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 2012 R10592

Thema Integrale Veiligheid Vraaggestuurd Programma 2011-2014 VP Veilige Maatschappij Bijstelling 2013

Datum	september 2012
Auteur(s)	Dr.ir. J.A. Don
Aantal pagina's	50 (incl. bijlagen)
Aantal bijlagen	0
Regievoerend departement	Ministerie van Veiligheid en Justitie
Projectnummer	032.32799/01.05

Autorisatie door drs. H.G. Geveke, directeur TNO-thema Integrale Veiligheid

Handtekening:

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. Defence Research
2. Safety and Security Research

Voor de ontwikkeling van de strategie en de programmering van het Vraag-gestuurde onderzoek voor het Innovatiegebied Defence 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 Safety and Security Research 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 business Lines:

1. *Resilience and Society*
   Crises en rampen als een grieppandemie, terroristische aanslag, overstroming of elektriciteits-uitval kunnen de maatschappij ontwrichten. Maar ook kleinschaliger incidenten als brand en ongevallen met gevaarlijke stoffen eisen jaarlijks hun tol. TNO helpt overheid en bedrijfsleven om de risico's in kaart te brengen en ondersteunt met oplossingsrichtingen zoals betere bescherming van vitale infrastructuren of grotere zelfredzaamheid van burgers. TNO helpt ook om de communicatie met burgers te verbeteren en hun competenties optimaal te benutten. Sociale media vormen daarbij een nieuw fenomeen. TNO ontwerpt innovatieve toezichtconcepten en wil een betere informatiepositie voor iedereen die bij veiligheid is betrokken, wat slim gestructureerde systemen met gebruiksvriendelijke interfaces vereist

2. *Security and Protection*
   Beveiliging van gebouwen, terreinen, massatransport en infrastructuur is van belang in verband met criminele activiteiten en eventueel een terroristische aanslag. TNO helpt in het vinden van nieuwe concepten en systemen om proportioneel maatregelen te treffen die betaalbaar en implementeerbaar zijn. Voor de overheid is effectief en efficiënt opsporen na gepleegde misdaden een uitdagende doelstelling; TNO draagt hieraan bij door het helpen ontwikkelen en toepassen van bijzondere technieken, het creëren van voorspellend vermogen en het ontwerp van concepten voor preventie en bestrijding van cybercrime.

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

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

De resultaten van het VP Veilige Maatschappij in 2011 zijn in een voortgangsrapportage vastgelegd, terwijl voor de topics 1, 2, 3 en 4 de resultaten en plannen ook in een bijeenkomst met elk enkele tientallen vertegenwoordigers uit het veiligheidsveld zijn gedeeld. Op basis daarvan zijn nu meerdere partijen structureel aangesloten bij de begeleiding van de topics en is de betrokkenheid bij de ontwikkelingen toegenomen. In dit rapport is een voorlopige verslaglegging van resultaten tot nog toe in 2012 opgenomen.

In juni 2012 heeft het ministerie VenJ per brief aan TNO gevraagd ook in 2013 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 2012 en de hoofdlijnen voor 2013 per topic. De topic-plannen voor 2013 zullen voor 1 november 2012 worden uitgewerkt in zgn. KIP-plannen.

NB. In verband met het Topsectorenbeleid van de overheid is het budget voor het VP Veilige Maatschappij vanaf 2012 met 2,7 M€/jaar verminderd. Het gekorte budget is opnieuw geprogrammeerd in een VP Security gebaseerd op de Roadmap Security in de Topsector High Tech Systems & Materials (zie www.htsm.nl). Bij deze roadmap zijn ca. 25 bedrijven, de industriële koepelorganisatie NIDV, de gemeente Den Haag, NWO/STW en de ministeries VenJ, Defensie en EL&I betrokken. Met instemming van het Roadmapteam Security zijn voor dit nieuwe VP vier onderdelen gedefinieerd, die bij de prioriteiten van de industriële stakeholders en van overheden aansluiten. Drie van de vier onderdelen bouwen voort op de ontwikkelingen in topics van het VP Veilige Maatschappij:

- *System-of-systems* sluit aan op de topics 3 en 4 van het VP Veilige Maatschappij
- *Cybersecurity* sluit aan op topic 5 van het VP Veilige Maatschappij
- *Passieve sensoren* sluit aan op topic 1 van het VP Veilige Maatschappij

Voor elk van deze drie onderdelen en voor het vierde onderdeel *Actieve sensoren* is ook aansluiting bij voor Defensie uitgevoerde onderzoekprogramma's

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. Eén 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. *Defence Research*
   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 cq. Business Lines om Defensie bij deze uitdaging te helpen:
   - Military Operations
   - Military Information Superiority
   - Force Protection
   - Human Effectiveness
2. *Safety and Security Research*
   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 cq. Business Lines:

- Resilience and Society
- Security and Protection

Voor de ontwikkeling van de strategie en de programmering van het Vraag-gestuurde onderzoek voor het Innovatiegebied Defence 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 Safety and Security Research verder uitgewerkt.

2. Safety and Security Research

2.1 Missie van het Innovatiegebied Safety and Security Research

Binnen het Innovatiegebied Safety and Security Research initieert en faciliteert TNO innovaties. De kennisinvesteringen en de contractresearch beogen impact met als doel:

Veilig voelen, Veilig zijn
Slimmer en kosteneffectiever oplossen van actuele en toekomstige veiligheidsvraagstukken in samenwerking met overheden, bedrijven en veiligheidsorganisaties. Wij onderscheiden ons door het bieden van inspirerende oplossingen op basis van ons multidisciplinair en experimenteel onderzoek.

De activiteiten worden aangestuurd vanuit een tweetal business Lines:

1. *Resilience and Society*
   Crises en rampen als een grieppandemie, terroristische aanslag, overstroming of elektriciteits-uitval kunnen de maatschappij ontwrichten. Maar ook kleinschaliger incidenten als brand en ongevallen met gevaarlijke stoffen eisen jaarlijks hun tol. TNO helpt overheid en bedrijfsleven om de risico's in kaart te brengen en ondersteunt met oplossingsrichtingen zoals betere bescherming van vitale infrastructuren of grotere zelfredzaamheid van burgers. TNO helpt ook om de communicatie met burgers te verbeteren en hun competenties optimaal te benutten. Sociale media vormen daarbij een nieuw fenomeen. TNO ontwerpt innovatieve toezichtconcepten en wil een betere informatiepositie voor iedereen die bij veiligheid is betrokken, wat slim gestructureerde systemen met gebruiksvriendelijke interfaces vereist.

2. *Security and Protection*
   Beveiliging van gebouwen, terreinen, massatransport en infrastructuur is van belang in verband met criminele activiteiten en eventueel een terroristische aanslag. TNO helpt in het vinden van nieuwe concepten en systemen om proportioneel maatregelen te treffen die betaalbaar en implementeerbaar zijn. Voor de overheid is effectief en efficiënt opsporen na gepleegde misdaden een uitdagende doelstelling; TNO draagt hieraan bij door het helpen ontwikkelen en toepassen van bijzondere technieken, het creëren van voorspellend vermogen en het ontwerp van concepten voor preventie en bestrijding van cybercrime.

2.2 Doelstelling en resultaten 2011-2014 Innovatiegebied Veilige Maatschappij

Het Innovatiegebied heeft goede aansluiting op de beleidsintensiveringen van het kabinet Rutte. Zodra de plannen van het nieuwe kabinet na de verkiezingen van 12 september 2012 beschikbaar zijn, zullen mogelijke consequenties voor de inhoud van dit VP worden geïnventariseerd. In verband daarmee wordt voor 2013 een beperkt budget voor bijstelling gereserveerd.

De drie hoofddoelstellingen van het kabinet Rutte 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) • Basis voor netcentrisch werken • Mentale weerbaarheid
Stevige aanpak van overlast, agressie en geweld; niet dader maar slachtoffer centraal	• *Sociale media tbv burgerbetrokkenheid* • Slim cameratoezicht (automatische detectie/ training operators voor herkennen van 196 afwijkende gedragingen/ snelle koppelingen) • Buurtlab Transvaal Den Haag • Living Lab Veiligheid
Terugdringen van overlast en criminaliteit rondom prostitutie en drugs	• Living Lab Veiligheid
Strenger op immigratie	• @migo-concept voor mobiel toezicht vreemdelingen • Schiphol toezichtsconcepten

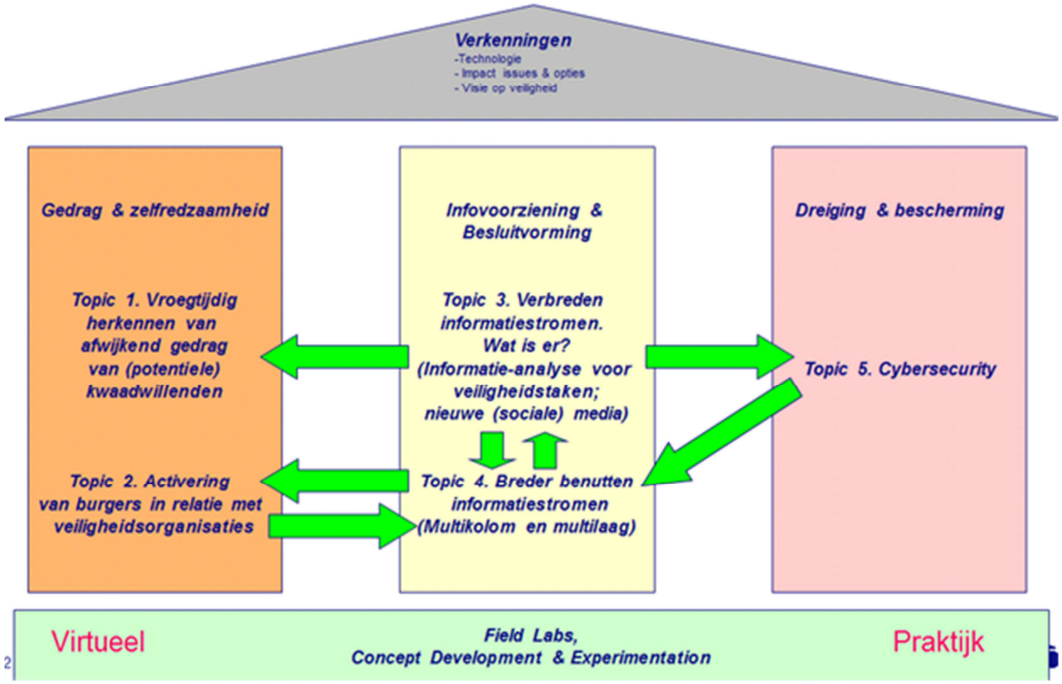
Ook buiten deze maatregelen in het kader van de beleidsintensiveringen van het kabinet Rutte draagt TNO met de uitvoering van opdrachten bij aan de veiligheid in de Nederlandse Maatschappij:

