiligheidsapparaat een slechte zaak: Hoe kun je op voorhand bepalen of bepaalde informatie relevant zal zijn; hoe pas je het "select before you collect" doelmatig toe? [anoniem rechercheren / revocable privacy] Hoe kun je tegelijkertijd de (maatschappelijke) veiligheid verhogen en de privacy beter beschermen door systemen zo in te richten dat je alleen informatie over overtreders te zien krijgt. ***(Probleemoplossend)***
- Hoe kunnen (de in ontwikkeling zijnde) technieken voor efficiënte data verrijking, semantic annotation (web 3. 0 technieken -o.a. het semantische

web-, collaborative tagging en rating) goed worden ingezet in het maatschappelijke veiligheidsdomein? ***(Beschrijvend, Evaluerend, Probleemoplossend)***
- Kun je afwijkende informatiepatronen in openbare bronnen (twitter, discussiefora, etc…) herkennen en hieruit mogelijke dreigingen/risico's en opportunities afleiden (afwijkend gedrag in informatiestromen). Hieronder valt ook het opstellen van profielen en normen, trends, indicatoren (kwalitatief en kwantitatief) ***(Testcases/ experimenteren)***
- Hoe ontwikkelen de sociale media zich de komende 10 jaar? Welke impact heeft dit op de samenleving en veiligheidsbeleving? ***(Beschrijvend/ Voorspellend)***

**Vraag 2: Ontwikkeling van betere informatievoorzieningsystemen voor ondersteuning en sturing van veiligheidstaken**

Bij deze onderzoeksvraag ligt de focus op het matchen van de behoefte aan informatie voor het uitvoeren van operationele veiligheidstaken met de potentieel te verkrijgen informatie uit nieuwe en bestaande bronnen. Invalshoeken zijn:
- Waar is potentieel hoge meerwaarde voor operationele veiligheidstaken te verwachten van het simultaan analyseren van (meer) reguliere informatiesystemen, actueel binnenkomende meldingen/waarnemingen en nieuwe media. Wat zijn bruikbare producten voor crisismanagement en voor meer heterdaads bij opsporing? **(Evaluerend)**
- Op welke wijze moeten informatiebronnen (intern, extern, intern + extern, beeld – tekst –geluid) worden gekoppeld om te leiden tot informatieverrijking bruikbaar voor operationele diensten (1+1 =3)? ***(Probleemoplossend)***
- Op welke wijze kunnen open en gesloten databronnen worden gecombineerd? Hoe kunnen informatiegebruikers/analisten tools en databronnen naar eigen inzicht koppelen? ***(Probleemoplossend)***
- Hoe kun je een proces inrichten dat automatisch relevant materiaal crawlt en vastlegt op een wijze die forensisch onderzoek faciliteert? ***(Probleemoplossend)***
- Op welke wijze kan kennis over afgesloten zaken en de effectiviteit van de interventies die daarin gebruikt zijn beschikbaar gemaakt worden voor een beslissingsondersteunend systeem ***(Evaluerend)***
- Verkenning van noodzakelijke vernieuwingen/ innovaties bij operationele veiligheidsdiensten om optimaal gebruik te kunnen maken van de nieuwe informatie-analysebenaderingen (training/opleiding personeel/ soort personeel, aanpassing van proces, organisatie, technologie etc…) **(Probleemoplossend/ Voorspellend)**

**Vraag 3: Hoe kunnen privacy en vertrouwelijkheid de vereiste aandacht krijgen bij de nieuwe informatieanalyse-methoden voor ondersteuning van veiligheidstaken?**

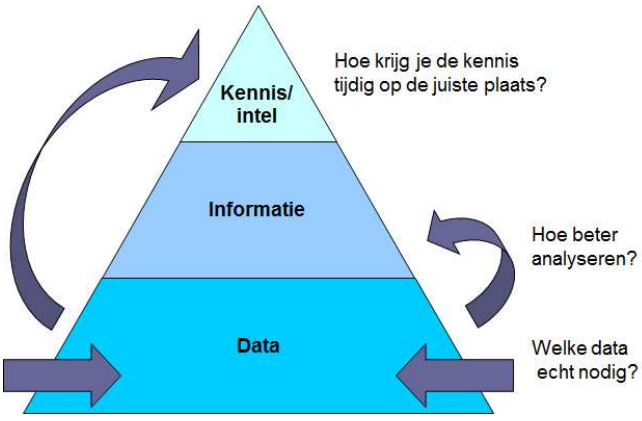
Bij deze onderzoeksvraag ligt de focus op de randvoorwaarden en belemmeringen bij het benutten van potentieel te verkrijgen informatie uit nieuwe en bestaande bronnen voor het uitvoeren van operationele veiligheidstaken met de. Invalshoeken zijn:
- Wat zijn de verwachte ontwikkelingen op gebied van privacy en welke impact heeft dit voor het gebruik van sociale media, burgerparticipatie etc… in operationele veiligheidstaken ***(Voorspellend)***

- Bij het verzamelen en combineren van allerlei gegevens worden profielen van personen, groepen en locaties opgebouwd. Op basis van deze profielen worden verwachtingen over eventueel maatschappelijk ongewenst gedrag geformuleerd, waarop eventueel weer acties worden ondernomen (bv. preventief surveilleren, volgen, hinderen, vastzetten). Hoe ver moet/mag je hierin gaan? Wat is het morele kader ***(Evaluerend),*** welke gevolgen heeft dat voor de maatschappij ***(Evaluerend)*** en op welke manier zou dit via wetgeving vormgegeven kunnen worden ***(Probleemoplossend)***?
- Hoe maak je het proces van burgerparticipatie controleerbaar/beheersbaar: in hoeverre sta je anonieme aangiftes toe? Welke risico's zijn er ten aanzien van zwartmaken van onschuldige personen? Welke informatie kan burgerparticipatie opleveren? Zijn er contexten waarbinnen burgerparticipatie juist wel of juist minder zinvol is? ***(Evaluerend)***

#### *3.2.3.4 Voortgang in 2011*

In samenspraak met de voor dit topic relevante stakeholders (MinJus, KLPD/IPOL, Politie, NCtb, BZk) wordt in 2011 gewerkt aan vijf onderwerpen in parallelle projectgroepen:

1. **Anomaliedetectie**: ontwikkelen van een demonstrator die automatisch afwijkende patronen in communicatie op internet herkent (twitter als casus). Resultaat: demonstrator
2. **Gecombineerde analyse beeld en tekst**: ontwikkelen van een demonstrator waarmee tekst- en beeldmining gecombineerd worden bij het zoeken. Resultaat: demonstrator
3. **Betrouwbaarheid van crowdsourcing**: hoe te waarborgen? Resultaat: artikel/paper
4. **Informatieoverload**: welke maatregelen zijn effectief in het voorkomen danwel bestrijden van informatieoverload? Resultaat: rapport maatregelen; advies rondom mogelijke toepassing van maatregelen bij KLPD/ IPOL
5. **Experiment 'Zoeken in video':** verder ontwikkelen van video zoektechnologie voor personen, object en locaties met deelname aan internationale benchmark 'TRECVID 2011'.




