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

R10298

Vraaggestuurd Programma 2012-2014
Voortgangsrapportage 2013
VP Security
Thema VII High Tech Systemen en Materialen

Datum	februari 2014
Auteur(s)	dr. ir. J.A. Don
Regievoerend departement	Ministerie van Economische Zaken
Aantal pagina's	40 (incl. bijlagen)
Authorisatie door	I. Haisma, innovatiedirecteur Safety & Security Research
Projectnummer	053.01011/01.02

Samenvatting

1.1 Inleiding

De roadmap *Security* voor de topsector *High Tech Systems & Materials* wordt gedragen door een breed consortium van bedrijven, overheden, TNO, NLR en STW/NWO (zie www.htsm.nl). Onder regie van het roadmapteam Security is het plan 2013 voor TNO-Vraaggestuurd Onderzoeksprogramma Security 2012-2014 opgesteld en in uitvoering genomen. Daarbij gaat het tegelijkertijd om het realiseren van impact op de toekomstige veiligheidssituatie in Nederland, het versterken van het Nederlandse bedrijfsleven en het uitbouwen van de kennisbasis bij TNO: de Gouden driehoek. Dit rapport biedt voor het TNO-management, het roadmap team Security van de topsector HTSM en het voor de topsectoren regievoerend departement Economische Zaken inzicht in de voortgang in 2013.

1.2 Uitvoering

Het VP Security zet in op de technologische uitdagingen die te maken hebben met bedreiging van de veiligheid van onze samenleving. We kijken zowel naar oplossingen die bijdragen aan het voorkomen dan wel beheersen van geweld door opzettelijk handelen, als ook naar oplossingen die de schadelijke effecten van incidenten (crises, rampen) beperken, binnen de domeinen van de volgende vier deelroadmaps:

1. System of systems: voor een geïntegreerde aanpak van de uitdagingen op het gebied van openbare orde, veiligheid en beveiliging is ontwikkeling van concepten voor een ‘systeem van systemen’ essentieel. Hierbij zijn alle stakeholders betrokken.
2. Cyber security: de steeds grotere invloed van ICT op de samenleving vergroot ook het belang van cyberresilience en de bestrijding van cybercrime.
   De groeiende ketenafhankelijkheid van onderlinge verbonden ICT-systemen vereist nieuwe concepten.
3. Sensoren: voor effectieve beveiliging zijn waarnemingen en informatie cruciaal. Er zijn twee invalshoeken:
   a. Actieve sensoren (radars) verder verfijnen en daarmee intelligentere systemen vormen. Nederland heeft hier een excellente positie op het gebied van R&D, en een leidende marktpositie op de toegankelijke wereldmarkt.
   b. Passieve sensoren leveren steeds meer data. Dat vereist nieuwe concepten voor data processing en het filteren van irrelevante data. Er zijn veelbelovende ontwikkelingen op het gebied van intelligente sensoren en zelflerende systemen.

