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

TNO-rapport

TNO 2014 R10424

Vraaggestuurd programma 2011-2014
Voortgangsrapportage 2013
Thema XI Maatschappelijke Veiligheid

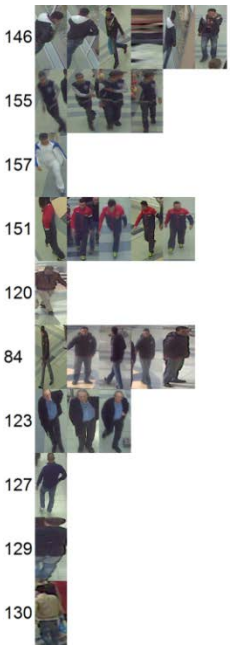
Datum	maart 2014
Auteur(s)	Dr. ir. J.A. Don
Aantal pagina's	47
Regievoerend departement	Ministerie van Veiligheid en Justitie
Projectnaam	Vraaggestuurd Programma Veilige Maatschappij
Projectnummer	053.01011/01.02
Geauthoriseerd door	Drs. H.G. Geveke
Handtekening	

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 presenteert de voortgang in 2013.

In 2013 zijn op de vijf topics van het VP Veilige Maatschappij als belangrijkste resultaten bereikt:

Topic 1 Herkennen afwijkend gedrag
In 2013 is het gelukt een basis-ontwerp te maken voor een tool voor het combineren van observaties van verschillende toezichthouders op een complexe locatie. Met deze tool kunnen toezichthouders op een beeldscherm mogelijke verdachten ‘taggen’. Op het moment dat meerdere toezichthouders dezelfde persoon getagd hebben kan vanuit de toezichtscentrale opvolging op de vloer in gang worden gezet. Het gebruik van deze tool draagt bij aan het vergroten van de hit-kans bij het aanhouden van mensen met kwade intenties en het verminderen van de kans op onterechte staande houdingen.



Figuur 1 Door de her-herkenningstool gegenereerde beelden van individuen op basis van meerdere ‘tags’ door professionele beveiligers bij een experiment met zakkenrollers in het winkelcentrum Kanaleneiland in Utrecht. Deze tool kan verder uitgebouwd worden met opties om het afgelegde traject van getagde personen te volgen.

In 2013 zijn ook stappen gezet in de ontwikkeling van een taal om afwijkend gedrag te beschrijven. Deze ontwikkeling is van belang voor het kunnen annoteren van het beeldmateriaal van incidenten en het ter beschikking komen van intelligente software voor analyse van grote stromen videobeelden. Met gebruikmaking van de in 2012 aangelegde beeldbank met enkele honderden videofragmenten van partners zoals de NS, KMAR en de politie Antwerpen bleek het mogelijk voor het delict zakkenrollen een modi operandi map (MOMAP) op te stellen. Met deze

kennis is het ook mogelijk sneller en effectiever patronen van afwijkend gedrag op locaties te identificeren en delen.
Nader onderzoek heeft onderbouwd dat prikkelen kan helpen in het zichtbaar van kwade intenties.

Topic 2 Activering van burgers
Aan de informatie-uitwisseling tussen professionals en burgers bij crisis en rampen is in de TNO-publicatie *Hallo! Over crisiscommunicatie en zelfredzaamheid van burger*s. Daarbij is ingegaan op het gericht aandacht geven aan handelingsperspectief, voorafgaand informeren en het geven van procesinformatie. Deze aanpak voor crisiscommunicatie blijkt in gesprekken met veiligheidsregio's goed bruikbaar te zijn in de praktijk.
De hele crisiscommunicatie in de Veiligheidsregio is recent organisatorisch opnieuw opgezet. De taakprofielen van de commissie Grooter bieden daarbij voldoende inzicht in wat er van de verschillende crisiscommunicatieadviseurs mag worden verwacht. TNO heeft in het verlengde hiervan geholpen aanknopingspunten voor ontwikkeling en training te definiëren. Met behulp van de resultaten van de experimenten in dit topic zijn de taakprofielen "vertaald" naar competentieprofielen en daarmee wil men nu een trainingsmiddel ontwikkelen om de vaardigheden van de crisiscommunicatie-adviseurs te kunnen versterken.
Voor de ontwikkeling van de vaardigheden rond crisiscommunicatie is ook een papieren nul-versie voor een game ontwikkeld binnen het Flood Control programma. De wetenschappelijke basis, de inhoud van de communicatie en het interactie design in de game is mede gebaseerd op de bevindingen vanuit dit topic. De nul-versie zal in 2014 verder ontwikkeld worden naar een web-based game dat daardoor vlot gespeeld kan worden met beperkte begeleiding; aan deze doorontwikkeling in samenwerking met het IFV is financiële ondersteuning uit het HSD stimuleringsfonds toegezegd. De presentatie van onze visie op ontwikkelingen bij een congres in Riga heeft ertoe geleid dat TNO (Hester Stubbe) is gevraagd toe te treden tot het EENA netwerk (European Emergency Number Association).
Dit biedt toegang tot internationale expertise en kan ook helpen om de voorbereiding op samenwerking bij grensoverschrijdende calamiteiten verder uit te bouwen.

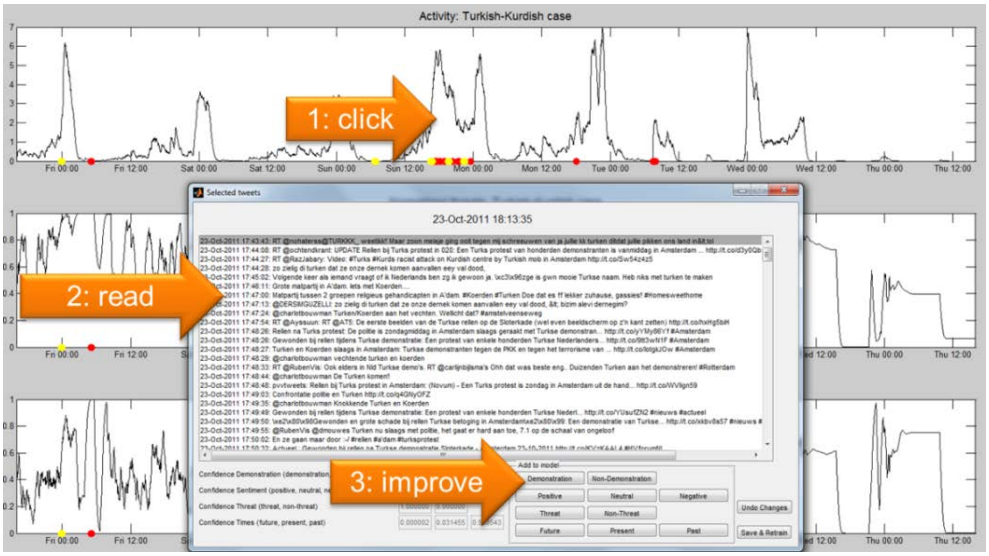
De activiteiten hebben ook de interesse gewekt van adviesbureaus, die voor de veiligheidsregio's werken. Zo heeft de V&R academie (http://www.vracademie.nl/pages/vr-academie/home.php) TNO gevraagd te helpen bij het (her-)formuleren competentieprofielen in een vervolgproject.

Topic 3 Slimmer omgaan met grote hoeveelheden informatie
De ontwikkelingen in dit topic richten zich op innovatieve tooling, methoden of procesverbeteringen om slimmer grote hoeveelheden data en informatie te verwerken. De deelprojecten (WP's) richten zich -in samenwerking met één of meerdere stakeholders- op verschillende lagen of overgangen van data naar informatie, van informatie naar kennis en van kennis naar intelligence; ook de human factor krijgt aandacht.

Een voorbeeld van de in 2013 bereikte resultaten betreft de analyse van de inhoud van berichten voor vroegsignalering van dreigingen in open bronnen op het internet. Het daarvoor ontwikkelde framework van een systeem is gedemonstreerd en in nauwe interactie met het veiligheidsveld is er een kader

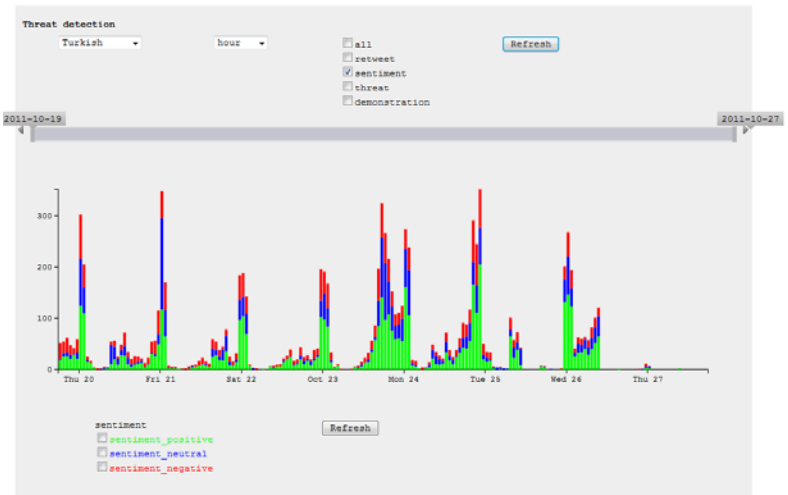
gecreëerd voor de gebruiks-eisen en -mogelijkheden voor een grafische user interface.

Uit analyses van data-verzamelingen met zo'n 100.000 berichten van diverse cases, waaronder ProjectXHaren in 2012 en de Kroningsdag in 2013, bleek een nauwkeurigheid (i.e. percentage correct gelabelde tweets) van 90% haalbaar. Dan moet het echter wel gaan om data-verzamelingen die qua context vergelijkbaar zijn met eerder met het model geanalyseerde verzamelingen. Door interactie met de database kan het model nog worden geoptimaliseerd:



Figuur 2 De verzameling berichten in een geselecteerd tijdsinterval kan handmatig beoordeeld worden, waardoor het model leert wat wel of niet relevant is.

Voor het analyseren van data en informatie uit vele bronnen zal naast automatische informatie-analyse de mens altijd nog een belangrijke rol spelen. Voor een snelle en effectieve interpretatie van gegevens is slimme datavisualisatie vereist. Eén van de uitgewerkte interfaces betreft het vroegtijdig signaleren van de behoefte aan extra aandacht voor veiligheid bij evenementen (zie onderstaande figuur).



Figuur 3 Screenshot van interactieve visualisatie van data-analyses voor vroegdetectie.

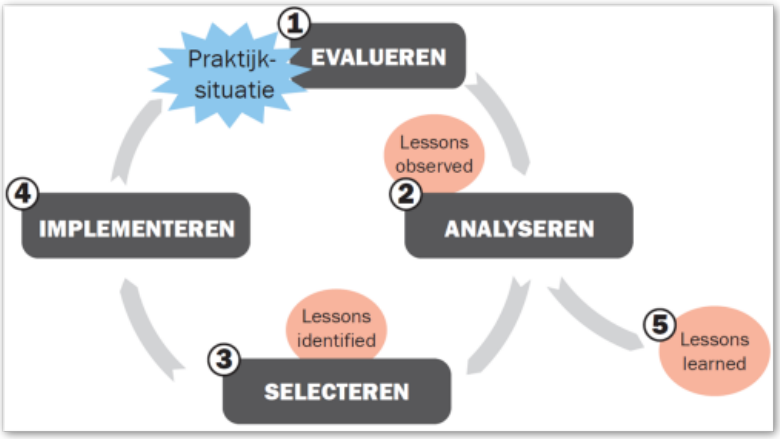
Daarnaast is er gewerkt aan:

- Het aanpassen van standaard zoekmachines voor het doorzoeken van het internet met een aantal algoritmes en filters die de basis vormen voor het combineren van zoekvragen (TNO prototype ‘Needle Custom Search’).
- Het slimmer samenwerken voor het fenomeen Mobiel Banditisme; daarbij is verder ingezoomd op het:
  - Versnellen van het genereren van inzicht in de mobiele netwerken.
  - Versnellen van de beschikbaarheid van de daaruit voortvloeiende intelligenceproducten (op landelijk niveau) voor het districtsniveau, om zo een snellere herkenning van verdachten te bewerkstelligen.
- Versterking van de digitale leiderschapskwaliteiten op bestuurlijk niveau bij het omgaan met sociale media in de openbare orde. Met steun van het Nederlands Genootschap voor Burgemeesters is een extra scenario voor de burgemeestersgame ontwikkeld, waarin meerdere dilemma’s uit het veld aan de orde komen.

Topic 4 Beter benutten van informatiestromen en samenwerking
Met het landelijk project netcentrisch werken is door samenwerking van de veiligheidsregio’s, IFV en TNO de informatievoorziening van de grond gekomen. TNO zet nu in op het vergroten van haar kennis over de volgende stap *samen werken* in het groeimodel netcentrisch werken. In 2011 en 2012 heeft het team van TOPIC4 kennis op gedaan over knelpunten die hierbij naar voren komen; aansluitend zijn daar interventies voor ontwikkeld. In 2013 zijn deze interventies verder uitontwikkeld en gevalideerd, zodat deze hun weg kunnen vinden naar veiligheidsregio’s en hun betrokken ketenpartners.

De kennisbank (2012) is uitgebouwd naar een supporttool ‘expertise selectie’ voor hoogwatersituaties (2013). Hierbij is gekozen om aan te sluiten bij nieuwe ontwikkelingen binnen het IFV, waarbij informatie (bijv. over GRIP0 incidenten bij gemeenten) via een zogenaamde infographic beschikbaar komt. Hiermee wordt een offline product gecreëerd dat overzicht geeft en ook direct als geheugensteuntje en aantekeningblad gebruikt kan worden. TNO heeft op basis van kennis opgedaan uit dit en andere projecten de basis gelegd voor de infographic over hoogwatersituaties.

Met behulp van onze leerketen helpen we inzichtelijk maken hoe oefenen en anders evalueren kunnen leiden tot meer verbetering. Daarvoor is het nodig om (systematisch) te kijken welke observaties moeten worden opgevolgd, welke interventies daarop ontwikkeld moeten worden, en welke aanpassingen moeten worden getest om te kijken of het tot gewenste resultaten leidt. Vervolgens moeten de werkwijze en opleiding aangepast worden. Pas dan kunnen we spreken van leren. Met die boodschap helpen we MOTO en haar leden om de ontwikkeling van de leerketen op de agenda te krijgen. Daarmee wordt het hele oefenveld in context en perspectief geplaatst.



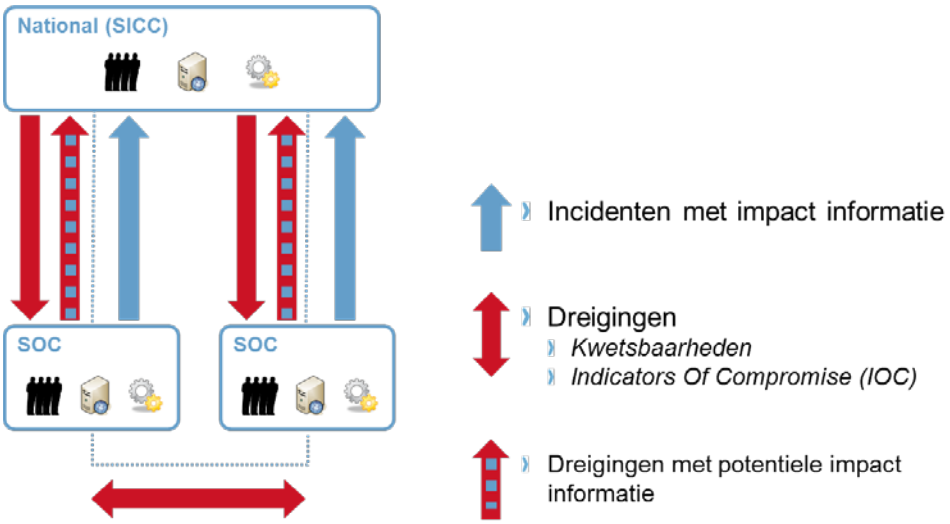
Figuur 4 Model voor de ontwikkeling van de leercyclus.