Daarnaast wordt een visie rondom toepassing van **social media** door veiligheidsorganisaties opgesteld (resultaat: beknopt boekwerk). Tot slot wordt een advies opgesteld voor het omgaan met **privacy** in relatie tot de 5 bovengenoemde vraagstukken (resultaat: richtlijnen voor omgaan met privacy).

De onderwerpen worden zoveel mogelijk samen met stakeholders uitgewerkt. Bijvoorbeeld rondom anomaliedetectie is input/ casuïstiek geleverd vanuit KLPD/IPOL en Politie Haaglanden en wordt overlegd over de beoogde en behaalde resultaten.

**Intensivering samenwerking**
Als gevolg van de activiteiten binnen topic 3 is de samenwerking tussen TNO en de diverse stakeholders versterkt: zo zijn er contacten gelegd met het IRN (internet recherchenetwerk) wat heeft geleid tot samenwerking bij het opstellen van een voorstel voor analysetooling voor het IRN; met het PAC (programma aanpak cybercrime) waarbij de projecten zijn afgestemd en opgelijnd over en weer en het programma HDIef (Digital Fingerprinting) van de NCTb. Daarnaast is een samenwerkingsovereenkomst gesloten tussen TNO en IPOL waarin diverse initiatieven zijn opgestart voor gezamenlijk onderzoek. Daarnaast staan afspraken gepland met de politieacademie en het KLPD om mogelijkheden voor verdergaande samenwerking te verkennen.

**Kennisdeling**
Het netwerk dat is en wordt opgebouwd maakt het mogelijk dat de kennis die binnen het onderzoeksprogramma wordt opgebouwd snel aan de relevante stakeholders beschikbaar kan worden gesteld en kan worden getoetst of dit ook voldoet aan de behoeften.
Op 12 oktober 2011 wordt door SMVP/CCV een congres georganiseerd rondom het thema publiek-private samenwerking (wie maakt Nederland veiliger?). Op dit congres verzorgt TNO een workshop rondom het onderwerp sociale media.

*3.2.3.5 Voorgestelde zwaartepunten voor voortzetting in 2012*
Op basis van de bereikte resultaten in 2011 en gesprekken met de stakeholders is voor 2012 gekozen voor een vijftal onderwerpen. In oktober 2011 worden de onderwerpen in overleg met de stakeholders uitgewerkt tot concrete projecten. Hierbij streven we ernaar om zoveel mogelijk samen met één of meerdere stakeholders een onderwerp uit te werken. Op die wijze zijn we in staat om snel zicht te krijgen op de toepasbaarheid van de ontwikkelde kennis.

1. Hoe gaan veiligheidsprofessionals die met grote hoeveelheden informatie werken te werk? Op welke wijze kun je deze groep het beste ondersteunen met technologie, training/opleiding en slimme processen (zoals gedistribueerde taken, bijv. telepolitie)? Focus op mens – systeem interactie.
2. "Hoe meet je de meerwaarde (kwalitatief en kwantitatief) van de inzet van instrumenten/ tools die worden ingezet voor het verwerken van grote hoeveelheden informatie?" Het combineren van diverse (reeds bestaande) losse tools; beoordeling van effectiviteit en kwaliteit van tools. Welke tools werken goed voor welk soort vragen in welke omstandigheden/omgeving? Hier inzicht in genereren. Denk hierbij aan inzet van sociale media, textmining, beeldanalyse etc.
3. Anomaliedetectie. In aansluiting op de activiteiten van 2011 uitbreiden en verfijnen van de mogelijkheden. Zorgen voor brede toepasbaarheid bij stakeholders. Uitvoeren diverse gerichte experimenten (vb. vroegtijdig opkomende incidenten signaleren; toepassing op meerdere sociale media (handhaving/opsporing)).

4. Het zoeken en vinden van individuen (bv. passagierslijsten, of op internet). Profiling uitwerken. Niet alleen netwerkanalyse op naam/nummer, maar ook op basis van kenmerken, of als afwijking. (Niet zoeken naar de speld in de hooiberg, maar zoeken naar het ding in de hooiberg dat geen hooi is.) Wat is de echte identiteit (veel mensen gebruiken meerdere identiteiten)? Verandert de identiteit?
5. Het ontwikkelen van een triagemethode om het Select-before-you-collect principe vorm te geven. De hoeveelheid data explodeert, en dat is onwenselijk. Door het ontwikkelen van methoden en technieken die het mogelijk maken het verwachte toekomstig nut van informatie te bepalen (conform risico gebaseerde analyse of bijvoorbeeld proportionaliteit kwantificeren) kan het “select before you collect”- principe op een zo laag mogelijk niveau worden toegepast zodat grote hoeveelheden (onbruikbare) informatie ten behoeve van handhaving en opsporing worden voorkomen.

De onderwerpen sociale media en privacy zullen in al deze onderwerpen een rol blijven spelen. Op dat vlak zullen dus ook nog activiteiten worden verricht. De exacte vorm ervan zal in oktober worden vastgesteld als duidelijk is op welke wijze bovengenoemde vijf onderwerpen nadere uitwerking zullen krijgen.

**Beoogde resultaten**
We verwachten bij het uitwerken van deze thema’s tot concrete handvatten te komen voor stakeholders aan de hand waarvan ze beter in staat zijn om hun eigen informatieverwerking in goede banen te leiden en te stroomlijnen. De resultaten zijn ondersteunend voor het verder professionaliseren van het informatie gestuurd werken van de veiligheidsorganisaties. Het vormt de basis voor de processen intelligence, handhaving, opsporing en crisisbeheersing.
Concrete toepasbaarheid ligt vooral op het domein van de toezichtcentrales/meldkamers (Nationale Politie, KMar), analysewerkzaamheden (o.a. BZK, NCTb, IPOL), (internet-) recherchewerkzaamheden (Nationale Politie, KMar), ondersteuning van de informatiefunctie in het front-office/ back- office concept (Nationale Politie).

**Intensivering samenwerking**
In 2012 wordt de samenwerking met de huidige partijen gecontinueerd en verder uitgebouwd. Daarnaast is het de intentie om de samenwerking met de Nationale Politie te verstevigen. Hiertoe is vanuit de korpsleiding van de KLPD ook de intentie uitgesproken.

### *3.2.4 Delen en benutten van informatiestromen voor het samen uitvoeren van veiligheidstaken (Beter benutten van informatiestromen)*

#### *3.2.4.1 Omschrijving van het topic*
De informatievoorziening in het veiligheidsveld staat voor de uitdaging om beschikbare gegevens, informatie, interpretaties en lessons learned beter te benutten over de grenzen van organisaties en onderdelen daarvan. De belangrijkste sleutels om daartoe te komen zijn samenwerking en het gebruik maken van de collectieve kennis en ervaring. Informatie kunnen verspreiden is niet genoeg. Delen (ook bewaren) en benutten van de informatiestromen zijn cruciale vervolgstappen.