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 Safety and Security Research door:

- Hoogwaardige kennis op nieuwe technologische ontwikkelingsgebieden met gebruikmaking van de kennis bij universiteiten kennisinstellingen binnen en buiten Nederland,
- Kennis van het veiligheidsdomein, relaties met belangrijke spelers daarbinnen en samenwerking met domein specifieke instituten (waaronder Politieacademie, (N)IFV en NFI),
- Onafhankelijke, gezaghebbende positie voor evaluatie van complexe afwegingen en validatie van innovaties met behulp van modellen, experimentele faciliteiten en fieldlabs in samenwerking met 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 4. Delen informatiestromen 5. Cybersecurity
Stevige aanpak van overlast, agressie en geweld; niet dader maar slachtoffer centraal	1. Herkennen afwijkend gedrag 2. Burgerbetrokkenheid 3. Slimmer inzetten info 5. Cybersecurity
Terugdringen van overlast en criminaliteit rondom prostitutie en drugs	pm
Strenger op immigratie	1. Herkennen afwijkend gedrag 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) 4. Delen informatiestromen (crisismanagement) 5. Cybersecurity
Groei economie (met name beveiligingssector met 50 000 medewerkers en high tech sector)	1. Herkennen afwijkend gedrag 3. Slimmer inzetten info
Kabinetsdoel 2 Het huishoudboekje van Nederland op orde	
Minder ambtenaren	2. Burgerbetrokkenheid 4. Delen informatiestromen

2.3 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 macro-niveau. 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-sensornetwerken, 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.

2.4 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, behoeftestellers 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 2011 en juni 2012 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.

3 Vraaggestuurd Programma Veilige Maatschappij

3.1 Beoogde Impact en Doelgroep

In het TNO-Innovatiegebied *Safety and Security Research* zijn de contractresearch en de kennisinvesteringen in de strategieperiode 2011-2014 gericht op de volgende impact:

1. Effectiever/ efficiënter optreden veiligheidsorganisaties door innovatie van intelligence, 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 kunnen 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) - Economie (EZ) - Infrastructuur (EZ, V&W, VROM)
Decentrale overheid	- Veiligheidsregio's (brandweer, GHOR, meldkamers) - Gemeenten
Bedrijfsleven	- Veiligheidsbranche (industrie en diensten) - Vitale infrastructuur - Mainports
Veiligheid-gerelateerde Instituten	- Onderzoek (NFI, CCV, Verweij-Jonker e.a.) - Opleiding (Politieacademie, NIFV e.a.)
Internationaal	- Overheden (EU, EU-lidstaten, DHS in VS) - Bedrijfsleven (Multinationals) - Complementaire kennisinstituten
Consortia voor publiek-private samenwerking	- Veiligheid op luchthavens - Vitale infrastructuur - e.a.

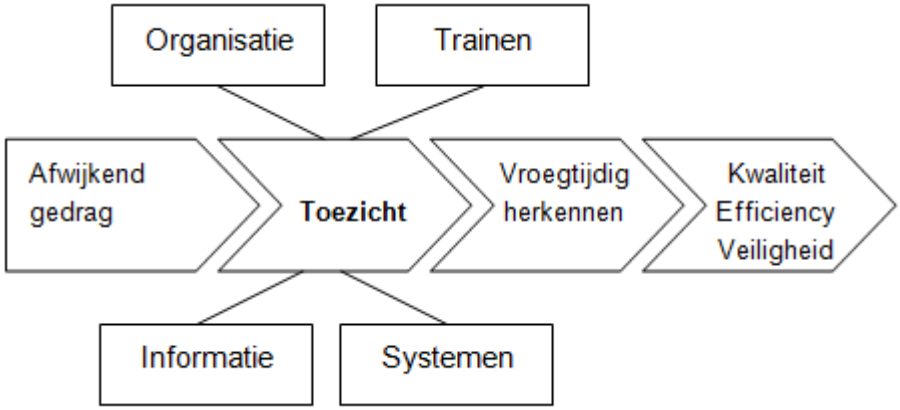
3.2 Focus van onderzoeksvragen en roadmap

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

3.2.1 Topic 1: Vroegtijdig herkennen afwijkend gedrag

3.2.1.1 Omschrijving van topic 1

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 topic 1

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: - VenJ (NCTb, DJI) - Gemeenten - Politie KLPD, Marechaussee - Openbaar Vervoer, mainports - Winkeliers, detailhandel, bedrijfsterreinen - Beveiligingsbedrijven
Waarom is het onderzoek van belang?	- Veiligheid in het openbaar vervoer (issues groepsgedrag jeugd, gedragsbeïnvloeding reizigers/bestuurders, crowd management evenementen) - Veiligheid in gevangenissen (monitoren gevangenen en bezoekers - Toezicht in winkels en winkelcentra (preventie diefstal, vandalisme) - 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 - Waarnemen, vroeg interpreteren en beïnvloeden van afwijkend gedrag (weak signals, prikkelen individuen/groepen) - Optimale samenwerking tussen toezichthouders, gebruikmakend van alle beschikbare bronnen en informatie die afwijkend gedrag kunnen signaleren en duiden - Intelligente sensornetwerken (spot, track & trace, intelligente camera's) - Ontwikkeling van in de surveillancepraktijk bruikbare risicoprofielen van een gebied, groepen en personen op basis van tijd, plaats, omgevingskenmerken, eigenschappen; randvoorwaarde: privacywetgeving - Concept development & experimentation faciliteit, Living lab in stedelijke omgeving/ Fieldlab in winkelcentrum
Wie begeleidt?	Desiree Geerts (VenJ/NCTV), J. Lavèn (Subarena Geïntegreerde Systemen /CIV), AIVD
TNO-team	Maaike Lousberg (trekker), Dianne van Hemert, Gert-Jan Burghouts, Remco Wijn 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 Topic 1 in 2012

Het zwaartepunt voor topic1 ligt in 2012 op twee werkpakketten: *Concretiseren van de definitie van afwijkend gedrag* en *Optellen van zwakke signalen: 0+0=1*. In het eerste werkpakket is dit jaar gewerkt aan een taal om afwijkend gedrag te beschrijven. Deze taal heeft als doel om afwijkend gedrag te formaliseren voor het gebruik in intelligente software toepassingen. Daarnaast is het een methode om

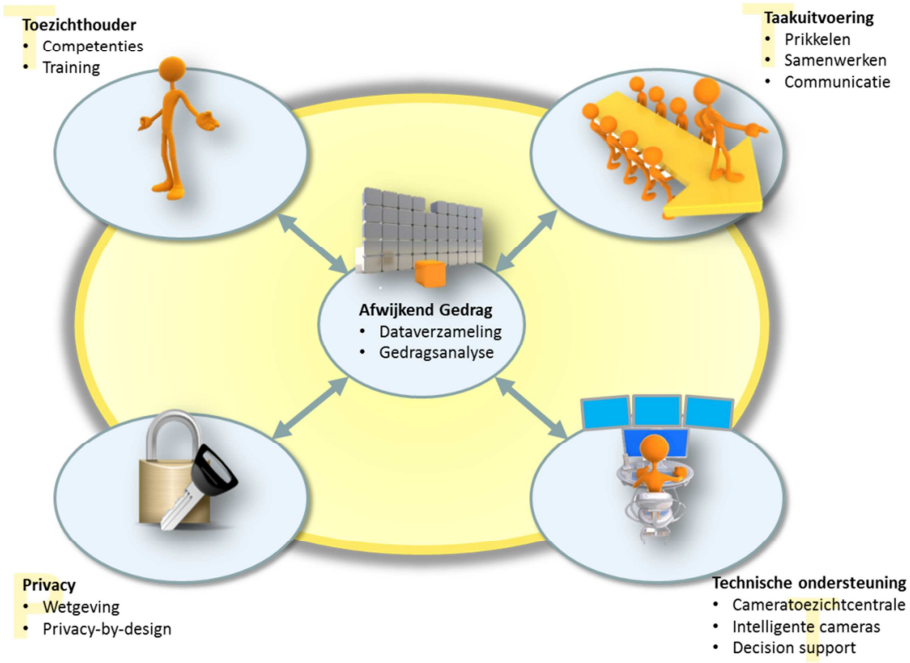
overeenstemming te krijgen tussen de disciplines die zich het meest met afwijkend gedrag bezig houden, namelijk de gedrags-, informatie- en technologiewetenschappen. Met betrekking tot deze taal is een paper geschreven die gepubliceerd zal gaan worden in een special issue van het MTAP.[1] Dit paper biedt een basis voor het ontwikkelen van een methodiek om beeldmateriaal van incidenten te annoteren. In dit werkpakket is daarvoor gewerkt aan het aanleggen van een beeldbank. De beeldbank is opgebouwd met hulp van partners als de NS met wie overeenkomsten zijn gesloten voor het analyseren van hun beeldmateriaal. Op dit moment bevat de beeldbank al enkele honderden videofragmenten.