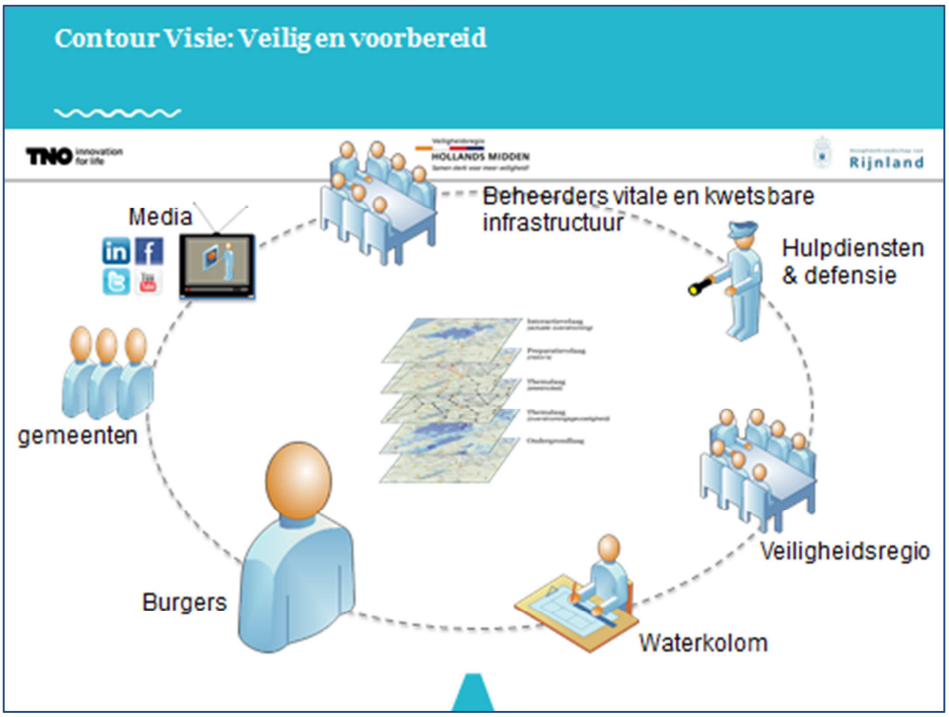
1.3 Resultaten

De belangrijkste resultaten voor de vier deelroadmaps binnen het programma zijn:

1. Deelroadmap Systems-of-systems
In 2013 is het proces voor innovaties van industriële aanbieders in nauwe samenwerking met behoeftestellers uit de veiligheidssector geanalyseerd en vastgelegd in een praktisch toolbook en een white paper *Innovatietoolkit Samen innoveren: politie, bedrijven en kennisinstellingen*.
Verder is samen met het D-CIS lab van Thales een roadmap voor Systems-of-systems opgesteld.
Deze roadmap is behulpzaam bij het identificeren van nieuwe kansen voor onderzoek en ontwikkeling, en wordt gebruikt als discussiestuk in gesprekken met marktpartijen en behoeftestellers.
In het kader van Real Time Intelligence zijn in 2012 met landelijke onderdelen van de politie samenwerkingsambities uitgewerkt. Na de veel omvattende reorganisatie ter vorming van de nationale politie zal hieraan in 2014 een vervolg worden gegeven. In 2013 zijn drie nieuwe clusters van publieke en private partijen gevormd. Dit zijn:

- Beveiliging van de Internationale Zone in Den Haag.
- Omgaan met Big data bij burgerparticipatie voor handhaving en opsporing.
- Informatiepreparatie op overstromingsrisico's.

Als voorbeeld wordt de laatste van deze drie hieronder nader uitgewerkt.



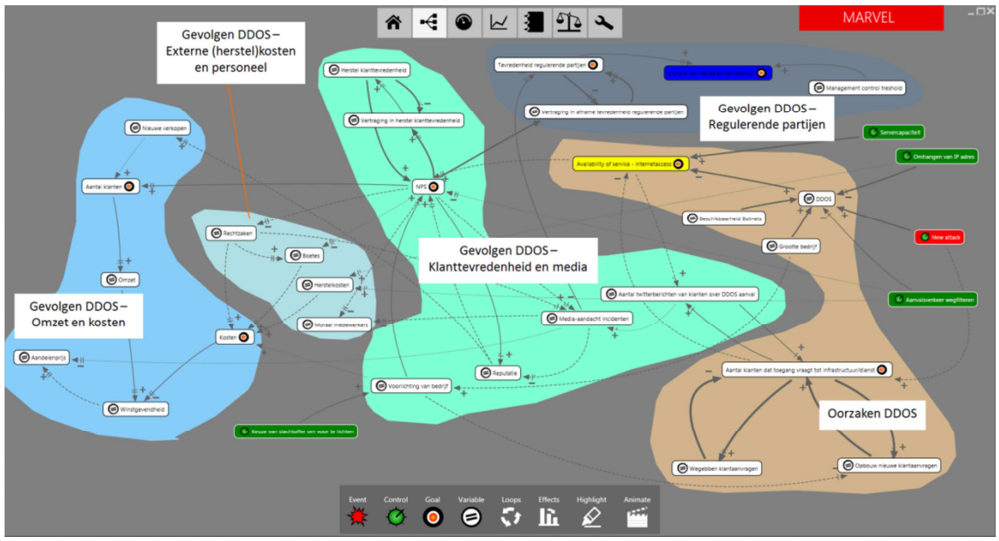
Figuur 1 Stakeholders bij (cascade-effecten van) overstromingen