Wij kunnen bij elke stap de ‘best practices’ uit de praktijk inbrengen. Nadrukkelijk sluiten we hierbij aan bij initiatieven uit de praktijk, zoals de resultaten van het WODC-onderzoek naar evalueren[1]. Onze resultaten en adviezen passen goed binnen de constateringen van de commissie Hoekstra die de wet op de veiligheidsregio’s onderzocht en constateerde dat er noodzakelijk aandacht moet komen voor multidisciplinaire samenwerking en multidisciplinair oefenen en leren.

Een ander onderzocht onderwerp in dit topic is het ontwikkelen van een informatiebasis voor meer synergie tussen de werkvelden fysieke en sociale veiligheid. Het concept-tool VISI (VeiligheidsInformatie bij Signalering) geeft een beeld van de informatie welke men (nodig) heeft om een sociaal incident te kunnen duiden. Deze eerste stap van duiding is noodzakelijk om een totaalbeeld van de situatie te kunnen opstellen. Dat totaalbeeld ligt ten grondslag aan de verdere aanpak van het incident.

Topic 5 Cybersecurity
De informatiebehoefte van het ministerie VenJ betreft het detecteren van cybermisbruik en het opbouwen van een geaggregeerd operationeel beeld van cybersecurity in Nederland. In dit topic is onderzocht wat de technologische mogelijkheden zijn voor het ontwerpen en testen van een systeem daarvoor. Deze werkzaamheden vonden plaats in samenwerking met het VP onder de Topsector HTSM, zodat nauw kon worden samengewerkt met het bedrijfsleven (bijvoorbeeld IBM, HP).
De studie onderkende dat het delen van cybersecurity-informatie twee doelen kan dienen. Enerzijds het verhogen van de weerbaarheid van de (vitale) cyber infrastructuur, anderzijds het verhogen van de situational awareness om zo grootschalige verstoring tijdig te kunnen detecteren. Om dit te bereiken is een infrastructuur vereist die het delen van beschikbare cybersecurity informatie tussen organisaties op een adequate en veilige manier mogelijk maakt.

[1] http://www.wodc.nl/onderzoeksdatabase/ontwikkeling-evaluatie-crisis.aspx?cp=44&cs=6796



Figuur 5 Informatiestromen bij het delen van cybersecurity informatie tussen organisaties.

De huidige state of the art op het gebied van protocollen en standaarden om bovenstaande informatie geautomatiseerd uit te kunnen wisselen is in afdoende mate beschikbaar voor dreigingsinformatie maar op het gebied van impactinformatie (t.b.v. detectie grootschalige verstoringen) bestaat een gap. Tijdens de testen van nu beschikbare tools blijkt duidelijk dat het maturity level nog niet voldoende gevorderd is.

In 2013 is ook een nationale en internationale inventarisatie uitgevoerd van methoden en technieken voor het delen van informatie over cybersecurity in de vitale infrastructuur. Hierbij is een onderverdeling gemaakt tussen de verschillende typen informatie zoals gegevens over kwetsbaarheden en dreigingen, nieuwe technologische ontwikkelingen, en incidenten. Per categorie wordt aangegeven wat good practices zijn, bijvoorbeeld om gegevens vertrouwelijk te kunnen delen. Tevens wordt gezocht naar mogelijkheden om de informatie meer toegankelijk te maken, ook sector-overstijgend, rekening houdend met de vertrouwelijkheid van de gegevens. Hierbij wordt ook gekeken naar de benodigde definities en standaarden om de gegevens eenduidig te kunnen uitwisselen.

Op basis van de uitgevoerde inventarisatie zijn een aantal kansrijke onderwerpen gedefinieerd voor het ontwikkelen van nationale modellen waarmee afhankelijkheden oftewel keteneffecten van storingen/aanvallen binnen vitale sectoren, kunnen worden bestudeerd en geoptimaliseerd. Om de behoeften verder te concretiseren zijn de volgende drie richtingen onderkend als kansrijk:

- simulatieomgeving om keteneffecten zichtbaar te maken;
- dependency analysis om afhankelijkheden zichtbaar te maken; bijvoorbeeld conform de opzet van MSB (Zweden);
- analysemodellen als aanzet voor een ‘Cyber Plan Bureau’.

Voor elk van de onderzoeksonderwerpen is in het afgelopen jaar verdere samenwerking met de universiteiten gezocht, onder andere door het gezamenlijk werken aan voorstellen in het kader van de NWO call voor cybersecurity. Daarnaast is ook samenwerking in Europese onderzoeksprojecten gestart (onder andere Cyspa en CAPITAL)

Vooruitzicht

De kennisontwikkeling in de vijf topics heeft in 2013 geleid tot concrete resultaten en toepassingen bij politie en veiligheidsregio's. Dit was mede het gevolg van de intensieve afstemming en samenwerking van de onderzoekers met het veiligheidsveld. Voor een verdere en bredere doorvertaling naar de maatschappelijke praktijk zijn diverse projecten als vervolg op de ontwikkelingen in dit VP opgestart. De toenemende aandacht voor innovatie bij het ministerie VenJ en de centralere aansturing van innovatie bij de Nationale Politie en de Veiligheidsregio's is van wezenlijk belang voor het benutten van het potentieel aan vernieuwende opties voor vergroting van efficiency, effectiviteit en multidisciplinaire samenwerking. In dit opzicht is ook de uitbreiding van de samenwerking met Defensie een gunstige ontwikkeling. Verder is in 2013 de nationale krachten-bundeling voor veiligheidsinnovaties fors versneld door het opgebouwde commitment voor The Hague Security Delta. Ook in het EU programma Horizon 2020 heeft Security een prominente plaats met groeiende financiële kaders verworven.

Inhoudsopgave

1 Inleiding

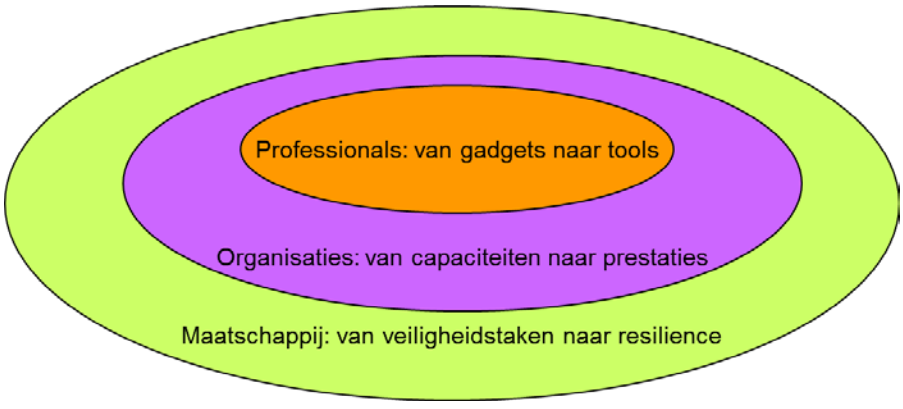
1.1 Beschrijving van TNO-thema Integrale Veiligheid

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.

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 2013 was het derde jaar van de uitvoering van het Vraaggestuurde Programma 2011-2014 Veilige Maatschappij.

De vorming van de Nationale Politie en de schaalvergroting binnen de veiligheidsregio's en de meldkamerinfrastructuur zijn belangrijke externe ontwikkelingen. Enerzijds geeft dit een nieuw perspectief op bundeling van decentrale innovatie-initiatieven, anderzijds is er nog steeds sprake van een opstartfase. 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 2013 geleid tot concrete resultaten. Dit was mede het gevolg van de intensievere afstemming en samenwerking van de onderzoekers met het veiligheidsveld. 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 2012 in een bijeenkomst met 100 top-vertegenwoordigers van het veiligheidsveld aan minister Opstelten werd overhandigd. In 2013 is daarop voortgebouwd met een intensieve deelname van TNO in The Hague Security Delta. Dit Onafhankelijke initiatief wordt gesteund door de ministeries VenJ en Defensie, het bedrijfsleven, de gemeenten Den Haag, Enschede en Eindhoven/Tilburg en de kennisinstellingen TNO en NFI.

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 in 2010 voor focussering van het 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.

Tijdens de looptijd is in de Stuurgroep van het VP diverse malen besproken of dit vijftal aanpassing behoeft, waarbij steeds is geconcludeerd dat het een goede basis is voor het vernieuwende onderzoek in het VP

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 2013

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 een begeleidingsteam dat betrokken was bij het opstellen van het kennisontwikkelingsplan voor 2013.

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, NCTV
4. **Infobenutting voor samenwerken** (Josine van de Ven)	Centrum Innovatie en Veiligheid, Utrecht
5. **Cybersecurity** (Marieke Klaver)	VenJ, DG-NCTV, NCSC

Gedurende het jaar 2013 zijn er voor ieder topic minstens drie bijeenkomsten van het begeleidende team geweest. Verder zijn ook de coördinerend begeleiders in mei en december bijeen geweest.

Namens het departement Veiligheid en Justitie werd de regievoering over het VP uitgevoerd door But Klaassen.

2.3.2 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
ISITEP	Interoperability en Crisismanagement	EU	4
CAPITAL	Roadmap voor Cybersecurity	EU	5
ETCETERA/ INNOSEC	Verkenning security technologie	EU	6
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

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.

2.4 Rapportages 2013

2.4.1 Rapportages topics

De in 2013 bereikte resultaten zijn vastgelegd in de KIP-verslagen en onderzoeks-verslagen en publicaties. In hoofdstuk 3 van deze voortgangsrapportage 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 2013 is rond topic 3 een boekje Informatie die stuurt! (topic 3), terwijl een concept voor een in 2014 uit te brengen rapport “Maatschappelijk verantwoord herkennen van afwijkend gedrag” werd opgesteld.
In 2013 zijn voor de topics 1, 3 en 5 bredere bijeenkomsten georganiseerd. Verder werden er voor alle topics bijdragen verzorgd aan discussies met belanghebbende organisaties in diverse congressen en symposia.

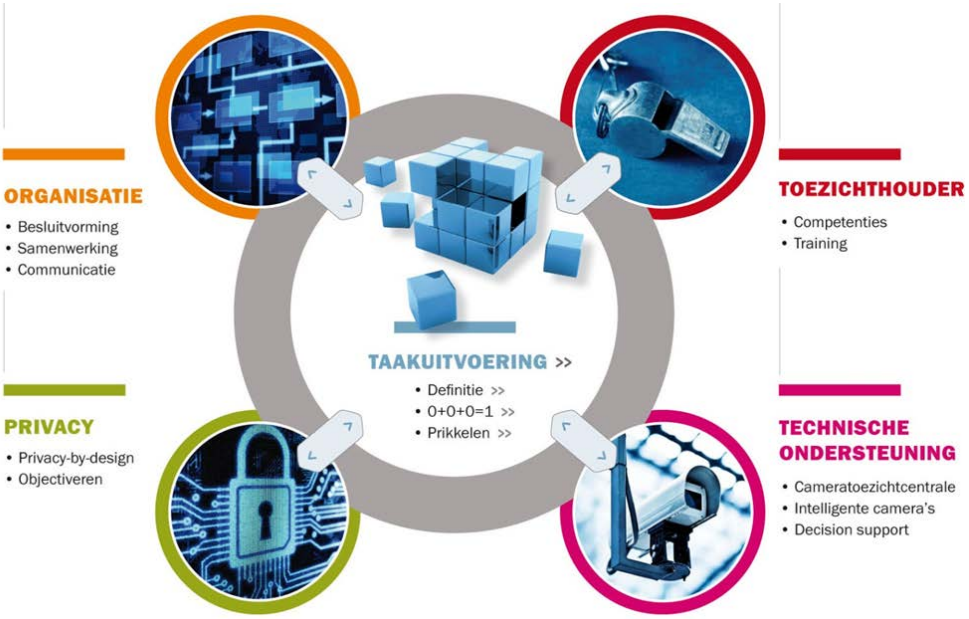
Op 31 mei en 10 oktober presenteerde TNO een aantal ontwikkelingen van het VP Veilige Maatschappij in het kader van door VenJ georganiseerde bijeenkomsten “Veilig door Innovatie”.

3 Resultaten van het VP Veilige Maatschappij in 2013

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[2] 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.



Figuur 6 Basismodel toezicht op afwijkend gedrag.

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). 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

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

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.

Het onderzoek is gericht op een vijftal vragen:

- **Hoe is afwijkend gedrag te definiëren?**
  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?
- **Wanneer wijkt gedrag voldoende af om terecht te verdenken?**
  Een enkele verdachte aanwijzing komt relatief veel voor en geeft onvoldoende indicatie of iemand werkelijke kwaadwillige intenties heeft. Een goed oordeel kan pas gegeven worden wanneer er meerdere verdachte aanwijzingen zijn. 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 veronderstellen dat de combinatie meerdere kleine afwijkingen dat wel kunnen. Dan ontstaat een robuuste verdenking: een “1”. 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?
- **Hoe kunnen in een toezichtsysteem meerdere waarnemingen worden vastgelegd?**.
  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. Voor een goede registratie hiervan kan een geautomatiseerd systeem van enorme meerwaarde zijn.
- **Hoe kan afwijkend gedrag door prikkelen beter zichtbaar worden gemaakt?**
  Prikkelen is een methode voor toezichthouders om afwijkend gedrag beter zichtbaar te maken zodat het gemakkelijker te observeren wordt.
  Daarbij zenden toezichthouders subtiele signalen uit met als doel een reactie te ontlokken. Uit onderzoek blijkt dat dit inderdaad kan helpen om kwade intenties beter zichtbaar te maken. Vooralsnog is het onduidelijk waarin die kwade intenties tot uiting komen (waar reageren zij op?). Hoewel beoordelaars het onderscheid kunnen maken, weten we niet hoe ze dat doen en waarop ze dan letten. Weten we dit wel, of weten we welke vaardigheden ervoor zorgen dat sommige mensen beter zijn in het herkennen van afwijkend gedrag na prikkels, dan kunnen we toezichthouders trainen in die relevante kennis of vaardigheden.
- **Hoe kunnen we effectiviteit en de efficiency van een toezichtstaak optimaliseren?**
  Met de antwoorden op bovenstaande vraagstukken zijn we in staat om de toezichtstaak zowel effectiever als efficiënter te maken: door het optimaal