In het werkpakket *0+0=1* is verkend hoe observaties van verschillende toezichthouders gecombineerd kunnen worden om met die gecombineerde observaties nauwkeuriger uitspraken te kunnen doen over de mogelijke schuld van individuen die afwijkend gedrag vertonen. Nauwkeuriger betekent in dit geval een grotere hit-kans en tegelijkertijd een kleinere kans dat iemand onterecht staande gehouden wordt. Hiertoe is een experiment uitgevoerd waarbij ervaren beveiligers beelden van incidenten bekeken en mensen op het scherm konden aanwijzen (taggen) wanneer ze afwijkend gedrag waarnamen. Wanneer een dergelijke methode in een cameratoezichtcentrale gebruikt zou worden, is intelligente software nodig om de verschillende getagde individuen met elkaar te vergelijken. Deze software moet beoordelen of een individu die door operator 1 is getagd dezelfde is als die door operator 2 is getagd. In grote publieksstromen kan dit niet handmatig worden gedaan. In dit werkpakket is gewerkt aan dit herkenningsalgoritme. Dit algoritme is in de huidige set van videobeelden in staat om minimaal 76% van de getagde personen correct te matchen met dezelfde persoon die door een andere operator is getagd. Deze succesmaat willen we in de volgende fase van onderzoek verder omhoog brengen. De tagging-data is vervolgens gebruikt om methoden te onderzoeken die antwoord moeten geven op vragen als: hoeveel operators zijn in een uitkijkcentrale nodig om een vooraf gedefinieerd percentage daders uit een groep te halen (bv 90%, 70%, 50%), hoeveel operators moeten het dan eens zijn met elkaar over de potentiële schuld van een individu en hoeveel onterechte aanhoudingen zou dat opleveren. Op basis van de hier gebruikte tagging-data zijn tabellen geproduceerd die op deze vragen antwoorden geven.
Een tweede deel van dit werkpakket betrof onderzoek naar prikkelen, een methode om afwijkend gedrag beter zichtbaar te maken zodat het gemakkelijker te observeren wordt door toezichthouders. Bij prikkelen zenden toezichthouders subtiele signalen uit met als doel een reactie te ontlokken aan de omgeving. Data-analyses van een vorig jaar uitgevoerd experiment laten zeer bemoedigende resultaten zien. In dit experiment lieten we mensen legale en illegale pakketjes vervoeren. Op de geplande route stond een beveiliger die hen op zou kunnen pakken als ze daartoe aanleiding zagen. Onder deze omstandigheden ervoeren deelnemers met illegale pakketjes de veronderstelde psychologische effecten. Bovendien bleken ervaren toezichthouders beter in staat om uit een groep mensen de illegale-pakketjes-vervoerders te halen wanneer de beveiliger op de route een prikkel had uitgezonden dan wanneer die dat niet had gedaan. Dit is een eerste empirische ondersteuning voor het prikkelen-concept. Om deze kennis verder uit te

[1] J. van Rest, F.A. Grootjen, M. Grootjen, L. Alic, R. Wijn, O. Aarts, M. Roelofs, G.J. Burghouts (in druk). Human Behaviour and Surveillance in a multimedia metadata scheme. *Multimedia Tools and Applications.*

breiden en toepassing beter mogelijk te maken is een tweede experiment voorbereid die volgend jaar zal worden uitgevoerd en geanalyseerd. Over de theoretische, psychologische basis van prikkelen en afwijkend gedrag in het algemeen is een hoofdstuk geschreven voor een samengesteld boek[2] en een artikel voor in het vaktijdschrift Security Management[3]. Ook zijn en worden er over dit onderwerp presentaties gegeven op professionele en wetenschappelijke symposia, zoals NISA seminar in juni 2012 en het Behavioural Analysis of Crime and Investigation 2012 symposium in december in London.

Twee andere werkpakketten betroffen “Service en veiligheid” en “Profiling”. In het eerste van deze twee is de vraag onderzocht of veiligheidsmaatregelen meer het karakter van service kan aannemen om zo de acceptatie te vergroten onder nu nog vaak sceptische burgers. In het werkpakket over profiling is het doel in kaart te brengen wat er bekend is over profiling. Dit gebied blijkt te worden gekenmerkt door een wir-war van termen waarmee grofweg dezelfde methodes worden aangeduid en waarvan de theoretische en empirische onderbouwing vaak zeer matig zijn. In een paper proberen we orde in deze chaos te scheppen en kaf van koren te scheiden. Bovendien verkennen we hier welke typen profiling en welke methoden gebaat zijn bij nader onderzoek, en welke typen een doodlopende weg lijken te bewandelen. In dit werkpakket wordt verder in samenwerking met het NCTV een symposium georganiseerd binnen de CCR Summit in Kerkrade in oktober.



Figuur: Basismodel “Toezicht op afwijkend gedrag”

[2] R. Wijn, G. J. Burghouts, J. H. C. van Rest en M. Lousberg (in druk). Naar een beter begrip van afwijkend gedrag: Herkenning door mens en computer. (Ed. E. Muller). *Veiligheid*.
[3] B. van Pelt & R. Wijn (in druk). Security Questioning en Prikkelen. *Security Management.*

Eind september 2012 zal ook het FP7 project TACTICS worden opgestart. 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 voor het herkennen van afwijkende ontwikkelingen (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.

3.2.1.5 Voorgestelde zwaartepunten voor voortzetting in 2013:

In het jaar 2013 ligt de nadruk op effectiviteit en laten zien wat we hebben bereikt met het onderzoek naar het herkennen van afwijkend gedrag. Het toetsen van concepten aan realistische settings en het verspreiden en delen van kennis staat hierbij centraal. Dit vertaalt zich voorlopig naar de volgende onderwerpen: ·

1. Analyse gedrag (video):

In 2011 hebben we de basis gelegd voor een database van surveillance video's. In 2012 hebben we deze verder uitgebreid en hebben we de *Modus Operandi map* (MOMAP) ontwikkeld voor het zakkenrollen scenario. In 2013 willen we de cirkel rond maken door weer terug te gaan naar de professionele eindgebruiker. We willen de MOMAP in de praktijk toetsen en bruikbaar maken voor andere soorten afwijkend gedrag (heftiger incidenten, complexer gedrag) en operationeel koppelen aan techniek en taakbelasting. In overleg met de industrie (topsectoren) willen we het draagvlak en de mogelijkheden verkennen om de MOMAP structureel in het toezichtdomein in te zetten. Dit kan bijvoorbeeld door samen met eindgebruikers 3 gebruiksscenario's uit te werken.

2. Prikkelen:

We hebben nu meerdere studies gedaan naar het prikkelen concept. Deze studies tonen aan dat prikkels inderdaad helpen om kwade intenties beter zichtbaar te maken. Vooralsnog is het echter onduidelijk waarin die kwade intenties tot uiting komen. Hoewel beoordelaars het onderscheid kunnen maken, weten we niet hoe ze dat doen en waarop ze dan letten. Weten we dit wel, of weten we welke vaardigheden ervoor zorgen dat sommige mensen beter zijn in het herkennen van afwijkend gedrag na prikkels, dan kunnen we toezichthouders trainen in die relevante kennis of vaardigheden.

3. 0+0=1:

Afgelopen jaren is het 0+0=1 concept bedacht en er is mee geëxperimenteerd. Dit was behoorlijk complex. We hebben nu inzicht in de potentie van het "systeem" en in hoe we het effect ervan beter kunnen laten zien. Daarom willen we het 0+0=1 concept valideren in een realistische setting, zoals Schiphol. In 2012 hebben we veel geleerd over hoe je het taggen moet opzetten (klikken op persoon of precies een vakje eromheen zetten?), hoe moet je mensen instrueren (veel of weinig taggen, grof of precies?), hoeveel taggers heb je minimaal nodig? (voor een betrouwbare optelsom van tags), hoeveel tags geven een goede indicatie van een "1"? Dit jaar was een grove verkenning. Volgend jaar kunnen we het goed opzetten, met bruikbare conclusies, op een relevante locatie. Het resultaat: een nieuw toezichtsconcept, dat is beproefd in een realistisch kader.

4. Profiling:

Profiling monitoring/besluitvormings tool. Hoe kun je de mensen die het werk aan het uitvoeren zijn helpen? Afgelopen jaar hebben we in kaart gebracht welke typen

profiling er allemaal zijn, waarvan de effectiviteit al is beproefd en in welke domeinen ze worden gebruikt. Eén van de conclusies is dat profiling heel goed kan werken, maar dat het wel moet voldoen aan bepaalde randvoorwaarden, en dat de prestaties gemonitord zouden moeten worden. Hoe zou je dit het beste kunnen inrichten? Met de resultaten zou in de toekomst in samenwerking met het bedrijfsleven/overheid een tool ontwikkeld moeten kunnen worden.

3.2.2 Topic 2: Activering burgers

3.2.2.1 Omschrijving van Topic 2

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 (rookdetectors, 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 topic 2

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 - Politie, brandweer en GHOR - Veiligheidsregio's - Gemeenten - Bedrijven, waar veiligheid bijzondere aandacht krijgt i.v.m. risico's en/of hoeveelheid mensen
Waarom is het onderzoek van belang?	Beïnvloeden veiligheidsbewustzijn Verankeren van verantwoordelijkheid t.a.v. eigen veiligheid bij burgers en bedrijven Handelingsperspectief en handelingsbereidheid van burgers en bedrijven Terugtredende overheid Opbouwen community resilience
Waarmee kunnen we dit doen? (Focus)	Communicatie voor beïnvloeding van perceptie en gedrag (incl. sociale netwerken) Leren en instructie van burgers en professionals voor optimale samenwerking (serious gaming) Stimuleren en belonen om motivatie voor participatie te bewerkstelligen 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 voor topic 2

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 Topic 2 in 2012

Profilering vrijwilligers en eerste ontwerp interactiemedium voor werving
De data die in 2011 zijn verzameld over de kenmerken van vrijwilligers zijn in 2012 aangevuld met de response van enkele vrijwilligersorganisaties (Lopv, Brandweer). De tabel toont nu een overzicht van de organisaties die waren betrokken bij het onderzoek.

Organisatie	Aantal respondenten
RODE KRUIS	514
REDDINGSBRIGADE	407
KNRM	382
BRANDWEER	267
LOPV	103
NATRES	92
ORANJE KRUIS	67
ANDERS	98
TOTAAL	**1930**

In 2012 zijn alle verzamelde dat geanalyseerd met als resultaat per organisatie een profiel met kenmerken van de vrijwilligers die daar werkzaam zijn. Deze profielen bevatten o.a. een overzicht van de gemiddelde leeftijd, urenbelasting per week, motivatie, toekomstverwachtingen en communicatie. Daarbij zijn de beelden voor de verschillende organisaties met elkaar vergeleken. Op basis hiervan is gestart met de beschrijving van een interactiemedium. Dit medium kan door de betreffende organisaties worden benut bij het gerichter informeren van potentiële vrijwilligers over wat zij kunnen verwachten van het werk en de organisatie. De potentiële vrijwilliger kan zich daardoor beter oriënteren op vrijwilligerswerk in veiligheidsorganisaties. Daarnaast is er belangstelling voor meer uitgebreide terugkoppeling over de resultaten van het onderzoek. Hiertoe wordt de data verder in detail geanalyseerd en teruggekoppeld. Op basis van deze resultaten wordt verwacht dat betreffende organisaties gerichte maatregelen kunnen nemen om vrijwilligers te werven, begeleiden en boeien.

Hieronder volgen enkele wordclouds van de belangrijkste genoemde kenmerken van twee organisaties. De woordgrootte geeft de mate waarin de woorden zijn genoemd door de respondenten en dus het belang aan.

