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 2013 R10305

Vraaggestuurd programma 2011-2014 Voortgangsrapportage 2012 Thema XI Maatschappelijke Veiligheid

Datum	1 maart 2013
Auteur(s)	Dr.ir. J.A. Don
Aantal pagina's	40 (incl. bijlagen)
Aantal bijlagen	0
Regievoerend departement	Ministerie van Veiliigheid en Justitie
Projectnaam	Vraaggestuurd Programma Veilige Maatschappij
Projectnummer	053.01011/01.02
Geauthoriseerd door	Drs. H.G. Geveke
Handtekening	

Samenvatting

Het Vraaggestuurde programma Maatschappelijke Veiligheid 2011-2014 is gericht op het realiseren van impact op de toekomstige veiligheidssituatie in Nederland en het versterken van de basiskennispositie bij TNO. Dit rapport biedt een rapportage van de voortgang in 2012.

Omdat de omvang van het VP Veilige Maatschappij ten opzichte van 2011 werd gehalveerd, moesten in gang gezette trajecten worden afgebroken. Het ministerie van Veiligheid en Justitie heeft vervolgens voor het jaar 2012 een subsidie toegekend van 1 M€ om dreigende kapitaalsvernietiging te voorkomen en de betreffende deelprogramma's op een lager ambitieniveau af te ronden. De resultaten van het gebruik van deze (extra) subsidie zijn integraal opgenomen in deze voortgangsrapportage. In de loop van 2012 is in het kader van het topsectorenbeleid een nieuw Vraaggestuurd Programma Security opgestart. Hierin krijgen ook enkele onderzoektrajecten die in het kader van het VP Veilige Maatschappij gestopt moesten worden een doorstart, gezien het draagvlak voor de beoogde innovaties bij zowel bedrijfsleven als overheid.

In 2012 zijn op de vijf topics van het VP Veilige Maatschappij als belangrijkste resultaten bereikt:

- *Topic 1. Herkennen afwijkend gedrag*
  Met een praktijk-experiment is nu voor het eerst aangetoond dat het concept van prikkelen een positief effect heeft. Prikkelen is 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. De theoretische, psychologische basis van prikkelen en afwijkend gedrag in het algemeen is geanalyseerd om systematisch toepassen voor te bereiden. Deze inzichten zijn vastgelegd in een hoofdstuk van het boek Veiligheid (editor prof. Erwin Muller) en ook gepubliceerd in een artikel in het vaktijdschrift Security Management.
  In het praktijk-experiment lieten we mensen legale en illegale pakketjes vervoeren.

  Op de geplande route stond een beveiliger die hen zou kunnen oppakken als ze daartoe aanleiding zagen. Onder deze omstandigheden ervoeren deelnemers met illegale pakketjes de veronderstelde psychologische effecten. Bovendien bleken toezichthouders in de “centrale” 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. Ook zijn ervaren politiemensen hier beter in dan studenten. Deze uitkomsten rechtvaardigen nader onderzoek om van deze methode verder uit te bouwen.

Figuur 1. Studenten en ervaren agenten bekeken beelden van proefpersonen die een legaal of illegaal pakketje vervoerden. Bij het passeren van een toezichthouder werden de proefpersonen matig of juist sterk geprikkeld. Taak van de studenten en ervaren agenten: wijs op de videobeelden aan wie volgens jou de crimineel (die met een illegaal pakket) is.

Daarnaast is een taal ontwikkeld voor een video analyse tool, waarbij men in het scherm benoemd ziet welke gedraging in beeld te zien is. In het VP Security is parallel onderzoek gestart naar de waarneembaarheid op video's van de benoemde (onderdelen van) gedragingen.
Ook is er kennis opgebouwd over hoe toezichthouders optimaal verdenkingen ("0"-en) kunnen signaleren en hoe ze die waarnemingen kunnen combineren voor een effectieve inschatting van afwijkend gedrag ("1"). Dit moet de basis voor een "0+0=1"- toezicht worden, waarbij combinatie van zwakke signalen tot betere besluitvorming van beveiligers over wel of niet interveniëren kan gaan leiden.

- *Topic 2. Activering van burgers*
  De inzet en de keuze van media voor communicatie met de omgeving zijn niet altijd gebaseerd op te bereiken doelstellingen. Zo zijn in de praktijk op een aantal plaatsen met social media experimenten gedaan om 'mee te kunnen doen' of om 'niet achter te blijven'. Koppeling tussen beoogd doel, doelgroep en keuze voor een communicatiemiddel is essentieel voor de effectiviteit.
  Om de effectiviteit van communicatie in specifieke situaties te kunnen sturen, zijn SMART doelstellingen nodig, die vertaald kunnen worden in zogenaamde 'Key Performance Indicatoren' ofwel KPI's. Per situatie is er vervolgens een optimale mix van communicatiekanalen samen te stellen. Voor dit soort keuzes is er nu een concept ontwikkeld voor een 'communicatie-dashboard' met vier samenhangende elementen:
  1. Organisatie doelstellingen, meetbaar en tijdsgebonden
  2. Keuze van interventies
  3. Organisatorische randvoorwaarden
  4. Kenmerken van de (online) doelgroep

  In 2013 wordt dit verder uitgewerkt.

- *Topic 3. Slimmer omgaan met grote hoeveelheden informatie*
  Wanneer op het internet onderzoek wordt gedaan naar individuen, dan is het van belang om uitingen op sociale media te kunnen relateren aan het individu waar onderzoek naar gedaan wordt. Op het internet en in sociale media maken mensen vaak gebruik van meerdere online identiteiten: een alias of nickname, een e-mailadres etc. In veel gevallen vermelden ze niet hun fysieke identiteit: hun eigen naam. Omdat mensen (door middel van hun verschillende online identiteiten) verschillende gedaanten aannemen op het internet, is het lastig om een compleet beeld op te bouwen over een individu. Dit is extra urgent als grote tijdsdruk is om een beeld op te bouwen, bv bij een acute dreiging.

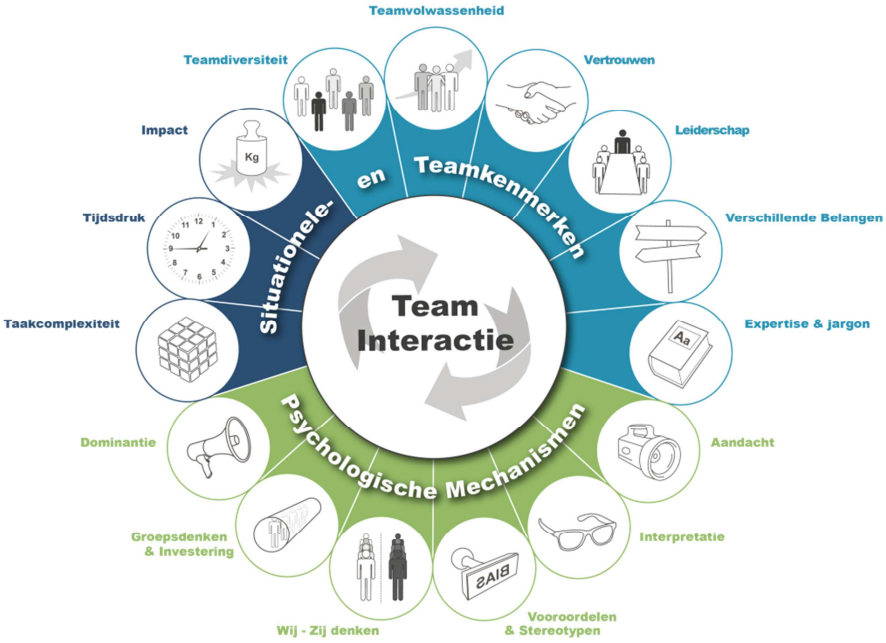
  Een voorbeeld:

Figuur 2. Uitgaande van een dreigtweet en bijbehorende online identiteit (@dreigerhenk) is een overzicht gecreëerd de online identiteiten behorende bij hetzelfde individu. De tweet is daadwerkelijk aangetroffen, de online identiteiten zijn gefingeerd

In het onderzoek is uitgegaan van een karakteristieke situatie naar aanleiding van bovenstaande dreigtweet (NB Juridische randvoorwaarden en privacy worden nadrukkelijk meegenomen). Aan de hand van deze praktijkvraag is in een vertrouwelijk TNO-rapport vastgelegd wat er nodig is aan functionaliteit en informatie in sociale media voor het aan elkaar kunnen relateren van online identiteiten.
Daarnaast is er gewerkt aan:

- Anomaliedetectie, een techniek die kan helpen om in grote hoeveelheden data de abnormale veranderingen (anomalieën) snel terug te vinden,
- een nieuwe online interventie: digitaal prikkelen bij detecteerde anomaliën op Twitter en andere social media,
- Een betere balans van informatiebenutting om enerzijds informatie-overload te voorkomen en anderzijds het negeren van waardevolle gegevens uit te sluiten,
- Een systematische uitwerking van het principe Select Before You Collect bij informatieanalyse voor specifieke veiligheidstaken. Dit geldt ook als een essentieel criterium bij het delen van informatie tussen samenwerkende instanties van de veiligheidsketen.

- *Topic 4. Beter benutten van informatiestromen en samenwerking*
  In het kader van het programma Flood Control 2015 zijn de verschillen in rollen en expertises in multidisciplinaire crisisteams onderzocht. Deze verschillen beïnvloeden de informatie die mensen waarnemen en hoe mensen deze informatie interpreteren. Hierdoor kunnen gemakkelijk misverstanden ontstaan. De zgn. MIRROR-methode geeft voor leden van multidisciplinaire crisisteams inzicht in het eigen gedrag, het gedrag van andere teamleden en mogelijkheden om het teamproces te verbeteren. Dit draagt bij aan beter geïnformeerde teamleden en breder gedragen beslissingen. Voortbordurend op het project MIRROR is ook kennis opgedaan over welke sociaal psychologische theorieën en interventies bekend zijn om ervoor te zorgen dat men zich openstelt voor andere partijen. Deze kennis is toegepast in de trainingsmodule IMPACT. Verder is in een door het Veiligheidsberaad georganiseerde workshop over vitale partnerschappen MIRROR in de praktijk toegepast.

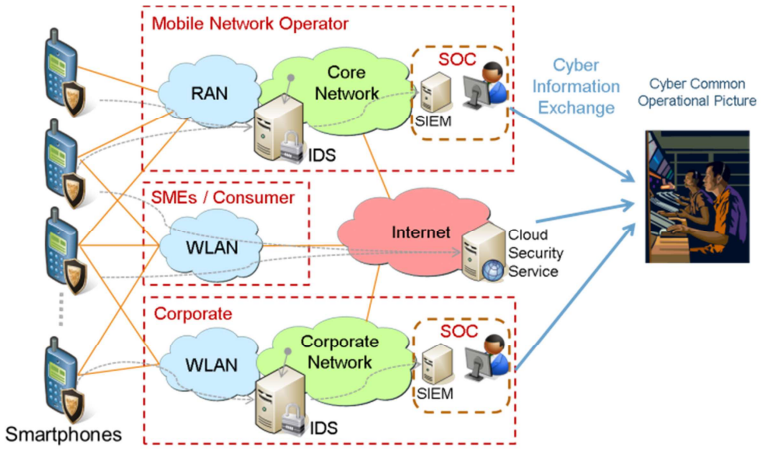


Figuur 3. MIRROR: overzicht van factoren die van invloed zijn op de interactie in een multidisciplinair crisisteam.

Andere onderzochte onderwerpen in dit topic zijn, het sluiten van de leercyclus, nadat evaluaties tot aanbevelingen hebben geleid en het leggen van een informatiebasis voor meer synergie tussen de werkvelden fysieke en sociale veiligheid.

- *Topic 5. Cybersecurity*
  In de werkzaamheden voor 2012 stond detectie van grootschalig misbruik centraal, met de focus op mobiele infrastructuur. Hiertoe is behoefte aan een mobiel sensornetwerk, met de mogelijkheid om gecentraliseerd grote hoeveelheden sensorinformatie (loggegevens, incidentgegevens, etc) te kunnen analyseren. Deze architectuur dient dusdanig generiek te zijn, dat het kan worden toegepast op verschillende infrastructuren, waarbij een grote diversiteit van informatie kan worden verwerkt, zodanig dat verschillende vormen van misbruik kunnen worden gedetecteerd.

Om een beeld te krijgen van de huidige mogelijkheden van detectie in een mobiele omgeving, is begin 2012 een state of the art onderzoek uitgevoerd. In dit literatuuronderzoek is zowel gekeken naar detectiesystemen op de mobiele apparatuur zelf (vaak matig tot slecht van kwaliteit) en systemen gericht op de operator. Daarnaast is een globaal ontwerp gemaakt van een gedistribueerde sensorarchitectuur waarin gegevens uit verschillende systemen gecombineerd kunnen worden in een centraal beeld. Dit globale ontwerp is vervolgens getoetst bij enkele stakeholders (een mobiele operator en het NCSC).