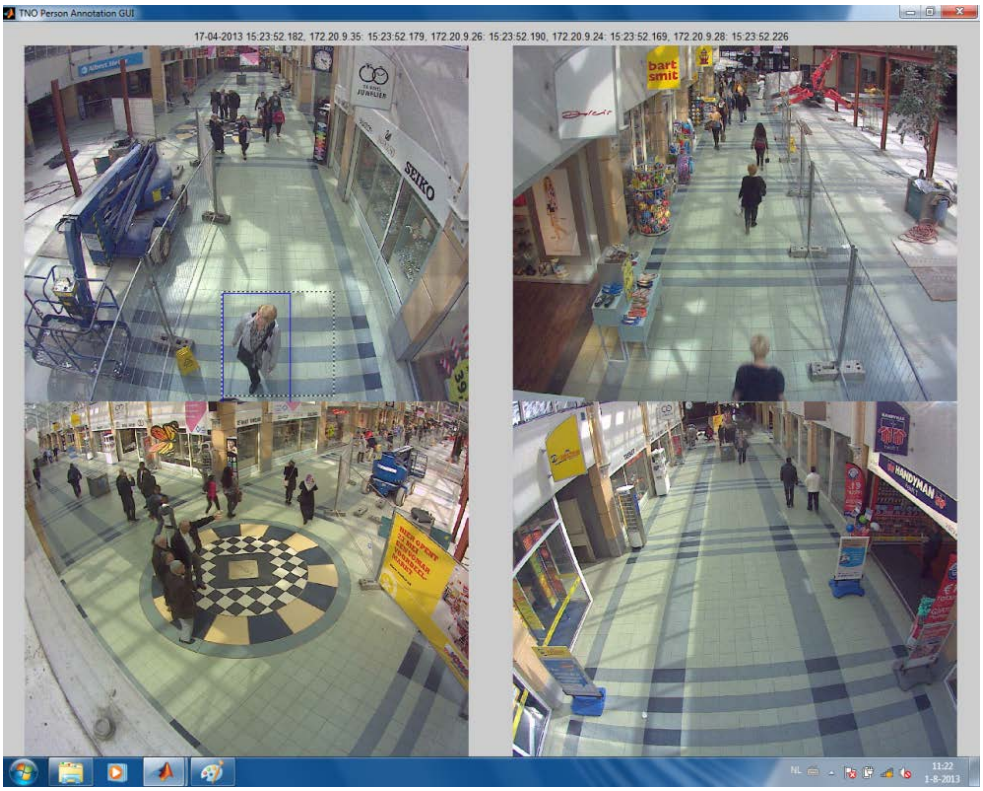
zoeken naar afwijkend gedrag en door het combineren van observaties. Dit onderzoek geeft inzicht in welke aanwijzingen toezichthouders het beste kunnen verzamelen, hoe ze het beste aanwijzingen kunnen verzamelen, en hoeveel aanwijzingen nodig zijn voor goede beslissingen. Bovendien kan de automatische registratie in een technologisch systeem gecombineerd worden met de voordelen van de camera's ter plekke.

3.1.2 Gerealiseerde voortgang

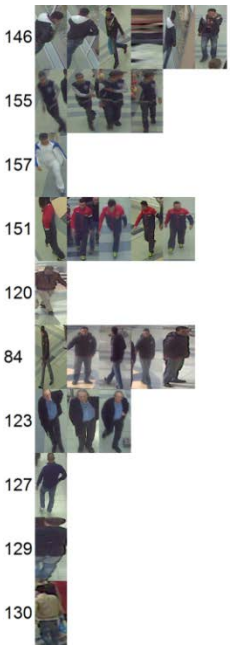
In 2013 is de ontwikkeling van een taal om afwijkend gedrag te beschrijven voor gebruik in intelligente software toepassingen voortgezet. Zo'n taal helpt ook om gericht samen te werken tussen de betrokken disciplines, namelijk de gedrags-, informatie- en technologiewetenschappen. Er is nu een basis gelegd voor een methodiek om beeldmateriaal van incidenten te annoteren. Met de in 2012 aangelegde beeldbank met enkele honderden videofragmenten van partners zoals de NS, KMAR en de politie Antwerpen bleek het mogelijk voor het delict zakkenrollen een modi operandi map (MOMAP) op te stellen. De methodiek en MOMAP zijn beschreven in een tussentijdse rapportage. **Met deze kennis is het mogelijk sneller en effectiever patronen van afwijkend gedrag op locaties te identificeren en delen.**

Ook zijn we in 2013 verder gegaan met het combineren van observaties van verschillende toezichthouders. Het doel daarvan is de hit-kans van het aanhouden van mensen met kwade intenties te vergroten en tegelijkertijd de kans te verkleinen dat iemand onterecht staande gehouden wordt. Hiertoe is een tool ontwikkeld waarmee toezichthouders op een beeldscherm mogelijke verdachten kunnen 'taggen'. Op het moment dat meerdere verschillende toezichthouders dezelfde persoon getagd hebben kunnen toezichthouders op de vloer er opvolging aan geven. De tool bevat een mogelijkheid om camerabeelden uit te lezen, personen te taggen en verschillende tags te combineren (door middel van her-herkenning). **Met deze tool en de onderliggende kennis is het in de toekomst mogelijk op een specifieke locatie in te schatten hoeveel operators in een uitkijkcentrale nodig zijn om een vooraf gedefinieerd percentage daders uit een groep te halen (bv 90%, 70%, 50%) en hoeveel operators het met elkaar eens moeten zijn over de wenselijkheid om een zeker persoon aan te houden en hoeveel onterechte aanhoudingen dat op kan leveren.**

Zowel het MOMAP als de tagging tool zijn in 2013 gebruikt in een groots opgezet onderzoek waarbij acteurs met behulp van de MOMAP kennis getraind zijn in zakkenrollerstechnieken om vervolgens zakkenrollersscenario's na te spelen tussen het winkelende publiek in Winkelcentrum Kanaleneiland in Utrecht.
De ca. 20 incidenten die zijn nagespeeld zijn met de CCTV-systemen ter plaatse opgenomen. De opgenomen data zijn door Securitas beveiligers bekeken en getagd door ze aan te klikken op de computerschermen.



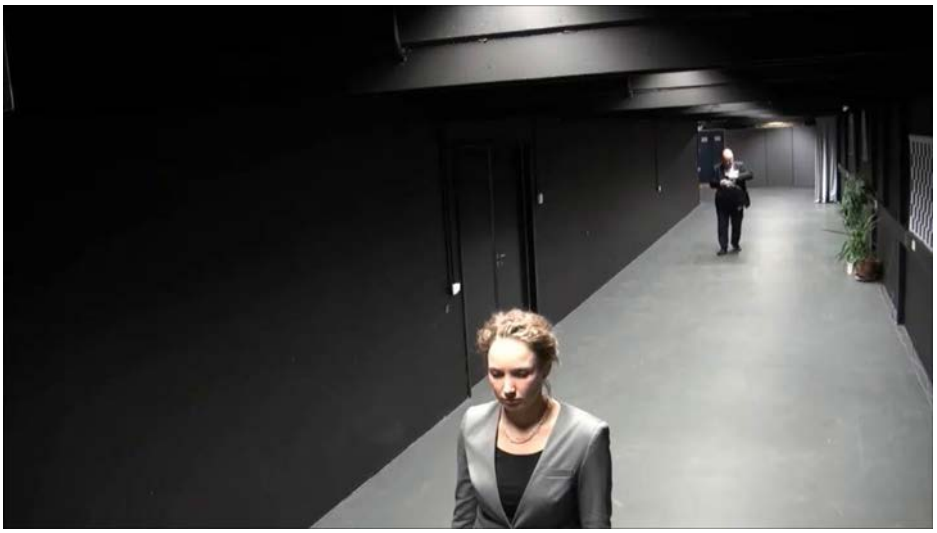
Figuur 7 Screenshot van het scherm dat operators tijdens het experiment in Winkelcentrum Kanaleneiland te zien kregen. Op basis van deze beelden moesten zij verdachte personen ‘taggen’.



Figuur 8 Door de her-herkenningstool gegenereerde individuen op basis van meerdere ‘tags’.

Het onderzoek naar prikkelen is vervolgd met de in 2012 effectief gebleken experimentele opzet. Daar ondervonden proefpersonen die illegale pakketjes bij zich droegen de veronderstelde psychologische effecten, zoals toegenomen spanning en zelf-focus. Ervaren toezichthouders bleken toen beter in staat zijn 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. In 2013 is een nieuw onderzoek gedaan met gebruik van een andere prikkel (namelijk een geluid van een portofoon in plaats van een politieman) en met verhoogde cognitieve druk (door deelnemers hun stappen te laten tellen).
Uit analyses bleek dat mensen die een illegaal pakketje bij zich droegen beter werden herkend door toezichthouders als ze geprikkeld werden met een onverwacht geluid en ze ook hun stappen moesten tellen. Prikkelen heeft dus effect op het herkennen van afwijkend gedrag, in ieder geval in combinatie met het verhogen van de cognitieve druk. Hierbij kan men denken aan het onverwacht veranderen van looppaden of ambigue borden. **Met de opgedane kennis kan toezicht effectiever worden ingezet en kunnen praktijktoepassingen worden ontwikkeld om de opgedane kennis te valoriseren.**



Figuur 9 Experiment naar prikkelen, waarbij deelnemers met een onschuldig of een illegaal pakketje door een gang moesten lopen. Een deel van de deelnemers hoorde halverwege de gang een onverwacht geluid, en een deel van de deelnemers moest hun stappen tellen, zodat ze mentaal beziggehouden werden.

Een laatste studie is halverwege 2013 gestart en had tot doel vragen met betrekking tot effectiviteit en efficiëntie van toezicht maatregelen te verkennen. Tijdens het TNO InFocus event is een workshop verzorgd waar deze vragen met stakeholders werden besproken. Op basis van deze workshop en interne expertsessies is een artikel in een vaktijdschrift (Security Management) gepubliceerd. Een expertsessie is georganiseerd met stakeholders van onder andere KMar en beveiligingsbedrijven over effectiviteit van proactief beveiligen, waarin nieuwe ideeën naar voren kwamen voor het in kaart brengen van effectiviteit, zoals de motivatie van beveiligers, het imago van het beveiligingsvak, de kosten van incidenten en trendanalyses. **De kennis die is opgedaan in dit deel van het topic wordt gebruikt voor zowel de uitvoering van het proof-of-concept in 2014 als het vermarkten van de ontwikkelde toezichtconcepten.**

3.1.3 Publiciteit

- Bouma, H., Vogels, J., Aarts, O., Kruszynski, C., Wijn, R., Burghouts, G. J. (2013). Behavioral profiling in CCTV cameras by combining multiple subtle suspicious observations of different surveillance operators, Proc. SPIE, 8745.
- Van Hemert, D.A., Identificatie van verdachte personen, presentatie t.b.v. bezoek Pieter Cloo (Secretaris-Generaal at Ministerie van Veiligheid en Justitie) bij TNO, januari 2013.
- Van Hemert, D.A., Effectiviteitsmetingen voor Detectie van Afwijkend Gedrag, presentatie bij Politie Antwerpen, maart 2013.
- Van Hemert, D.A., De Human Factor, gedrag en observatie, presentatie t.b.v. ISZW bezoek aan TNO, maart 2013.
- Van Hemert, D.A., College afwijkend gedrag, college t.b.v. HvA Aviation Security, sep 2013.
- Van Hemert, D.A., & Van den Berg, H., Effectiviteit van menselijk toezicht, artikel in: Security Management, nr 12 2013.
- Van Pel, B., Verhagen, B., & Wijn, R. (2012). Predictive profiling of proactief beveiligen: Security questioning & Prikkelen. Security Management, 9, 40-43.
- Van Rest, J. (2013). In Focus: afwijkend gedrag. Presentatie bij In Focus, Delft, 13 juni 2013.
- Van Rest, J. et al (2013), Designing Privacy by Design. In: Annual Privacy Forum 2012. Lecture Notes in computer science, Springer (to be published).
- Van Rest, J., F.A. Grootjen, M. Grootjen, R. Wijn, O. Aarts, M.L. Roelofs, G.J. Burghouts, H. Bouma, L. Alic, W. Kraaij, “Requirements for multimedia metadata schemes in surveillance applications for security”, Multimedia Tools and Applications, (2013).
- Van Rest, J., Roelofs, M., & Van Nunen, A. (2013). Definiëren van Afwijkend Gedrag in de Context van Veiligheid. TNO Rapport.
- Wijn, R., & Van der Kleij, R., Prikkelen versterkt afwijkend gedrag, TNO productblad 2013.
- Wijn, R., Van den Berg, H., Lousberg, M. (2013). On operator effectiveness: the role of expertise and familiarity of environment on the detection of deviant behavior. Personal and Ubiquitous Computing, 1, 35-42.
- Wijn R. (2013). Herkennen van afwijkend gedrag: Hoe subtiele prikkels kunnen helpen om kwaadwillende intenties zichtbaar te maken. Presentatie bij BedrijvenOverleg Rotterdam (BOR). Rotterdam, 11 april 2013.
- Wijn, R. (2013). Recognizing deviant behaviour: How subtle prodding actions can help to reveal malicious intent. Paper presented at the Detecting Illicit Substances: Explosives & Drugs Gordon Research Conference. Les Diablerets, May 27, Switserland.
- Wijn R. (2013). Herkennen van afwijkend gedrag: Hoe subtiele prikkels kunnen helpen om kwaadwillende intenties zichtbaar te maken. Presentatie bij In Focus, Delft, 13 juni 2013.
- Wijn R. (2013). Herkennen van afwijkend gedrag: Hoe subtiele prikkels kunnen helpen om kwaadwillende intenties zichtbaar te maken. Presentatie bij Bedrijvendag Securitas, Maarssen, 19 juni 2013.
- Wijn R. (2013). Herkennen van afwijkend gedrag: Hoe subtiele prikkels kunnen helpen om kwaadwillende intenties zichtbaar te maken. Presentatie bij ISPS - Port Facility and Security Officers bijeenkomst, Ridderkerk, 7 oktober 2013.

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 2013 zijn gesteld:

- Ontwikkeling van een medium om interactie tussen burgers en beroepskrachten in veiligheidsorganisaties te intensiveren over verwachtingen van taken en om verantwoordelijkheden en wederzijds begrip te vergroten. Hierin is ook een trial met gebruikersgroepen opgenomen.
- Demoversie van een game inzetten voor de voorbereiding van een oefening waar interactie burgers en hulpverleners centraal staat. Hulpverleners laten ervaren wat de verzonden informatie met burgers doet.
- Effectiviteit van communicatie tussen burgers en hulpverleners maximaliseren door gerichte evaluatie van alle in aanmerking komende kanalen en advies. Voor een evaluatie-dashboard eerste ontwerprichtlijnen maken en een trial met oefening uitvoeren.
- Integratie conceptmodellen fysieke maatregelen zelfredzaamheid en maatregelen sociale veiligheid. Geïnventariseerde laag menselijk gedrag toevoegen aan model. Hiermee kan de effectiviteit van maatregelen beter worden benoemd.

3.2.2 Gerealiseerde voortgang

Interactie burgers en hulpverleners

In 2012 zijn motivatie-profielen opgesteld voor de vrijwilligers 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 om de betreffende organisaties bij het gerichter werven, begeleiden en boeien van vrijwilligers. In 2013 is als vervolg daarop een keuze-instrument ontwikkeld dat burgers bewust maakt van hun eigen persoonlijke voorkeuren ten aanzien van vrijwilligerswerk. Mensen krijgen korte videofragmenten te zien waarin verschillende acteurs een bepaald aspect van het vrijwilligerswerk belichten, bijvoorbeeld overwegingen als ‘je hoort iets voor de samenleving te doen’, ‘je kunt er iets van leren’ of ‘het is goed voor je sociale netwerk’ . Een voorbeeld geeft onderstaande figuur.