Het beperken van de effecten van (dreigende) overstromingen is bij uitstek een uitdaging voor complexe samenwerkingen over de grenzen van organisaties heen. Samen met inhoudelijke expertise en financiële bijdragen van de Veiligheidsregio Hollands Midden en het Hoogheemraadschap Rijnland is geïnventariseerd wie welke informatie nodig heeft in zulke situaties. Bijzondere aandacht kreeg het

anticiperen op zogenaamde ‘cascade-effecten’ bij overstromingen (denk bijvoorbeeld aan verkeersinfrastructuur en energievoorziening). Dit initiatief resulteerde in een contour voor een intelligent platform (kaart en kaartlagen), waarmee bij een (dreigende) overstroming belangrijke stakeholders hun eigen maatregelen optimaal kunnen plannen en besluitvorming in de verantwoordelijke gremia voor crisismanagement wordt ondersteund. De bijbehorende roadmap voor samenwerking is enthousiast ontvangen en zal in 2014 leiden tot een ontwikkelingsprogramma met participatie van meerdere veiligheidsregio’s en waterschappen en verschillende ministeries; ook zullen in dat traject industriële aanbieders en bedrijven uit de infrastructurele sectoren aansluiten.

2. Deelroadmap Cybersecurity

Van de vijf in 2012 geïdentificeerde onderwerpen voor gezamenlijke innovatie-trajecten is het opzetten van een CyberSecurityLab in Den Haag afgerond met de opening door DG Schoof van het ministerie VenJ in juni 2013. In het jaar 2013 kwam door de stroom aan cyberincidenten het ontwikkelen van oplossingen steeds hoger op de publieke en private agenda. Voor een toenemend aantal bedrijven is hier sprake van serieuze risico’s voor de continuïteit van de business.
Aan gevalideerde tools om dit inzichtelijk te maken is grote behoefte. Dit was de aanleiding tot het opstellen en uitbrengen van de TNO-publicatie Advanced Risk Management. Eén van hierin opgenomen resultaten is het model voor de beoordeling van de gevolgen van DDOS-aanvallen op bedrijven; hierbij speelt ook het identificeren van bedrijfs- of sectorkenmerken die bepalend zijn voor de kwetsbaarheid.



Figuur 2 Model voor beoordeling van de gevolgen van een DDOS-aanval op een telecom-bedrijf. Met dit model is het mogelijk betrekkelijk snel zicht te krijgen op zowel de aanvalsvector als de impact van een specifieke cyberaanval op een bepaalde sector. Ook de effectiviteit van tegenmaatregelen en bepaalde monitoringsopties is hierin goed te modelleren.

3. Deelroadmap Passieve Sensoren

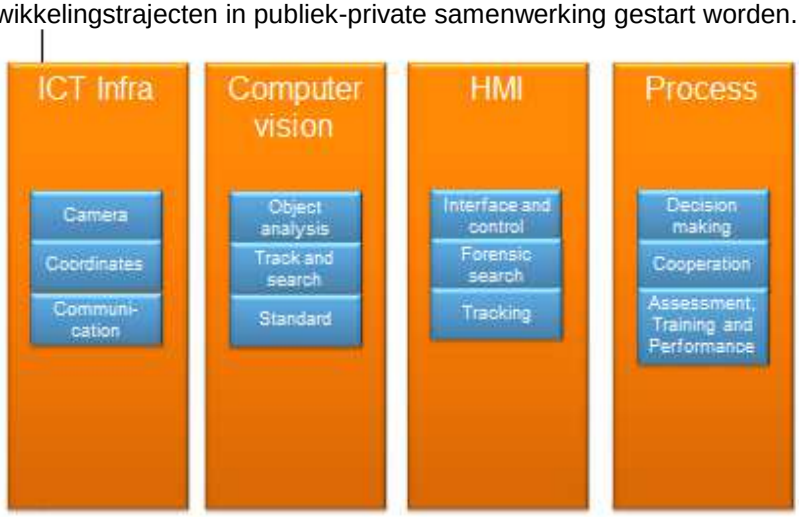
Succesvol veiligheidstoezicht in o.a. luchthavens, openbaar vervoer, beurzen, buitenwijken, musea, overheidsgebouwen, evenementen en grote winkelcentra vereist het vroegtijdig kunnen beoordelen of er sprake is van een op handen zijnde incident, vergrijp of delict. Om met zo weinig mogelijk mens- en machinekracht een zo groot mogelijk veiligheidseffect te bereiken is het inzetten van slimme sensoren