Figuur 4. Globaal ontwerp van een gedistribueerde sensorarchitectuur voor detectie van misbruik in netwerken van mobiele platformen

Voor deze stakeholders is essentieel dat een ontwikkeling in deze richting gefaseerd wordt opgezet. De uitwisseling van informatie vindt momenteel vooral plaats via face-to-face contacten en overlegstructuren (ISAC's, OITO). Het delen van gedetailleerde detectie-informatie kan niet zonder meer worden doorgevoerd.
In dit topic wordt ook gewerkt aan een dedicated verzameling modellen die de effecten van verstoringen in de cyberinfrastructuur kunnen analyseren en daarmee what-if analyses mogelijk maken. Als ondersteuning van onderzoekslijn 1 (mobiele platformen in cyberinfrastructuur-systemen) gaat het om meer gedetailleerde modellen die de effecten van ICT-uitval of -verstoring binnen een vitale infrastructuur kunnen bepalen. Hiermee kunnen patronen van misbruik worden geanalyseerd. De effecten van incidenten kunnen worden bepaald, en tevens kan de effectiviteit van eventuele beschermende maatregelen worden bepaald.
Binnen onderzoekslijn 3 (vitale infrastructuur) gaat het om modellen die de impact van grootschalige verstoringen binnen de vitale infrastructuur bepalen en de mogelijke keteneffecten in kaart brengen.
Na de inventarisatie van de op de keteneffecten gerichte modellen in 2011 is het onderzoek in 2012 onderzoek gericht op gedetailleerde modellen voor het analyseren van het ontwerp van netwerken en op modellen voor de ondersteuning van training en opleiding. Tevens is de samenwerking met internationale partners voor de selectie van modellen versterkt. Binnen EU verband is het voorstel voor een Network-of-excellence op dit onderwerp gegund (CIPRNET). Daarnaast wordt ook deelgenomen aan een werkgroep in NAVO verband voor cyber defence modellen.

Conclusie
De kennisontwikkeling in de vijf topics heeft in 2012 geleid tot concretere resultaten. Dit was mede het gevolg van de intensievere afstemming en samenwerking van de onderzoekers met het veiligheidsveld. Mede gezien de decentralisatie van een aantal voor overheidstaken naar het gemeentelijke niveau en de ambitie om de zelfredzaamheid en resilience van de maatschappij ten aanzien van fysieke en sociale veiligheid te versterken is aansluiting met deze doelgroep een nader te onderzoeken uitdaging.

Inhoudsopgave

1 Inleiding

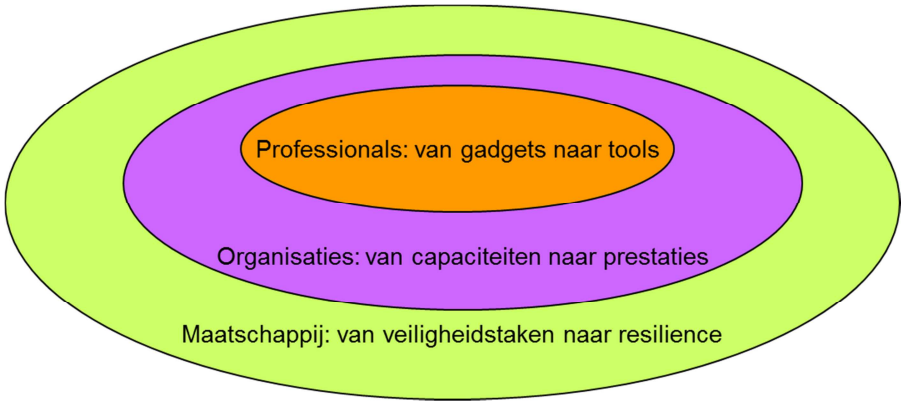
1.1 Beschrijving van TNO-thema Integrale Veiligheid

In het Strategisch Plan 2011-2014 van TNO is het Thema Integrale Veiligheid gericht op een veiliger samenleving. Veiligheid is 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:

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 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. Daarbij is het verankeren van verantwoordelijkheden van burgers en bedrijven voor de veiligheid van henzelf en hun omgeving een belangrijk issue. TNO richt zich op het onderling samenhangende innovaties op drie niveaus:



TNO gaat de uitdagingen voor een veiliger maatschappij aan, door te focussen op de volgende onderwerpen c.q. business lines:

- Security and Protection
- Resilience and Society

1.2 Vraaggestuurd onderzoek in de strategieperiode 2011-2014 voor het Thema Integrale Veiligheid

Voor de ontwikkeling van de strategie en de programmering van het Vraaggestuurde onderzoek voor het Innovatiegebied Defence Research vindt de afstemming tussen de overheid en TNO plaats onder regie van het Ministerie van Defensie. Hiervoor zijn strikte procesafspraken voor het jaarlijks bijstellen en vernieuwen van de portfolio van meerjarenprogramma's.

Met ingang van 2012 zijn er aan het Innovatiegebied Safety and Security Research twee Vraaggestuurde Programma's (VP's) primair verbonden:

- het VP Veilige Maatschappij
- het VP Security

Voor de ontwikkeling van de strategie en de programmering van het VP Veilige Maatschappij, vindt de afstemming tussen de overheid en TNO plaats onder regie van het Ministerie van Veiligheid en Justitie (VenJ) en in nauwe samenspraak met stakeholders uit de diverse overheidsgeledingen. In deze voortgangsrapportage van Thema XI Maatschappelijke Veiligheid wordt alleen het VP Veilige Maatschappij behandeld.

Het VP Security wordt gerapporteerd in de voortgangsrapportage van Thema High Tech Systems & Materials. Dit VP is de vertaling van de HTSM-roadmap Security (zie www.htsm.nl) naar TNO-onderzoeksprojecten. De uitvoering wordt begeleid door een roadmapteam waarin vertegenwoordigd zijn: het bedrijfsleven (NIDV, Thales), de departementen VenJ, Defensie en EZ, de gemeente Den Haag en NWO/STW. Bij de projecten in het VP Security zijn bedrijven en/of veiligheidsorganisaties van de overheid betrokken met in-kind- en/of cash-commitment.

Omdat de omvang van het VP Veilige Maatschappij ten opzichte van 2011 werd gehalveerd, moesten in gang gezette trajecten worden afgebroken. Het ministerie Veiligheid en Justitie heeft vervolgens voor het jaar 2012 een subsidie toegekend van 1 M€ om dreigende kapitaalsvernietiging te voorkomen en de betreffende deelprogramma's op een lager ambitieniveau af te ronden (brief van Ministerie VenJ, dd. 29 november 2011, nr. 2011-2000533746, ondertekend namens de Minister van Veiligheid en Justitie door de directeur Nationale Veiligheid, mw. R.W.C. Clabbers). De resultaten van deze subsidie zijn integraal opgenomen in deze voortgangsrapportage.

Deze rapportage is allereerst een verantwoording van het vraaggestuurde programma op hoofdlijnen. In overeenstemming met het verzoek van EZ zal TNO een aanduiding van de hiermee gemoeide projecten en hun resultaten met een redelijk termijn op de TNO-website plaatsen.

1.3 Management oordeel over de uitvoering

Het jaar 2012 was het tweede jaar van de uitvoering van het Vraaggestuurde Programma 2011-2014 Veilige Maatschappij. Door de medio september 2011 aangekondigde halvering van het budget 2012, was een forse bijstelling nodig. Uiteindelijk is door de noodhulp van het ministerie van VenJ, met een eenmalige injectie van 1 M€ en een intensieve afstemming tussen de departementen VenJ en EZ over het belang van een Roadmap Security, voorkomen dat er een ongewenste vernietiging van reeds gedane kennisinvesteringen plaatsvond. Momenteel kan gesproken worden van een verantwoorde borging van lopende innovatietrajecten en een versterking van draagvlak voor het benutten van de resultaten van het verkennend onderzoek van TNO op het gebied van Maatschappelijke Veiligheid.

De vorming van de Nationale Politie en de schaalvergroting binnen de veiligheidsregio's en de meldkamerinfrastructuur waren belangrijke externe ontwikkelingen. Enerzijds gaf dit een nieuw perspectief op bundeling van decentrale innovatie-initiatieven, anderzijds was er nogal wat onduidelijkheid over de aansturing daarvan. Het krachtiger verbinden van de kennisontwikkeling binnen instituten als IFV, PA, RIVM en TNO met de nationale veiligheidsorganisaties is een prioriteit voor het vervolg. En dat houdt niet op bij onze grenzen. Daarom is het een goede zaak dat de samenwerking van Nederlandse partijen onderling maar ook met partners uit andere EU-lidstaten voor het ontwikkelen van onderzoeksprojecten met Brusselse steun verder is uitgebreid.

De kennisontwikkeling in de vijf topics heeft in 2012 geleid tot concretere resultaten. Dit was mede het gevolg van de intensievere afstemming en samenwerking van de onderzoekers met het veiligheidsveld. Mede gezien de decentralisatie van een aantal voor overheidstaken naar het gemeentelijke niveau en de ambitie om de zelfredzaamheid en resilience van de maatschappij ten aanzien van fysieke en sociale veiligheid te versterken is aansluiting met deze doelgroep een nader te onderzoeken uitdaging.

Als TNO zetten we ons in op het helder krijgen van de winst die de publieke en private veiligheidsstakeholders, door het toepassen van de ontwikkelde kennis, kunnen realiseren. Samen met diverse partijen worden "business cases" ontwikkeld, die duidelijk maken dat innovatie geen kostenpost is maar een renderende investering. Dit is ook de kern van de publicatie "Veiligheid schreeuwt om innovatie", die op 10 december in een bijeenkomst met 100 top-vertegenwoordigers van het veiligheidsveld aan minister Opstelten werd overhandigd.

2 Vraaggestuurd programma Veilige Maatschappij

2.1 Vragen waar het VP Veilige Maatschappij zich op richt

Het regievoerend departement Veiligheid en Justitie (VenJ, destijds Binnenlandse Zaken) heeft voor focussering van de Meerjarenprogramma 2011-2014 de volgende organisaties geconsulteerd: 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 VP-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

2.2 Aansluiting bij het VP Security

Vier van de vijf topics van het VP Veilige Maatschappij zijn aangesloten op ontwikkelingen voor een deelroadmap in het VP Security:

Topic VP Veilige Maatschappij	**Project voor Deelroadmap in VP Security**
Topic 1. Herkennen afwijkend gedrag	3b Passieve sensoren
Topic 2. Activering burgers	-
Topic 3. Slimmer omgaan met veel informatie	1. Systems of systems
Topic.4. Delen en benutten van informatie-stromen voor het samen uitvoeren van veiligheidstaken	1. Systems of systems
Topic 5. Cybersecurity	2. Cybersecurity
-	3a Actieve sensoren

De aansluiting van het VP Security op de topics in het VP Veilige Maatschappij is geborgd, doordat binnen TNO de projectleiders van de projecten in het VP Security en het VP Veilige Maatschappij duo's vormen die aangestuurd worden door de TNO-programma-manager die voor beide programma's gelijk is.

2.3 Uitvoering in 2012

2.3.1 Begeleiding van de topics

Voor elk van de vijf topics is een coördinerend behoeftesteller voor de verdere uitwerking en uitvoering aangewezen. Elke coördinerend behoeftesteller heeft vervolgens een begeleidingsteam gevormd en het kennisontwikkelingsplan voor 2012 opgesteld.

VP-topic (TNO-projectleider per 31.12.2012)	Coördinerend behoeftesteller (per 31.12.2012)
1. **Herkennen afwijkend gedrag** (Dianne van Hemert)	VenJ, DG-NCTV
2. **Activering burgers** (Gerard Veldhuis)	Brandweer Nederland
3. **Info-mining** (Arnout de Vries)	VenJ, DG RR
4. **Infobenutting voor samenwerken** (Josine van de Ven)	Centrum Innovatie en Veiligheid, Utrecht
5. **Cybersecurity** (Marieke Klaver)	VenJ, DG-NCTV, NCSC

Gedurende het jaar 2012 zijn er voor ieder topic minstens drie bijeenkomsten van het begeleidende team geweest. Verder zijn ook de coördinerend begeleiders in mei en november bijeen geweest (maart, september, november).

Namens het departement Veiligheid en Justitie werd de regievoering over het VP tot 1oktober uitgevoerd is door Kees Lebon en Edmée Moojen. Per 1 oktober 2012 is Kees Lebon opgevolgd door But Klaassen.