Dit vraagt het tot stand brengen van een rolgericht (risico- en vraaggestuurd) informatieaanbod in de veiligheidsketen. (Kosten)effectiever samenwerken in ad hoc samengestelde keten en netwerken wordt dan mogelijk. Nu is veelal sprake van of een te klein, of een te groot aanbod van informatie. Informatie wordt beperkt gedeeld, of de gedeelde informatie wordt zonder rekening te houden met de gebruiker in grote hoeveelheden “op zijn of haar bordje gelegd”. Dit laatste met het risico van informatie overload en micromanagement. Basis voorwaarden om dit te veranderen zijn:

- vertrouwen
- inzicht in elkaars competenties, verantwoordelijkheden en prioriteiten (organisational awareness)
- interoperabiliteit (technisch, semantisch en qua uitwisselingsbereidheid)
- gedeeld begrip
- samenwerking en afstemming op diverse niveaus voor wat betreft doelstellingen, planning en uitvoering

Onderzoeksuitdagingen die daarmee gepaard gaan zijn:

- Hoe bereiken we dat genetwerkte organisatiedelen voldoende vertrouwen hebben in (bereid zijn afhankelijk te zijn van) elkaar en van techniek?
- Hoe kunnen we binnen een genetwerkte en dynamische organisatie een beeld onderhouden van de structuur van die organisatie en van de competenties, verantwoordelijkheden, activiteiten en prioriteiten van de verschillende organisatiedelen?
- Hoe zorgen we ervoor dat de verschillende deelorganisaties elkaar werkelijk begrijpen – overbruggen van semantische verschillen – welke beelden en handelingsperspectieven roept een situatiebeschrijving bij de verschillende deelorganisaties op?
- Welke rolgerichte gebruikersinterfaces zijn nodig voor het creëren van op elkaar afgestemde situational awareness en coördinatie van taken?
- Hoe creëren we een toegankelijk collectief geheugen en hoe kunnen we op basis daarvan voorspellend vermogen opbouwen? Het gaat dan zowel om locatie specifieke historie als om lessons learned van soortgelijke incidenten in het verleden.

Niet alleen binnen de veiligheidsketen maar ook de samenwerking tussen publiek en privaat vereist structurele verankering in de informatievoorziening voor de uitvoering van veiligheidstaken. Netcentrisch werken komt binnen het veiligheidsveld op gang. Een volgende stap is publiek private netcentrische informatievoorziening, waarbij de vitale sectoren onderdeel worden van het (virtuele en fysieke) netwerk. Dit is een belangrijke vervolgstap op de afspraken zoals die nu tussen het veiligheidsveld en de private sector worden gemaakt.

Inzicht in bovenstaande vraagstukken is noodzakelijk om veiligheidstaken (kosten)effectiever uit te kunnen voeren. Technologische doorbraken spelen daarbij slechts een beperkte rol. Innovatie op het vlak van de mens (cultuur en opleiden/trainen/oefenen), proces, organisatie en rond het juridisch kader zijn zeker zo belangrijk. In het VP zal basiskennis worden ontwikkeld met een focus zoals die onderstaand is uitgewerkt en afgestemd met de door VenJ gecoördineerde begeleidingsgroep. De basiskennis zal veelal tot stand worden gebracht binnen fieldlabs en in nauwe samenwerking met het veiligheidsveld zelf. Als vervolg op de kennisontwikkeling is doorontwikkeling in nationale en internationale

innovatieprogramma's voorzien gevolgd door vanuit stakeholders gefinancierde innovatietrajecten.

Voorbeelden hiervan zijn:

- Politie informatiesysteem (bijvoorbeeld in de vorm van PDA's)
- Alerteringsysteem Terrorismebestrijding (ATb) versie X.0
- Crisis Management Systeem versie X.0
- Vernieuwing meldkamers / meldkamerconcept
- Mobiele Data Terminal (MDT) versie X.0
- Hulpverlener InformatieManagement Systeem (HIMS) versie X.0
- Vernieuwing uitkijkcentrales
- Control rooms - samenwerkende teams
- Daar waar voorspellend vermogen direct toegevoegde waarde heeft

#### *3.2.4.2 Focus van het topic*

| | |
|---|---|
| Waar gaat het precies over? | Delen en benutten van informatiestromen voor het samen uitvoeren van veiligheidstaken.<br>Informatievoorziening als basis voor het verbeteren van de beeldvorming, oordeelsvorming, besluitvorming en evaluatie; zowel gericht op multi-kolom/-laag optreden als op optreden binnen kolommen en zowel gericht op repressie als op preventie en pro-actie). |
| Wie betreft het? | Brandweer, Politie, GHOR, Defensie, Gemeenten, Veiligheidsregio's, de waterkolom, de vitale sectoren, private beveiligingsorganisaties en burgers/bedrijfsleven (multi-kolom) - vanaf het lokale tot en met internationaal niveau (multi-laags) |
| Waarom is het onderzoek van belang? | Informatie- en risico-gestuurd en gedifferentieerd (preventief, proactief, of repressief) veiligheidsoptreden zijn essentieel voor een verdere doorgroei van het kwaliteitsniveau van dit optreden (*doing better things* versus *doing things better*). Dit type optreden valt of staat met het hebben van de juiste informatie op het juiste moment op de juiste plaats, en het hierop laten volgen van de juiste actie van de juiste actor(en). |
| Waarmee kunnen we dit doen? (Focus) | • Ontwikkeling behoefte- en risico gestuurd informatieaanbod dat het handelingsperspectief duidelijk maakt, incl. de middelen om dit aanbod te generen en de werkwijzen om met dit aanbod effectief op te treden<br>• Intuïtieve human interfaces die de gebruiker ondersteunen in zijn handelen<br>• Ontwikkeling collectief geheugen van effectiviteit van gerealiseerde operationele aanpak en simulatiemethoden voor het vergroten van het voorspellend vermogen bij voorbereiden en uitvoeren van operationele taken<br>• Inrichting van de informatie-uitwisseling tussen publiek en privaat (m.n. vitale sectoren) |
| Wie begeleidt? | Jan Lavèn (Coördinator; subarena Geïntegreerde systemen /CIV), Marjan Heijman (NVBR), NCTV (alerteringssysteem terrorisme-bestrijding, VTSPN |
| TNO-team | Josine van der Ven (trekker), Willem Treurniet |

*3.2.4.3 Met VenJ en stakeholders afgestemde onderzoeksvragen*

**Vraag 1: Informatieaanbod voor samenwerkende professionals in de veiligheidsketen**
Hoe kan het aanbod aan informatie voor de professionals zo worden georganiseerd (zowel vraag als risico gestuurd) dat het handelingsperspectief duidelijk is voor alle betrokken niveaus van de samenwerkende organisaties en op basis daarvan effectief wordt geacteerd?

Focus op
- Professionele gebruikerscategorieën, hun behoeften aan informatie, hun motivatie tot delen van informatie met anderen
- Hergebruik en reorganiseren van informatie afhankelijk van risico en doel/behoefte gebruiker, verticaal (alle niveaus eigen keten) en horizontaal (tussen ketenpartners)
- Structuur van informatievoorziening afgestemd op de rollen van de samenwerkende gebruikers in de veiligheidsketen (databronnen, geautomatiseerde voorbewerking van gegevens tot snel interpreteerbare informatie, karakteristieke vraagstellingen van gebruikerscategorieën)
- Voorselectie van handelingsperspectieven op basis van risicoprofielen
- Draaiboeken (werkwijzen) voor specifieke handelingsperspectieven; CD&E

**Vraag 2: Nieuwe generatie gebruikersinterfaces**
Hoe kan beschikbare informatie zo worden gepresenteerd dat de situational awareness voor gebruikers maximaal is?