Sociale contacten zijn zo belangrijk. Ik ben eigen ondernemer en dan is het heel nuttig om een groot sociaal netwerk te hebben. Vanuit dat netwerk komen vaak de opdrachten binnen. Om mijn netwerk uit te breiden ben ik vrijwilligerswerk gaan doen. Ik zit nu als vrijwilliger in een Raad van Toezicht waardoor ik veel nieuwe mensen ontmoet. Via hen krijg ik nog wel eens een opdracht. Dus… uuh heel nuttig.

Figuur 10 Een beeld uit een videofragment met de daarbij uitgesproken tekst. Hiermee worden mensen geholpen om een betrouwbaar inzicht te krijgen in hun voorkeur voor bepaalde vrijwilligerstaken.

Voor elke overweging zijn twee verhaaltjes opgenomen: één verhaaltje waarin de acteur beargumenteerd dat het motief belangrijk voor hem of haar is en één verhaaltje waarin dat niet het geval is. Op deze manier worden alle kanten van het vrijwilligerswerk belicht en wordt voorkomen dat de gebruiker in een bepaalde richting wordt gestuurd.
Als mensen zo'n verhaaltje horen weten ze vaak direct of het ze aantrekt of niet. Het roept een gevoelsmatige reactie op en geeft daarmee dus informatie over onbewuste voorkeuren. Door die gevoelsmatige reactie op de video worden mensen zich bewust van wat ze kennelijk belangrijk en minder belangrijk vinden in het vrijwilligerswerk.
De meerwaarde van dit instrument is experimenteel onderzocht. Daarbij moesten dertig mensen vragen beantwoorden nadat ze het instrument hadden geraadpleegd en dertig andere mensen kregen alleen informatie over verschillende voor- en nadelen. De data van dit experiment zijn nog niet allemaal binnen, maar zullen begin 2014 worden geanalyseerd. Er is op 21 november 2013 aandacht besteed aan deze ontwikkelingen in de oratie van prof. dr. Kerstholt aan Universiteit Twente over de beslissende burger.

Informatiecirkel professionals en burgers
Over de experimenten in 2011-2012 is gerapporteerd in de TNO-*publicatie 'Hallo! Over crisiscommunicatie en zelfredzaamheid van burgers'.* Daarbij is ingegaan op het gericht aandacht geven aan handelingsperspectief, voorafgaand informeren en het geven van procesinformatie. Op deze aanpak voor crisiscommunicatie zijn in gesprekken met veiligheidsregio's zeer positieve en constructieve reacties ontvangen. De resultaten blijken goed bruikbaar in de praktijk. In contacten met het Veiligheidsbureau Haarlem (Kennemerland) is door TNO meegedacht en gebouwd aan de vormgeving van oefeningen. De afgelopen periode blijkt dat men hard heeft

gewerkt aan het reorganiseren van de hele crisiscommunicatie in de Veiligheidsregio. Nu dat organisatorisch op poten staat, staat men open voor verbetering van de wijze van communicatie met burgers. Concreet wil men nu een trainingsmiddel ontwikkelen en inzetten om de vaardigheden van de crisiscommunicatieadviseurs te versterken. Hiervoor is intensief afstemming geweest tussen experts en TNO. De taakprofielen van de commissie Grooter bieden voldoende inzicht in de taken van de verschillende crisiscommunicatie- adviseurs, maar onvoldoende aanknopingspunten voor ontwikkeling en training. TNO heeft vanuit het perspectief van de resultaten van de experimenten deze taakprofielen nu “vertaald” naar competentieprofielen. Deze competentieprofielen worden nu als basis gebruikt voor de ontwikkeling van training en de beoordeling van prestaties van crisiscommunicatie-adviseurs.

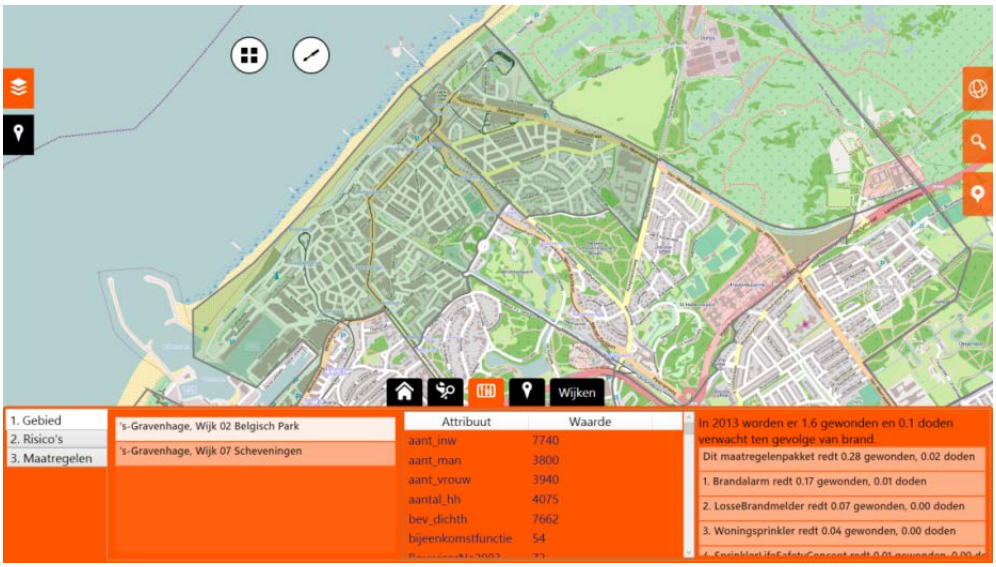
In voorbereiding op oefeningen is men op zoek naar een manier om hun crisiscommunicatieadviseurs erbij te betrekken. TNO denkt mee over de oefening en het in kaart brengen van de effecten. In 2014 wordt bezien op welke wijze de ondersteuning kan worden voorgezet om de effectiviteitsmeting te organisatoren. De volgorde van informatievoorziening, duiding en handelingsperspectief vormen hierbij de kern.

De papieren nul-versie van de ontwikkelde game is ontwikkeld binnen het *Flood Control* programma. De wetenschappelijke basis, de inhoud van de communicatie en het interactie design in de game is mede gebaseerd op de bevindingen vanuit dit topic. De nul-versie zal in 2014 verder ontwikkeld worden naar een web-based game dat daardoor vlot gespeeld kan worden met beperkte begeleiding; aan deze doorontwikkeling in samenwerking met het IFV is financiële ondersteuning uit het HSD stimuleringsfonds toegezegd. De deelname aan het congres en presentatie in Riga heeft ertoe geleid dat TNO (Hester Stubbe) is gevraagd toe te treden tot het EENA netwerk (European Emergency Number Association) van onderzoekers in crisiscommunicatie en hulpverlening.

De activiteiten hebben ook de interesse gewekt van adviesbureaus, die voor de veiligheidsregio’s werken.
Zo heeft de V&R academie http://www.vracademie.nl/pages/vr-academie/home.php TNO gevraagd te helpen bij het (her-)formuleren competentieprofielen in een vervolgproject. De bevindingen van het onderzoek worden beschreven in de TNO rapportage over dit werkpakket: Crisiscommunicatie in beweging.

Modelontwikkeling voor maatregelen met betrekking tot zelfredzaamheid in gebouwen
Voor het zgn. *SafeMe*-model van de koppeling van maatregelen in gebouwen en gebouwde omgeving aan zelfredzaamheid is een demonstrator ontwikkeld en een korte film waarin de mogelijkheden van het model worden uitgelegd.
De demonstrator bevat de kaart van Nederland met een verdeling in wijken.
Per wijk is in te zoomen op de generieke data (zoals risicoprofielen, samenstelling bevolking qua leeftijd/nationaliteiten/opleidingsniveaus, fysieke kenmerken gebouwen en wegen), historische gegevens van opgetreden incidenten, de uit de CBS data afkomstige verwachte aantallen slachtoffers (doden/gewonden per jaar) en de verwachte effecten van mogelijke en afzonderlijke en gecombineerde maatregelen. Tevens is met Verwey Jonker Instituut afgestemd over de wijze waarop sociale veiligheidsincidenten ondergebracht kunnen worden in het model.

Zowel de data over aantal en type incidenten als de ervaren subjectieve veiligheid worden als maat meegenomen. Een groep experts van potentiele gebruikers (Veiligheidsregio's, WODC, vertegenwoordigers van NGO, gemeenten) hebben op de demonstrator gereageerd en dit model potentieel waardevol genoemd; vanzelfsprekend werd afhankelijk van de werkomgeving meer belangstelling voor hetzij fysieke of sociale veiligheidsincidenten gelegd. De mogelijkheden om meerdere incidenten/calamiteiten te koppelen aan te nemen maatregelen spreekt aan. Op basis van deze inzichten kan met meer zekerheid worden bepaald waar investeringen voor maatregelen het meeste effect kunnen geven.
Voor een mogelijke uitbreiding van de gebruikswaarde van het model is verkend of een koppeling met andere databronnen mogelijk is. Door bijvoorbeeld data over het zorg-domein te koppelen kan in lagen worden gekeken naar de mogelijke ontwikkeling van multi-problematiek in een bepaald gebied/wijk. Zo zullen er in een wijk waar relatief veel jongeren wonen andere maatregelen wenselijk zijn dan in een wijk met veel ouderen: daarbij kunnen ook de niveau van onveiligheid en inbraakfrequentie sterk verschillen. De gemeentediensten die hierbij waren betrokken proberen de eigen datastromen te optimaliseren. De integraliteit wordt gezien als potentieel kansrijk. In een opdracht van het WODC wordt de ontwikkelde kennis gebruikt voor het ontwikkelen van methoden om de weerbaarheid te bepalen. Daarnaast wordt met Falck verkend op welke wijze en onder welke voorwaarden zij het ontwikkelde model kunnen gebruiken en hoe de verdere ontwikkeling van het model voor hun gebruik kan worden gefaciliteerd.



Figuur 11 Voorbeeld van een screen van het SafeMe-model, waarop de uitkomst te zien is van de effecten van een aantal maatregelen op de veiligheid in 2 Haagse wijken.

Effectiviteit van social media en aanzet dashboard voor community communicatie
De inzet en de keuze van media voor communicatie met de omgeving zijn 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.
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.

In 2013 is een interactieve versie ontwikkeld van het dashboard/ adviestool voor multimedia communicatietoepassingen. Om de werking te expliciteren van de zeven stappen is een demonstrator en een filmpje gemaakt. Dit is ook voorgelegd aan een tweetal Veiligheidsregio's. Men is geïnteresseerd, maar tot een toepassing in hun crisisvoorbereiding is het nog niet gekomen. Er is nu een aanpak ontwikkeld om te peilen wat de gebruikswaarde kan zijn van een dergelijk adviestool. Op basis van de uitkomsten hiervan wordt bepaald welke vervolgstappen er gezet moeten worden voor het verder ontwikkelen en implementeren van de tool in de praktijk. Hierbij zal nav de gesprekken met de VRs worden ingezoomd op MoE = Maten van Effectiviteit. De prestatie-eisen (MoP's) die nu aan grootschalig optreden worden gesteld[1], zijn gekoppeld aan de processen *melding & alarmering*, *op- en afschaling*, *informatiemanagement* en *leiding & coördinatie*. Deze prestatie-eisen hebben vooral betrekking op maximale doorlooptijd. Er wordt gekeken naar het moment dat voldaan is aan de criteria voor grootschalige alarmering, ten opzichte van de alarmering zelf, het tijdstip van bijeenroepen van het beleidsteam of het beschikbaar zijn van gegevens.
Deze prestatie-eisen hebben slechts een indirecte relatie met de werkelijke effectiviteit van het grootschalig optreden. De laatste jaren is echter uit diverse incidentevaluaties op te maken dat b.v. ook op het gebied van crisiscommunicatie een aantal leerpunten te constateren zijn (Brouwer et al., 2012). Prestatiematen en effectiviteitsmaten (MoE's) op dit gebied ontbreken in het besluit veiligheidsregio's. In het vergroten van de werkelijke effectiviteit van grootschalig optreden speelt real-time intelligence en real-time omgevingsanalyse een belangrijke rol. Het dashboard zal hiermee rekening moeten houden en draagt bij aan het expliciet maken van de te bereiken doelen en effectiviteitsmaten.

3.2.3 Publiciteit

- Stubbe, H. Van Emmerik, M, Bloeme, D. (in bewerking). Resultaten experiment informatie-uitwisseling burgers en hulpverleners (werktitel).
- Trijssenaar I, & Veldhuis, G. (2013). Maatregelen voor zelfredzaamheid van burgers in gebouwen en de gebouwde omgeving, Naar een kwantitatief model voor het bepalen van de effectiviteit van maatregelen op de veiligheid van de burger. NVVK congres publicatie (paper).
- Trijssenaar, I., Van Wonderen, R, & Veldhuis, G. (2013). Zelfredzaamheid en veiligheid van burgers bij rampen en incidenten, naar een analyse tool die inzicht biedt welke maatregelen zelfredzaamheid en veiligheid het meest effectief kunnen vergroten, TNO-060-UT-2013-00700.
- *SafeMe* prototype, 2013.
- DemoFilm *SafeMe*, Erik Vullings, 28 november 2013.
- Group Decision Room workshop 'Zelfredzaamheid en veiligheid van burgers bij rampen en incidenten' met stakeholders en gebruikers, 4 december 2013, Den Haag.
- Meeting sphere report 'Zelfredzaamheid en veiligheid van burgers bij rampen en incidenten, 4 December 2013, H.L. Duijnhoven, I.J.M. Trijssenaar, Memorandum refnr. 010005455.
- 'Verslag uitwerking model sociale veiligheid', I.M.E. Raben, H.L. Duijnhoven, Memorandum refnr. 0100005444, februari 2014.