2.3.2 Verkenningen

In juni 2012 is er een tweetal onderwerpen voor het uitvoeren van een verkenning afgesproken, terwijl de rest van het gereserveerde budget voor verkenningen werd toegevoegd aan de deelprojecten voor de topics 1, 3 en 5.

Titel verkenning (TNO-projectleider)	Begeleider	Projectleider TNO
Whole community approach	Marjan Heijman (Brandweer Nederland) / Jan Lavèn (Centrum Innovatie en Veiligheid, Utrecht)	Lisette de Koning (rapportage resultaat bij topic 2)
Harmonisatie werkwijze incidenten, rampen en crises	Marjan Heijman (Brandweer Nederland) / Jan Lavèn (Centrum Innovatie en Veiligheid, Utrecht)	Josine van de Ven (rapportage resultaat bij topic 4)

2.3.3 Deelname in projecten met nationale of EU-funding

In onderstaande tabel staan de projecten met nationale en internationale funding waarin met een financiële bijdrage vanuit het VP is deelgenomen.

Project-naam	**Onderwerp**	**Bron Funding**	**Topic VP 2011-2014**
Livinglab	Veiligheidsinnovaties in stad	PiD	2
Flood Control 2015	Crisiscommunicatie, serious gaming, zelfredzaamheid	IP-Water	2 en 4
BESECURE	Veilige stedelijke omgeving	EU	2 en 5
ACRIMAS	Crisismanagement systems of systems	EU	4
ETCETERA/ INNOSEC	Verkenning security technologie	EU	6
DITSEF	Uitrusting First Responders	EU	Vorig VP
RSTV	Sensors voor rookanalyse brand	MIA-V	Vorig VP
SECUR-ED	Veilig stedelijk transport	EU	Vorig VP
EMPHASIS	Opsporing explosieven productie	EU	Vorig VP
PREVAIL	Precursors zelfgemaakte explosieven	EU	Vorig VP
SPIRIT	Bescherming gebouwde infrastructuur	EU	Vorig VP
VITRUV	Resilience stedelijke omgeving	EU	Vorig VP
PRACTICE	Resilience tegen CBRN	EU	Vorig VP
HYPERION	Self-made explosives	EU	Vorig VP
SAFIRE	Verminderen radicalisering	EU	Vorig VP
Forensic Fieldlab	3D-model van plaats delict	PiD	Vorig VP

Deze projecten bouwen voort op de kennisontwikkeling in de afgesproken topics, of op de kennisontwikkelingsgebieden uit het VP 2007-2010. Voor nieuwe verplichtingen is afgesproken dat deze moeten passen in het kader van de actuele VP- topics.

2.3.4 EZ-cofinanciering

In 2010 is gestart met de uitvoering van het zgn. STARS-project (Sensor Technology Applied in Reconfigurable systems for sustainable Security). Het project is gericht op het kunnen produceren van reconfigureerbare sensor(netwerken) voor de beveiliging van onze maatschappij. Dit FES-project wordt getrokken door een consortium, waarvan de bedrijven Thales, NXP en RECORE deel uitmaken. Ook zijn de ministeries VenJ, EL&I en Defensie betrokken. Beoogde eindgebruikers zijn naast beveiligingsbedrijven diensten als de KLPD, de kustwacht, de havendienst en Defensie.

In 2012 kregen de twee projecten gericht op verbetering van het herkennen van menselijk gedrag door toezichthoudend personeel een vervolg. Het gaat daarbij zowel om surveillanten als operators van uitkijkcentrales. Een bijzonder project is de samenwerking met sociale werkplaatsen om de beperking van autisten als kwaliteit te benutten.

Het project voor de ontwikkeling van indoor lokalisatie met radar tags moest tussentijds gestopt worden door financiele problemen van de industriële co-financier. Met name voor bewakingsdoelen worden hier toepassingen voorzien (o.a. monitoring gedetineerden in gevangenissen).

Een nieuw project voor het ontwikkelen van een onderwater-sensornetwerk voor bewaking in het Rotterdamse havengebied werd opgestart.

2.4 Rapportages 2012

2.4.1 Rapportage topics

De in 2012 bereikte resultaten zijn vastgelegd in de KIP-verslagen en onderzoeksverslagen en publicaties. In hoofdstuk 3 van deze voortgangs-rapportage wordt op hoofdlijnen verslag gedaan van de resultaten voor de vijf topics.

Eerder is besloten gedurende de looptijd van het VP voor elk topic een diepte-publicatie uit te brengen, die bovendien aansluit op actuele uitdagingen voor innovatie. In 2012 zijn in dit verband gepubliceerd:

- Activering van burgers, voortgangsrapportage topic2 (gepresenteerd op 21 juni 2012)
- Hallo!, Zelfredzaamheid en crisiscommunicatie, Programma Flood Control 2015 (topic 2)
- Informatie aan het werk! (topic 3)

Voor elk topic worden bredere bijeenkomsten georganiseerd. Zo vond op 8 mei 2012 in het kader van topic 4 een bijeenkomst plaats over “Leren leren”. Deze bijeenkomst werd bezocht door ca. 40 deelnemers, waarbij meer dan de helft van 25 veiligheidsregio’s, defensie en de politie vertegenwoordigd waren. Op 21 juni vond de bijeenkomst voor topic 2 met ca 35 deelnemers plaats, waar de veiligheidsregio’s goed vertegenwoordigd waren en ook de gemeente Rotterdam een presentatie hield. Op 10 december vond een stakeholdersbijeenkomst plaats voor topic 3. In de eerste helft van 2013 staat een bijeenkomst topic 5 (Cybersecurity) in de planning.

In het verlengde van de rapportage van dit VP is er ook een meer omvattende publicatie uitgebracht: “Veiligheid schreeuwt om innovatie!” (http://www.tno.nl/content.cfm?context=kennis&content=nieuwsbericht&laag1=60&laag2=69&item_id=2012-11-12%2009:40:40.0) Dit boek is in een brede bijeenkomst met stakeholders op 10 december 2012 overhandigd aan minister Opstelten.

3 Resultaten van het VP Veilige Maatschappij in 2012

3.1 Topic 1. Herkennen afwijkend gedrag

3.1.1 Doelstelling

Succesvol veiligheidstoezicht is afhankelijk van de capaciteit om vroegtijdig te beoordelen of er sprake is van een incident, vergrijp of delict. Dat is een complexe taak bij luchthavens, openbaar vervoer, beurzen, buitenwijken, musea, overheidsgebouwen, evenementen, grote winkelcentra, etc. Dat heeft twee oorzaken. Ten eerste zijn er op deze locaties veel mensen aanwezig en is de toezichtstaak vergelijkbaar met het zoeken naar een speld in de hooiberg. Doorgaans is niet een enkele, duidelijk zichtbare afwijkende gedraging[1] reden voor een verdenking, maar vaak gaat het juist om een reeks subtiele afwijkingen. Mensen zijn redelijk goed in het herkennen van die subtiele afwijkingen, maar minder goed in het combineren van die langere reeksen over tijd en in het opslaan van grote hoeveelheden informatie. Bovendien verschillen mensen in wat ze zien, waar ze op letten en waar ze blind voor zijn. De tweede oorzaak voor de complexiteit van de toezichttaak is dat voortdurend met zo weinig mogelijk mens- en machinekracht een zo groot mogelijk veiligheidseffect bereikt moet worden.

Als gevolg van de complexiteit van de beveiligingstaak en een groeiende nadruk op preventie van incidenten neemt de kans op onterechte alarmen (false alarms) toe. Als gevolg van de complexiteit van de beveiligingstaak en een groeiende nadruk op preventie van incidenten (Minister van Justitie, 2003) kan de kans toenemen op loze alarmen (false alarms) toe. In een onderzoek onder camera operators in Rotterdam werd bijvoorbeeld gevonden dat bijna 80% van de onschuldige omstanders op CCTV beelden onterecht als verdacht werden beoordeeld. De operators werden door de aard van dit onderzoek wellicht extra gestimuleerd om verdachten aan te wijzen. Dit impliceert dat het aantal false alarms ook omhoog gaat. De instructie die operators krijgen is dus direct relevant voor het aantal onterechte verdachten, tenzij de methoden verbeteren om overtreders van onschuldigen te onderscheiden..

- *Definitie van afwijkend gedrag*: Welke gedragingen zijn voorspellend voor criminele of terroristische activiteiten? Zijn er cruciale combinaties van deze gedragingen te onderscheiden? Welke verschillende modus operandi zijn te onderscheiden? Wat kunnen we hiervan leren en hoe kunnen toezichthouders en operators ondersteund worden in de uitvoering van hun taken?

Tegelijk is de constatering dat een goed oordeel pas gegeven kan worden wanneer er meerdere verdachte aanwijzingen zijn. Een enkele verdachte aanwijzing komt relatief veel voor en geeft onvoldoende indicatie van iemand werkelijke kwaadwillige intenties. De optelsom van verdachte aanwijzingen noemen we “0+0=1”. Hierbij staat de 0 voor een opgemerkte afwijking van een normaal patroon dat evenwel niet voldoende is om een verdenking te substantiëren. We veronder-

[1] Met afwijkend gedrag bedoelen we alle gedrag dat voorafgaat en gerelateerd is aan ongewenste handelingen zoals terrorisme, zakkenrollen, dealen, enzovoort.

stellen dat de combinatie meerdere kleine afwijkingen dat wel kunnen. Dan ontstaat een robuuste verdenking: een “1”. Hoe succesvol 0+0=1 toegepast kan worden in de praktijk, hangt af van de volgende vraagstukken:

- *Wanneer wijkt gedrag voldoende af:* Het principe “0+0=1” heeft pas waarde als we weten hoeveel “0”-en een “1” vormen, en of de “1-en” die hieruit volgen ook daadwerkelijk een goede indicatie geven van iemands kwaadwillende intenties. Beide aspecten zijn vooralsnog onbekend. Ook is onbekend wanneer een toezichthouder die “0” moet signaleren: waar dient hij specifiek op te letten en hoe snel dient hij een “0” aan te geven. Wat kunnen toezichthouders bovendien doen om afwijkend gedrag beter zichtbaar te maken?

- *Toezichtssysteem*. Op locaties waar veel mensen aanwezig zijn, is een toezichthouder niet alleen. Het gebeurt vaak dat een toezichthouder een “0” herkent maar vervolgens het individu uit het oog verliest. Wanneer een andere toezichthouder bij hetzelfde individu weer een “0” herkent, zouden de onafhankelijke observaties gekoppeld moeten worden om het toezicht te verbeteren. Momenteel worden vermoedens (0-en) nauwelijks gedeeld door toezichthouders. Om hier een goede registratie van te maken, is technische ondersteuning nodig. Het is voor toezichthouders moeilijk om alles tegelijk te blijven zien en onthouden. Daar kan een geautomatiseerd systeem van enorme meerwaarde zijn.

Hoewel veiligheid op toezichtlocaties erg belangrijk is, is dit meestal niet het hoofddoel van de eigenaren van de toezichtlocaties. Op veel grote toezichtlocaties zoals winkelcentra, grote stations, grote evenementen, musea en vliegvelden is naast veiligheid, service of klantvriendelijkheid net zo belangrijk. Het is belangrijk om een goede balans te vinden tussen deze twee fenomenen. Immers, zodra er teveel aandacht wordt besteed aan veiligheidsmaatregelen, bestaat de kans dat de meeste mensen zich niet prettig voelen op een locatie. Dit heeft nadelige consequenties voor hoe lang ze op een bepaalde locatie blijven, op hun koopgedrag en hoe vaak ze er terug zullen keren. Dat kan de eigenaar van een toezichtlocatie doen besluiten om de veiligheidsmaatregelen te beperken. Aan de andere kant heeft te weinig focus op toezicht negatieve consequenties voor het niveau van veiligheid op toezichtlocaties.

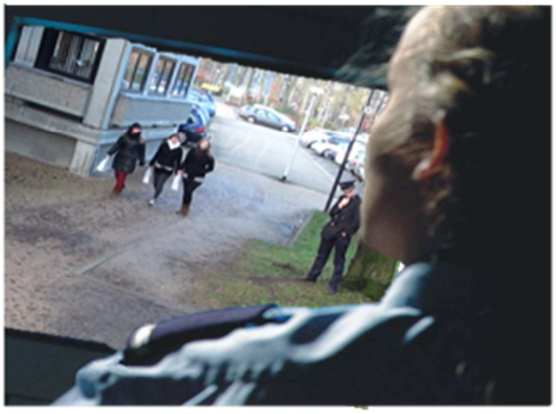
De antwoorden op bovenstaande vraagstukken met betrekking tot de definitie van afwijkend gedrag, “0+0-1” en “Service & Veiligheid” moeten de toezichtstaak zowel effectiever, efficiënter en kansrijker kunnen maken.