en sensorsystemen van steeds groter belang.
De sterk versnipperde markt is gebaat bij validatie en standaardisatie van te realiseren praktijkoplossingen; TNO acteert hier met het inbrengen van Nederlandse visies in een Europees gedragen roadmap voor Surveillance van de vitale infrastructuur (Thematic Group on Surveillance & Video Analytics van het European Research Network on Critical Infrastructure Protection ERNCIP) .

In 2013 is voor vijf kruispunten van toezichttypen en toepassingsgebieden is met in-kind-bijdragen van het bedrijfsleven gewerkt aan gestructureerde verkenningen (zogenaamde “challenges”) van de kansen om in te spelen op concrete vraagstellingen van probleemeigenaars:

- Volgen en terugvinden van personen op Schiphol.
- Evenementenveiligheid bij de Nijmeegse Vierdaagse.
- Aanpak van woninginbraken onder regie van Nationale politie.
- Crowdmanagement en flow-beheersing op grote, drukke locaties.
- Civiel-militaire samenwerking voor toezichts- en waarnemingstaken.

Verwacht wordt dat in 2014 voor minstens twee van de items concrete ontwikkelingstrajecten in publiek-private samenwerking gestart worden.



Figuur 3 Pijlers van de roadmap voor het volgen en terugvinden van personen op grote luchthavens.

In 2013 zijn ook resultaten geboekt bij technologisch onderzoek aan twee specifieke onderwerpen die aansluiten bij de behoeftes van de LoI ondertekenaars (middellang / lange termijn kennisontwikkeling voor bedrijven):

- afwijkend gedrag detectie op situatie-niveau middels combineren van losse activiteiten om tot ketens van gedrag te komen,
- activiteitsherkenning op signaal- en objectniveau middels wide baseline multi-viewpoint sensoren (camera’s).

4. Deelroadmap Actieve Sensoren

Voor de deelroadmap Actieve Sensoren bestaat er al jaren een intensieve samenwerking tussen Defensie, Thales, TNO en TU-Delft. Er is hier sprake van een Gouden driehoek avant la lettre. In het kader van de Roadmap Security is er in 2013 naast de lopende defensieprogramma’s gewerkt aan een drietal projecten

STARS, MAGNUS en StrICt. Deze ontwikkelingen zijn ook van belang voor toepassingen van actieve sensoren (technologie) buiten defensie.

PPS en aansluiting bij Topsector
In samenwerking met private en publieke stakeholders heeft TNO de ontwikkeling van breed gedragen visies op benodigde lange termijn ontwikkelingen in gang gezet. Gezamenlijke investeringsinitiatieven zijn dichterbij gekomen door de gerealiseerde voortgang met betrekking tot:

- Groei van vertrouwen en intimiteit in relatief korte termijn gerichte PPS-investeringsprojecten.
- Aansluiting bij de meer centrale verankering van innovatie bij politie en veiligheidsregio's.
- Versterking civiel-militaire samenwerking op het gebied van innovatie.
- Ontwikkeling van PPS in de eerste call van het Europese Horizon 2020, inclusief initiatieven voor standaardisatie en interoperabiliteit.