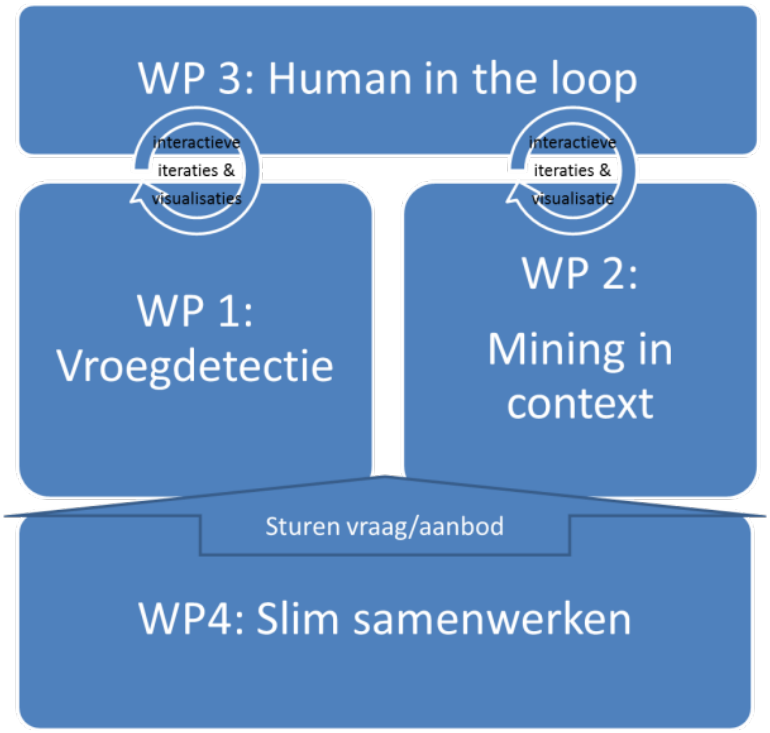
- TNO-Rapporten Maatregelen voor zelfredzaamheid van burgers in gebouwen en de gebouwde omgeving:
  - Trijssenaar, I., Duijnhoven, H., & Kruse, A-M. (2013). Onderdeel 1: 'Casus: sociale veiligheid op scholen', TNO 2013 R10328.
  - Trijssenaar, I., Duijnhoven, H., & Kruse, A-M. (2013). Onderdeel 2, 'Menselijk gedrag in bedreigende situaties', TNO2013 R10329.
  - Raben, I.M.E., & Trijssenaar-Buhre, I . (2013). Onderdeel 3, 'Kwantificering van maatregelen – brand in een gebouw, literatuurstudie', TNO2013 R10330.
- Stubbe, H. e.a. (2013). NL versie van de TNO-publicatie 'Hallo! Over crisiscommunicatie en zelfredzaamheid van burgers'.
- Stubbe, H. & Veldhuis, G (in bewerking). Crisiscommunicatie in beweging. TNO rapport verschijnt in 2014.
- Kerstholt. J., & Huis in 't Velt, M. (in bewerking). Effectiviteit keuze-instrument.
- Zevenstappenmodel HTML versie ondersteuning keuze media-aanpak communicatie crisis demonstrator. Link
- Online promo video van de advies tool voor multimedia. Communicatietoepassing. http://youtu.be/rq4kHKcIhnQ
- Interactieve versie van de 'advies tool voor multimedia communicatietoepassing light'. Link
- Brochure advisetool voor multimedia communicatie.

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 data en informatie neemt de afgelopen jaren explosief toe, waardoor doorgaan op de huidige (veelal niet-geautomatiseerde) wijze van informatieontsluiting een te grote inzet van de menskracht zou vergen. 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.

In 2013 heeft dit zich vertaald in een viertal samenhangende projecten:



Figuur 12 De samenhang tussen de deelprojecten van topic 3.

Na de zomer 2013 is een vijfde project toegevoegd: Digitaal leiderschap en digitale dilemma's. Alle projecten richten zich op innovatieve tooling en methoden of procesverbeteringen om slimmer te verwerken. De deelprojecten (WP's) richten zich op verschillende lagen of overgangen van data naar informatie, van informatie naar kennis. In een aantal projecten is de human factor daarnaast cruciaal.
De onderwerpen zijn zoveel mogelijk samen met één of meerdere stakeholders uitgewerkt. Deze manier van werken stelt ons in staat om snel zicht te krijgen op de toepasbaarheid van de ontwikkelde kennis.

3.3.2 Gerealiseerde voortgang

Vroegsignalering van dreigingen
In 2012 is een framework ontwikkeld dat de inhoud van berichten analyseert [Bouma, 2012], maar het was nog onduidelijk hoe goed dit systeem werkt op grotere aantallen en op nieuwe cases. In 2013 is daarom gewerkt aan een evaluatie en verbetering. Allereerst is er interactie geweest met gebruikers van diverse veiligheidsorganisaties. Tijdens de besprekingen is uitleg gegeven over het systeem voor vroegsignalering van dreiging, het systeem is gedemonstreerd, er is gesproken over de mogelijkheden voor de grafische user interface, en de gebruikers hebben feedback gegeven op het systeem met suggesties voor verbetering.

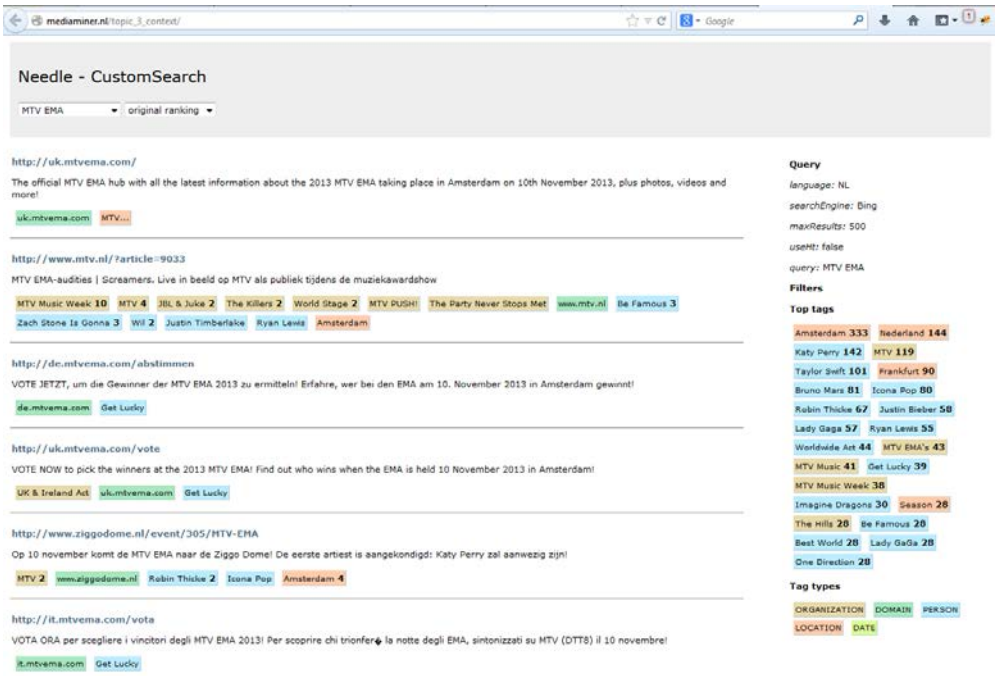
Figuur 13 Door interactie met het systeem kan het model worden verbeterd.

Er is ook data verzameld van diverse cases, waaronder ProjectXHaren in 2012 en de Kroningsdag in 2013. Uit de experimenten bleek het volgende. Met cross validatie experimenten wordt getraind op een deel van de data en geëvalueerd op een ander deel van de data, om overtraining te voorkomen en om een eerlijke schatting te krijgen van de prestaties van het systeem. Hiermee is berekend dat een nauwkeurigheid (i.e. percentage correct gelabelde tweets) van 90% kan worden gehaald als de training set representatief is voor de test set.
Met representatief wordt bedoeld dat het data moet zijn met een vergelijkbare context. Door interactie met de database kan het model worden verbeterd, wat leidt tot betere zoekresultaten.

Het systeem bleek zwak te zijn in het terugvinden van dreigingen in de nieuwe cases omdat het systeem niet goed generaliseert. Met een drietal alternatieve methoden om data te analyseren is geëxperimenteerd om de dreigingsduiding van tweets te karakteriseren. Voor een verzameling van 89.000 tweets van de Kroningsdag (30 april 2013, 10-12 uur) bleek nu aanzienlijk sneller een top-100 te vinden die veel “rijker” is aan berichten met serieus lijkende dreigingen dan bestaande methoden. Op deze veelbelovende richting zal worden voortgebouwd.

Data-mining in context
Op dit moment worden bij het doorzoeken van het internet vaak standaard zoekmachines gebruikt, zoals bijvoorbeeld Google en Bing. Elk van deze zoekmachines heeft zijn eigen voor- en nadelen ten behoeve van online rechercheren. Als voorbeelden van belangrijke nadelen zijn te noemen het niet ‘neutraal’ zijn van deze zoekmachines, het niet kunnen inzoomen op de vanuit opsporingsoptiek meest interessante individueel gegenereerde data en het niet kunnen combineren van zoekvragen. In dit project hebben we een aantal algoritmes ontwikkeld die de basis vormen voor het TNO prototype ‘Needle Custom Search’. Het is geen zoekmachine op zich zelf, maar een toevoeging op bestaande zoekmachines die een oplossing biedt voor de hierboven genoemde beperkingen. De Needle Custom Search-tool maakt gebruik van Bing en Google om te zoeken naar resultaten voor de ingegeven zoekvraag (query). De websites die als zoekresultaat worden gepresenteerd worden vervolgens in hun geheel gedownload

en opgeslagen. De opgeslagen documenten worden voorzien van annotaties met entiteiten, waarmee in de presentatie door toepassing van open-source software op verschillende manieren gefilterd en gesorteerd kan worden.



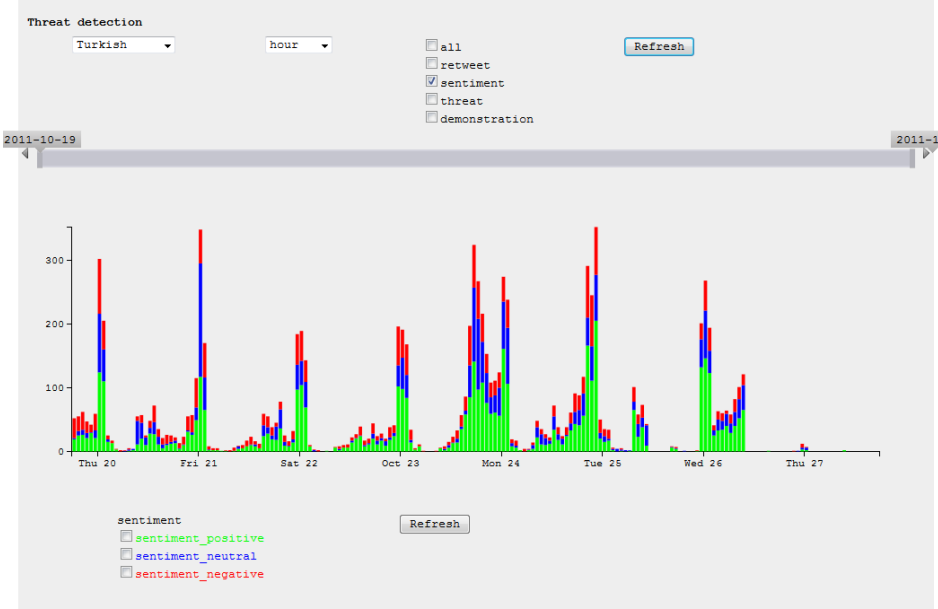
Figuur 14 Resultaat pagina van Needle Custom Search tool met een kleur-labeling van de vijf te markeren entiteiten : organisatie, locatie, persoon, domein en datum.

Bij een toetsing van de waarde van het NCS-tool blijkt het labelen van zoekresultaten meerdere potentiele gebruikers van de politie zeer aan te spreken. Ook werd - los van elkaar - aangegeven dat het mooi zou zijn om als rechercheur te kunnen werken met een makkelijk digitaal in te vullen formulier van de 7Ws (Wie, Wat, Waar, Wanneer, Waarmee, Waarom, Welke Wijze). In dit formulier zouden zaken die bekend zijn ingevuld kunnen worden. Onderlinge relaties moeten worden gevisualiseerd en onzekere informatie moet ook worden opgenomen.
Er dient wel onderscheid te worden gemaakt tussen onzekere informatie en de al vaststaande feiten. Als gebruiker zou je een dergelijk formulier willen gebruiken als leidraad bij het online rechercheren. Het formulier, of elementen daarvan, zou gebruikt worden om zoekresultaten te filteren. Of om binnen bepaalde resultaten verder te exploreren, waarbij men goed overzicht blijft houden op de filtering (om tunnelvisie te voorkomen). De functionaliteiten die de NCS tool nu omvat kunnen een waardevolle bijdrage leveren aan een dergelijke ondersteuning voor het online rechercheren.

The human-in-the-loop: datavisualisatie en interactie
Voor het analyseren van data en informatie uit vele bronnen zal naast automatische informatie-analyse de mens altijd nog een belangrijke rol spelen.
Zo is er betrokkenheid van de mens nodig om de context te duiden, analyse-componenten te variëren en een inschatting van betrouwbaarheid en relevantie te maken. Datavisualisatie is er opgericht de menselijke betrokkenheid te optimaliseren. Visueel gepresenteerde gegevens worden immers sneller en effectiever geïnterpreteerd dan verbale of numerieke weergaves. In dit werkpakket

zijn een aantal methoden geëvalueerd en vertaald in richtlijnen voor gebruik. Ook is voor de werkpakketten 1 en 2 een aantal aantrekkelijke opties uitgewerkt.

Zo is voor *Vroegdetectie* (werkpakket 1) een basisontwerp gemaakt voor een interface waarmee snel een indruk kan worden gekregen van de resultaten van zogenaamde anomalieën-detectie in de berichten op social media. De gedachte hierbij is dat rondom een evenement of onderwerp het vroegtijdig gesignaleerd kan worden als de veiligheid extra aandacht verdient.



Figuur 15 Screenshot van de interactieve visualisatie voor vroegdetectie.

In de visualisatie waarvan wij een prototype hebben gebouwd is bewust gekozen voor een aanpak die de gebruiker in staat stelt om de data en de keuzes die door het algoritme gemaakt worden zo volledig mogelijk te kunnen controleren en begrijpen. Onderliggend werkt het algoritme als volgt; eerst worden de inkomende berichten geclassificeerd op enkele dimensies waaronder sentiment en dreigingsniveau. Daarna wordt op basis van de verhoudingen, bijvoorbeeld de verhouding tussen het aantal positieve en negatieve tweets door het algoritme vastgesteld of er in een bepaalde tijdsperiode wel of niet een anomalie is opgetreden. Historische data wordt daarbij gebruikt om het normale patroon te schatten, waarbij een anomalie een significante afwijking is van dit patroon. Deze verhoudingen en de historische data zijn duidelijk terug te vinden in de bovenste staafdiagram, waar in de onderste staafdiagram ook nog het samenspel tussen de verschillende classificaties geïnspecteerd kan worden. Door op een van de balken te klikken kun je zo bijvoorbeeld alle tweets bekijken die zowel met een negatief sentiment als een hoog dreigingsniveau aangemerkt zijn.

Het is buitengewoon relevant om de methoden van dataverrijking af te stemmen op de gebruiker en het door hem te hanteren interface.

Slim samenwerken
In 2012 is op het fenomeen Mobiel Banditisme[3] een inventarisatie uitgevoerd naar de aanpak en aansturing daarvan in de opsporings- en strafrechtketen (Nationale Politie, Openbaar Ministerie), en is op basis van de bevindingen een aantal oplossingsrichtingen voor de geïnventariseerde problemen geschetst.
Als oplossingsrichting voor de eerste bevinding (een snellere en betere awareness over het fenomeen Mobiel Banditisme in beide ketens) is vervolgens een *demonstrator* ontwikkeld als analysehulpmiddel voor de Landelijke Eenheid/Dienst Landelijke Informatie Organisatie (DLIO): de MoB Monitor.
In combinatie met een aantal andere bevindingen is op een workshop in 2012 met vertegenwoordigers van het Ministerie van Veiligheid en Justitie (MinVenJ), de DLIO, de Regionale Eenheid Rotterdam-Rijnmond en Europol de volgende stap geïdentificeerd als meest kansrijke oplossingsrichting: het op basis van een betere informatiepositie effectiever en efficiënter samenwerken binnen en tussen beide ketens op dit fenomeen in de eerste zes uur van aanhouding. Dit moet bewerkstelligen dat een betere aansturing mogelijk is van de schaarse capaciteit in de volgende fasen (drie dagen en drie weken) van aanhouding van personen en/of de identificatie van flexibele netwerken.