3.1.2 Gerealiseerde voortgang

In 2012 lag het zwaartepunt voor topic1 op twee werkpakketten: de definitie van afwijkend gedrag en het WP 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 gebruikt 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. Dit paper

moet een handvat bieden 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 tweede werkpakket 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 dat zowel de hit-kans vergroot moet worden, terwijl tegelijkertijd de kans dat iemand onterecht staande gehouden wordt, verkleint moet worden.
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 potentiele schuld van een individu en hoeveel onterechte aanhoudingen zou dat opleveren. Op de tagging-data die hier is gebruikt 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.



Figuur 5. Studenten en ervaren agenten bekeken beelden van proefpersonen die een legaal of illegaal pakketje vervoerden. Bij het passeren van een toezichthouder werden de proefpersonen matig of juist sterk geprikkeld. Taak van de studenten en ervaren agenten: wijs op de videobeelden aan wie volgens jou de crimineel (die met een illegaal pakket) is.

Om deze kennis verder uit te breiden en toepassing beter mogelijk te maken, is een tweede experiment voorbereid, dat 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 en een artikel voor het vaktijdschrift Security Management. 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 wirwar 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.

3.1.3 Publiciteit

- 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.
- 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*, in boek Veiligheid (Ed. E. Muller).
- B. van Pelt, R. Wijn, *Security Questioning en Prikkelen*, Security Management(2012)
- M. Lousberg, *Profiling and deviant behaviour, a clarification*, Gepresenteerd tijdens de CCR-Summit, Kerkrade 3-5 Oktober 2012.

- G.J. Burghouts, M. Lousberg, *How 0 and 0 make 1. Towards effective proactive CCTV surveillance by combining and optimizing strengths of human factors and technology*, Presented at the CCTV Rail Conference, London 28-29 November 2012.
- H. van den Berg, *Recognizing Hostile Intentions: How Subtle Prickles Can Help to Articulate Deviant Behaviour*, presentation at the 14th International Academy for Investigative Psychology Conference, London, 5-7 December 2012.
- D.A. van Hemert, *The Role of Competences of Security Personnel in Detecting Deviant Behaviour*, presentation at the 14th International Academy for Investigative Psychology Conference, London, 5-7 December 2012.

3.2 Topic 2. Activering van burgers

3.2.1 Doelstelling

Het topic *Activering van burgers* is gericht op kennis en oplossingen voor het verstrekken van betere en gerichte informatie aan burgers en heeft als doel daarbij ook aan te geven op welke wijze burgers kunnen handelen en om veiligheids-organisaties kunnen ondersteunen bij de taakuitvoering. Hierbij worden ook maatregelen bedoeld die de sociale veiligheid, het handelingsperspectief en –bereidheid bevorderen.

Als doelen voor 2012 zijn gesteld:

- Ontwerp van een medium om interactie tussen burgers en veiligheids-professionals te intensiveren over verwachtingen van taken en om verantwoordelijkheden en wederzijds begrip te vergroten. Daarbij hoorde ook het verder uitwerken van de vrijwilligersscan.
- Een experiment gericht op de wijze waarop burgers informatie benutten bij vormen van participatie met hulpverleners. Resultaten moeten kunnen landen in een concept voor een game.
- Het modelleren van het effect van maatregelen op zelfredzaamheid bij ramptypen/ type incidenten en hun onderlinge interactie. In tweede instantie wordt kennis over de wijze waarop mensen reageren op maatregelen en aanwijzingen van hulpdiensten toegevoegd om de effectiviteit van maatregelen te benoemen.
- De ontwikkeling van een concept meetmiddel om effectiviteit van sociale media als bijdrage aan de communicatie te kunnen bepalen. De ontwikkeling van een concept dashboard om een type communicatie te kiezen, gekoppeld aan de wensen en beperkingen van de doelgroep.

3.2.2 Gerealiseerde voortgang

Interactie burgers en hulpverleners

In 2012 zijn de, met de vrijwilligersscan verzamelde, data aangevuld en geanalyseerd. Uiteindelijk kon met de gegevens van 1930 vrijwilligers een motivatie-profiel worden opgesteld voor een zevental organisaties: het Rode Kruis, de Reddingsbrigades, de KNRM, de brandweer, het LOPV, de Natres en het Oranje Kruis. Deze profielen tonen welke kenmerken deze vrijwilligers hebben en bevatten o.a. een overzicht van hun gemiddelde leeftijd, urenbelasting per week, motivatie, communicatie en toekomstverwachtingen.

Op basis hiervan is gestart met de beschrijving van een interactiemedium. Dit medium kan door de betreffende organisaties worden benut bij het gerichter informeren aan potentiële vrijwilligers wat zij kunnen verwachten van het werk en de organisatie. Daarmee kunnen de betreffende organisaties maatregelen nemen om vrijwilligers gerichter te werven, te begeleiden en te boeien.

Figuur 6. Een Wordcloud gebaseerd op reacties van vrijwilligers van het Rode Kruis op de vraag wat ze het meest waarderen.

In 2013 wordt het interactiemedium uitgebouwd en getoetst in een experiment met potentiële gebruikers. Het effect van het instrument wordt bepaald op basis van het aantal mensen dat een vervolgactie (contact, informatievraag, aanmelding) richting betreffende organisaties zet.

Als vervolg op deze activiteit heeft TNO een opdracht gekregen van VBV en NVBR om meer zicht te krijgen op de vrijwilliger van de toekomst.

Informatiecirkel professionals en burgers
Voortbouwend op een beperkt experiment in 2011 naar de reactie van mensen bij een geënsceneerd incident, is in het najaar een groter experiment uitgevoerd naar de wijze waarop burgers omgaan met informatie over een incident. Er is in een gesimuleerde omgeving onderzocht of mensen pas gaan handelen wanneer men overtuigd is dat er een probleem is; in totaal hebben ruim 130 mensen geparticipeerd in het experiment. Communicatie die een handelingsperspectief geeft voordat er informatie over het incident 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 niks gecommuniceerd wordt, maar uiteindelijk zijn ze toch op zoek naar informatie, handelingsperspectief en duiding. De voorbereidingen omvatten het bouwen van het scenario in een game-omgeving en de verschillende type informatie: gericht op handelingsperspectief, voorafgaand informeren en het geven van procesinformatie. Aanvankelijk zou naast het experiment ook bij een praktijkoefening in het najaar met vergelijkbare informatievormen worden geëxperimenteerd. Helaas zijn geschikte oefeningen hiervoor uitgesteld naar voorjaar 2013.

Modelontwikkeling voor maatregelen met betrekking tot zelfredzaamheid in gebouwen
De ontwikkeling van een model voor de van koppeling maatregelen in gebouwen en gebouwde omgeving en zelfredzaamheid is verder doorgezet. De onderlinge beïnvloeding - positief dan wel negatief - van maatregelen bij verschillende incident of ramp typen is nu opgenomen met behulp van input van het bedrijf Efectis. Tevens is een nieuw domein in het onderzoek opgenomen: verkend is of en hoe de beïnvloeding van sociale veiligheid in een schoolomgeving door maatregelen inzichtelijk kan worden gemaakt. Tenslotte is gestart met het indexeren van reacties van mensen/populaties op maatregelen. Belangrijk ontwikkelpunt voor het model is nog de koppeling met menselijke factoren.

Effectiviteit van social media en aanzet dashboard voor community communicatie
Een belangrijke bevinding van de verkenning in 2011 was, dat de inzet en de keuze van media voor communicatie met de omgeving niet altijd gebaseerd zijn op te bereiken doelstellingen. Zo zijn in de praktijk op een aantal plaatsen met social media experimenten gedaan om ‘mee te kunnen doen’ of om ‘niet achter te blijven’. Koppeling tussen beoogd doel, doelgroep en keuze voor een communicatiemiddel is van belang voor de effectiviteit.
De effectiviteit van sociale media toepassingen wordt ook sterk bepaald door de wijze van uitvoering en de manier waarop de verantwoordelijkheid voor gebruik van social media binnen de organisatie wordt verankerd. Voor een OOV organisatie moet het gebruik van social media opgenomen worden in een continu proces, waarbij in de benodigde randvoorwaarden is voorzien. De koppeling met het onderzoek naar de informatiecirkel is dat voorafgaand aan een incident of ramp er al informatie gedeeld en geduid kan worden, zodat er door gedeelde informatie tijdens een ramp beter en sneller kan worden opgetreden.
Om de effectiviteit te kunnen meten zijn SMART doelstellingen nodig. 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 nu een concept voor een ‘communicatie-dashboard’ ontwikkeld. Het dashboard zal uit vier samenhangende elementen bestaan.

1. Organisatie doelstellingen, meetbaar en tijdsgebonden.
2. Keuze van interventies.
3. Organisatorische randvoorwaarden
4. Kenmerken van de (online) doelgroep

3.2.1 Publiciteit

- J. Kerstholt, *Vrijwilligers in Veiligheid*, Presentatie op het landelijk symposium van de Nederlandse Organisaties Vrijwilligerswerk (NOV), 30 oktober 2012.
- H. Stubbé, D. Bloeme, *Communicatie Burgers & Hulpverleners. Ervaar het experiment!* , workshop tijdens congres Brandweer Nederland, 1 november 2012.
- I. Trijssenaer, S. Wijnant, R. Witberg, G. Veldhuis, *Determining the Effectiveness of Safety Measures for Self-rescue in the Built Environment* , 7th Future security Conference, Bonn, 4-6 september 2012

- G. Veldhuis cs., *Activering van burgers*, 2012, TNO publicatie. Download: 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
- J. Haven, *De vrijwilliger centraal*, Brand en Brandweer, 2012 (7/8) p 6-7
- J. Haven, *Visie op Vrijwilligheid: wat zoekt de Brandweer en wat wil de vrijwilliger?*, Brand en Brandweer 2012 (7/8) p 12-13
- A. Brouwer, A. de Vries, C. Caljouw, C. Broekman, D. Bloeme, G. Veldhuis cs., *Hallo…About crisis communication and citizen preparedness*., TNO-brochure, november 2012.
- Van den Broek, J., De vries, A. Huis in 't veld, M., Van Son, R. (2012). Sociale media en Sociale Veiligheid, de rode draad. White paper
- Van den Broek, J., De vries, A. Huis in 't veld, M., Van Son, R. (2012). Sociale media, Burgerparticipatie en sociale veiligheid, het grote plaatje TNO-DV-2012 M201
- Stubbe, H. Van Emmerik, M, Bloeme, D. (in bewerking). Resultaten experiment informatie-uitwisseling burgers en hulpverleners (werktitel.
- Trijssenaar, I ea (in bewerking). Resultaten maatregelenmodel zelfredzaamheid fysieke en sociale veiligheidsaspecten (werktitel).
- J. Kerstholt, Community resilience: concepten en *interventies*, Congres Voorbereid op Zelfredzaamheid, Houten, 14 november 2012

3.3 Topic 3. Slimmer omgaan met veel informatie

3.3.1 Doelstelling

In de veiligheidsketen is het noodzakelijk dat grote hoeveelheden informatie snel verwerkt worden tot bruikbare kennis. De hoeveelheid beschikbare informatie neemt explosief toe. De huidige (veelal niet-geautomatiseerde) wijze van informatieontsluiting vergt een te grote inzet van de menskracht. Het is de vraag in hoeverre meer informatie op dit moment ook meer kans op een geslaagde aanhouding of interventie oplevert. Meer is niet altijd beter en wegen de kosten voor het verzamelen en analyseren van informatie wel op tegen de resultaten? De uitdagingen waarmee de spelers in de veiligheidsketen worden geconfronteerd hebben betrekking op een overvloed aan informatie (informatie-overload), een tekort aan menselijke verwerkingscapaciteit (personele krapte) en de noodzaak om proactief te analyseren en te beslissen (sneller voorin de keten komen). Daarnaast is er aansluiting nodig op de paradigma verschuiving die nieuwe en sociale media als vorm van communicatie met zich meebrengen; communicatie vindt in steeds mindere mate hiërarchisch of lineair plaats, maar juist diffuus door en met het publiek.

Dit topic richt zich op slimmer inzetten van beschikbare informatie en nieuwe (sociale) media voor operationele veiligheidstaken. Specifieker betreft dit de verwerking van grote hoeveelheden informatie, waarnemingen en meldingen uit verschillende bronnen tot direct bruikbare informatie. Het gaat dan om de volgende aandachtsgebieden:

1. Select before you collect (wat heb je nodig?)
2. Slimme ontsluitingsmethoden en kennismanagement (wat heb je al en waar?)
3. Analysemethoden (hoe krijg je de juiste kennis uit de informatie?)
4. Verspreiding/ delen van kennis (hoe krijg je de kennis tijdig op de juiste plaats?)