Rode kruis

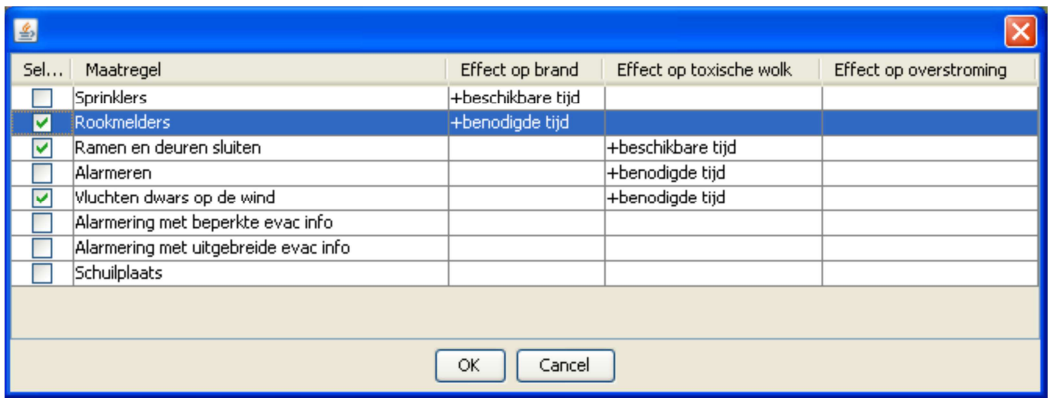
Op 30 oktober 2012 worden de resultaten gepresenteerd tijdens het landelijk symposium van de Nederlandse Organisaties Vrijwilligerswerk. Ook heeft de brandweer (VBV/NVBR) opdracht gegeven voor een vervolgonderzoek naar de vrijwilliger van de toekomst. In Brand en Brandweer 7/8 (juli/aug 2012) wordt de opzet daarvan en meerdere keren verwezen naar de TNO-betrokkenheid daarbij.

Informatiecirkel professionals en burgers

Voortbouwend op de resultaten in 2011, hoe mensen in een beperkt experiment reageerden op een geënsceneerd incident, wordt in het najaar 2012 een omvangrijker experiment uitgevoerd, naar de wijze waarop burgers omgaan met informatie over een incident. Er wordt in een gesimuleerde omgeving onderzocht wat er nodig is voor het gaan handelen van mensen bij berichten over een veiligheidsprobleem dat hen raakt. In totaal gaan ruim 100 mensen participeren in het experiment in verschillende condities. Communicatie die een handelingsperspectief geeft, voordat er informatie over de veiligheidsproblemen gegeven is, zal niet leiden tot handelen van mensen (behalve als er een overduidelijke levensbedreigende situatie is). Burgers die procesinformatie ontvangen, als: ‘We zijn er mee bezig’, ‘We komen er aan’, ‘Alles is onder controle’ zullen niet snel zelf tot handelen overgaan. Waarschijnlijk zijn zij wel meer tevreden over de communicatie dan wanneer er niet gecommuniceerd wordt, maar uiteindelijk is men toch op zoek naar informatie, handelingsperspectief en duiding. De voorbereidingen omvatten het bouwen van het scenario in een gameomgeving en de verschillende typen informatie: gericht op handelingsperspectief, informeren voorafgaand en geven van procesinformatie. Daarnaast in de werving van voldoende proefpersonen. Aanvankelijk zou naast het experiment ook een oefening in het najaar met vergelijkbare informatievormen worden geëxperimenteerd. Helaas zijn geschikte oefeningen hiervoor uitgesteld naar voorjaar 2013.

Tijdens het jaarlijkse NVBR congres (nov 2012) zal er een workshop worden verzorgd over dit onderzoek en de impact voor hulpverlenersorganisaties. Ook wordt een glossy voorbereid voor verspreiding van de resultaten uit dit onderzoek.

Modelontwikkeling in gebouwen maatregelen voor zelfredzaamheid
Er is verder gewerkt aan de ontwikkeling van een model voor koppeling van maatregelen in gebouwen en gebouwde omgeving aan zelfredzaamheid. Hierbij is gekeken naar de onderlinge beïnvloeding, positief dan wel negatief, van maatregelen op verschillende incident- of ramp-typen. Het in 2011 ontwikkelde conceptmodel is hiermee verder ingevuld.
Tevens is voor sociale veiligheid als nieuw domein verkend, hoe daar de invulling van de eigen verantwoordelijkheid en de zelfredzaamheid in een model kan worden gevat. Sociale veiligheid is een meer diffuus en moeilijker in te kaderen domein. Daarom is bij de verkenning ingezoomd op sociale veiligheid in een schoolomgeving en hoe daar effecten, maatregelen en onderlinge relaties (pos/neg) inzichtelijk kunnen worden gemaakt. Tenslotte is een begin gemaakt van het indexeren van reacties van mensen/populaties op maatregelen. De maatregelen en de mogelijke reacties van mensen op deze maatregelen versterken de mate van validiteit van het model.



Over dit onderzoek is door de deelprojectleider Inge Trijssenaar tijdens de Future Security Conference (september 2012, Bonn) een paper gepresenteerd: 'Determining the Effectiveness of Safety Measures for Self-Rescue in the Built Environment'.

Effectiviteit social media en aanzet dashboard communicatie
Een belangrijk inzicht uit de verkenning in 2011 is, dat de wijze van inzet en de keuze van media voor communicatie over veiligheid niet altijd gebaseerd is op te bereiken doelstellingen. Soms wordt de keuze zelfs ingegeven door de motivatie om ‘mee te kunnen doen’ of om ‘niet achter te blijven’. Een heldere koppeling tussen beoogd doel en middel kan een belangrijke bijdrage leveren aan de effectiviteit. Daarom is in 2012 gewerkt aan een concept methodiek om effectiviteit van sociale media toepassingen te kunnen meten.
Het gebruik van social media kan geen doelstelling op zichzelf zijn, maar moet een onderdeel worden van overkoepelende veiligheidsdoelstellingen en aansluiten bij de beoogde doelgroepen. De effectiviteit van sociale media toepassingen wordt ook sterk bepaald door de manier waarop de communicatie plaatsvindt en de manier waarop het gebruik van social media binnen de organisatie wordt verankerd.
Voordat je social media actief kunt inzetten, is het van belang om vast te stellen wie de verantwoordelijke is. Een OOV organisatie moet zich realiseren dat het gebruik van social media een continu proces is, inclusief de benodigde randvoorwaarden.
De koppeling met het onderzoek naar de informatiecirkel is, dat voorafgaand aan

een incident of ramp er al informatie gedeeld, geduid kan worden, zodat er tijdens een ramp beter en sneller kan worden opgetreden door gedeelde informatie.
Om de effectiviteit te kunnen meten is het nodig om doelstellingen SMART te maken, zodat deze richtinggevend worden. Een gebruikelijke manier om doelstellingen meetbaar te maken is door ze te vertalen naar zogenaamde 'Key Performance Indicatoren' ofwel KPI's. Deze geven aan wat er bereikt moet worden en wanneer dit moet worden bereikt. Bijvoorbeeld, met actie x willen we binnen een maand 5.000 volgers op Twitter hebben. Bedrijven en organisaties kunnen deze doelstellingen tussentijds evalueren en bij het achterblijven van resultaten eventueel bijsturen.
Om sturing te kunnen geven aan het halen van doelstellingen wordt er tevens een concept 'dashboard' ontwikkeld waarmee inzicht gegeven kan worden in de passende vorm van communicatie gekoppeld aan het incident, de doelgroep en het beoogde effect. Het dashboard zal uit vier samenhangende elementen bestaan:

1. Organisatie doelstellingen, meetbaar en tijdsgebonden.
2. De keuze van interventies (we noemen het interventies omdat er vaak meerdere aspecten gecombineerd moeten)
3. Organisatorische randvoorwaarden
4. Kenmerken van de (online) doelgroep

De primaire focus in 2012 is de ontwikkeling van een instrument voor meting van de effecten van social media communicatie. De communicatie moet gericht zijn op het bereiken van specifieke doelstellingen.

Topic 2 dag
Op 21 juni 2012 vond in Soesterberg een bijeenkomst plaats over het onderzoek en de consequenties voor betrokken organisaties. Naast een plenaire introductie werden de verschillende deelonderzoeken toegelicht in interactieve sessies.
Bij de aanwezigen vanuit veiligheidsregio's, ministeries, gemeenten, politie en hulpverleners- en vrijwilligersorganisaties, is nog meer interesse gewekt voor participatie in de onderzoeken. Betrokkenen gaven aan graag de voortgang van de ontwikkelingen van het onderzoek blijven volgen. Aan de deelnemers is ook een voortgangsrapportage van het topic Activering van burgers meegegeven. Deze rapportage en meer informatie is te vinden op:
http://www.tno.nl/content.cfm?context=overtno&content=nieuwsbericht&laag1=37&laag2=69&item_id=2012-06-26%2013:21:04.0&Taal=1

3.2.2.5 Voorgestelde zwaartepunten voor voortzetting topic 2 in 2013

Ontwerp interactiemedium voor werving nieuwe vrijwilligers
In 2013 zal het interactiemedium worden uitgebreid en getoetst in een experiment met potentiële gebruikers. Het effect van het instrument zal worden bepaald op basis van het aantal mensen dat een vervolgactie (contact, informatievraag, aanmelding) richting betreffende organisaties zet.

Informatiecirkel professionals en burgers
In 2013 zal worden verkend hoe neutraliseren van informatie(dempen) passieve reacties veroorzaakt en wanneer je zelfredzaamheid wil stimuleren werkt (positieve priming). Tevens worden de bevindingen uit het experiment 2012 verder geconcretiseerd tot een demoversie van een game waar hulpverleners in kunnen ervaren wat verschillende informatie doet met burgers.

Modelontwikkeling in gebouwen en maatregelen voor zelfredzaamheid
Voorgesteld wordt om verder te gaan met de koppeling in het model van de menselijke factor. Waar mogelijk zal de waarschijnlijke reactie van mensen of groepen mensen worden gekoppeld aan de voorgestelde maatregelen versus incident of ramptypen. In 2013 wordt tevens een inhoudelijke check uitgevoerd met experts om te bepalen hoe effectief het model voorspelt. Daarnaast wordt een schoolorganisatie gekoppeld aan de ontwikkelingen van het model.

Effectiviteit social media en aanzet dashboard communicatie
In 2013 wordt het onderzoek naar een meetinstrument voor de effectiviteit van social media uitgebreid naar het meten van de effectiviteit van een breder palet van communicatiemiddelen.
De stand van zaken is dat een factoren model wordt opgesteld in afstemming met stakeholders die social media hebben toegepast in hun bedrijfsprocessen, al dan niet als experiment. Hiermee worden relevante meetitems en –middelen geïdentificeerd. Daarnaast wordt een concept interface ontwikkeld voor het visualiseren van het conceptdashboard.