In het werkpakket Slim samenwerken is in 2013 voor het fenomeen Mobiel Banditisme verder ingezoomd op het:
- Versnellen van het genereren van inzicht in de mobiele netwerken, en
- Versnellen van de beschikbaarheid van de daaruit voortvloeiende intelligenceproducten (op landelijk niveau) voor het districtsniveau, om zo een snellere herkenning van verdachten te bewerkstelligen.

Naast een verdere uitwerking van de MoB Monitor (De MoB Monitor Light) en de toepassing ervan bij woninginbraken, is inzicht verkregen in het verbeteren van de samenwerking tussen politie en OM. Speciale aandacht ging uit naar de meerwaarde van de landelijke intelligenceproducten voor het OM en de uitwerking van het programma ZSM (Zo Snel, Slim, Selectief, Simpel, Samen en Samenlevingsgericht Mogelijk) op de aanpak Mobiel Banditisme. Hiermee is een basis gelegd voor een nader uit te werken meer geïntegreerde ondersteunende informatie-omgeving voor de samenwerking tussen de politie en het OM.

Naast samenwerking tussen de opsporings- en strafrechtketen zijn er private partijen die met de publieke partijen samenkomen in de keten voor de bestrijding van Mobiel Banditisme. In 2013 heeft TNO in opdracht van MinVenJ de studie “Ondersteuning GIO Mobiel Banditisme” uitgevoerd. Hierin is door TNO een inventarisatie gemaakt van de wensen voor een Gemeenschappelijke Informatie Organisatie (GIO) en zijn er aanbevelingen gedaan voor de inrichting ervan.
Deze GIO moet als Publiek Private Samenwerking leiden tot een betere informatiepositie voor de bestrijding van Mobiel Banditisme en heeft een sterke relatie met de ontwikkelingen in dit werkpakket.

Digitaal leiderschap en digitale dilemma’s
Diverse bestuurders - ook vanuit het ministerie van Veiligheid en Justitie – hebben signalen laten horen dat door de opkomst van de sociale media er dringend behoefte is aan versterking van de digitale leiderschapskwaliteiten op bestuurlijk niveau. Daarop is besloten met steun van het Nederlands Genootschap voor

[3] Vermogensdelicten gepleegd door Mobiel Banditisme zijn onder andere winkeldiefstal, voertuigcriminaliteit (inclusief ladingdiefstal) en woninginbraken

Burgemeesters een extra scenario voor de burgemeestersgame te ontwikkelen. In het nieuwe scenario komen meerdere dilemma's uit het veld naar voren waarover tot en met het bestuurlijke niveau beslissingen gemaakt moeten kunnen worden. Incidenten als de 'kopschoppers van Eindhoven' met dilemma's rondom burgeropsporing via internet, het sluiten van de scholen in Leiden na een dreigbericht op 4Chan en Project X Haren met grootschalige mobilisatie via social media zijn inspiratie geweest om een fictief doch realistisch scenario samen te stellen. In de game omgeving van Thales/T-XChange is het scenario vervolgens ingevoerd om een speelbare versie te krijgen. Het scenario kan op aanvraag gespeeld worden door een groep van bestuurders. Bij het scenario hoort een handleiding met extra achtergrondinformatie.

Figuur 16 Een screen uit de burgemeestersgame voor het scenario 'omgaan met sociale media'.

De Burgemeestersgame is als 'web based' trainingsinstrument beschikbaar via de Academie voor Crisisbeheersing van het IFV. Momenteel wordt er met de Nationale Politie bekeken hoe het ook daar ingezet kan worden nadat vanuit de top van de NP erg veel enthousiasme is getoond. Begin 2014 zal de lancering van het nieuwe 'digitale' scenario gepaard gaan met een evenement waarbij o.a. Rob Bats (nu burgemeester van Terschelling) heeft aangegeven graag te helpen met het initiatief om de noodzaak van digitaal leiderschap op die manier breder onder de aandacht te brengen. Naast de lancering middels een evenement om de doelgroep te laten weten dat er met een nieuw scenario getraind kan worden, zal er een train-de-trainer sessie worden verzorgd zodat er voldoende trainers zijn die de game kunnen begeleiden.

3.3.3 Publiciteit

- [A. de Vries, 2013] Arnout de Vries, c.s., *Informatie die stuurt!*, Slimmer omgaan met grote hoeveelheden informatie in de veiligheidsketen, Resultaten van topic 3 in 2013, Bedrijfsvertrouwelijk TNO-rapport, december 2013.
- [Kaptein, 2013a] Rianne Kaptein, Egon L. Van den Broek, Gijs Koot, Mirjam A.A. Huis in 't Veld, 2013, *Recall oriented search on the web using semantic annotations*, Proceedings of the sixth international workshop on exploiting semantic annotations in information retrieval (ESAIR '13). ACM, New York, NY, USA, 45-48.

- [Kaptein, 2013b] Rianne Kaptein, Gijs Koot, Mirjam A.A. Huis in 't Veld, Egon L. Van den Broek,2013, *Needle Custom Search, Recall-Oriented Search on the Web using Semantic Annotations* (ECIR '14).
- NGB Burgemeestersgame: acht dilemma's in 15 minuten. http://www.burgemeesters.nl/seriousgame
- IFV (infopunt veiligheid), 'Train de trainerscursus Burgemeestersgame' http://www.infopuntveiligheid.nl/DossierItem/113/3817/train-de-trainercursus-burgemeestersgame-.html

Voordrachten

- 14-18 januari 2013, Analyse Project X Haren met als resultaat oa een film: http://www.youtube.com/watch?v=5WZL-h7J9UA en blog: http://socialmediadna.nl/category/cases/projectxharen-cases/
- 6 februari 2013: Dag van de Ambtenaar 2.0*. Project X Haren: impact van social media op openbare orde*. Zie http://www.slideshare.net/ArnoutdeVries/project-x-impact-of-social-media-on-publicsafety
- 4 april 2013: Dag van de Veiligheidsregio: TNO aanwezigheid middels workshops (oa over meldkamer van de toekomst, RTIC en social media) en stand met demo's.
- 9 april 2013: Studiedag manifestaties en Evenementen met KCEV: presentatie *Project X: impact van social media op evenementen*.
- 12 juni 2013: Landelijke dag opsporingsberichtgeving: Presentatie *Opsporing Verzocht en social media*.
- 18 juni 2013: Communicatie symposium (Communicipals) 'communiceren over (on)veiligheid' bij Johannes Post Kazerne. Presentatie: *Impact van social media op veiligheid.*
- 18 september 2013: Social Media Club Amsterdam: social media en georganiseerde misdaad. Georganiseerd met politie Amsterdam en OM. Zie: http://socialmediadna.nl/smc-amsterdam-rol-van-sociale-mediabij-georganiseerde-misdaad/
- 3 oktober 2013: NIK themadag. TNO verzorgde hier een informatiestand waar diverse innovaties werden getoond. http://www.nikthemadag.nl/
- 22 oktober 2013: Opsporingsdag met proceseigenaren opsporing: *Social media - Het Nieuwe DNA*
- 5 november 2013: Symposium Voorspellen en beïnvloeden van gedrag met sociale media met presentatie *Social media- The Good, the Bad and the Ugly,* http://socialmediadna.nl/sonm/
- 18 december 2013: Domeinvakdag school voor de recherche (team intelligence): 'Hoe blijf ik effectief met Big Data?'

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.

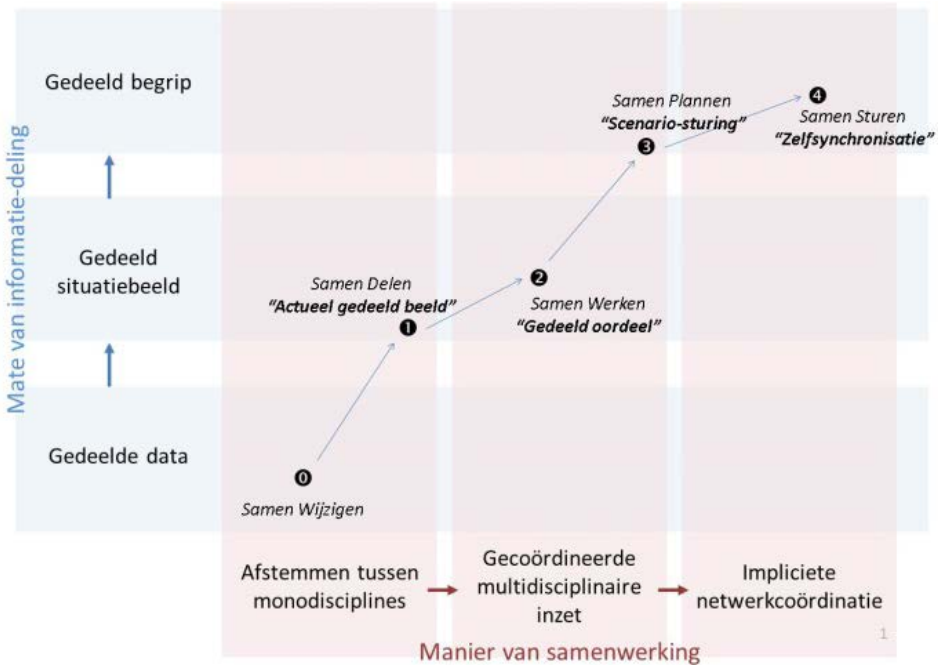
Onderzoeksuitdagingen die daarmee gepaard gaan zijn:

1. Hoe bereiken we dat genetwerkte organisatiedelen voldoende vertrouwen
2. hebben in (bereid zijn afhankelijk te zijn van) elkaar en van techniek?
3. 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?
4. 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?
5. Welke rolgerichte gebruikersinterfaces zijn nodig voor het creëren van op elkaar afgestemde situational awareness en coördinatie van taken?
6. 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 veiligheids-veld op gang. Een volgende stap is publiek private netcentrische informatie-voorziening, 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.

Met het landelijk project netcentrisch werken is door samenwerking van de veiligheidsregio’s en TNO de informatievoorziening van de grond gekomen. Daarom zet TNO nu in op het vergroten van haar kennis over de volgende stap *samen werken* in het groeimodel netcentrisch werken. Afgelopen jaren (2011 en 2012) heeft het team van TOPIC4 kennis op gedaan over knelpunten die hierbij

naar voren komen; aansluitend zijn daar interventies voor ontwikkeld. In 2013 zijn deze interventies verder uitontwikkeld en gevalideerd, zodat deze hun weg kunnen vinden naar veiligheidsregio's en hun betrokken ketenpartners.

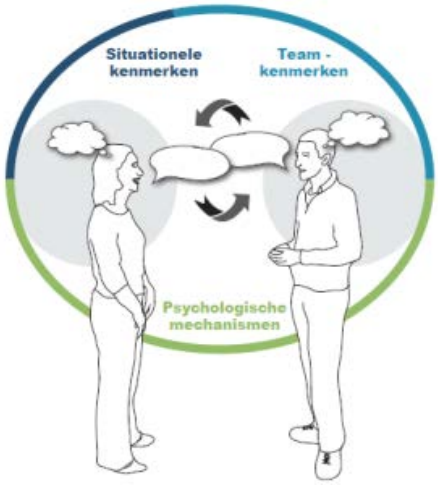


Figuur 17 Groeimodel Netcentrisch werken.

3.4.2 Gerealiseerde samenwerken tussen veiligheidsorganisaties voor crisisbeheersing en rampenbestrijding

De kennisbank (2012) is uitgebouwd naar een supporttool 'expertise selectie' voor hoogwatersituaties (2013). Hierbij is gekozen om aan te sluiten bij nieuwe ontwikkelingen binnen het IFV, waarbij informatie (bijv. over GRIP0 incidenten bij gemeenten) via een infographic beschikbaar komt. Hiermee wordt een offline product gecreëerd dat overzicht geeft en ook direct als geheugensteuntje en aantekeningblad gebruikt kan worden. TNO heeft op basis van kennis opgedaan uit dit en andere projecten de basis gelegd voor de infographic over hoogwatersituaties.

Het MIRRORraamwerk is in 2013 verder uitgewerkt in een training, die getoetst is in de veiligheidsregio Utrecht. De trainingen zijn goed ontvangen en worden ingezet als een aanvulling op het huidige aanbod. De meerwaarde hiervan is dat er inzicht gegeven wordt in de verschillen die kunnen ontstaan tijdens een samenwerking en die – indien niet tijdig gesignaleerd – voor grote problemen kunnen zorgen. Bewustzijn van deze factoren bij enkele teamleden zorgt dat problemen vroegtijdig gesignaleerd en geadresseerd worden, waarna interventies gepleegd kunnen worden om verder escalatie te voorkomen. Een makkelijk voorbeeld is dat iedereen zijn eigen referentiekader heeft. Iets ingewikkelder wordt het al als je je realiseert dat iedereen met een andere bril (focus) naar dezelfde situatie kijkt.

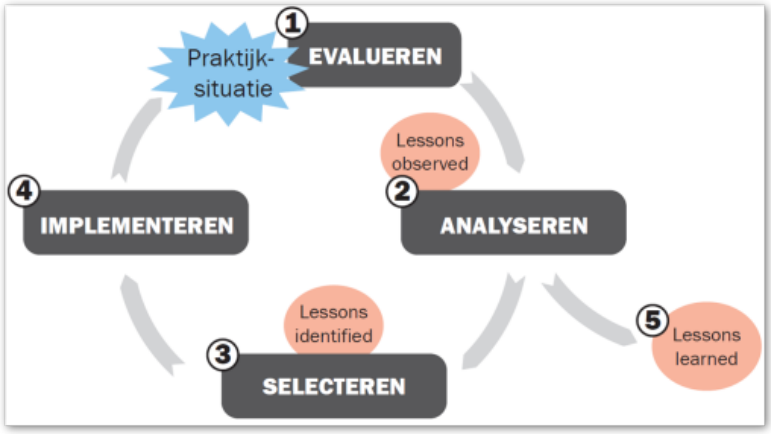


Figuur 18 illustratie uit de instructie voor de MIRROR-training.

Multidisciplinaire leerketen

Afgelopen jaren is steeds beter in kaart gebracht welke fasen er zijn bij het sluiten van de leerketen (2011) en wat er binnen de brandweer al gebeurt om lessen uit inzet en oefeningen te verzamelen en te analyseren om er ook daadwerkelijk van te leren. In 2013 zijn we verder gegaan om dat beeld verder te completeren.
Wat gebeurt er al in de veiligheidsregio's? Dan blijkt dat er diverse goede initiatieven zijn in diverse regio's, zonder dat men van elkaar op de hoogte is.
Er blijven echter ook zaken liggen omdat de urgentie wel gevoeld wordt op de werkvloer, maar het is moeilijk die urgentie zichtbaar en voelbaar naar bestuurders en beleidsmakers door te geven. De Inspectie VenJ constateert in het rapport Staat van de rampenbestrijding 2013) dat een aantal veiligheidsregio's de eigen prestaties tijdens incidenten en oefeningen nauwelijks evalueren. Zij hebben hierdoor slechts zeer beperkt inzicht in de eigen operationele slagkracht. Ook wordt in dit rapport gesteld dat de veiligheidsregio's door de toenemende oefendruk maar beperkt in staat zijn om op basis van een risicoanalyse prioriteiten te stellen in oefeningen en een daadwerkelijke leercyclus toe te passen.
Met behulp van onze leerketen kunnen we helpen inzichtelijk maken hoe oefenen en anders evalueren kunnen leiden tot meer verbetering. Daarvoor is het nodig om (systematisch) te kijken welke observaties moeten worden opgevolgd, welke interventies daarop ontwikkeld moeten worden, en aanpassingen moeten worden getest om te kijken of het tot gewenste resultaten leidt. Vervolgens moeten de werkwijze en opleiding aangepast worden. Pas dan kunnen we spreken van leren.
Met die boodschap helpen we MOTO en haar leden om de ontwikkeling van de leerketen op de agenda te krijgen. Daarmee wordt het hele oefenveld in context en perspectief geplaatst.
Wij kunnen bij elke stap de 'best practices' uit de praktijk inbrengen. Nadrukken sluiten we aan bij initiatieven uit de praktijk, zoals de resultaten van het WODC-onderzoek naar evalueren[4]. Verder passen onze resultaten en adviezen goed binnen de constateringen van de commissie Hoekstra die de wet op de veiligheidsregio's onderzocht en constateerde dat er noodzakelijk aandacht moet komen voor multidisciplinaire samenwerking en multidisciplinair oefenen en leren.