In overleg met de behoeftestellers is de focus voor 2012 gelegd op de domeinen handhaving en de strafrechtketen (opsporing) en is deze dit jaar uitgebreid met toepassing in crisisbeheersing. De doelstelling daarbij is het ontwikkelen van innovatieve (deel)concepten waardoor beschikbare informatie bruikbaar wordt voor operationele veiligheidsdiensten.

3.3.2 Gerealiseerde voortgang

Informatie-overload in de politiepraktijk
Onderzocht of politiemedewerkers informatie-overload ervaren in hun dagelijkse praktijk. Er is sprake van informatie-overload als aanwezige informatie onbenut blijft voor het nemen van een besluit of het volbrengen van een taak. Of dit het geval is hangt af van:

- Hoeveelheid informatie (de load)
- De beschikbare reactietijd
- De (persoonlijke) verwerkingscapaciteit

Wat tijdens het onderzoek opviel is een discrepantie tussen de zienswijze van leidinggevenden en de ervaring van de werkvloer. Waar leidinggevende aangaven dat ze dachten dat hun personeel wel informatie-overload zou ondervinden met alle informatie die nu beschikbaar is en de werkzaamheden die gevraagd worden, geven werknemers aan geen informatie-overload te ondervinden. Men mist geen informatie om goed te kunnen presteren en ondervindt daarom geen informatie-overload. Bij doorvragen blijkt dat zij filteren door bepaalde informatiebronnen te negeren (bijvoorbeeld social media of andere openbare bronnen) of niet als relevant te achten.
Feitelijk geven de geïnterviewden aan dat ze potentieel relevante informatie moeten negeren door tijdgebrek. Hier is dus wel degelijk perspectief op verbetering.

Figuur 7. Op internet komt per minuut gigantisch veel informatie bij (http://www.go-globe.com/, bezocht 16-08-2012)

De geïnventariseerde problemen en oorzaken zijn velerlei. Oplossingen moeten gezocht worden in de techniek, menselijke capaciteit en procesinrichting:

- TECHNIEK: Aandacht is nodig voor interoperabiliteit van de diverse informatie-bronnen evenals de daarbij behorende juridische en privacy gerelateerde vraagstukken. Dit is een voorwaarde om technische oplossingen mogelijk te maken.
- MENS: Er is bij medewerkers veel kennis gefragmenteerd aanwezig, maar deze is niet toegankelijk. Dit vraagt verbetering van kennis- en informatie-management
- PROCES: Tijdig nemen van 'voldoende geïnformeerde' besluiten vereist het expliciet inrichten van de processen rondom besluitvorming. Om antwoord te geven op 'wat is voldoende' is ontwikkeling van beslissingsondersteunende middelen nodig.

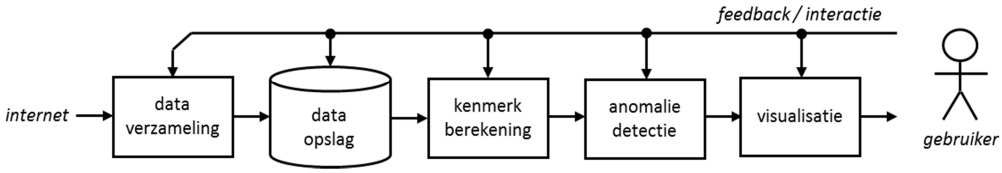
Meerwaarde van open bronnen bij recherche-onderzoek
De meerwaarde van open bronnen intelligence (OSINT) wordt beïnvloed door de kenmerken van zoekmachines en door trainingen van het ontsluiten van open bronnen met dergelijke tools. In een in 2011 uitgevoerd onderzoek van de vts Politie Nederland is een overzicht opgesteld van de tools en technieken zoals die gebruikt worden in 23 korpsen in Nederland, waarbij iBase, BRAINS, DataDetective en Palantir diepgaand zijn geanalyseerd. Met aanvullingen op dit onderzoek uit interviews, literatuur en websites zijn de meest relevante factoren voor vergroting van de meerwaarde van het gebruik van open bronnen geïdentificeerd:

1. Automatisering (workflow; big data analyse)
2. Zoeken in open bronnen (beperkingen van zoekmachines en ontsluiten van deep web; analyse van context, profiel en sociaal netwerk)
3. Standaardisering (werkwijzen en training; dossiervorming)

Automatische Anomaliedetectie
Anomaliedetectie is een techniek die kan helpen om in grote hoeveelheden data de abnormale veranderingen (anomalieën) snel terug te vinden.
Steeds vaker kunnen dreigingen voor personen en infrastructuur in de echte wereld worden gerelateerd aan activiteiten van personen op sociale media, blogs en fora op het internet. Internet surveillance beoogt het vroeg detecteren van deze dreigingen en helpt bij het vinden van verdachten gebaseerd op informatie op het web. De hoeveelheid data op het internet stijgt echter snel en het is tijdrovend om de continue stroom van tweets, posts en updates van webpagina's te volgen.

In dit project is een nieuwe methode ontwikkeld om trends automatisch te monitoren en abnormaal gedrag op Twitter of andere social media te detecteren. We presenteren een systeem voor het vroeg detecteren van dreigingen gebaseerd op een aantal kenmerken, zoals activiteit, sentiment, dreiging en tijdindicatie, toegepast in de context van demonstraties. De lijst van kenmerken die de inhoud van berichten analyseert kan gemakkelijk worden aangepast en uitgebreid om tegemoet te komen aan de behoefte van gebruikers. Het systeem is getest op Twitter data. De resultaten tonen aan dat het systeem succesvol abnormale dreigingen kan waarnemen gebaseerd op de inhoud van berichten.

De ontwikkelde methode bestaat uit de volgende stappen: dataverzameling en -opslag, kenmerkberekening, anomaliedetectie en visualisatie.



Figuur 8. Architectuur van de ontwikkelde methode voor anomaliedetectie

Om de ontwikkeling en validatie op relevante data uit te voeren is een tool gemaakt die zowel de historische als de nieuwe berichten van Twitter verzamelt en opslaat.

Voor het evalueren is gebruik gemaakt van de volgende data, die is verzameld van Twitter:

- Turks-Koerdische data (gewelddadige botsing; Amsterdam, oktober 2011; 9600 tweets).
- 4daagse data (vreedzaam wandel evenement van vier dagen; Nijmegen, juli 2012; 4100 tweets).

De eerste dataset bevat 9600 tweets over een gewelddadige botsing tussen Turken en Koerden in Amsterdam in oktober 2011. In de nacht van donderdag op vrijdag waren de eerste oproepen tot een demonstratie die vrijdagmiddag (21 okt) plaatsvond. Vervolgens was er op zaterdagmiddag nog een oproep tot een protest. De onrust begon zich zondag (23 okt) rond het middaguur te ontwikkelen en vanaf 16.00 werd het zeer dreigend en de incidenten vonden plaats tussen 16.30 en 17.30 uur. Na zondag waren er nog enkele oproepen tot rellen, maar die hebben niet plaatsgevonden. De tweede dataset bevat 4100 tweets over een vreedzaam wandel evenement in Nijmegen in juli 2012. Deze dataset bevat geen dreigingen of rellen.
De dreigende anomalieën die automatisch gedetecteerd worden in de Turkse-Koerdische data komen overeen met de ons bekende beschrijving van de incidenten. We detecteren toekomstige dreigingen op vrijdag vroeg in de morgen die overeen komen met een oproep tot demonstraties. Vervolgens vindt op diezelfde dag een demonstratie plaats, die wordt gedetecteerd als een huidige dreiging. Later was er weer een oproep voor een demonstratie op zaterdag (toekomstige dreiging) en de grote uitbraak van gewelddadigheid vindt plaats op zondagmiddag (huidige dreiging). Op maandag en dinsdag werd nogmaals opgeroepen tot meer rellen (die worden gedetecteerd als toekomstige dreigingen). Voor de vierdaagse data werden geen dreigingen gedetecteerd. De resultaten tonen wel abnormale wijzigingen, maar het gemeten dreigingsniveau is zo laag dat deze worden verwijderd in de nabewerking.

Het koppelen van online identiteiten van dezelfde persoon
Wanneer op het internet onderzoek naar individuen gedaan wordt, dan is het van belang om uitingen op sociale media te kunnen relateren aan het individu waar onderzoek naar gedaan wordt. Op het internet en in sociale media maken mensen vaak gebruik van meerdere online identiteiten: een alias of nickname, een emailadres etc. In veel gevallen vermelden ze niet hun fysieke identiteit: hun eigen naam. Omdat mensen (door middel van hun verschillende online identiteiten) verschillende gedaanten aannemen op het internet, is het lastig om een compleet beeld op te bouwen over een individu. Dit is extra urgent als grote tijdsdruk is om een beeld op te bouwen, bv bij een acute dreiging.

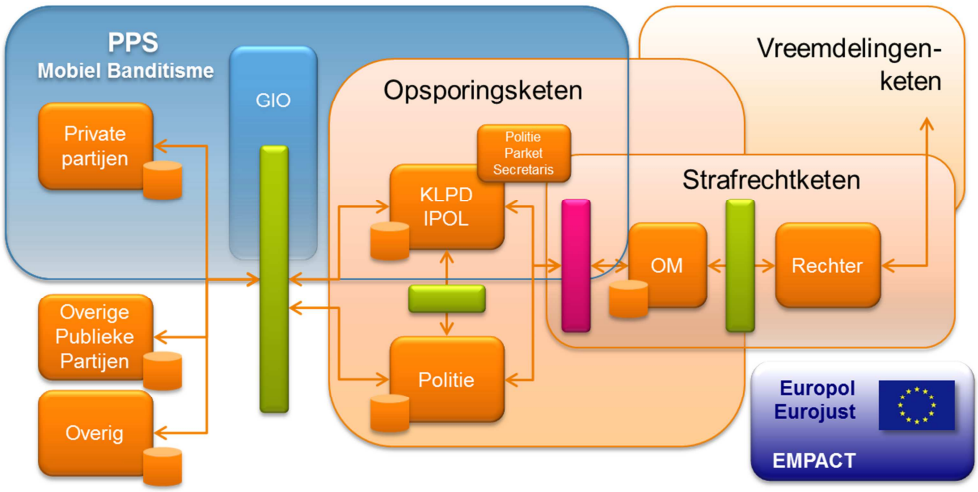
In het onderzoek is uitgegaan van een karakteristieke situatie naar aanleiding van een dreigtweet (NB Juridische randvoorwaarden en privacy worden nadrukkelijk meegenomen):

Figuur 9. Uitgaande van een dreigtweet en bijbehorende online identiteit (@dreigerhenk) is een overzicht gecreëerd de online identiteiten behorende bij hetzelfde individu. De tweet is daadwerkelijk aangetroffen, de online identiteiten zijn gefingeerd.

Aan de hand van deze praktijkvraag zijn de volgende resultaten in een vertrouwelijk TNO-rapport vastgelegd:

1. Een analyse van functionaliteit die nodig is voor het aan elkaar kunnen relateren van online identiteiten
2. Een analyse van informatie in sociale media die bruikbaar kan zijn voor het aan elkaar kunnen relateren van online identiteiten
3. Een experimentele beproeving van de bruikbaarheid van enkele stukken informatie voor het aan elkaar kunnen relateren van online identiteiten

Select B4U collect
Door rondtrekkende bendes wordt een breed scala aan vermogensdelicten gepleegd: winkeldiefstallen, inbraken in woningen en bedrijven, oplichting, skimming, zakkenrollerij, diefstal van metalen, ladingdiefstal, voertuigcriminaliteit en diefstal op bouwplaatsen. Om de grensoverschrijdende georganiseerde bendes effectief en efficiënt te bestrijden is een aanpak zowel op nationaal als op Europees niveau nodig. Deze aanpak gaat uit van een integrale set aan maatregelen voor zowel preventie, tegenhouden, opsporen en vervolgen van mobiel banditisme. Daarbij wordt door VenJ en KLPD zoveel mogelijk aangesloten op initiatieven en mogelijkheden op Europees niveau om mobiele bendes te bestrijden.



Figuur 10. De keten die zich bezighoudt met het bestrijden van mobiel banditisme

In bovenstaande figuur zijn schematisch de verschillende partijen en ketens weergegeven, die samenwerken bij de aanpak van mobiel banditisme. Naast de opsporings-, strafrecht- en vreemdelingenketen zijn dat private partijen die met de publieke partijen samenkomen in de nog op te richten GIO PPS: Gemeenschappelijke Informatie Organisatie Publiek Private Samenwerking. De GIO heeft als doelstelling om de verschillende partijen effectiever te laten opereren door de afzonderlijk geregistreerde en bewerkte gegevens te normaliseren, te sorteren, te filteren, te analyseren en te combineren.