Focus op
- Effectieve human interfaces met gebruikmaking van augmented reality (samensmeden van camerabeelden en andere gegevens uit de werkelijkheid met realistische modellen tot een geïntegreerd geheel, zodat de gebruiker een met gegevens verrijkte werkelijkheid voor zich ziet)
- Multimodale communicatie (zichtbare/hoorbare/tactiele alerteringssignalen, voorbewerkte beelden, instructies via beeldscherm/gesproken tekst, expliciteren van dilemma's waarover besluit urgent is)

**Vraag 3: Collectief geheugen en simulaties voor voorspellen**
Hoe kunnen het collectieve geheugen en simulaties worden ingezet om voorspellend vermogen te creëren voor preventie, repressie en pro-actie?

Focus op
- Consequenties per inzetfase
- Ondersteuning besluitvorming over op- en afschaling
- Ontsluiten en borgen van events en gebeurtenissen
- Simulaties; CD&E
- Nader te specificeren doelgroep.

**Vraag 4: Publiek-private informatievoorziening**
Welke onderlinge informatievoorziening is noodzakelijk om hulpdiensten en de vitale sectoren effectief met elkaar te laten samenwerken, zowel bij incidenten en crisis als bij de voorbereiding daarop, en hoe is die informatievoorziening in te richten (middelen, typen informatie, koppelvlakken, werkwijzen)?

Focus op

- Ketenafhankelijkheidsanalyses
- Koppelvlakken, zowel wat betreft systemen als processen
- Selectie geschikte middelen
- Type informatie
- Simulatie van incidentontwikkeling met handelingsperspectief in verschillende scenario's
- CD&E
- Uitwerking voor een karakteristieke functie (suggestie: Alerteringssysteem Terrorismebestrijding)

*3.2.4.4 Voortgang in 2011*

De werkzaamheden in deze beginfase van het programma hebben zich met name toegespitst op het nader uitwerken van de onderzoeksvragen zoals genoemd in de vorige paragraaf en de verkenning van te betrekken deskundigen uit het veld. De uitdaging bij een vraaggestuurd programma zoals "Delen en benutten van informatiestromen voor het samen uitvoeren van veiligheidstaken" is daarbij voldoende ver vooruit te kijken en ook aan te sluiten bij actuele plannen van belangenpartijen.

**Informatieaanbod voor samenwerkende professionals in de veiligheidsketen**

De werkzaamheden met betrekking tot deze vraag hebben zich toegespitst op de ontwikkeling van een informatiestructuur ten behoeve van de vraag 'wat moeten professionals **over** elkaar weten om een doelgerichte samenwerking en afstemming te bereiken bij de bestrijdingsinzet? (Collaboration Awareness)'. Anders dan bij vraag 4 gaat het hier niet over welke incidentgegevens men met elkaar moet delen ten einde een beter beeld van de situatie te krijgen. Het doel binnen dit vraagstuk ligt op het uitwisselen van cruciale gegevens over de betrokken hulporganisaties om tot een beter op elkaar afgestemde aanpak van de bestrijdingsmogelijkheden te komen. Hiertoe is er samenwerking gezocht met een aantal veiligheidsregio's en de Inspectie Openbare Orde en Veiligheid om vast te stellen op welke manier het ontbreken van 'collaboration awareness' op dit moment al impact heeft op de samenwerking tussen professionele hulporganisaties. Er wordt ook samengewerkt met de VU waar in een promotietraject meer onderzoek wordt gedaan naar totstandkoming van wederzijdse afstemming bij hulporganisaties. De resultaten van 2011 zijn een artikel waarin inzichtelijk wordt gemaakt voor de regio's wat de problemen aangaande dit onderwerp zijn en hoe zij die kunnen herkennen, en een eerste prototype oplossing.

**Nieuwe generatie gebruikersinterfaces**

Het speelveld betreffende de meldkamers is in beeld gebracht. Op dit moment is er veel gaande op meldkamergebied. In de eerste plaats is er sprake van een herindeling (schaalvergroting) van de meldkamers. Denk hierbij aan het samengaan van de meldkamers van Friesland, Groningen en Drenthe in de Meldkamer Noord-Nederland op 28 november a.s. Daarnaast is er in de regio's Flevoland, Gooi en Vechtstreek en Utrecht ook sprake van concentratie van meldkamercapaciteit. Aanvullend wordt kritisch gekeken naar de bemensing en uitrusting van deze nieuwe meldkamers. Dit zijn ontwikkelingen die nu gaande zijn. Om het VP-topic goed aan te laten sluiten bij deze nieuwe ontwikkelingen kijken we o.a. naar de ontwikkelingen die TNO heeft helpen realiseren bij commandocentrales binnen

Defensie. TNO heeft in het kader hiervan het concept van ‘abstractiehiërarchie’ toegepast. Het idee hierachter is dat de informatie over de omgeving op verschillende niveaus van abstractie kan worden gerepresenteerd aan de meldkamercentralist. Deze manieren van abstractie helpen de centralist straks bijv. beter de schaalgrote (ernst en impact) te bepalen, de betrokken ketenpartners vast te stellen en hulpdiensten beter te informeren ten behoeve van de bestrijding. De vertaling zal eind van 2011 opgeleverd worden, zodat het in de komende jaren ingezet kan worden binnen de verdere ontwikkeling van het programma. Daarnaast ligt er een memo met een schets van de belangrijkste –huidige- knelpunten die momenteel in de meldkamers worden ervaren.

**Collectief geheugen en simulaties voor voorspellen**
Op basis van onze huidige onderzoeken is de vraagstelling aangescherpt. De literatuurstudie naar collectief geheugen bracht twee punten naar voren die belangrijk zijn voor toekomstige ontwikkelingen: het betreft de ervaringen van het individu welke opgenomen worden door het collectief. Het is dus enerzijds belangrijk te onderzoeken hoe een individu zijn/haar ervaring kan delen. Minstens zo belangrijk is te onderzoeken hoe de individuele ervaringen opgenomen kunnen worden door het collectief. Hierbij kan ook gekeken worden hoe de impact van lessen uit evaluaties (o.a. Inspectie en Onderzoeksraad) vergroot kan worden. Het onderzoek in 2011 zal zich daarom richten op het in kaart brengen van de keten van het ‘ontstaan van de les’ (evaluatie) tot de opname van die les door het collectief (opleidingen voor starters dan wel professionals) en de drempels die daarbij spelen. Bij externe domeinen zal gekeken worden naar de succesverhalen zodat er –in 2011- een overzicht komt van succesvolle manieren om lessen van het individu beschikbaar te maken aan de rest, zowel in de eigen organisatie als over organisatiegrenzen heen.