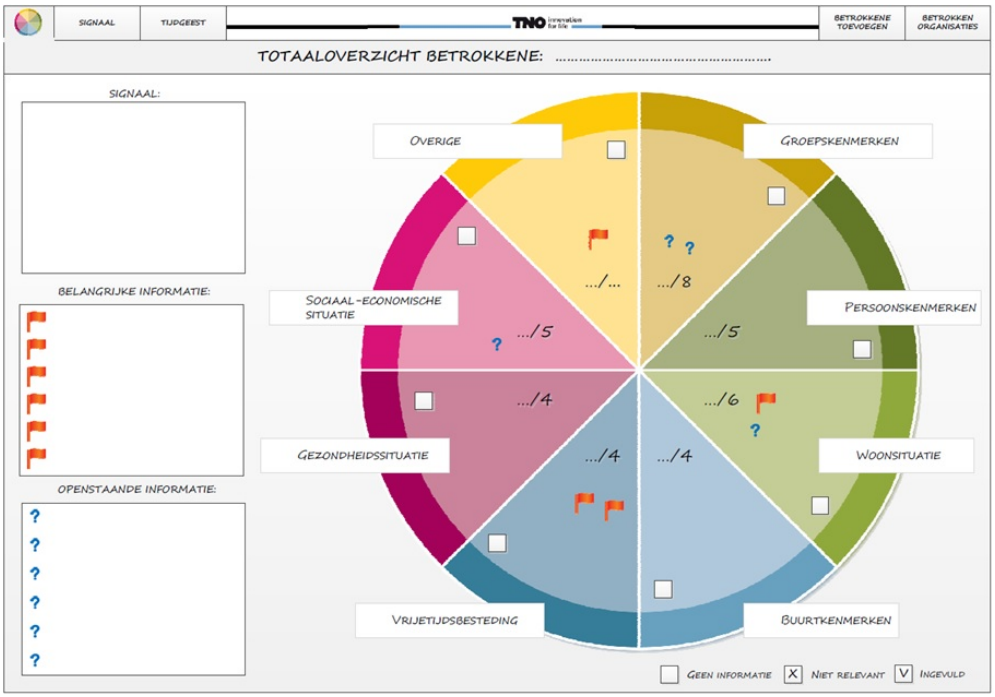
[4] http://www.wodc.nl/onderzoeksdatabase/ontwikkeling-evaluatie-crisis.aspx?cp=44&cs=6796



Figuur 19 Model voor de ontwikkeling van de leercyclus.

Samenwerking in het veiligheidsdomein

In 2012 zijn de werkzaamheden voor dit werkpakket gestart en hebben we een eerste onderzoek gedaan naar een preciezere vraagstelling. Samen met een kleine groep ambassadeurs (abtenaren openbare orde en veiligheid uit diverse gemeenten) is daar in 2013 aan doorgewerkt. Op basis van de onderzoeken van TNO is concept-tool VISI (**V**eiligheids**I**nformatie bij **Si**gnalering) ontstaan welke een beeld geeft welke informatie men (nodig) heeft om een sociaal incident te kunnen duiden. Deze eerste stap van duiding is noodzakelijk om een totaalbeeld van de situatie te krijgen of te kunnen opstellen. Dat totaalbeeld ligt ten grondslag aan de verdere aanpak van het incident.



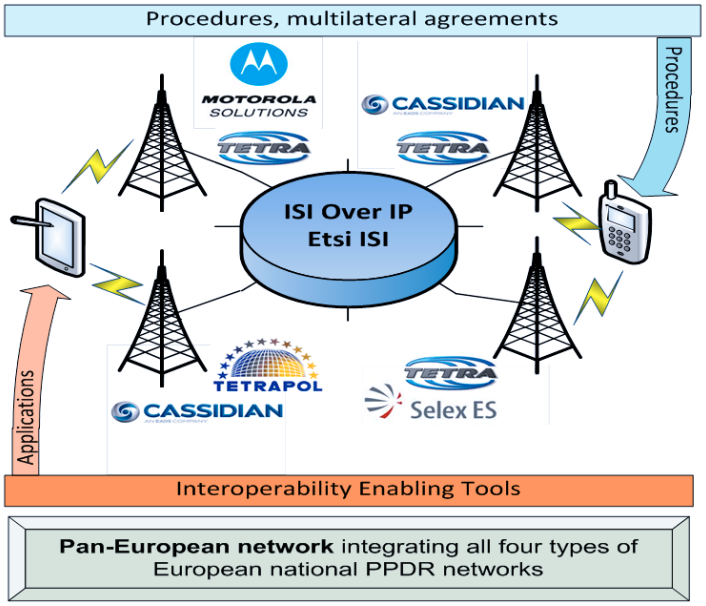
Figuur 20 Processchema uit het VISI-tool voor duiding van sociale veiligheidsincidenten.

Aansluitende werkzaamheden in projecten met matchende financiering uit het VP
De werkzaamheden van het topic 4 team sluiten goed aan bij het onderzoek in het Europese project BESECURE, waarin de Gemeente Den Haag participeert. In dat project worden tools ontwikkeld die ondersteunen bij de vergelijking van interventies. Die interventies zouden (in de toekomst) kunnen worden geselecteerd en voorgesteld op basis van informatie die met behulp van VISI is vastgelegd. Met behulp van de ambassadeurs is een oefening gehouden om de bruikbaarheid van de concept-tool vast te stellen. Vervolgens zijn er nog enkele bijstellingen doorgevoerd, zoals het direct toevoegen van bepaalde informatie uit het fysieke domein (zoals bereikbaarheid en informatie over gebouwen)

Het EU-programma *Inter System Interoperability for TEtra-tetraPol networks* (ISITEP) is gestart in 2013 (kick-off event 29-30 oktober 2013). Het doel van ISITEP is "*the project will allow first responders of European ISITEP federated countries to seamlessly interoperate overcoming current legal, operational and technological barriers*".
Daartoe zijn er twee objectives geformuleerd:

- *Achieve an operational interoperability among European first responders both at regulative, organizational, operational and at technical level*
- *Standardize the technical improvements obtained by the ISITEP project in the European body, study the scalability of the ISI prototypes at European level, submit its functional model to the specialized European agencies (LEWP, Frontex, ERC…)*

De TNO bijdrage in ISITEP voor 2013 betrof het volgende onderdelen de werkpakketten *Application scenario definition* (WP2.1) en *Security requirements* (WP 2.2). TNO heeft een rapportage opgesteld over het gebruik van scenario's een state of the art overzicht van huidige TETRA / TETRAPOL netwerken bij de verschillende deelnemende landen. Daarnaast is TNO verantwoordelijk voor een security analyse met betrekking tot de dreigingen vanuit interconnectie van infrastructuur en dreigingen met betrekking tot de privacy van burgers.
Meer info over het EU-project is te vinden op de website http://isitep.eu/



3.4.3 Publiciteit

- N. Vink, K.van Buul, J. van de Ven, *De samenhang tussen de werkvelden fysieke en sociale veiligheid*, TNO-Rapport 2012-R11169, januari 2013.
- 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.
- Treurniet, Willem. (2014). Shaping comprehensive emergency response networks. In T. Grant, H. Monsuur & R. Janssen (Eds.), Network Topology in Command and Control: Organization, Operation, and Evolution. Hershey, USA: IGI Global.

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 cybersecurity 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 incidentgegevens 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.

Topic 5 kent in 2013 de volgende doelstellingen:

1. Het definiëren van doelen, use cases, eisen en een informatiemodel voor het genereren van een geaggregeerd beeld.
2. Inventarisatie en testen van methoden & technieken voor cybersecurity informatie uitwisseling en creëren van gezamenlijk geaggregeerd beeld.

3. Te komen tot ondersteunende methoden en modellen voor de uitwisseling van ‘security posture’ en gegevens die de cyberstatus van de vitale infrastructuur (gedeeld ICT-risicobeeld) en de effectiviteit van beschermingsmaatregelen inzichtelijk maken.

Ondersteunend aan elk van deze onderzoekdoelstellingen:

4. Het ontwikkelen van een modellenbasis als ondersteuning bij het herkennen van mogelijke cyberaanvalspatronen 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.

Detectie van misbruik en opbouwen geaggregeerd beeld

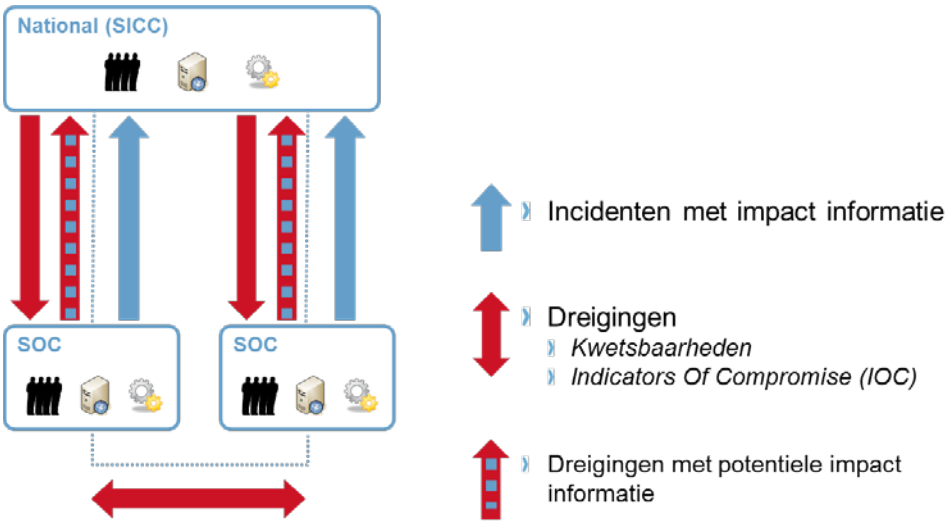
Een groot aantal organisaties beschikt over detectiesystemen die misbruik binnen de eigen organisaties proberen te detecteren. Om hieruit een geaggregeerd beeld op te kunnen bouwen is het nodig om de informatiebehoefte en mogelijk uit te wisselen gegevens tussen organisaties te identificeren.
Voor het onderzoek binnen dit topic wordt de nadruk gelegd op de informatiebehoefte vanuit de overheid om te komen tot een geaggregeerd beeld en te onderzoeken welke methoden en technieken nodig zijn om gegevens uit verschillende bronnen te combineren in een gezamenlijk geaggregeerd beeld. Hierbij wordt naast de technische aspecten en mogelijkheden ook aandacht besteed aan organisatorische aspecten van het delen van vertrouwelijke gegevens over verschillende organisaties.
Binnen dit onderwerp wordt nauw samengewerkt met het bedrijfsleven binnen het aanpalende VP Security onder de topsector HTSM. In het VP Security worden in samenwerking met bedrijven de technische mogelijkheden voor monitoring en het verzamelen en analyseren van gegevens verder uitgewerkt. Hiervoor wordt samengewerkt met mogelijke leveranciers (bijv IBM, maar indien mogelijk ook met SOC’s van bedrijven).

Het onderzoek rond detectie richt zich op het ontwerpen en testen van een mogelijk systeem waarmee het geaggregeerd operationeel beeld van cybersecurity in Nederland kan worden gerealiseerd. Zo’n systeem bestaat feitelijk uit een infrastructuur voor het delen van operationele cybersecurity informatie en systemen voor het creëren van een geaggregeerd beeld van cybersecurity in Nederland (ook wel situational awareness en Common situational Picture genoemd). Doel van het project is het opstellen van een blueprint met daarin een ontwerp van het system zowel op technisch als organisatorisch vlak en het testen van technieken waarmee het systeem gerealiseerd kan worden.
Het project wordt opgedeeld in drie onderdelen:

1. Definiëren van doelen, Use Cases, eisen en informatie model voor geaggregeerd beeld.
2. Inventarisatie en testen van methode & technieken voor cyber security informatie uitwisseling en creëren van COP (binnen het VP security onder de Topsector HTSM).
3. Ontwerp van een systeem voor geaggregeerd operationeel beeld van cyber security in NL.

De activiteiten van dit werkpakket richtten zich op het onderzoeken van de informatiebehoefte van het Ministerie van Veiligheid en Justitie en in het bijzonder het NCSC. Hiervoor zijn in nauwe samenwerking met het NCSC een aantal use cases gedefinieerd. Vervolgens is geanalyseerd welke typen informatie-uitwisseling in deze situaties nodig is.

Op basis van deze informatiebehoefte is onderzocht wat de technologische mogelijkheden zijn. Deze werkzaamheden vonden plaats in samenwerking met het VP onder de Topsector HTSM, zodat nauw kon worden samengewerkt met het bedrijfsleven (bijvoorbeeld IBM, HP).
De studie onderkende dat het delen van cybersecurity informatie twee doelen kan dienen. Enerzijds het verhogen van de weerbaarheid van de (vitale) cyber infrastructuur, anderzijds het verhogen van de situational awareness om zo grootschalige verstoring tijdig te kunnen detecteren. Om dit te bereiken is een infrastructuur vereist om de cybersecurity informatie die beschikbaar is binnen de ene organisatie op een adequate en veilige manier te kunnen delen met andere organisaties.



Figuur 21 high level overzicht informatiestromen.