3.2.3 Topic 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 topic 3
Informatie en informatiegestuurd 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 topic 3

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) Justitie/NFI/politie (opsporing) 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 **Procesinnovatie gericht op informatiegestuurd optreden**: risicoprofilering voor analyse van grote informatiestromen en koppeling van bronnen (kredietregistratie, kenteken, onroerend goed, …), burgerparticipatie **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	Arnout de Vries (trekker), Lotte de Groen, Henri Bouma, Kees den Hollander, John Schavemaker, Peter Jan Doets

3.2.3.3 Met VenJ en stakeholders afgestemde onderzoeksvragen voor topic 3

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,) T.b.v. 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:

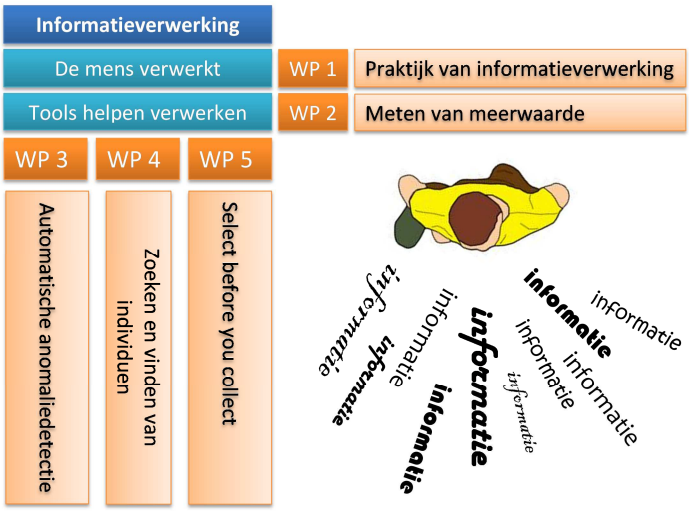
- Waar is potentieel hoge meerwaarde voor operationele veiligheidstaken te verwachten van het simultaan analyseren van (meer) reguliere informatiesystemen, actueel binnenkomende meldingen/waarnemingen en nieuwe media. Wat zijn bruikbare producten voor crisismanagement en voor meer heterdaads bij opsporing? (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 topic 3 in 2012

Topic 3 bestaat uit 5 werkpakketten, en een zesde die sinds de tweede helft van dit jaar wordt opgestart (digitale fenomenen), welke hieronder worden besproken op onderzoeksvraag, huidig resultaat en beoogd eindresultaat (doel).



Samenhang tussen de werkpakketten van topic 3

Het resultaat van de gebundelde activiteiten moet zijn: Het slimmer (efficiënter en effectiever) afstemmen van informatievraag en informatieaanbod binnen de domeinen handhaving en strafrechtketen, waarbij toegesneden technologie het proces en de mens zo goed mogelijk ondersteunt.

WP 1 – 'Informatie-overload in de praktijk'

Huidige resultaat:
Middels interviews met politiemedewerkers is inzicht verkregen in de problematiek, de oorzaken en mogelijke oplossingen voor informatie-overload. De problematiek en de oorzaken zijn getoetst bij een externe stakeholdersgroep. Op de vraag welke oorzaken zij het meest belangrijk achten om op te lossen, kwamen zij met de volgende top vijf, welke met mogelijke oplossingen zijn aangevuld door TNO experts op deze gebieden:

1. de complexiteit van integreren en structuren;
2. de complexiteit van het vaststellen van betrouwbaarheid van informatie;
3. de complexiteit van het vaststellen van de relevantie van informatie;
4. de arbeidsintensiteit van het verzamelen van informatie;
5. de administratieve druk in het werk.

Beoogd eindresultaat en nog uit te voeren activiteiten:
De gevonden problematiek, oorzaken en oplossingen worden vastgelegd in een rapportage.

WP 2 – 'Meten van meerwaarde'

Huidige resultaat:
Een overzicht is gemaakt van digitaal rechercheren, zoals dit nu veel al gebeurd. Dit is gebeurd op basis van interviews, (interne) documentatie van stakeholders en eigen onderzoek. Ook is er een overzicht van de bronnen die hierbij geraadpleegd worden. Daarnaast is een overzicht van de tools die in de praktijk gebruikt worden en vooral ook hoe deze gebruikt worden.

Beoogd eindresultaat en nog uit te voeren activiteiten:
Momenteel worden aanvullende interviews gepland met verschillende stakeholders om de processen beter te kunnen analyseren. Vervolgens zal een integraal overzicht van beschikbare tools worden gegenereerd. Daarna zal, mede op basis van de opgedane kennis zoals zojuist beschreven, een vergelijkend onderzoek (een zogenaamde benchmark) worden gedaan om de waarde van de verschillende tools te bepalen. Waar mogelijk zal de meerwaarde van tools t.o.v. elkaar worden

gekwantificeerd, om zo hun waarde tastbaar te maken. Waar mogelijk zullen resultaten statistisch getoetst worden.

WP 3 – 'Automatische anomaliedetectie'

Huidige resultaat:

- De eerste analyse van de inhoud van tweets op aspecten zoals sentiment en agressie/dreiging is gedaan die gevoed kunnen worden aan de anomalie-detector.
- De ontwikkeling van een anomalie-detector op basis van diverse kenmerken die vroeg dreigingen kan waarnemen is begonnen.
- Invited paper op conferentie "Information technologies and security" (ITSEC 2012).

Nog uit te voeren activiteiten op korte termijn:

- (28 sept) Ontwikkeling anomalie detector en het schrijven van paper voor ITSEC 2012.
- (15/16 okt) Presentatie op ITSEC 2012.

Beoogd resultaat:

- Demonstrator voor anomaliedetectie op een social medium.
- Rapportage met de geïnventariseerde, gewaardeerde en, waar mogelijk, geteste oplossingsprincipes.

WP 4 – 'Het zoeken en vinden van individuen'

Huidige resultaat:

- Beschrijving en analyse van huidige praktijk en uitdagingen, op basis van huidige inzichten uit stakeholder interviews, deskresearch en eigen analyse.

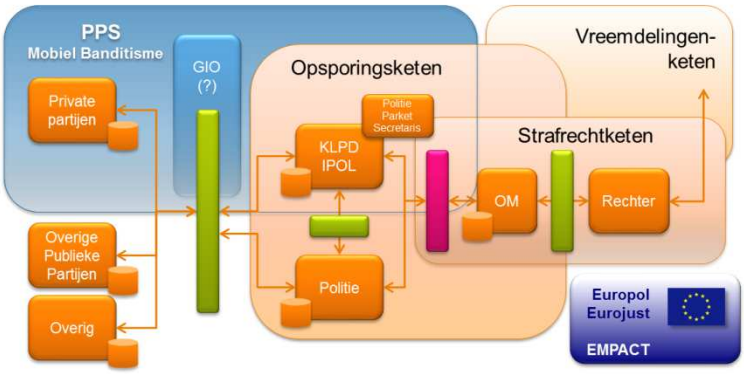
Nog uit te voeren activiteiten op korte termijn:

- Overzicht en analyse bestaande tools toegespitst op koppelen online identiteiten, in samenwerking met WP2 dat een breder overzicht van tools maakt.
- Aanvullende gesprekken met stakeholders
- Identificatie witte vlekken.

- Definitie en uitvoering van experiment op basis van geïdentificeerde witte vlekken.

Beoogd eindresultaat:
Aanpak voor herkennen van individuen op het internet middels het aan elkaar koppelen van de verschillende online identiteiten van een individu, getoetst m.b.v. experiment.

WP 5 – 'Select before you collect'



Hoe kan select-before-you-collect worden gebruikt om te voorkomen dat teveel data binnenkomt en hoe kan de juiste prioriteit worden aangegeven, zoals bij Triage? 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.

Huidige resultaat en nog uit te voeren activiteiten:
De opdracht wordt uitgevoerd in de context van Mobiel Banditisme, een relatief nieuw fenomeen voor de samenwerking van het KLPD, politie en OM in de opsporings- en strafrechtketen. De eerste stap is om inzicht te krijgen in de totale keten, om af te kunnen leiden op welke wijze ondersteuning m.b.t. het efficiënt omgaan met informatie nodig is.
Op dit moment zijn de meeste spelers in de opsporings- en strafrechtketen geïnterviewd. De betrokken organisaties zijn: KLPD, een aantal politieregio's, VenJ, OM (w.o. OvJ belast met Mobiel Banditisme), IND en Europol. (Beschrijven van (de rol van) private partijen en de PPS Mobiel Banditisme (waarin de verschillende organisaties samenwerken) zullen mogelijk vanuit een ander project worden gedaan als onderdeel van de inrichting van de PPS).
De voorlopige resultaten leveren een overzicht op van de workflow en knelpunten in de keten m.b.t. Mobiel Banditisme en het SelectB4UCollect stuurmechanisme. Mobiel banditisme is zoals gezegd een relatief nieuw fenomeen voor de gehele keten. Er blijkt daarom als eerste stap in het omgaan met informatie al een sterke behoefte voor politie en OM om inzicht te krijgen in de ernst en ontwikkeling van mobiel banditisme. Er is om die reden in het project gestart met het uitwerken van een van de mogelijke oplossingsrichtingen: het ontwikkelen van een aantal analysefunctionaliteiten die op politiedata wordt losgelaten, zodat snel inzicht verkregen kan worden in de informatiepositie. Naast de toets voor dit specifieke

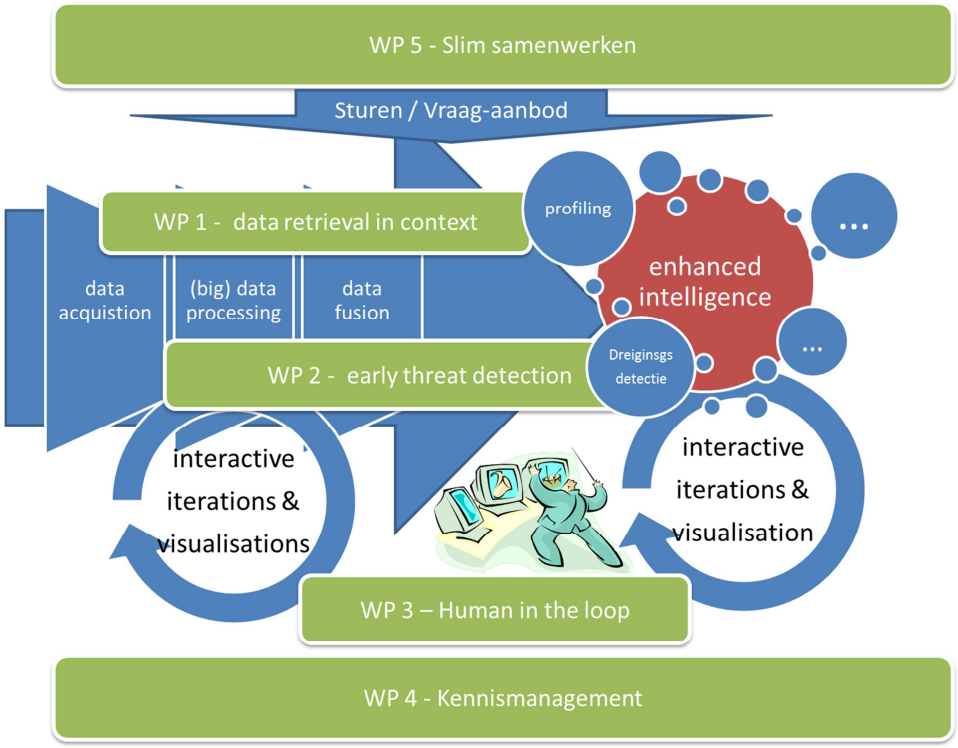
fenomeen, zal in de plenaire sessie later dit jaar ook gevraagd worden in hoeverre de resultaten toepasbaar zijn voor andere fenomenen dan alleen mobiel banditisme.