**Publiek-private informatievoorziening**
D nadruk in 2011 heeft gelegen op het operationaliseren van het raamwerk dat inzicht geeft in ‘**wat** publieke en private partijen met elkaar moeten delen om tot een samenwerking te kunnen komen.’ Anders dan bij de eerste vraag gaat het hier dus niet om organisatie informatie (wie is er bij betrokken) maar om het vaststellen van wat er aan de hand is, het opbouwen van het gedeelde actuele beeld. Dit raamwerk wordt in 2011 samen met een aantal veiligheidsregio’s en vitale (private) partners aan de hand van een scenario uitgewerkt. Daarmee komt er een methode beschikbaar hoe het raamwerk door publieke en private partijen kan worden ingezet als onderdeel van de gesprekken om te komen tot bijvoorbeeld convenanten over informatie-uitwisseling en samenwerking.

**Informatiestromen beter benutten en samenwerken**
Om het onderzoek in 2012 beter op te lijnen en gerichter op de ontwikkelingen in de veiligheidsregio en bij de politie te laten aansluiten is er een vijfde onderzoeksvraag geformuleerd: de ontwikkeling van een visie op “Informatiestromen beter benutten en samenwerken”. Hierbij wordt ingespeeld op de huidige ontwikkelingen van het netcentrisch werken concept. Hierbij ligt momenteel de nadruk op het ondersteunen van het delen van informatie tussen professionele hulporganisaties. Deze ontwikkeling is niet alleen een technische, waarbij systemen het mogelijk maken om informatie uit te wisselen. De impact op de manier van werken (proces) en de capaciteiten en vaardigheden van de mensen (mens/organisatie) spelen daarin een belangrijke rol om te komen tot een benutting van de voordelen van informatie-delen. Volgens het gedachtengoed achter het netcentrisch werken concept heeft

het delen van informatie een grote impact op de manier waarom mensen (en organisaties) samen gaan werken en hun plannen gaan maken. Deze gevolgen zijn reeds op hoofdlijnen vastgelegd in een ‘netcentrisch groeimodel’, gebruikmakend van dezelfde drie hoofdstromen: mens, proces en techniek. Door deze hoofdlijnen te verwerken in de visie ontstaat een roadmap die gebruikt kan worden om voor 2012 de werkzaamheden binnen het programma op te lijnen (met de toekomstige ontwikkelingen in het domein). Daarnaast kan deze visie gebruikt worden om het veld handvatten te geven bij de doorontwikkeling van het netcentrisch werken concept volgens het door TNO ontwikkelde groeimodel.

Daarnaast zijn bijdragen geleverd aan:

- Symposium van het IP-Water-programma Flood Control 2015 d.d. 20 april 2011; in de vorm van twee workshops: *Liaison 2.0* en *Crisiscommunicatie op maat*.
- Het FP-7-project ACRIMAS. Aftermath CRIsis MAnagement System-of-systems (ACRIMAS). In de projectbeschrijving wordt het doel als volgt geformuleerd: “The project will lead to the validation of shared user needs and the definition of a demonstration and assessment method with associated metrics to define a continuous process of capability improvements. […] The final objective is to enable a gradual evolvement of CM capabilities, procedures, technologies, policies and standards through real field tests, facilitating European wide collaboration, cooperation and communication in CM and improving cross-fertilisation between MS organisations”. In dit project wordt samengewerkt met trendsettende partijen op het gebied van crisismanagement in een consortium onder leiding van Fraunhofer Gesellschaft.
- Het pijler 2-project TOKO (Trainingsomgeving voor Grootschalig Keten optreden). Dit project gaat binnenkort formeel van start.

Het FP7-project XP-DITE is gegund en bevat ook werkpakketten gericht op het samenwerken door slimmer informatie te delen. De doelstelling luidt: “The objective of XP-DITE is to develop, demonstrate and validate a comprehensive approach to the design and evaluation of integrated (air port) security checkpoints”. TNO is leider van een groot internationaal consortium, waarin ook Schiphol en de KMar participeren.

#### *3.2.4.5 Voorgestelde zwaartepunten voor voortzetting in 2012*

De ervaring en verwachte resultaten van 2011 hebben er toe geleid dat we voor 2012 een aanscherping willen voorstellen om beter aan te sluiten bij de ontwikkelingen die wij in de nabije toekomst voorzien. Drie belangrijke ontwikkelingen waarop alle vier de onderzoeksvragen in het topic “Delen en benutten van informatiestromen voor het samen uitvoeren van veiligheidstaken” wordt aangescherpt:

1. Aansluiten bij de ontwikkelingen in de veiligheidsregio’s inzake het netcentrisch werken concept en nieuwe concepten voor ‘Leiding en Coördinatie’.
2. Netcentrisch werken binnen het sociale veiligheidsdomein.
3. Onderzoek niet alleen ondersteunen met wetenschappelijke ‘argumenten’, maar ook met evidence-based ‘argumenten’.

– Ad 1. Aansluiten bij de ontwikkelingen in de veiligheidsregio’s inzake het netcentrisch werken concept
  Afgelopen jaar is er in de verschillende veiligheidsregio’s veel ervaring

opgedaan met het netcentrisch werken principe, waarbij het delen van informatie het belangrijkste aandachtspunt was. Nu in de ketens de informatie via dit principe gedeeld wordt, zien we dat de samenwerking zich daarop gaat aanpassen. Mensen gaan informatie langzaam op een andere manier met elkaar delen, meer gericht op de kennis die men heeft van de andere partij en de verwachtingen van diens inzet. Om die nieuwe vorm van samenwerking, informatiegestuurde samenwerking, verder te ondersteunen, en de volgende stap van het netcentrisch werken principe (samen werken) te ondersteunen moet het programma aangescherpt worden. Het gaat hierbij om ondersteuningen op het gebied van mens/organisatie, proces en techniek. Als de veiligheidsregio's en hun ketenpartners bij deze doorontwikkeling niet gesteund worden zal men de nieuw verworven efficiëntie niet verder kunnen benutten. Denk hierbij bijvoorbeeld aan de tijdswinst die men nu behaald door informatie over de situatie snel te kunnen delen. Het doel hiervan is om sneller met een multi-disciplinair bestrijdingsplan te komen, zodat het incident sneller bestreden wordt, met minder slachtoffers. Niet alle teams zullen in staat zijn om van 'informatie-delen' ten behoeve van een actueel gedeeld beeld te komen naar een integraal bestrijdingsplan. Dat stelt eisen aan de experts die betrokken zijn bij de incident bestrijding, dat vraagt om een procedure die het vertrouwen ondersteunt. Zonder handreikingen hoe teams deze stap voorwaarts kunnen maken ligt het voor de hand dat zij terug zullen vallen op procedures en technieken die zij kennen.