Het project ‘SelectB4UCollect’ heeft zich in 2012 gericht op de procesgang, informatiebehoefte, gegevensverzameling en bewerking, en keuzecriteria (indicatoren) omtrent de aanpak van mobiel banditisme in de in bovenstaande figuur geschetste keten, met de nadruk op de opsporings- en strafrechtketen. ‘Select before you collect’ richt zich in deze context op zo goed mogelijke beslissingen over het inzetten van opsporings- en strafrechtcapaciteit op zaken die (mogelijk) zijn gerelateerd aan mobiel banditisme.
Betrokken zijn vertegenwoordigers van KLPD/IPOL, Ministerie van VenJ, het Openbaar Ministerie, Politie Rotterdam Rijnmond en Europol. De bevindingen en resultaten zijn getoetst in een plenaire bijeenkomst.

Als resultaat van het onderzoek is een kwalitatief Systeem Dynamisch model van mobiel banditisme en de opsporings- en strafrechtketen ontwikkeld. Hiermee zijn de werking van verschillende causale relaties en een aantal mogelijke effecten van maatregelen en interventies gedemonstreerd. Deze methodiek heeft de potentie om de verdere ontwikkeling van een geïntegreerde aanpak mobiel banditisme te ondersteunen.
Als afgeleide van de bevindingen is in nauwe samenwerking met het KLPD/Dienst IPOL een *demonstrator* ontwikkeld: de *MoB Monitor* (Mobiel Banditisme Monitor). De Dienst IPOL heeft als experiment de demonstrator getoetst in lopende landelijke tactische operaties rondom mobiel banditisme. De functionaliteit blijkt een belangrijke aanvulling te zijn op de bestaande analysetools van het KLPD bij de opsporing en monitoring van de verschillende vormen van vermogensdelicten van mobiel banditisme.

In het onderzoek is ook geconstateerd dat de samenwerking in de keten, met name tussen opsporingsketen en strafrechtketen kan worden verbeterd. De actoren in de keten weten onvoldoende van elkaars processen en welke criteria worden gehanteerd bij prioriteitstelling en welke informatie ze dus aan elkaar zouden moeten aanleveren. Afstemming over begripsvormen (voorbeeld: “criminele samenwerkingsverbanden” versus “flexibele netwerken”) was beperkt, maar daar is inmiddels verbetering in aangebracht.

Bij alle ontwikkelingen in dit werkpakket zijn reeds verschillende initiatieven in de keten gaande. In dit werkpakket zijn stappen geïdentificeerd die sneller kunnen worden gezet en tot betere resultaten kunnen leiden.
De volgende stap is geïdentificeerd als meest kansrijke: het op basis van een betere informatiepositie beter (effectiever en efficiënter) samenwerken binnen en tussen beide ketens (i.e. Politie en OM) op dit fenomeen in de eerste zes uur van aanhouding. Dit moet bewerkstelligen dat een betere aansturing gedaan kan worden op de inzet van de schaarse capaciteit in de volgende fasen (drie dagen en drie weken) van aanhouding van personen en/of de identificatie van netwerken die zich bezighouden met mobiel banditisme.
Hiervoor moet nagedacht en geëxperimenteerd worden over de blauwdruk van deze samenwerking tussen Politie en OM op basis van een meer geïntegreerde ondersteunende informatie(verwerking). Het eerste prototype van de *MoB Monitor* vormt hier een bouwsteen in.

Signalering van gedragingen op open bronnen op internet
Verkend is of vanuit kennis over gedrag op open bronnen op internet patronen zijn te herkennen die mogelijk duiden op delicten. Voorbeelden van dit soort gedragingen zijn:

- Criminelen zoeken op open bronnen op internet wie op vakantie is, wie een nieuwe inboedel of een nieuwe auto gekocht heeft en bieden gestolen goederen via marktplaats aan
- Pedofielen zoeken contact met jonge kinderen, vragen om foto’s, telefoonnummers en video’s
- Grote groepen mensen, al dan niet (notoire) geweldplegers gebruiken sociale media om tijd en datum van ontmoeten af te spreken

Vooruitlopend op de rapportage van dit nieuwe project-onderdeel wordt hier al vast één aspect benoemd: onderzocht is de vraag of een afwijkende, potentieel verdachte tweet beter op waarde geschat kan worden door te reageren met een zogenaamde digitale “por”. De benodigde inspanning hiervoor kan geminimaliseerd worden door op uitgefilterde berichten automatisch (subtiele) interactie-alternatieven te selecteren. Wanneer zo’n subtiel signaal vanuit de politie is verstuurd, is het zaak de reactie van de ontvanger en omgeving te observeren. Voor deze benadering is een opzet ontwikkeld (de zgn. Context Creator). Bij dit onderzoek wordt terdege rekening gehouden met juridische kaders en privacy wetgeving.

3.3.3 Publiciteit

- M.C. van Hekken, C.J. den Hollander, J.M.B. Ribbens, *Informatie die werkt! Voorkomen van informatie-overload door betere sturing op het proces*, TNO-DV 2012 C057, maart 2012, POLITIE INTERN

- de Vries, L. de Groen, Informatie aan het werk!, Slimmer omgaan met grote hoeveelheden informatie in de veiligheidsketen, TNO-rapport, december 2012
- L. de Groen, *Informatie-overload in de politiepraktijk*, TNO-rapport, december 2012
- H. Bouma, O. Rajadell, D. Worm, C. Versloot, H. Wedemeijer, *On the early detection of threats in the real world based on open-source information on the internet*, Int. Conf. Information Technologies and Security ITSEC, (2012).
- H. Bouma, S. Raaijmakers, A. Halma, H. Wedemeijer, *Anomaly detection for internet surveillance*, Proc. SPIE, vol. 8408, (2012).
- T. Terpstra, A. de Vries, R. Stronkman, *Towards a realtime Twitter analysis during (flood) crises for operational (flood) crisis management*, Flood risk management conference, November 2012.
- Rapportage aanpak voor herkennen van individuen op het internet, getoetst mbv experiment en prototype, begin 2013.
- Bijdrage aan Bijeenkomst ProjectX (Social media analyse); zie: www.hetccv.nl/agenda/2012/11/bijeenkomst-project-x.html

3.4 Topic 4. Delen en benutten van informatiestromen voor het samen uitvoeren van veiligheidstaken

3.4.1 Doelstelling

De informatievoorziening (keten en multidisciplinair) in het veiligheidsveld staat voor de uitdaging om beschikbare gegevens, informatie, interpretaties en lesson learned beter te benutten over de grenzen van organisaties en onderdelen daarvan.
De belangrijkste sleutels om daartoe te komen zijn samenwerking en het gebruik maken van de collectieve kennis en ervaring. Informatie kunnen verspreiden is niet genoeg. Delen (ook bewaren) en benutten van de informatiestromen zijn cruciale vervolgstappen. Dit vraagt het tot stand brengen van een rolgericht (risico- en vraaggestuurd) informatieaanbod in de veiligheidsketen. (Kosten)effectiever samenwerken in ad hoc samengestelde ketens 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 rol, competenties, verantwoordelijkheden en prioriteiten
- interoperabiliteit (technisch, semantisch en qua uitwisselingsbereidheid)
- gedeeld begrip
- samenwerking en afstemming op diverse niveaus voor wat betreft doelstellingen, planning en uitvoering

Onderzoeksuitdagingen die daarmee gepaard gaan zijn:

1. Hoe bereiken we dat genetwerkte organisatiedelen voldoende vertrouwen hebben in (bereid zijn afhankelijk te zijn van) elkaar en van techniek?
2. 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?

3. 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?
4. Welke rolgerichte gebruikersinterfaces zijn nodig voor het creëren van op elkaar afgestemde situational awareness en coördinatie van taken?
5. Hoe creëren we een toegankelijk collectief geheugen en hoe kunnen we op basis daarvan voorspellend vermogen opbouwen? Het gaat dan zowel om locatiespecifieke historie als om lessons learned van soortgelijke incidenten in het verleden.

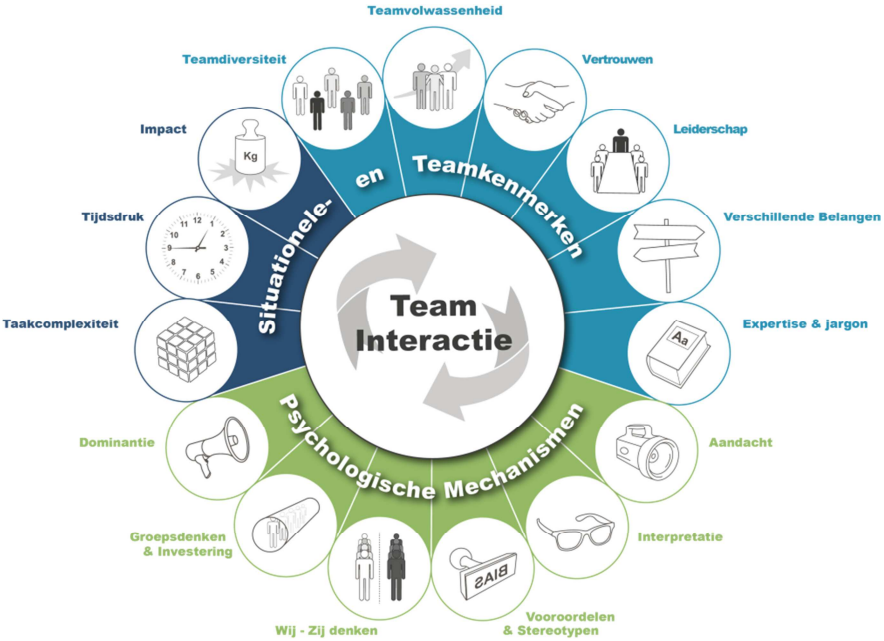
Niet alleen binnen de veiligheidsketen, maar ook de samenwerking tussen publiek en privaat vereist structurele verankering in de informatievoorziening voor de uitvoering van veiligheidstaken. Netcentrisch werken komt binnen het veiligheidsveld op gang. Een volgende stap is publiek private netcentrische 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.

3.4.2 Gerealiseerde voortgang

Ondersteuning van samenwerking tussen veiligheidsorganisaties voor crisisbeheersing en rampenbestrijding
Voor versterking van de ad hoc samenwerking binnen crisisbeheersing en rampenbestrijding is onderzoek gedaan naar het daarvoor benodigde inzicht en interventies. Dit gebeurt op basis van internationaal literatuur onderzoek en eigen onderzoek (MIRROR). Om mogelijke interventies te beoordelen is aansluiting met de praktijk gezocht in een tweetal workshops (Zuid-Holland Zuid, expertmeeting Veiligheidsberaad) en bovendien is aangesloten bij oefeningen. We hebben onderzocht wat knelpunten zijn bij het bepalen van de impact van een incident. Het bepalen van de impact van een incident is onder andere belangrijk om vast te stellen welke spelers je bij een incident moet betrekken. Vervolgens is bepaald wat nodig is om de impact van een incident te bepalen. Deze kennis is toegepast bij het ontwikkelen van de tool impactmatrix en de trainingsmodule IMPACT.

In het kader van het programma Flood Control 2015 zijn de verschillen in rollen en expertises in multidisciplinaire crisisteams onderzocht. Deze verschillen beïnvloeden de informatie die mensen waarnemen en hoe mensen deze informatie interpreteren. Hierdoor kunnen gemakkelijk misverstanden ontstaan. De zgn. MIRROR-methode geeft voor leden van multidisciplinaire crisisteams inzicht in het eigen gedrag, het gedrag van andere teamleden en mogelijkheden om het teamproces te verbeteren. Dit draagt bij aan beter geïnformeerde teamleden en breder gedragen beslissingen. Voortbordurend op het project MIRROR is ook kennis opgedaan over welke sociaal psychologische theorieën en interventies bekend zijn om ervoor te zorgen dat men zich openstelt voor andere partijen. Deze kennis is toegepast in de trainingsmodule IMPACT. Verder is in een door het

Veiligheidsberaad georganiseerde workshop over vitale partnerschappen MIRROR in de praktijk toegepast.