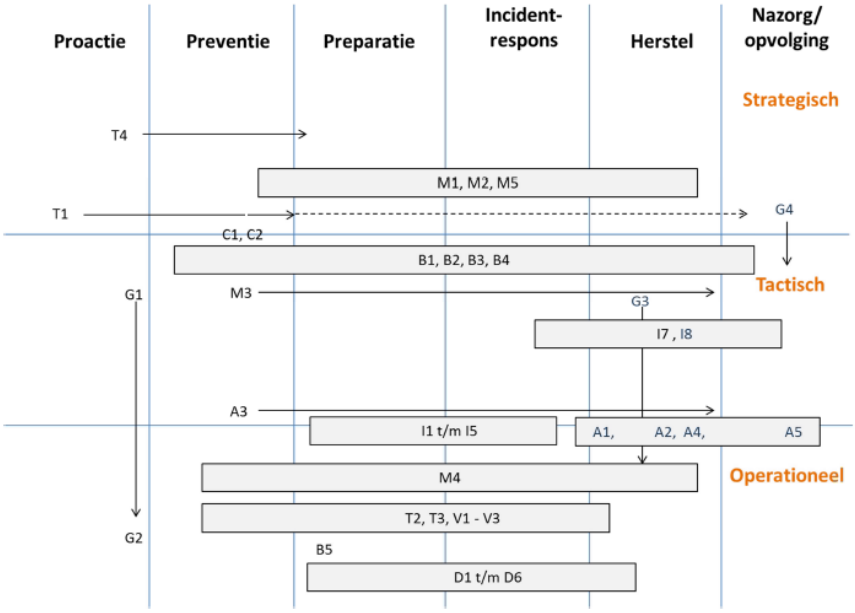
De huidige state of the art op het gebied van protocollen en standaarden om bovenstaande informatie geautomatiseerd uit te kunnen wisselen is in afdoende mate beschikbaar voor dreigingsinformatie maar op het gebied van impactinformatie (t.b.v. detectie grootschalige verstoringen) bestaat een gap.
De standaarden en protocollen STIX en TAXII van MITRE geven hierbij het beste invulling aan de gestelde behoeften. ITU-T en IODEF lijken hier minder geschikt.
Er is op dit vlak ook slechts zeer beperkt tooling beschikbaar ten behoeve van de genoemde doelen. Er zijn commerciële ontwikkelingen zichtbaar, waarvan de scope echter beperkt is, en zodoende afdoende zijn binnen één organisatie, maar welke niet toegepast kunnen worden voor cybersecurity informatie uitwisseling tussen organisaties. Verder zijn er enkele tools beschikbaar vanuit CERT-organisaties. Binnen deze tools valt op dat deze allemaal de nadruk hebben op het verzamelen en communiceren van de al bekende cybersecurity informatie. Tijdens de testen komt duidelijk naar voren dat het maturity level van de genoemde tools nog niet ver gevorderd is.

Cybersecurity status van de Nederlandse vitale infrastructuur
Zowel nationaal als internationaal vindt samenwerking en gegevensuitwisseling plaats over dreigingen, kwetsbaarheden, tegenmaatregelen en onderliggende modellen. In deze onderzoekslijn wordt onderzocht welke methoden en tools kunnen ondersteunen bij informatie-uitwisseling over dreigingen, kwetsbaarheden en good practices. Tevens wordt onderzocht welke methoden kunnen ondersteunen bij het beoordelen van de cyberstatus van organisaties in de vitale infrastructuur.
In 2013 is een nationale en internationale inventarisatie uitgevoerd van methoden en technieken voor het delen van informatie. Hierbij is een onderverdeling gemaakt tussen de verschillende typen informatie zoals gegevens over kwetsbaarheden en dreigingen, nieuwe technologische ontwikkelingen, en incidenten. Per categorie wordt aangegeven wat good practices zijn, bijvoorbeeld om gegevens vertrouwelijk te kunnen delen. Tevens wordt gezocht naar mogelijkheden om de informatie meer toegankelijk te maken, ook sector-overstijgend, rekening houdend met de vertrouwelijkheid van de gegevens. Hierbij wordt ook gekeken naar de benodigde definities en standaarden om de gegevens eenduidig te kunnen uitwisselen.

Er is een inventarisatie uitgevoerd naar internationale ontwikkelingen op het gebied van informatie-uitwisseling van cybersecurity-relevante informatie. Deze inventarisatie laat de volgende trends zien:

- Aanvulling op de kleinschalige informatie-uitwisseling binnen de sector met ontwikkelingen naar cross-sectorale informatie-uitwisseling en zelfs over landgrenzen heen;
- Toenemende aandacht voor internationaal delen van informatie binnen vertrouwde samenwerkingsverbanden (CERTs, NAVO, internationale oefeningen);
- Een verschuiving van informatie-delen in face-to-face meetings in kleine vertrouwde verbanden naar elektronische vormen van informatie-uitwisseling.
- Een verschuiving van informatie-uitwisseling naar meer geïntegreerde analyse (meer nadruk op de AC-component van een ISAC).

Daarnaast is een inventarisatie uitgevoerd van de verschillende typen informatie die worden uitgewisseld. Hiervoor is eerder werk van een NAVO werkgroep als startpunt gebruikt. Deze is vervolgens aangepast en aangevuld voor civiel gebruik. Vervolgens zijn de onderkende elementen geanalyseerd en ingedeeld aan de hand van een aantal belangrijke dimensies voor informatie-uitwisseling.
Op basis hiervan is een eerste framework van informatie-elementen opgesteld en zijn randvoorwaarden voor het delen van cyber-security gerelateerde informatie geïnventariseerd.



Figuur 22 overzicht van het framework voor het delen van cyber-security gerelateerde informatie.

Vervolgens is een aantal analyses uitgevoerd aan de hand van het framework. Het betrof de verschillende standaarden die van belang zijn voor de informatie-elementen, de gevoeligheid van de informatie en de mate waarin deze tijdkritisch is.

Informatie-element	Direct bruikbaar	Voldoet vrijwel geheel aan behoefte	Aanknopings-punten en ontwikkelingen
M - Sharing cyber situational awareness Metrics			
M1 – Cyber alert level		Vereist vertaling en implementatie in Nederland	Niveaus in MS-ISAC cyber alert level en InfoCon [31]
M2 – Incident global metrics / summary statistics			Incidentstatistieken in Cyber Security Beeld Nederland; VERIS
M3 – Vulnerability assessment metrics		CWSS en CVSS/CCSS (te koppelen aan nationale risico-methodiek)	CWSS, CVSS en CCSS

Figuur 23 een deel van het overzicht van standaarden.

Ondersteunende modellen

Cybersecurity is een belangrijk onderwerp binnen een groot aantal sectoren en organisaties. Hierbij spelen binnen elke sector echter specifieke eigenschappen en kan ook de impact van verstoringen sterk uiteen lopen. Met behulp van modellen kan getracht worden de verschillen en overeenkomsten in beeld te brengen en onderling te vergelijken. Er zijn beschrijvende/ kwalitatieve modellen die de onderlinge relaties in beeld brengen, op keteneffecten gerichte modellen die zich richten op het in kaart brengen van de impact van cascade-effecten van verstoring, specifiek op kosten gerichte modellen, meer gedetailleerde modellen voor het analyseren van het ontwerp van netwerken (bijvoorbeeld voor het evalueren van mogelijke beveiligingsmaatregelen), en modellen en systemen voor de

ondersteuning van oefenen en trainen. Elk van deze modellen kent zijn specifieke doelgroepen en toepassingen.

Op basis van de uitgevoerde inventarisatie zijn een aantal kansrijke onderwerpen gedefinieerd voor het ontwikkelen van nationale modellen welke zijn getoetst op toepasbaarheid in een workshop met NCSC en DCS (oktober 2013).
Op basis van de workshop is de behoefte aan modellen bij het NCSC aangescherpt. Er bestaat het meest behoefte aan inzicht in de afhankelijkheden oftewel keteneffecten van storingen/aanvallen binnen vitale sectoren, met de nadruk op het cyber perspectief.

Elk van deze omgevingen kent specifieke voor- en nadelen.
Voor het modelleren van de verschillende netwerken en de mogelijke keteneffecten, bestaan verschillende typen modellen, variërend van topologische, sterk geabstraheerde mathematische modellen, via een meer op de services van de infrastructuur gerichte benadering, tot gedetailleerde representatie van de onderlinge netwerken en hun fysieke componenten..

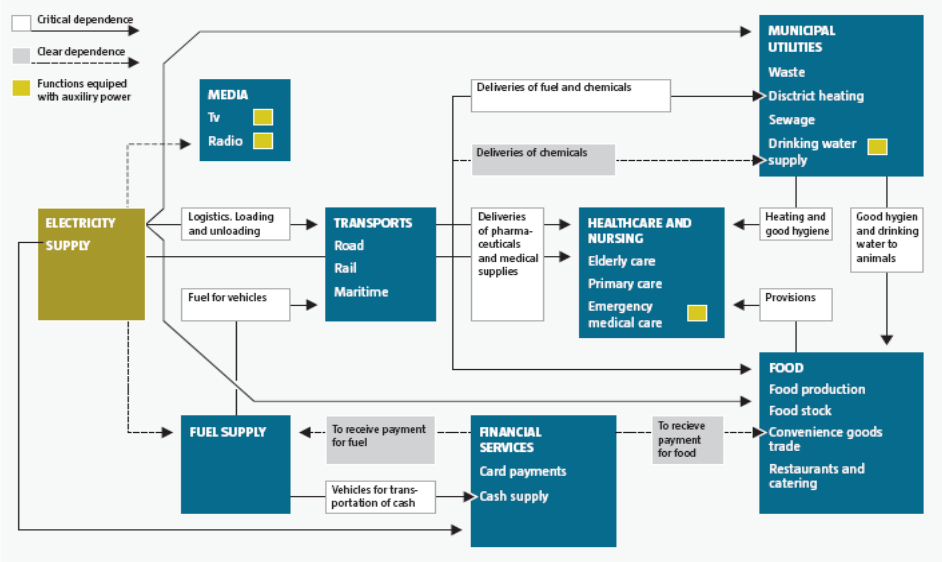
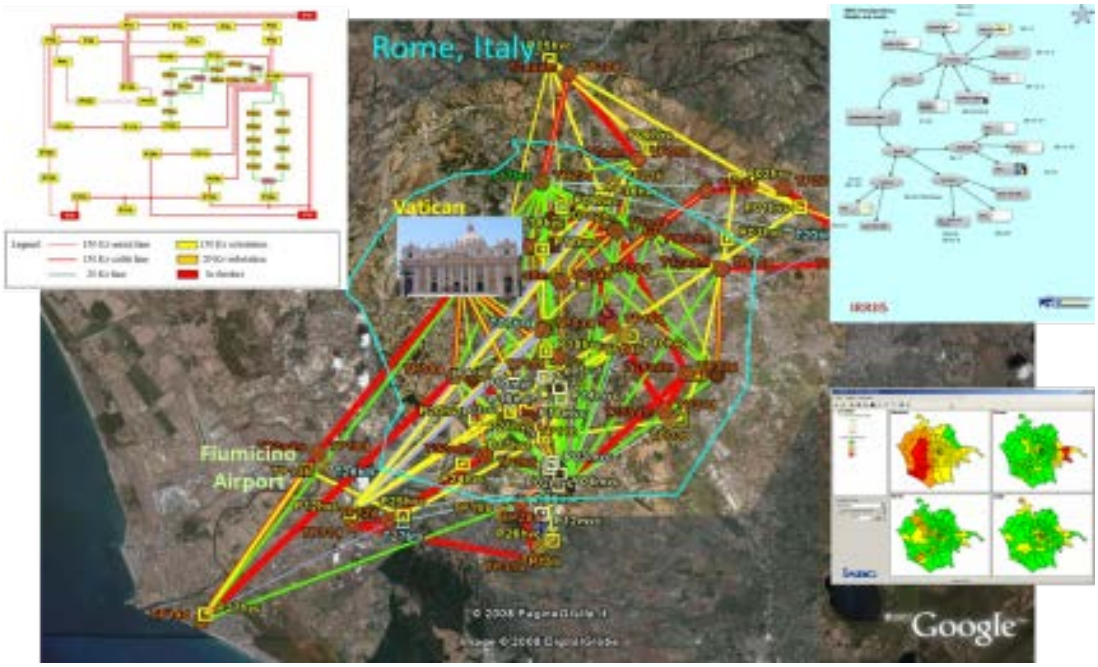


Figure 1. Focus chain:
Are functions with auxiliary power secure?

Voorbeeld – optie 1, methodiek MSB.
Voorbeeldvraagstelling: hoe afhankelijk is de maatschappij van elektronische communicatie ?

- globalere analyse op serviceniveau →nadeel,
- effecten minder gedetailleerd in beeld →voordeel,
- minder gedetailleerde input nodig,
- minder gevoelig voor wijzigingen.



Voorbeeld – optie 2, gedetailleerde simulatie.
Voorbeeldvraagstelling: welke componenten zorgden voor de grootschalige storing in Rome en wat waren mogelijke maatregelen?
- meer gedetailleerde analyse mogelijk,
- gedetailleerde input nodig→ nadeel,
- dynamiek te laten zien→ voordeel,
- meer gedetailleerde analyses,

Deze opties worden verder uitgewerkt in samenwerking met het NCSC.
Daarnaast wordt binnen dit werkpakket wordt samengewerkt met internationale partners, met name op het gebied van modellen voor de vitale infrastructuur (binnen het project CIPRNet) en binnen NAVO verband.

Versterking van de samenwerking rond cybersecurity
Voor elk van de onderzoeksonderwerpen is in het afgelopen jaar samenwerking met de universiteiten gezocht, onder andere door het gezamenlijk werken aan voorstellen in het kader van de NWO call voor cybersecurity. Daarnaast is ook samenwerking in Europese onderzoeksprojecten gestart (o.a. Cyspa en CAPITAL). Daarnaast is samengewerkt met het bedrijfsleven en andere stakeholders binnen het innovatiehuis Cyber van de HSD.

3.5.3 Publiciteit

- T. Hartog, F. Fransen, E.G. Broenink, A. Smulders; Cyber security informatie uitwisseling: Security intelligence voor situational awareness en automatisering van security operatien, december 2013.
- H.A.M. Luiijf, M.H.A. Klaver, R. Wolthuis, S.J.C. van Hooft: Cross-sector Information Sharing, december 2013.
- Luiijf, Eric; Hartel, Pieter (Eds.), Critical Information Infrastructures Security, 8th International Workshop, CRITIS 2013, Amsterdam, The Netherlands, September 16-18, 2013, Revised Selected Papers, Lecture Notes in Computer Science, Vol. 8328, Springer, Heidelberg, 2013

- Luiijf, H.A.M, Besseling, K., De Graaf, P., *Nineteen National Cyber Security Strategies*, International Journal on Critical Infrastructures (IJCIS), V9 N1/2, 2013, pp.3-31.
- Bijlsma, T,. de Kievit, S., van de Sluis, J., van Nunen, E., Passchier, I., Luiijf, E., Security Challenges for Cooperative and Interconnected Mobility Systems, in: Luiijf, Eric; Hartel, Pieter (Eds.), Critical Information Infrastructures Security, 8th International Workshop, CRITIS 2013, Amsterdam, Lecture Notes in Computer Science, Vol. 8328, Springer, Heidelberg, 2013, pp 1-15
- Luiijf, Eric. "Next Generation Information-Based Infrastructures: New Dependencies and Threats." Critical Information Infrastructure Protection and Resilience in the ICT Sector. IGI Global, 2013. 304-317. Web. 7 Feb. 2013. doi:10.4018/978-1-4666-2964-6.ch015
- Luiijf, H.A.M., Besseling, K., Spoelstra, M., de Graaf P., *Ten National Cyber Security Strategies: a Comparison*: Critical Information Infrastructure Security,in: S.Bologna et al. (eds.) Lecture Notes in Computer Science (LNCS) Volume 6983, Springer, pp. 1-17, 2013.
- Luiijf, E., Klaver, M., Zijderveld, A., Huyskes, E., "*CIPRNet: Critical Infrastructure Preparedness and Resilience Research Network*", in: Magazine nationale veiligheid en crisisbeheersing, Jaargang 11, nr 3, juni 2013, pp 52.
- Luiijf, E., Smulders, A., Kamphuis, P., "Kanttekeningen bij de Europese cyber security strategie", in: Magazine nationale veiligheid en crisisbeheersing, Jaargang 11, nr 2, april 2013, pp 21.
- Proceedings van de CRITIS 2013 conferentie.
- Diverse rapportages van het EU project CYSPA, o.a. impact reports voor verschillende sectoren waaronder energie, de financiële sector, transport en e-government.