- Ad 2. Netcentrisch werken binnen het sociale veiligheidsdomein
  Om de veiligheid in wijken en buurten op voldoende hoog niveau te krijgen en te houden moeten vele professionals van verschillende disciplines met elkaar informatie delen en samenwerken. Het veiligheidshuis richt zich op probleemjongeren die met justitie in aanraking komen, maar dan is het eigenlijk al te laat. Centra voor jeugd en gezin kunnen al vroeg signaleren dat het mogelijk mis gaat met een jongere, daarbij hebben zij relevante ` nauwelijks informatie met elkaar, laat staan dat zij samenwerken. Het netcentrisch gedachtengoed en de ervaringen met dit gedachtengoed binnen het fysieke veiligheidsdomein zou hier een waardevolle bijdrage kunnen leveren. Dit onderwerp zal bij de vier de onderzoeksvragen gedurende 2012 en verder steeds meer aandacht krijgen.
- 
- Ad 3. Onderzoek niet alleen ondersteunen wetenschappelijke 'argumenten', maar ook met evidence-based 'argumenten'.
  De belangrijkste basis voor het onderzoek was tot nu vooral gelegen in wetenschappelijke argumenten. Door hier ook kwantitatieve 'evidence' aan toe te voegen wordt inzichtelijk waarom juist 'deze vraag' of 'die bepaalde focus' belangrijk is. Een voorbeeld hiervan is de 'bewering' dat steeds dezelfde lessons learned naar boven komen in een evaluatie. Voor het komen tot een goede oplossing om lessons learned te laten landen bij het collectief is het niet alleen belangrijk om te weten of deze bewering daadwerkelijk waar is, maar ook of dit voor een bepaalde categorie wel/niet geldt, en of dat voor bepaalde incidenten waar is, maar voor andere niet. Daarmee kun je gerichter opzoek naar het probleem achter het probleem, namelijk het waarom lessons learned niet 'geleerd' worden en kan de oplossingsrichting nog beter toegesneden worden op de problemen die in de praktijk leven.

Andere activiteiten die voor 2012 voorzien worden, gebaseerd op kennis opgedaan in 2011:

- Aansluiten bij Europees KP7onderzoek op het gebied van meldkamerontwikkelingen en het analyseren van grote hoeveelheden informatie.
- Verdere samenwerking formuleren met bijv. het vernieuwde NIFV die vanuit hun wettelijke rol behoefte hebben aan nieuwe kennis op het gebied van informatiegestuurd samenwerken ter ondersteuning van de veiligheidsregio's.

### *3.2.5 Cybersecurity*

#### *3.2.5.1 Omschrijving van het topic*

Het toenemend gebruik van ICT in alle delen van de maatschappij brengt naast kansen ook kwetsbaarheden met zich mee. Trendrapportages van organisaties als GovCERT en de nationale recherche laten zien dat misbruik van ICT sterk stijgt. Het gaat daarbij zowel om criminaliteit als het berokkenen van schade.
Dit topic richt zich op de bescherming van de cyberinfrastructuur tegen grootschalige dreigingen als opzettelijke verstoringen en misbruik.
Effectieve bescherming bestaat in het algemeen uit een evenwichtige verzameling maatregelen op het gebied van preventie, preparatie, detectie en respons. Zowel overheid als bedrijfsleven nemen reeds een groot aantal maatregelen op dit gebied. De snelle veranderingen in de beschikbare technologie, de toenemende verwevenheid van infrastructuren, de snelle introductie van nieuwe gebruiksmogelijkheden en de incoherentie van maatregelen over organisaties heen zorgen echter voor nieuwe dreigingen en kwetsbaarheden en vergen steeds opnieuw risicoafwegingen en innovatieve maatregelen.
Om het onderzoek binnen dit topic vorm te geven is in een bijeenkomst met een aantal beleidsbepalende organisaties op het gebied van cybersecurity (waaronder NCTb, VENJ/DGV, AIVD, Justitie, Defensie, vtsPN en NICC) een drietal onderwerpen benoemd waarop innovatie gewenst is.

Een belangrijke pijler binnen het onderwerp cybersecurity wordt gevormd door *detectie van misbruik* en bijbehorende mogelijkheden voor *opsporing en vervolging*. Er is behoefte aan methoden voor het analyseren van grote hoeveelheden gegevens, en ondersteunende analyse- en simulatiemodellen om misbruik vroegtijdig te herkennen. Hierbij richt het onderzoek zich niet op de afzonderlijke detectiesystemen, maar op het opbouwen van een gezamenlijk beeld uit een diversiteit aan informatiebronnen, zowel in aantal als type systemen. Speciale aandacht wordt besteed aan de toenemende functionaliteit van mobiele systemen, de hierbij komende risicofactoren en de mogelijkheden om hier in de opsporing op in te kunnen spelen.

Aangezien voorkomen van incidenten beter is dan genezen, is het wenselijk om al in het ontwerpstadium van systemen rekening te houden met security ('*security by design*'). Hierbij richt het onderzoek zich op het opzetten van een referentiekader om risicofactoren van nieuwe technologie snel te kunnen inschatten en op het uitvoeren van technologiescans van opkomende technologieën.

Een speciaal aandachtsgebied wordt gevormd door *cybersecurity voor de vitale infrastructuur*. De vitale infrastructuur bestaat uit sectoren en voorzieningen waarvan verstoringen of uitval ernstige impact kunnen hebben op de Nederlandse samenleving, zoals de energievoorziening, drinkwatervoorziening en de transportsector. Ook deze vitale sectoren zijn in steeds grotere mate afhankelijk van ICT. Het risico van domino-effecten in de vitale infrastructuur ten gevolge van kwetsbaarheden in de cyberinfrastructuur vormt nationaal en internationaal een belangrijk aandachtspunt.
Internationaal vindt samenwerking en gegevensuitwisseling plaats over dreigingen, kwetsbaarheden, maatregelen en onderliggende modellen. Binnen dit topic vindt op het de onderliggende modelvorming van cybersecurity intensieve internationale samenwerking plaats. Om ook nationaal optimaal aan te kunnen sluiten bij de vraagstelling van de vitale sectoren wordt nauw samengewerkt met de Nationale Infrastructuur tegen Cybercrime (NICC). De goede samenwerking van de vitale sectoren binnen de informatieknooppunten van het NICC wordt gebruikt om de sectoroverstijgende onderzoeksvragen te identificeren en de onderzochte en bewezen oplossingsrichtingen zo direct mogelijk aan de vitale sectoren te kunnen terugkoppelen.

Het sector-overstijgende karakter van ICT zorgt ervoor dat dit topic relatie heeft met een aantal onderzoeksonderwerpen binnen andere TNO-thema's.

- binnen het TNO thema Informatiemaatschappij wordt aandacht besteed aan het ongeautoriseerd binnendringen van afzonderlijke computersystemen/ netwerken
- het actief gebruik van cybermiddelen en het verstoren/bespioneren van communicatiesystemen valt onder het innovatiegebied Wereldwijd inzetbare krijgsmacht.

Tussen topic 5 en de genoemde onderzoeksonderwerpen binnen de overige thema's en innovatiegebieden zal nauwe afstemming plaatsvinden om onderzoeksonderwerpen af te stemmen en resultaten uit te wisselen.