Beoogd eindresultaat:
Proof-of-principle voor select-before-you-collect en een aantal andere oplossingsrichtingen, gebaseerd op een verkenning in het domein van mobiel banditisme (rondtrekkende dadergroepen). De resultaten dienen ook direct als inzicht voor de stakeholders zelf die rond dit fenomeen beter moeten gaan samenwerken.

3.2.3.5 *Voorgestelde zwaartepunten voor voortzetting topic 3 in 2013*

Op basis van de bereikte resultaten in 2012 en gesprekken met de stakeholders is voor 2013 gekozen voor een vijftal speerpunten. Stakeholders die hebben bijgedragen aan de inhoud en prioritering van deze speerpunten zijn onder andere: Ministerie VenJ, NCTV, KLPD, rijksrecherche, inlichtingendiensten, vtsPN, politie (o.a. Haaglanden, A'dam Amstelland, Groningen), belastingdienst, en de Politie Academie.

De gekozen speerpunten zijn in onderstaande figuur in samenhang weergegeven en betreffen:



In oktober 2012 worden de onderwerpen in overleg met deze stakeholders uitgewerkt tot concrete projectvoorstellen. 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.

De werkpakketten hebben als gezamenlijk doel om de verschillende processen met betrekking tot (real-time) intelligence beter te ondersteunen (doelstelling). Visualisaties en gebruikersinteractie door dit gehele proces van het opwerken van data naar informatie en intelligence zorgt dat dat slimme technologie optimaler samenwerkt met de mens (human in the loop). Tezamen met slimmer samenwerken en slimmer kennisdelen draagt dit bij aan verbeterde intelligence (als proces en eindresultaat). Over de werkpakketten heen zullen enkele cases centraal staan, welke in overleg met de stakeholdergroep wordt gekozen, zoals: profiling van individuen of groepen, fenomeenstudies van bijvoorbeeld mensenhandel of dreigingsdetectie zoals doodsbedreigingen. In de diverse werkpakketten wordt gezamenlijk gewerkt middels diverse aanpakken en thema's om dit doel te bereiken.

- **WP 1 – Data retrieval in context.** Open bronnen zijn niet altijd eenvoudig te doorzoeken (data acquisitie wordt complexer), het verwerken van grote hoeveelheden data (big data) en meer halen uit al bestaande (multimodale) databronnen (data fusie) staat centraal in dit project om effectiever en efficiënter de context van misdaad of dreigingen in kaart te brengen, te analyseren of te verwerken. Van ongestructureerde data gestructureerde data maken en hierop kunnen redeneren.
- **WP 2 – Vroegsignalering van dreigingen**. Het herkennen van dreigingen, zowel concreet als subtiel opgebouwd over de tijd, gericht tegen personen, objecten, diensten en evenementen in het rijks- en decentraal domein.
- **WP 3 – Human in the loop.** Slimme data visualisatie en interactieve gedurende het gehele proces (in iteraties) van het opwerken van data naar informatie en intelligence. Denk bijvoorbeeld aan beslissingen bij zoekstrategieën (slim puzzelen) of afwijkingen in data visualisaties benutten om verder te onderzoeken.
- **WP4 – Kennismanagement** op het gebied van open bronnen intelligence. Wat zijn de bottlenecks waarom dit nu niet gebeurt/strandt en welke (innovatieve) oplossingen worden aangereikt die passen in genetwerkte werken en groeiende samenwerking tussen regio's/nationale politie, diverse veiligheidsorganisaties en op internationaal gebied.
- **WP5 Slimmer samenwerken.** Een meer integrale aanpak op fenomenen, genetwerkt samenwerken, beter koppelen van vraag –en aanbod en op elkaar afstemmen van (nu nog) parallel lopende informatiestromen (en dito processen) tussen organisaties in het veiligheidsdomein en op diverse niveaus (regio/nationaal/internationaal).

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, danwel gezamenlijke, informatieverwerking in goede banen te leiden en te stroomlijnen. De resultaten zijn ondersteunend voor het verder professionaliseren van het informatie/intelligence 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, KLPD, KMar), analysewerkzaamheden (o.a. inlichtingendiensten, NCTV en Nationale Politie), (internet-)

recherchewerkzaamheden (Nationale Politie, KMar) en ondersteuning van de informatiefunctie in het front-office/ back- office concept (Nationale Politie) als wel samenwerking in opsporings- en strafrechtketen (National Politie, regio's, OM en Publiek Private Samenwerkingsverbanden).

Intensivering samenwerking
In 2013 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 Topic 4: Delen en benutten van informatiestromen voor het samen uitvoeren van veiligheidstaken (Beter benutten van informatiestromen)

3.2.4.1 Omschrijving van topic 4

De informatievoorziening in het veiligheidsveld staat voor de uitdaging om beschikbare gegevens, informatie, interpretaties en lessons lerend 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; en
- 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 topic 4

Waar gaat het precies over?	Delen en benutten van informatiestromen voor het samen uitvoeren van veiligheidstaken. 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	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

belang?	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 • Intuïtieve human interfaces die de gebruiker ondersteunen in zijn handelen • 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 • 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 terrorismebestrijding), VTSPN
TNO-team	Josine van der Ven (trekker), Lisette de Koning, Sam Besselink, Kees van Dongen, Richelle van Rijk, Nathalie Vink

3.2.4.3 Met VenJ en stakeholders afgestemde onderzoeksvragen voor topic 4

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.

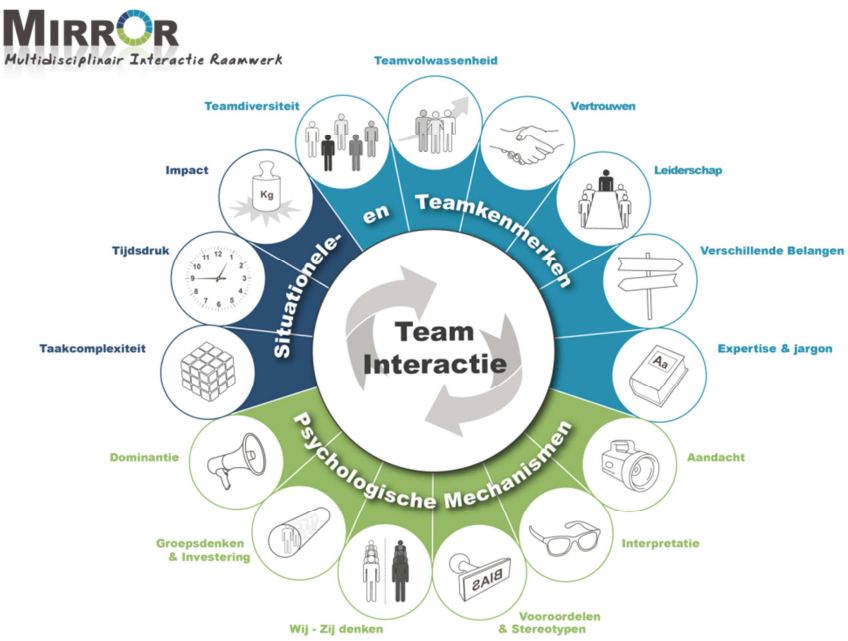
Vraag 4. Publiek-private informatievoorziening
Welke onderlinge informatievoorziening is noodzakelijk om hulpdiensten en de vitale sectoren effectief met elkaar te laten samenwerken, zowel bij incidenten en crisis als bij de voorbereiding daarop, en hoe is die informatievoorziening in te richten (middelen, 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 van topic 4 in 2012

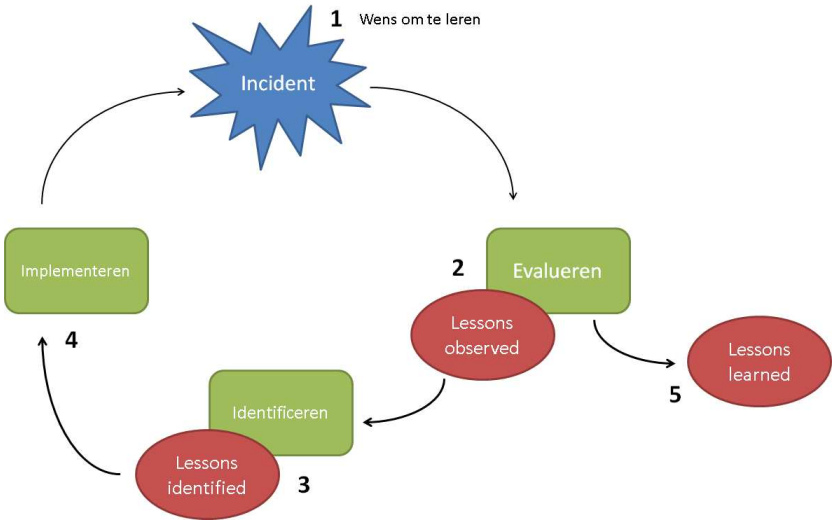
In 2012 zijn de belangrijkste onderzoeksvragen gericht op:

1. *Ondersteunen van Samenwerken:*
   Meer kennis, inzicht en interventies hoe de ad hoc samenwerking binnen crisisbeheersing en rampenbestrijding te versterken. Dit gebeurt op basis van internationaal literatuur onderzoek en eigen onderzoek (MIRROR). Hierbij is aansluiting met praktijk gezocht om mogelijke interventies te relateren aan de praktijk. Dit gebeurt door het uitvoeren van workshops (Zuid-Holland Zuid, expertmeeting Veiligheidsberaad) en het aansluiten bij oefeningen.