Figuur 11. MIRROR: overzicht van factoren die van invloed zijn op de interactie in een multidisciplinair crisisteam

Binnen de EU wordt op hele verschillende wijzen vorm gegeven aan crisismanagement. Tussen lidstaten en tussen de diverse organisaties zijn grote verschillen. Om hierin een harmonisatie –proces op gang te brengen heeft TNO een sleutelrol gespeeld in het opzetten van een groot demonstratieproject met een consortium van zo'n 40 partners uit de overheid, de industrie en kennisinstituten. Nederlandse partners zijn naast TNO: HKV, Ecorys, gemeente Den Haag en Esemble; ondersteuning is schriftelijk toegezegd door de directeur Weerbaarheid van DG NCTV van VenJ, de staf van de Nationale Politie, de directeur van de Veiligheidsregio Haaglanden. Het doel van dit initiatief is het vergroten van het innovatieve vermogen van crisis management organisaties. Diverse onderzoeken, zowel op Europees als nationaal niveau, belichten vaak slechts enkele aspecten (bv. Informatie uitwisseling, training van brandweer, interoperabiliteit), maar zelden of nooit op het hele systeem van crisis management. Belangrijk om te onderkennen is dat we 'systeem' hier nadrukkelijk niet interpreteren als een technisch systeem. Uiteraard is technologie een belangrijke component, maar het zijn toch vooral de mensen die zorgen voor de kwaliteit van het crisis management evenals de wijze waarop dit georganiseerd is. Hierbij gaan we er ook van uit dat niet alleen de professionals op de diverse niveaus en bij de vele verschillende organisaties een belangrijke rol spelen, maar dat ook de diverse burgers en groepen in de samenleving (de communities) een onmisbare schakel zijn. In maart wordt bekend of dit consortium vanuit Brussel financieel ondersteund zal worden.

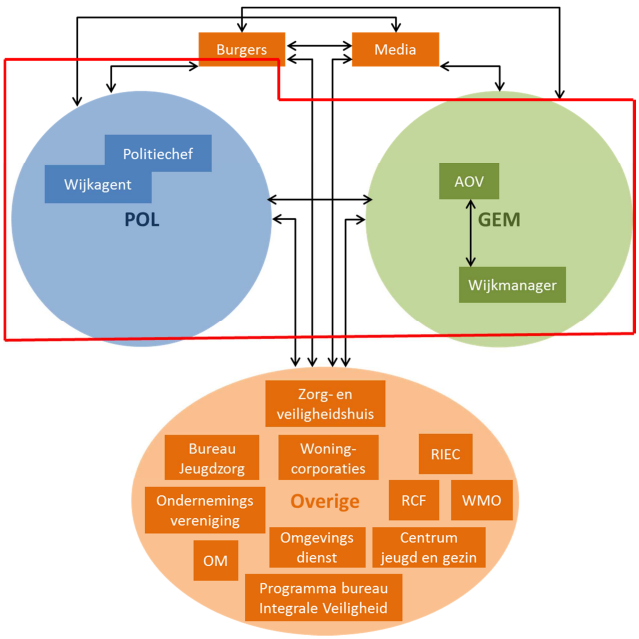
Collectief leren voor multidisciplinaire teams

Om de leercyclus te kunnen sluiten is het belangrijk dat er niet alleen geëvalueerd wordt, maar dat ook oplossingen geïmplementeerd en beschouwd worden; niet om 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. Om het veld handvaten te geven om het multidisciplinaire leren succesvol te kunnen oppakken is gewerkt aan een systematiek waarmee dit kan. Als voorbeeld kan genoemd worden de After-Action-Review(AAR)-methode, waarbij objectieve feedback en zelfcorrigerende teams centraal staan; hierbij is het feitelijk meten van wat er gebeurd is essentieel om sneller en effectiever te kunnen leren. Verder is het van belang te beseffen dat mensen tegenwoordig meestal niet meer 10 jaar of langer in dezelfde functie blijven en op die manier expert worden. Kennis moet sneller worden opgedaan en breder gedeeld en inzetbaar zijn. Sneller leren is mogelijk door tijdens het werk gerichte cognitieve oefeningen te doen zodat je bijvoorbeeld leert schatten en extrapoleren. Hiervoor zijn algemene ondersteunende psychologische vaardigheden nodig zoals tegen jezelf praten, mentale simulatie, concrete doelen stellen, jezelf kunnen ontspannen en goed kunnen plannen. Deze vaardigheden zijn te leren en kunnen in iedere situatie worden toegepast.

Synergie tussen fysieke en sociale veiligheid

Er is een verkenning gedaan naar sociale veiligheid, inclusief de uitdagingen die in het veld spelen. Vervolgens is er gekeken naar de samenhang tussen de werkvelden fysieke en sociale veiligheid. Als focus is gekozen voor de samenwerking tussen de traditionele partijen binnen het werkveld. Voor sociale veiligheid is dit de samenwerking tussen gemeente en politie (zie onderstaande figuur); voor fysieke veiligheid gaat het om de samenwerking tussen de primaire hulpdiensten en de gemeente.



Figuur 12 Operationeel speelveld van samenwerkingspartners van gemeente en politie binnen sociale veiligheid

Het onderscheid tussen sociale en fysieke veiligheid is voor een deel subjectief:

	Frequentie	Beleving
Sociale veiligheid	Komt regelmatig voor	Voelt als dichtbij
Fysieke veiligheid	Komt zelden voor	Voelt als ver weg

Na het aankaarten van de samenhang van beide werkvelden, is in dit onderzoek een eerste stap gemaakt in het identificeren van mogelijkheden waarin de fysieke veiligheid het sociale veiligheid werkveld kan versterken. Hiervoor is bekeken of ontwikkelingen binnen het werkveld van fysieke veiligheid ook mogelijke oplossingen kunnen zijn voor knelpunten in het werkveld van sociale veiligheid.

Meerlaagsveiligheid
In de brief aan de Tweede Kamer van staatssecretaris Atsma van november 2012 over de stand van zaken waterveiligheidsbeleid wordt gesteld dat de meerlaags-veiligheidsbenadering voor het kabinet de centrale benadering vormt conform het Nationaal Waterplan en dat een aantal gebiedspilots meerlaagsveiligheid (MLV) ondersteunt op dijkringniveau. In dit werkpakket is 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 gaat de nadruk uit naar de samenwerking tussen de lagen, en de 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 zullen begin 2013 worden vastgelegd in een notitie die daarmee inzichtelijk maakt voor bestuurders hoe ‘het veld’ het mlv-benadering beleefd en implementeert. Denk hierbij bijvoorbeeld aan een groeimodel dat richting geeft aan de ontwikkeling van samenwerken en informatie-delen in het kader van meerlaagsveiligheid.

Figuur 13. In Nederland groeit het draagvlak voor het beheersen van overstromingsrisico’s door maatregelen op drie niveaus: de fysieke bescherming door waterkeringen en dijken, de risicominimalisatie door planologisch beleid, de resilience van de leefomgeving door versterking van crisismanagement en zelfredzaamheid.

3.4.3 Publiciteit

- W. Treurniet, K. van Buul-Besseling, J.J. Wolbers, *Collaboration awareness: a necessity in response coordination*, In: Proceedings of the 9th International Conference on Information Systems for Crisis Response and Management ISCRAM, Vancouver April 2012, L. Rothkrantz, J. Ristvej and Z. Franco (eds.)
- W. Treurniet, *Multidisciplinaire hulpverlening: denken in netwerken*, Incident, 2012-2
- *Van evalueren naar leren, een hele stap*, Magazine Nationale Veiligheid en crisisbeheersing, augustus 2012
- Chr. Dekkers, L. de Koning, O. Nolet, *Liaison Vitaal en project Mirror*, Magazine Nationale Veiligheid en crisisbeheersing, augustus 2012
- L. de Koning, *Multidisciplinair samenwerken voor veiligheid? Kijk eens in MIRROR!*, Brochure TNO in kader van het programma Flood Control 2015, http://www.tno.nl/content.cfm?context=thema&content=prop_publicatie&laag1=893&laag2=910&laag3=94&item_id=900
- J. van de Ven, *Beter benutten informatiestromen en samenwerking*, documentatie topic 4 op website TNO: http://www.tno.nl/content.cfm?context=thema&content=prop_case&laag1=893&laag2=910&laag3=94&item_id=1742&Taal=1
- Stagerapport: Het openstellen van reeds samenwerkende partijen voor onbekende partijen binnen het crisisdomein (TNO 2012 S10502)
- Whitepaper “Van evalueren naar leren, een hele stap” nav symposium
- N. Vink, K.van Buul, J. van de Ven, *De samenhang tussen de werkvelden fysieke en sociale veiligheid*, TNO-Rapport 2012-R11169, januari 2013
- DRIVER: DRiving InnoVation in crisis management for European Resilience, EU- proposal AOR 607798, FP7-SEC-2013-1 (Voorstel voor EU-project met een budget van 40 M€, Consortiumpartners: eindgebruikers (o.a. International Federation of Red Cross, Bundesanstalt Technishes Hilfswerk (THW), de stad Den Haag en Swedish Civil Contingencies Agency - MSB), onderzoeksinstituten (o.a. TNO, FOI, Fraunhofer, JRC-EC, PRIO), en industrieën (o.a. Atos, Thales, Frequentis, ITTI).
- K. Boersma c.s., *Netcentrisch Werken in ontwikkeling, Een cultuuronderzoek naar multidisciplinaire samenwerking en gezamenlijke operationele beelden in de* Veiligheidsregio’s, gezamenlijk rapport VU Amsterdam en TNO, november 2012
- Werkgroep Netcentrische Werkwijze in samenwerking met TNO, *Referentiekader Netcentrische crisisbeheersing*, Staat van Netcentrisch Werken, www.infopunt.nl, augustus 2012

3.5 Topic 5. Cybersecurity

3.5.1 Doelstelling

Dit onderzoek richt zich op de bescherming van de Nederlandse cyberinfrastructuur tegen grootschalige verstoringen en misbruik.
Effectieve bescherming tegen een ongewenste verstoring bestaat in het algemeen uit een evenwichtige verzameling maatregelen op het gebied van pro-actie, preventie, preparatie, detectie en respons. Voor ICT geldt dat zowel de overheid als het bedrijfsleven ieder voor zich maatregelen op dit gebied nemen. De snelle veranderingen in technologie, de toenemende verwevenheid van op ICT gebaseerde infrastructuren, de snelle introductie van nieuwe gebruiksmogelijkheden en de incoherentie van beschermingsmaatregelen over

(ketens van) organisaties heen zorgen echter voor nieuwe dreigingen en kwetsbaarheden. Een goede beheersing vereist steeds opnieuw risicoafwegingen en innovatieve maatregelen.

Een belangrijke pijler binnen het onderwerp cyber security wordt gevormd door detectie van ICT-misbruik en bijbehorende mogelijkheden voor opsporing en vervolging. Bij bovengenoemde actoren is behoefte aan methoden voor het analyseren van grote hoeveelheden log- en incident¬gegevens en aan ondersteunende analyse- en simulatiemodellen om ICT-misbruik vroegtijdig te herkennen. Hierbij richt de vraag naar nader onderzoek zich niet op de afzonderlijke (vaak commercieel verkrijgbare) detectiesystemen, maar op het opbouwen van een gezamenlijk gedeeld beeld van ICT-misbruik uit een diversiteit aan informatiebronnen, zowel in aantal als type systemen. Speciale aandacht in het gevraagde onderzoek moet worden besteed aan de toenemende functionaliteit en nieuwe ICT, bijv. het toenemend gebruik van mobiele ICT, de hierbij komende risicofactoren en de noodzaak om hier in de opsporing tijdig op in te kunnen spelen.

Een speciaal aandachtsgebied wordt gevormd door cyber security voor de vitale infrastructuur. De vitale infrastructuur bestaat uit sectoren en voorzieningen waarvan verstoringen of uitval ernstige impact kunnen hebben op de Nederlandse samenleving (en daarbuiten), 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 onderwerp van aandacht en onderzoek. Internationaal vindt samenwerking en gegevensuitwisseling plaats over dreigingen, kwetsbaarheden, tegenmaatregelen en onderliggende modellen.
Binnen dit deelgebied vindt op de onderliggende modelvorming van cyber security intensieve internationale samenwerking plaats. Om ook nationaal optimaal aan te kunnen sluiten bij de vraagstelling van de vitale sectoren wordt samengewerkt met de ISACs. Met hen worden sectoroverstijgende onderzoeksvragen geïdentificeerd. Onderzochte en bewezen oplossingsrichtingen worden zo direct mogelijk aan de vitale sectoren teruggekoppeld.

De doelstelling voor de periode 2011 – 2014 bestond uit:

1. 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.
2. 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 securit- by-design te introduceren. Hiervoor wordt als case studie de smart grid ontwikkelingen in de energiesector gebruikt (NB In 2012 is nog maar een beperkte inspanning geleverd ivm de budgetkorting; vervolg in VP Security).
3. Ontwikkeling van 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.

4. Het ontwikkelen van een shared innovatieomgeving in de vorm van een fieldlab waarin de verschillende onderzoekspartijen en overige stakeholders kunnen samenwerken (In 2012 is dit niet meer in dit VP bewerkt ivm de budgetkorting; vervolg in VP Security).