#### *3.2.5.2 Focus van het topic*

| | |
|---|---|
| Waar gaat het precies over? | Dreigingen t.a.v. cyberinfrastructuur/cybergebruik en proactieve bescherming daartegen. Het gaat hier met name om opzettelijk verstoren om schade te berokkenen en om misbruik. |
| Wie betreft het? | Ministerie VenJ, NCTb, GovCERT, NICC, VTSPN, AIVD, KLPD, NFI, Logius, providers, VNO-NCW, Ministerie EZ, VNG, vitale sectoren, EU DG Home Affairs (p.m. Defensie, KMar, EDA) |
| Waarom is het onderzoek van belang? | Misbruik van de cyberinfrastructuur door kwaadwillenden dient tegengegaan te worden door proactieve en preventieve maatregelen, terwijl het daadwerkelijk misbruiken zo vroeg mogelijk moet worden opgespoord en geëlimineerd. Daarnaast dienen opzettelijke verstoringen tot een zo gering mogelijke schade te leiden aan de cyberinfrastructuur zelf en de daarvan afhankelijke gebruikers. |

| | |
|---|---|
| Waarmee kunnen we dit doen? (Focus) | • Methoden voor vroegtijdig herkennen en opsporen van misbruik van de cyberinfrastructuur.<br>• Ontwerp van de architectuur van de cyber-infrastructuur en gebruiksmodaliteiten die leiden tot vermindering van de mogelijkheid tot cybermisbruik (security by design).<br>Methoden voor verminderen van de afhankelijkheid van de vitale infrastructuur-sectoren in de maatschappij van verstoringen in de cyberinfrastructuur. |
| Wie begeleidt? | Rob Duiven (Coördinator VenJ/NCTV), Defensie, VTSPN, e.a. |
| TNO-team | Marieke Klaver (trekker) |

*3.2.5.3 Met VenJ en stakeholders afgestemde onderzoeksvragen*

**Vraag 1: Vroegtijdig herkennen en opsporen**
Hoe kan misbruik van de cyberinfrastructuur vroegtijdig worden herkend en opgespoord? Besteed hierbij speciale aandacht aan mobiele platformen.

Focus op:
- Instrumenten voor vroegtijdig herkennen van misbruik m.b.v. simulatie en modellen, rekening houdend met mogelijkheden voor opsporing en eliminatie
- Welke dreigingen kunnen ontstaan door de toenemende functionaliteit van mobiele platformen en wat zijn adequate maatregelen daartegen

**Vraag 2: Voorkomen door security by design**
Hoe is de schade door cybercrime tegen te gaan door security by design?

Focus op:
- Het opzetten van een referentiekader/-model van de cyberinfrastructuur voor een snelle beoordeling van potentiële additionele risico's van nieuwe ontwikkelingen (techniek, cybergebruik, dreigingen)
- Technology watch bescherming cyber-infrastructuur op architectuurniveau, inclusief gebruiksmodaliteiten die leiden tot vermindering van de mogelijkheid tot cybermisbruik
- Simulatie en analyse van effecten van dreigingen en effectiviteit bescherming cyberinfrastructuur (meerlaagsbescherming, keten-afhankelijkheid, noodvoorzieningen e.d.)
-

**Vraag 3: Hoe is het gevolg van cybermisbruik voor de vitale infrastructuur te beperken?**

Focus op
- Simulatie en analyse van effecten van dreigingen m.b.t. cyberinfrastructuur in relatie tot de vitale infrastructuur (keten-afhankelijkheid, meerlaags-bescherming) – internationale samenwerking
- Ontwikkeling generieke methoden en tools voor de beoordeling van de Cyberstatus van vitale sectoren – in samenwerking met de NICC

#### *3.2.5.4 Voortgang in 2011*

***Detectie van misbruik (mobiel systemen)***
*Doelstelling*: Het identificeren van dreigingen voor mobiele platformen en het ontwikkelen van oplossingsrichtingen voor het vroegtijdig detecteren van misbruik, inclusief het benoemen van mogelijkheden van opsporing en vervolging.
*Status:* De afgelopen periode is er een overzicht gemaakt van de ontwikkelingen op het vlak van mobiele apparaten en toepassingen en zijn de dreigingen op globaal niveau geïdentificeerd. De komende periode zullen er een aantal use cases worden gedefinieerd (op basis van de rol van de smartphone bij misbruik/misdaad). Op basis van deze use cases kan duidelijk gemaakt worden welke knelpunten er t.a.v. detectie bestaan en welke maatregelen er getroffen kunnen worden.
Voor de verdere uitwerking staan interviews gepland bij het Programma Aanpak Cybercrime en het NFI. Daarnaast zal er een presentatie worden gegeven voor het Informatieknooppunt Telecom.

***Security by design***
*Doelstelling*: Het ontwikkelen van een referentiekader en systematiek voor het beoordelen op beschermingsaspecten van nieuwe grootschalige technologieontwikkelingen en het ontwikkelen van methoden om hierin principes van security by design te introduceren. Hiervoor wordt als case studie de energiesector behandeld.
*Status:* Op het gebied van ICT binnen de energiesector staan veel ontwikkelingen gepland, met name rond smart grids. In de afgelopen periode is een overzicht opgesteld van de meest belangrijke ontwikkelingen en van de bijbehorende security aspecten. De komende periode zal worden gewerkt aan een referentiekader om deze security aspecten vanuit de perspectieven van de verschillende stakeholders inzichtelijk te maken. Hiervoor zal een referentie architectuur worden gebruikt.
Er wordt gezocht naar samenwerking met het informatieknooppunt energie en met Alliander.

***Cyber security vitale infrastructuur***
*Doelstelling*: Te komen tot ondersteunende methoden en modellen voor de uitwisseling van ‘security posture’ en gegevens die de cyberstatus van de vitale infrastructuur (gedeeld ICT-risicobeeld) en de effectiviteit van beschermingsmaatregelen inzichtelijk maken.
*Status:* Dit werkpakket werkt nauw samen met CPNI.nl en is iets later van start gegaan.
De werkzaamheden sluiten ook aan bij een Europees project Recipe, dat momenteel in de afrondende fase is.

***Ondersteunende modellen***
*Doelstelling*: Het ontwikkelen van een modellenbasis als ondersteuning bij het herkennen van mogelijke aanvalspatronen en het bepalen van het effect van maatregelen en de mogelijke impact van verstoringen.
*Status:* De afgelopen periode is een globale inventarisatie uitgevoerd van de requirements van modellen en is op hoofdlijnen onderzocht welke modellen beschikbaar zijn. Op grond van deze globale inventarisatie zal de komende periode meer gedetailleerd worden gekeken naar de binnen TNO en uit EU projecten beschikbare modellen.

***Aanvullende contacten***

In aanvulling op de in het kader van de werkpakketten gevoerde overleggen, is in de afgelopen periode inhoudelijk overleg gevoerd met een aantal partijen:

- Er is inhoudelijk overlegd met GovCERT. Deze zouden graag nauwer betrokken willen worden bij het programma. Er is afgesproken dat GovCERT ook kan deelnemen aan het begeleidingsteam.
- Daarnaast is samen met topic 3 overlegd met Ton Egberink van het Programma Aanpak Cybercrime. Het PAC wil graag nauwere afstemming met het VP.
- De Politie Academie, NFI en TNO willen de samenwerking op het gebied van cyber security versterken.

*3.2.5.5 Voorgestelde zwaartepunten voor voortzetting in 2012*

Door samenloop van privé-omstandigheden en vakanties van cruciale betrokken personen heeft de inhoudelijke afstemming over 2012 nog niet plaats gevonden. Mede gezien de snelle ontwikkelingen buiten TNO is dit overleg cruciaal en wordt er hier geen voorschot op genomen. Wel kan gezegd worden dat de omvang van dit aandachtsgebied snel toeneemt.