Figuur Het MIRROR raamwerk t.b.v. samenwerking

2. *Leren evalueren/Collectief geheugen:*
   Om de leercyclus te kunnen sluiten is het belangrijk dat er niet alleen geëvalueerd wordt, maar dat ook oplossingen geïmplementeerd en beschouwd worden; niet op de schuldige aan te wijzen als het mis gaat, maar de effectiviteit vast te stellen en te verbeteren. Het blijkt dat er goede plannen liggen om multidisciplinair te leren, maar die worden niet opgepakt in de praktijk. De drempels om multidisciplinair leren te slechten zijn in kaart gebracht en samen met de praktijk worden ze aangepakt.



Figuur De leercyclus

3. *Informatiegestuurd werken in sociale veiligheid:*
   Sociale veiligheid wordt altijd als de tegenhanger van fysieke veiligheid

gepresenteerd. Als je echter door de bril van informatiegestuurd samenwerken kijkt naar de beide gebieden van veiligheid is er veel van elkaar te leren. In de werkzaamheden van 2012 spreken we van integrale veiligheidsincidenten, met kenmerken van sociale veiligheid en fysieke veiligheid. In dit werkpakket staat de samenwerking tussen gemeente en politie centraal, beide werken in zowel fysieke als sociale veiligheid. We onderzochten aan de hand van casuïstiek hoe bepaalde incidenten op dit moment al kenmerken van beide domeinen in zich hebben, denk hierbij aan het schietincident van Alpen aan de Rijn.

4. *Waterveiligheid.*
   In de brief aan de Tweede Kamer van staatssecretaris Atsma van november 2011 over de stand van zaken waterveiligheidsbeleid wordt gesteld dat de meerlaagsveiligheidsbenadering voor het kabinet de centrale benadering vormt conform het Nationaal Waterplan en dat een aantal gebiedspilots meerlaagsveiligheid (MLV) ondersteunt op dijkringniveau. In dit werkpakket wordt in kaart gebracht hoe diverse organisaties binnen één laag de samenwerking oppakken en of die bijdraagt aan de waterveiligheid zoals dit bedoeld is binnen het MLV-benadering. In dit concept ligt de nadruk op samenwerking tussen de lagen en versterking van de waterveiligheid daardoor. Wordt dit ook zo ervaren door de organisaties in de drie lagen? Natuurlijk worden ook de successen en drempels in de samenwerking tussen de lagen zichtbaar gemaakt. De resultaten worden vastgelegd in een notitie die daarmee inzichtelijk maakt voor bestuurders hoe ‘het veld’ het mlv-benadering beleeft en implementeert. Denk hierbij bijvoorbeeld aan een groeimodel dat richting geeft aan de ontwikkeling van samenwerken en informatie-delen in het kader van meerlaagsveiligheid. Een proces aanpak die samenwerking en informatie uitwisseling in het kader van MLV faciliteert zijn andere toekomstige producten die op basis van de verzamelde informatie ontwikkeld kunnen worden.

Figuur Drie lagen uit Meerlaagsveiligheid

5. *Verkenning: harmonisatie werkwijze incidenten, rampen en crises*
   Bij TOPIC 4 wordt ook de terugkoppeling van de verkenning “Harmonisatie werkwijze incidenten, rampen en crisis” opgenomen. De onderwerpen van deze verkenning liggen in het verlengde van de onderwerpen bij Topic 4.
   Deze verkenning valt in twee delen uiteen, verkenning naar nationale mogelijkheden voor een harmonisatie van de werkwijze en een verkenning naar EU mogelijkheden voor een harmonisatie van de werkwijze.
   Er is begonnen met een verkenning naar de mogelijkheden binnen EU naar harmonisatie van de werkwijze. We maken daarbij gebruik van de kennis die is opgedaan in het ACRIMASproject, waarin diverse gaps geïdentificeerd zijn.
   De focus ligt nu op harmonisatie en afstemming via educatie en lessons learned voor crisisprofessionals en burgers. Het onderzoek richt zich op wat (methodiek, ondersteuningsmiddelen) op dit moment wordt ingezet (nationaal, EU en internationaal) om samenwerking tussen professionals en burgers te verbeteren en de effectiviteit (lesson learned) ervan. Slimme combinaties van bestaande methode zouden kunnen bijdragen aan het oplossen van de geïdentificeerde gaps. Of we kunnen concluderen dat er nieuwe methoden en tools ontwikkeld moeten worden (bijv. ivm culturele verschillen).

3.2.4.5 Voorgestelde zwaartepunten voor voortzetting topic 4 in 2013

Voor 2013 heeft het team van TOPIC4 de volgende impact voor ogen: Samen staan we sterker, in tijden van crisis en daarbuiten.

1. Samenwerken wordt nu vooral geoefend in de voorbereiding op de response fase. Samenwerken is echter niet alleen in de responsefase van cruciaal belang. TOPIC4 legt daarom in 2013 de focus op altijd en overal leren samenwerken, met intuïtieve ondersteuningstools en geheugensteuntjes gebaseerd op de MIRROR-methodiek. We zullen dit ontsluiten voor zowel het fysieke als het sociale veiligheidsveld. Denk hierbij aan het inzichtelijk maken hoe maatschappelijke impact van incidenten samenhangt met de bestrijding van een incident, en de keteneffecten waar men op uitvoerend niveau rekening kan houden. Daarmee wordt bijvoorbeeld communicatie naar burgers beter afgestemd. Maar ook informatie van burgers kan sneller haar weg vinden naar de uitvoerende teams (als mensen aan ‘de telefoon’ bijv. de informatiebehoeften kennen van de teams).

2. Het OTO budget neemt door de crisis af, maar de complexiteit van de incidentbestrijding neemt toe. Multidisciplinair leren ondersteunt daarbij zodat niet elke monodiscipline en veiligheidsregio het wiel opnieuw hoeft uit te vinden. TOPIC4 draagt daarmee bij aan de implementatie van multidisciplinair leren in de veiligheidsregio’s en dat het onderwerp onder de aandacht komt van betrokken managers. Multidisciplinair leren draagt niet alleen bij aan een landelijk werkwijze en een collectiefgeheugen, het zorgt ervoor dat OTO-inspanningen maximaal effect sorteren: doing better things ipv doing things better. We komen met interventies en een methodiek om multidisciplinair leren in te voeren in de praktijk. In dit werkpakket ontwikkelen we kennis en methoden samen met de praktijk.

3. Voor verdere uitwerking van informatiegestuurd samenwerken binnen integrale veiligheid, ligt de focus op het in figuur 3 'zichtbare' grijze gebied, waar zowel fysieke als sociale veiligheid van belang is. De rol van de gemeente voor zowel sociale als fysieke veiligheid wordt daarbij het vertrekpunt. Bij sociale veiligheid zit de gemeente vaak in het voortraject, bij fysieke veiligheid in de response- en herstelfase. In de toekomst zullen we steeds meer incidenten tegenkomen die zich afspelen in dat grijze gebied, en waar de gemeente bij elke fase aanschuift. Welke rol kunnen zij nemen, en hoe vul je die rol in? Om kennis van het ene domein naar het andere te vertalen willen we interventies ontwikkelen voor ontkleurd leiderschap/regievoerder en netwerkkaarten.

3.2.5 Topic 5: Cybersecurity

3.2.5.1 Omschrijving van topic 5

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 het Informatieknooppunt Cybercrime (IKC). De goede samenwerking van de vitale sectoren binnen het IKC 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 topic 5

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/ NCTV, CPNI.nl, VTSPN, AIVD, KLPD, NFI, Logius, providers, VNO-NCW, Ministerie EZ, VNG, vitale sectoren, EU DG Home Affairs, Defensie (p.m. 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. • Ontwerp van de architectuur van de cyber-infrastructuur en gebruiksmodaliteiten die leiden tot vermindering van de mogelijkheid tot cybermisbruik (security by design). • Methoden voor verminderen van de afhankelijkheid van de vitale infrastructuur-sectoren in de maatschappij van verstoringen in de cyberinfrastructuur.
Wie begeleidt?	Jos Leenheer (Coördinator VenJ/NCTV), Defensie, VTSPN, e.a.
TNO-team	Marieke Klaver (trekker), Robin de Haas, Frank Fransen, Eric Luiijff

3.2.5.3 Met VenJ en stakeholders afgestemde onderzoeksvragen voor topic 5

Onderzoeksvraag 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.

Onderzoeksvraag 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 (meer-laagsbescherming, keten-afhankelijkheid, noodvoorzieningen e.d.)

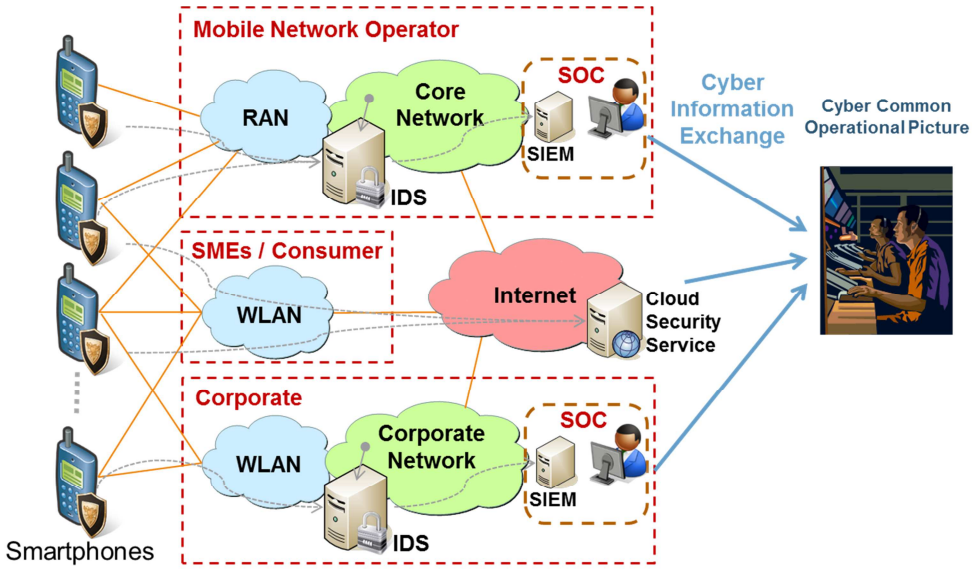
Onderzoeksvraag 3: Hoe is het gevolg van cybermisbruik voor de vitale infrastructuur te beperken?