Ondersteunend aan elk van deze onderzoeksdoelstellingen:

5. Het ontwikkelen van een modellenbasis als ondersteuning bij het herkennen van mogelijke cyber-aanvalspatronen en het bepalen van het effect van maatregelen en de mogelijke impact van cyber-gerelateerde verstoringen.

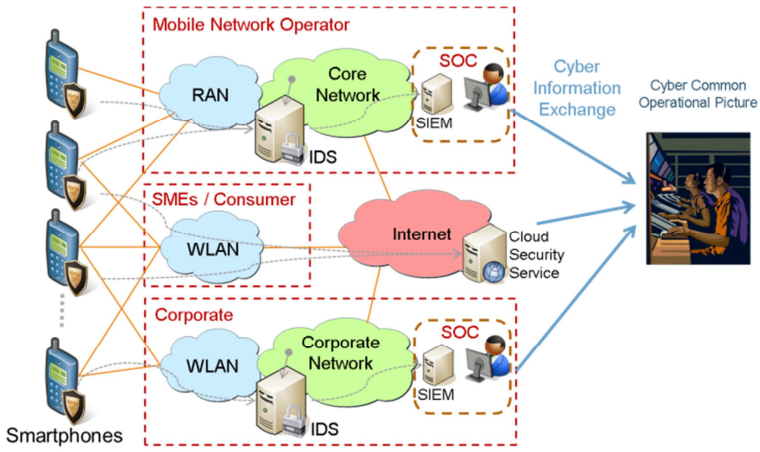
3.5.2 Gerealiseerde voortgang

Per onderzoekslijn zullen de geplande en uitgevoerde werkzaamheden worden beschreven.

1. Hoe kan misbruik van huidige en toekomstige mobiele platformen tijdig gedetecteerd worden op een wijze die effectieve opsporing en vervolging mogelijk maakt?

In de werkzaamheden voor 2012 stond detectie van grootschalig misbruik centraal met de focus op mobiele infrastructuur. Hiertoe is behoefte aan een mobiel sensornetwerk met de mogelijkheid om gecentraliseerd grote hoeveelheden sensorinformatie (loggegevens, incidentgegevens, etc) te kunnen analyseren. Deze architectuur dient dusdanig generiek te zijn dat het kan worden toegepast op verschillende infrastructuren waarbij een grote diversiteit van informatie kan worden verwerkt zodanig dat verschillende vormen van misbruik kunnen worden gedetecteerd.

Om een beeld te krijgen van de huidige mogelijkheden van detectie in een mobiele omgeving is begin 2012 een state of the art onderzoek uitgevoerd, In dit literatuuronderzoek is zowel gekeken naar detectiesystemen op de mobiele apparatuur zelf (vaak matig tot slecht van kwaliteit) en systemen gericht op de operator. Daarnaast is een globaal ontwerp gemaakt van een gedistribueerde sensorarchitectuur waarin gegevens uit verschillende systemen gecombineerd kunnen worden in een centraal beeld. Dit globale ontwerp is vervolgens getoetst bij enkele stakeholders (een mobiele operator en het NCSC).



Figuur 14. Globaal ontwerp van een gedistribueerde sensorarchitectuur voor detectie van misbruik in netwerken van mobiele platformen

Het globale ontwerp bleek voor deze stakeholders nog een stap te ver. De uitwisseling van informatie vindt momenteel vooral plaats via face-to-face contacten en overlegstructuren (ISAC's, OITO). Het delen van gedetailleerde detectieinformatie lijkt nog een brug te ver en zal meer gefaseerd dienen te worden opgezet. In november en december zijn in een gezamenlijke workshop met het NCSC de mogelijkheden voor een meer gefaseerde opzet onderzocht.

2. Hoe kan Security by design worden ingebed in op ICT gebaseerde vitale infrastructuur?
In 2011 en de eerste helft van 2012 lag de nadruk op de ontwikkelingen rond smart grid security. Hierbij zijn deze ontwikkelingen in kaart gebracht en is een overzicht opgesteld van de belangrijkste factoren die zorgen voor de security van de vitale op ICT-gebaseerde infrastructuur. Het betreft hier niet alleen technische factoren, maar ook organisatorische maatregelen zowel over organisaties heen als binnen een enkele organisatie, en aanpassingen in de gebruiksmogelijkheden. Er is onderzocht op welke wijze de stakeholders, elk met de eigen belangen en insteek, in een vroegtijdig stadium kunnen worden betrokken bij de risicobeoordeling en op welke wijze de basisprincipes van *security by design* het best voor het voetlicht kunnen worden gebracht.
Hiervoor is gewerkt aan een risicobenadering waarin de risicofactoren voor de gehele keten in beeld kunnen worden gebracht. Het gaat hierbij bijvoorbeeld om risicofactoren die de betrouwbaarheid van de elektriciteitsvoorziening kunnen beïnvloeden, om manipulatie van financiële of gebruiksgegevens, en om de waarborging van de privacy over de keten heen (persoonsgegevens, verbruiksgegevens).

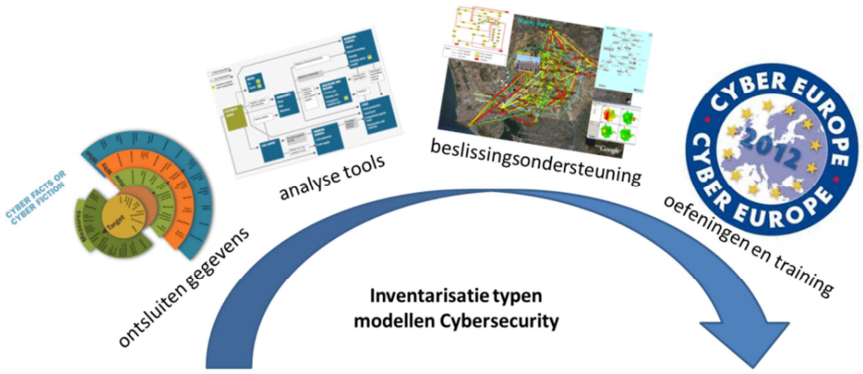
Deze ketenbenadering waarin rekening wordt gehouden met de belangen en gezichtspunten van de verschillende typen stakeholders is in 2012 ingebracht in verschillende Europese werkgroepen. Zo is bijgedragen aan een EU-taakgroep rond smart grid security. Een deel van de resultaten van het VP onderzoek is in dit kader getoetst. Daarnaast wordt deelgenomen aan een task group onder het EU project ERNCIP. Hierin wordt in een Europese werkgroep onderzocht welke rol standaarden en certificering zouden kunnen spelen binnen het onderwerp security voor IACS en Smart Grids.

3. Hoe kan de cyber security status van de Nederlandse vitale infrastructuur op uniforme wijze inzichtelijk worden gemaakt?
Binnen de zogeheten ISACs vindt nauwe samenwerking binnen de vitale sectoren op het terrein van ICT-veiligheid en –beveiliging. Zowel nationaal als internationaal vindt samenwerking en gegevensuitwisseling plaats over dreigingen, kwetsbaarheden, tegenmaatregelen en onderliggende modellen. In deze onderzoekslijn wordt in nauwe afstemming met de ISACs 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.
In 2011 is bij de ISACs onderzocht welke onderwerpen het meest aanspreken bij de deelnemers. Hierin sluiten vooral de onderwerpen gerichte aanvallen, sectoroverstijgende afhankelijkheden, trends in aanvalsvectoren en security by design aan.

De onderwerpen binnen dit VP sluiten aan bij deze onderwerpen: WP1 onderzoekt risico's voor mobiele systemen (hiervoor is samengewerkt met de telecomsector), WP2 naar security by design (in samenwerking met de elektriciteitssector). Voor sectoroverstijgende afhankelijkheden is een start gemaakt met een scan naar nationale en internationale methoden die worden gebruikt om deze afhankelijkheden in kaart te brengen en vast te leggen. Hiervoor is gekeken naar methoden en technieken uit verschillende nationale studies en samenwerkingsverbanden (bijvoorbeeld anonimisering, aggregatie, het traffic light protocol, Chatham House Rule, statistische analyses).

4. Hoe kunnen modellen en testomgevingen worden geïntegreerd in een shared innovatieomgeving om kennis en tools gezamenlijk te ontwikkelen en over te dragen?
Dit onderwerp was gepland in dit VP, maar is overgedragen aan het VP security binnen de Topsector HTSM.

5. Welke ondersteuning kunnen modellen leveren bij het beantwoorden van bovenstaande onderzoeksvragen 1-3? (modellenbasis)



Figuur 15. Er is een grote rijkdom aan modellen op cybersecurity-gebied. Onderzoek-uitdagingen zijn de match op het gebruiksdoel te verbeteren, validatie en harmonisatie

In deze onderzoekslijn wordt gewerkt aan een verzameling modellen die bovenstaande onderzoekslijnen 1 en 3 ondersteunen. Het gaat om modellen die de effecten van verstoringen in de cyberinfrastructuur kunnen analyseren en daarmee what-if analyses mogelijk maken. Als ondersteuning van onderzoekslijn 1 gaat het om meer gedetailleerde modellen die de effecten van ICT-uitval of -verstoring binnen een vitale infrastructuur kunnen bepalen. Hiermee kunnen patronen van misbruik worden geanalyseerd. De effecten van incidenten kunnen worden bepaald, en tevens kan de effectiviteit van eventuele beschermende maatregelen worden bepaald.
Binnen onderzoekslijn 3 gaat het om modellen die de impact van grootschalige verstoringen binnen de vitale infrastructuur bepalen en de mogelijke keteneffecten in kaart brengen.
Na de inventarisatie van de op de keteneffecten gerichte modellen in 2011 is het onderzoek in 2012 onderzoek gericht op gedetailleerde modellen voor het analyseren van het ontwerp van netwerken en op modellen voor de ondersteuning van training en opleiding. Tevens is de samenwerking met internationale partners op dit punt versterkt. Binnen EU verband is het voorstel voor een EU project op dit

onderwerp gegund (CIPRNET). Daarnaast wordt ook deelgenomen aan een werkgroep in NAVO verband voor cyber defence modellen.

3.5.3 Publiciteit

- Van Eeten, M., Nieuwenhuijs, A., Luiijf, E., Klaver, M., Cruz, E., *The State and the Threat of Cascading Failure across Critical Infrastructures: The Implications of Empirical Evidence from Media Incident Reports*, Public Administration, Vol. 89, No. 2, 2011, (381-400).
- Luiijf, *ICT and Energy networks*, Energy symposium, Amsterdam, November 2011.
- CRITIS 2011, conference presentatie "Ten National Cyber Security Strategies: a Comparison"
- H.A.M. Luiijf (ed) and E. Egozcue, Bijdrage aan Expert Group on the security and resilience of Communication networks and Information systems for Smart Grids, WP 2 – Threat Analysis, March 2012, 26 pages. (http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/expert_group_smart_grid/index_en.htm)
- H.A.M Luiijf, Besseling, K., De Graaf, P., *Nineteen National Cyber Security Strategies*, International Journal on Critical Infrastructures (IJCIS), V9 N1/2 2013, reviewed - pending publication 2012.
- H.A.M. Luiijf, *Understanding Cyber Threats and Vulnerabilities.*In: J. Lopez, R. Setola, S.D.Wolthusen (eds), Critical Information Infrastructure Security, Lecture Notes in Computer Science (LNCS) 7130, Springer, 2012. pp. 52-67.
- H.A.M. Luiijf, *Help! Onze gebouwinstallaties zijn gehackt!*, Facto Magazine, nummer 7/8, juli/aug 2012, pp 44-47.
- H.A.M. Luiijf, *Onbewust Onveilig*, Informatiebeveiliging, nr. 4, 2012, pp 4 - 7.
- H.A.M. Luiijf, *Procesbesturingen: Onbewust Onveilig*, Beveiliging, (25)03, 2012, pp 16 - 18.
- M. Klaver, *Cyber resilience in de bestuurskamer*, Beveiliging, nov 2012
- M. Klaver en A. Zielstra, *Cyber resilience in the Boardroom*, Meridian newsletter, nov 2012
- M. Klaver, *Cyber Resilience in de Bestuurskamer : The Grand Conference in Amsterdam*, Informatiebeveiliging, jan 2013.
- T. Hartog, F. Fransen, E.G. Broenink, *Detectie van grootschalige incidenten en verstoringen in de mobiele cyberinfrastructuur*, 2013 R10013, jan 2013
- K. van Buul – Besseling, C. van der Vliet – Hameeteman, M. Klaver, *Modellen en Simulaties voor (ICT) Afhankelijkheden tussen de Vitale Infrastructuren*, dec 2012.