Een inhoudelijke afstemming van de onderzoeksonderwerpen voor 2012 zal nog plaatsvinden in overleg met het begeleidingsteam van het topic cybersecurity. Tevens dienen de resultaten van de eerste bijeenkomst van de Cyber Security Raad op 30 juni hierin te worden meegenomen.
Het Ministerie van Defensie wil voor een aantal onderzoeksvragen nauw samenwerken met het VP. Hiervoor worden in onderling overleg de onderzoeksvragen verder uitgewerkt. Er wordt naar synergie met de onderzoeksonderwerpen uit het vraaggestuurde programma gezocht.

Voor het topic cyber security bestaat een begeleidingsteam. Hierin nemen deel: V&J (Mark Bökkerink, opgevolgd door Rob Duiven), V&J (Esther van Beurden), EL&I (Peter Hondebrink), CPNI.nl (Auke Huistra), Erwin Raemakers (Programma Aanpak Cybercrime), Defensie (Matthijs Veenendaal). Tevens zal GovCERT worden uitgenodigd.

*3.2.6 Verkenningen*

In het overleg met VenJ is besproken dat de huidige portfolio van kennistopics en onderzoeksvragen in het Vraaggestuurde onderzoekprogramma ook bijgesteld moet kunnen worden als er nieuwe ontwikkelingen plaatsvinden. De opkomst van nieuwe technologieën of maatschappelijke ontwikkelingen kunnen een forse impact hebben op de benodigde aanpak van veiligheidsvraagstukken. Daarom is afgesproken een deel van het VP-budget te alloceren voor verkenningen met verschillende invalshoeken:

| **Technologieverkenningen** | **Impactverkenningen** |
|---|---|
| Deze zijn gericht op het helder krijgen van de potentiële impact van opkomende technologieën die een dreiging of een kans met betrekking tot de veiligheid in de maatschappij kunnen vormen.<br><br>Bv: Wat kan “Augmented Reality”- technologie in het veiligheidsdomein betekenen?<br>Hoe benutten we de potentiële meerwaarde van nieuw ontwikkelde technologie in het VP-deelprogramma Effectief en Veilig Ingrijpen 2007-2010? | Deze zijn gericht op het verkennen van potentieel te ontwikkelen technologieën mogelijke oplossingen voor nieuwe vraagstellingen.<br><br>Bv: Welke dreiging betekent het breed beschikbaar komen van nieuwe bioagentia? Welke technologieën kunnen bijdragen aan de wens om hulpverleners meer op afstand te houden van plaatsen met een hoog veiligheidsrisico? |

Om de verkenningen optimaal te laten aansluiten bij de praktijkomstandigheden en wisselwerking tussen organisaties en stakeholders zullen zonodig activiteiten met inzet van een fieldlab of CD&E-faciliteiten worden uitgevoerd.

De in het kader van dit VP uit te voeren verkenningen zullen normaliter òf voortbouwen op ontwikkelde basiskennis òf potentieel kunnen leiden tot nieuwe onderzoeksvragen voor het VP. Om de investeringen niet onnodig te verdunnen zullen er jaarlijks ca 3-5 verkenningen plaatsvinden. Bovendien wordt door deelname in bredere Europees kader een continue scan van potentieel opdoemende nieuwe opties uitgevoerd. Huidige projecten waarin TNO participeert zijn follow-up initiatieven van ESRIF (European Security Research and Innovation Forum) en enkele EU-projecten (CRESCENDO en ETCETERA).

De keuze voor de in 2012 uit te voeren verkenningen zal pas in december 2011 worden gemaakt.

## 3.3 Samenwerking

### *3.3.1 Kennispartners van kennisopbouw*

Voor de kennisopbouw in het kader van dit VP zal optimaal worden aangesloten bij de expertise van nationale en internationale kennisinstellingen. Daarnaast zal zo goed mogelijk worden samengewerkt met nationale stakeholders in het veiligheidsdomein, die eigen kennis- of innovatie-afdelingen hebben. In het goedgekeurde programma 2011-2014 zijn de opties voor samenwerking bij de uitvoering van dit VP geïnventariseerd. Daarop zijn verdere initiatievn voor samenwerking binnen de topics genomen, terwijl op VP-niveau de afstemming met de Politie-academie aandacht krijgt.

### *3.3.2 Samenwerking met partners voor implementatie*

Nationaal zijn door het nieuwe kabinet Rutte omvangrijke stimuleringsprogramma’s voor Maatschappelijke Veiligheid gestopt. Momenteel worden intiatieven genomen om de aansluiting bij de topsectoren (mn Hightech, Logistiek en Water) te versterken en tevens Cybersecurity in de Nationale Digitale Agenda te verankeren. Internationaal zijn er nog wel omvangrijke en groeiende innovatiestimuleringprogramma’s op het gebied van een veiligheid in de maatschappij. In het kader van deze programma’s worden consortia gevormd die innovatieve concepten kunnen doorontwikkelen en doorbraken voor implementatie

tot stand kunnen brengen. TNO heeft bij dit soort programma's een erkende positie en wil ook de in dit VP te ontwikkelen kennis vroegtijdig verbinden met kennispartners en stakeholders om versterking van de ontwikkelingen te realiseren.

*3.3.3 Benutting van bestaande verankering in nationale en internationale innovatie-stimuleringsprogramma's*

Als resultaat van het Vraaggestuurde Programma Maatschappelijke Veiligheid 2007-2010 participeert TNO in een dertigtal projecten en initiatieven binnen nationale en internationale innovatiestimuleringsprogramma's. Kenmerk van deze stimuleringsprogramma's is dat alle partners een eigen investering meebrengen. Voor TNO zijn er daarom budgettaire verplichtingen, die gefinancierd moeten worden uit het vervolgprogramma 2011-2014. Gezien het belang van uitnutten van eerder gepleegde investeringen in kennisontwikkeling heeft VenJ toegestemd in allocatie van de benodigde middelen hiervoor. Voor 2012 gaat het ca 40% van het totale VP-budget.

## 3.4 Afpraken voor uitwerken van projectplannen voor 2012

Met VenJ is afgesproken dat TNO voor 1 november 2011 per topic een projectplan maakt voor de in 2012 uit te voeren activiteiten. Voor de vijf benoemde specifieke topics is er een klein groepje van 3 tot 4 behoeftestellers met een coördinator benoemd. Elk projectplan zal met het groepje behoeftestellers in de eerste helft van november worden besproken; de uitvoering van een project kan pas starten na daar verkregen instemming.

Met VenJ zullen eind november 2011 de conclusies van de vijf overleggen over de projectplannen worden besproken. Dan zal ook nader overleg plaatsvinden over de financiële planning. Verder zal dan op basis van geïnventariseerde opties een invulling plaatsvinden van het generieke topic Verkenningen.

Tweemaal per jaar zal er een bijeenkomst zijn onder leiding van VenJ met de coördinerende behoeftestellers. In het voorjaar gaat het dan om de resultaten van het achterliggende jaar en in het najaar om de invulling van de plannen voor het komende jaar.