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 topic 5 in 2012

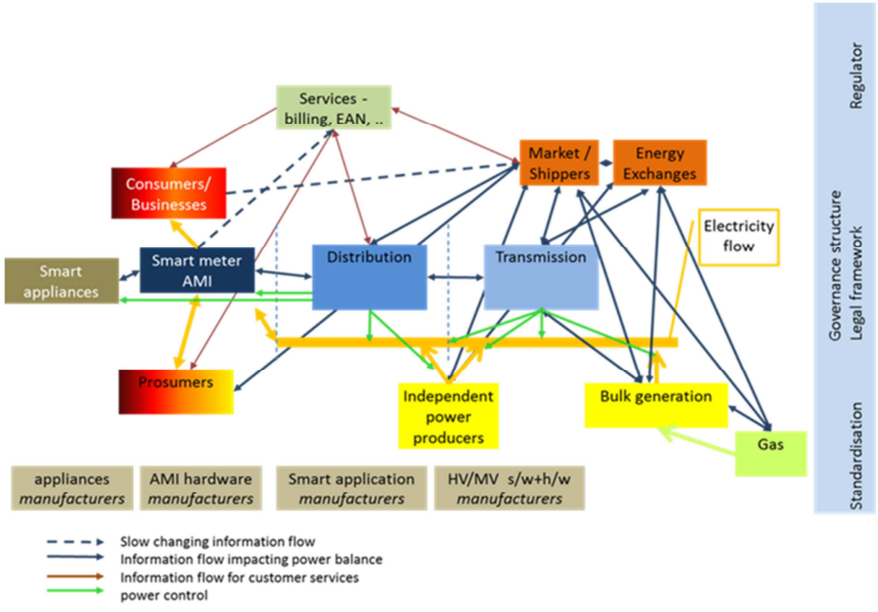
Detectie van misbruik (mobiele systemen)
Doelstelling: Het identificeren van dreigingen voor mobiele platformen en het ontwikkelen van oplossingsrichtingen voor het vroegtijdig detecteren van misbruik, inclusief het benoemen van mogelijkheden van opsporing en vervolging.
Status: De afgelopen periode is er een overzicht gemaakt van de ontwikkelingen op het vlak van mobiele apparaten en toepassingen en zijn de dreigingen op globaal niveau geïdentificeerd. Daarnaast zijn er een aantal use cases 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.
Op basis van de use case is een mogelijk ontwerp van een sensorinfrastructuur opgesteld die gegevens uit verschillende bronnen bij elkaar brengt. De haalbaarheid van dit concept is vervolgens getoetst bij een aantal stakeholders (een mobiele operator, NCSC). Het delen van gegevens over organisatiegrenzen bleek hierbij voorlopig een knelpunt.



Op basis hiervan is besloten de verdere werkzaamheden op te splitsen en te concentreren op (1) de informatiebehoefte en mogelijk uit te wisselen gegevens tussen organisaties en bijvoorbeeld het NCSC (2) de detectiemogelijkheden binnen één organisatie.

Vervolg in 2013
Voor het onderzoek binnen dit topic wordt voorgesteld voor onderwerp (1) in 2013 de nadruk te leggen op het overheidsdeel van de informatie en het onderzoek te richten op methoden en technieken om gegevens uit verschillende bronnen te combineren in een gezamenlijk geaggregeerd beeld. Hierbij wordt naast de technische aspecten en mogelijkheden ook aandacht besteed aan organisatorische aspecten van het delen van vertrouwelijke gegevens over verschillende organisaties.
Onderwerp (2) wordt in nauwe samenwerking met het bedrijfsleven uitgewerkt binnen het aanpalende VP Security (zie paragraaf 3.2.5.5). In het VP Security worden in samenwerking met bedrijven de technische mogelijkheden voor monitoring en het verzamelen en analyseren van gegevens verder uitgewerkt. Hiervoor wordt samengewerkt met mogelijke leveranciers (bijv. IBM, maar indien mogelijk ook met SOC's van bedrijven).

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. Een deel van de werkzaamheden en resultaten is ook internationaal benut. De dreigingsanalyse en het actorenmodel voor smart grids is ingebracht en uitgewerkt in een EU werkgroep (http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/expert_group_smart_grid/index_en.htm).
De afgelopen periode is gewerkt aan een referentiekader om deze security aspecten vanuit de perspectieven van de verschillende stakeholders inzichtelijk te maken.



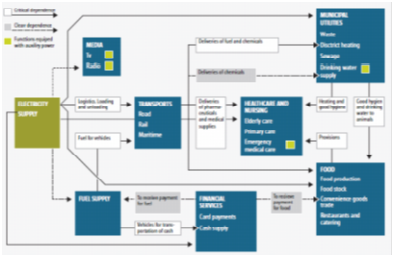
Op basis van de dreigingsanalyse en op basis van een referentiemodel is geïdentificeerd welke regels en principes voor een meer secure Smart Grid ontwerp kunnen zorgen. Hierbij is niet alleen gekeken naar techniek, maar ook naar de inrichting van processen en organisatie. Hiervoor zijn principes benoemd die binnen de scope van één organisatie spelen en naar aspecten die alleen op ketenniveau kunnen worden opgepakt.

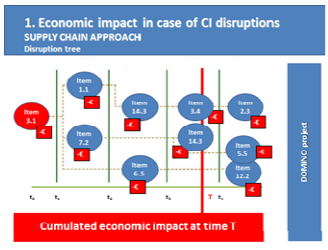
Vervolg in 2013:
Het voortbouwen op deze werkzaamheden zal in 2013 worden uitgevoerd binnen het VP Security in nauwe samenwerking met bedrijfsleven (met name Alliander).

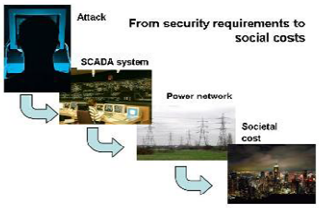
Cyber security vitale infrastructuur
Doelstelling: Te komen tot ondersteunende methoden en modellen voor de uitwisseling van 'security posture' en gegevens die de cyberstatus van de vitale infrastructuur (gedeeld ICT-risicobeeld) en de effectiviteit van beschermingsmaatregelen inzichtelijk maken.
Status: Zowel nationaal als internationaal vindt samenwerking en gegevensuitwisseling plaats over dreigingen, kwetsbaarheden, tegenmaatregelen en onderliggende modellen. In deze onderzoekslijn wordt onderzocht welke methoden en tools kunnen ondersteunen bij informatie-uitwisseling over dreigingen, kwetsbaarheden en good practices en wordt onderzocht welke methoden kunnen ondersteunen bij het beoordelen van de cyberstatus van organisatie in de vitale infrastructuur.

Vervolg in 2013:
Voor dit onderwerp bestaan mogelijkheden voor verdere internationale samenwerking bijvoorbeeld rond de ontwikkeling van een information sharing platform.
Voor 2013 zullen de werkzaamheden binnen deze onderzoekslijn worden gedefinieerd in nauwe samenwerking met het NCSC.

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: Er heeft een inventarisatie plaatsgevonden van typen modellen, zoals op keteneffecten gerichte modellen, specifiek op kosten gerichte modellen, en meer gedetailleerde modellen voor het analyseren van het ontwerp van netwerken.







Binnen dit werkpakket wordt samengewerkt met internationale partners, met name op het gebied van modellen voor de vitale infrastructuur (binnen het EU-project CIPRNET).

Vervolg in 2013:
Op basis van de uitgevoerde inventarisatie zullen een aantal kansrijke onderwerpen worden gedefinieerd voor het ontwikkelen van nationale modellen. Op basis van deze selectie zal in 2013 een aantal modellen verder worden uitgewerkt.

3.2.5.5 Voorgestelde zwaartepunten voor voortzetting in 2013

In de vorige paragraaf staat per onderwerp aangegeven waar in 2013 de nadruk zal worden gelegd in het onderzoek. De beschreven hoofdrichting sluit aan bij de Cyber security prioriteiten op het gebied van monitoring en de bescherming van de vitale infrastructuur.
Doordat Jos Leenheer wordt opgevolgd door Hasse de Graaf als begeleider van het topic moet de afstemming over de hoofdrichting voor de vervolgwerkzaamheden in september in meer detail nog plaatsvinden. Tevens zal nauwe afstemming plaatsvinden met het NCSC.

Daarnaast worden de vervolgwerkzaamheden ook nauw afgestemd met aanpalend onderzoek binnen het VP Security onder de topsector HTSM. Binnen deze topsector HTSM is het onderwerp cybersecurity ook als onderzoekstopic benoemd. Binnen het VP Security vindt onderzoek plaats in zeer nauwe samenwerking met het bedrijfsleven.

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. Bv: Wat kan “Augmented Reality”-technologie in het veiligheidsdomein betekenen? 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. Bv: Welke dreiging betekent het breed beschikbaar komen van nieuwe bi agentia? 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 2013 uit te voeren verkenningen zal op zijn vroegst in december 2012 worden gemaakt. Zo mogelijk wordt hierbij ingespeeld op de beleidsintensiveringen van een nieuw kabinet.

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 initiatieven voor samenwerking binnen de topics genomen, terwijl op VP-niveau de afstemming met de Politieacademie aandacht krijgt.

3.3.2 Samenwerking met partners voor implementatie

Nationaal zijn door het kabinet Rutte omvangrijke stimuleringsprogramma's voor Maatschappelijke Veiligheid gestopt. Momenteel worden initiatieven genomen om de aansluiting bij de topsectoren (m.n. Hightech, Logistiek en Water) te versterken en tevens Cybersecurity in de Nationale Digitale Agenda te verankeren.

Internationaal zijn er nog wel omvangrijke en groeiende innovatiestimuleringsprogramma'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 Veilige Maatschappij 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 2013 gaat het om ca. 40% van het totale VP-budget.

3.4 Afspraken voor uitwerken van projectplannen voor 2013

Met VenJ is afgesproken dat TNO voor 1 november 2012 per topic een projectplan maakt voor de in 2013 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 2012 de conclusies van de vijf overleggen over de projectplannen worden besproken. Dan zal ook nader overleg plaatsvinden over de financiële planning.

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.