Vanuit het roadmapteam wordt als bredere ambitie benadrukt dat er een uitbouw moet plaatsvinden van de launching customer rol van alle partners uit overheid en bedrijfsleven. In 2013 is door de founding parties van The Hague Security Delta sterk ingezet op structurele versterking van de Publiek-Private-Samenwerking. In februari 2014 resulteerde dit in de opening van een Campus in Den Haag door minister Opstelten. Landelijk wordt dit initiatief gedragen door de regio Haaglanden, Twente en Eindhoven/Tilburg. Naast de formele steun van de ministeries VenJ en Defensie zijn inmiddels maar liefst 180 partijen uit de overheid en het bedrijfsleven aangesloten. De ontwikkelingen vanuit HSD sporen uitstekend met de HTSM-roadmap Security en zullen in toenemende mate richtinggevend zijn voor het VP Security.

Zoals in deze voortgangsrapportage wordt toegelicht zijn er nu PPS-clusters in ontwikkeling voor de volgende vraagstukken bij de behoeftestellers van de overheid:

- Real Time Intelligence in de deelroadmap Systems-of-systems.
- Advanced Cyber-Riskmanagement in de deelroadmap Cybersecurity.
- Toezichtconcepten voor locaties met massa's mensen in de deelroadmap Passieve sensoren.
- Ontwikkeling radartechnologie in de deelroadmap Actieve sensoren.

In de eerste drie clusters zijn is met in kind- en ook beperkte cash-bijdragen van overheden en bedrijven de behoeftestelling nu zover uitgewerkt dat gezamenlijk gefinancierde projecten worden ontwikkeld. Als vervolg hierop zijn PPS-programma's voorzien. Voor het vierde cluster is er al een structurele samenwerking met substantiële in kind-betrokkenheid en enige cash-bijdragen; in dit cluster is het grootste deel van de basis van 200 k€ voor de TKI-toeslag van 2013 opgebouwd.

Inhoudsopgave

2 Inleiding

2.1 Het strategisch Plan 2011-2014 van TNO

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

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

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

De hoofdlijnen van het Strategisch Plan 2011-2014 van TNO zijn de volgende zeven thema's:
1. Gezond Leven.
2. Industriële Innovatie.
3. **Integrale Veiligheid.**
4. Energie.
5. Mobiliteit.
6. Gebouwde Omgeving.
7. Informatie Maatschappij.

2.2 Beschrijving van het TNO-Thema Integrale Veiligheid

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

Binnen het TNO Thema Integrale Veiligheid zijn 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 c.q. business lines om Defensie bij deze uitdaging te helpen:
- Military Operations.
- Military Information Superiority.
- Force Protection.
- Human Effectiveness.

2. *Safety and Security Research*
Veiligheid heeft zich ontwikkeld van een verzameling ad-hoc reacties op incidenten tot een samenhangend complex van maatregelen en effecten.
De potentiële impact en het domino-effect van incidenten, maar ook de maatschappelijke kosten/baten van veiligheidsmaatregelen vereisen een integrale op risico en effect gebaseerde aanpak en regie. Perceptie en acceptatie spelen een grote rol in de keuze van oplossingen.
TNO gaat deze uitdagingen aan door te focussen op de volgende onderwerpen c.q. business lines:
- Security and Protection.
- Resilience and Society.

2.3 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 twee Vraaggestuurde Programma's (VP's) die primair aan het Innovatiegebied Safety and Security Research verbonden zijn:
- 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 nauwe interactie met de departementen VenJ, Defensie en EZ en het bedrijfsleven is in de tweede helft van 2011 binnen de Topsector High Tech Systems & Materials een Roadmap Security opgesteld (zie www.htsm.nl).
Het VP Security is de vertaling van deze roadmap naar TNO-onderzoeksprojecten. Bij alle projecten in het VP Security zijn bedrijven en/of veiligheidsorganisaties van de overheid betrokken met in-kind- en/of cash- commitment.

Deze rapportage omvat een verantwoording van de uitvoering van het vraaggestuurde programma Security in 2013 op hoofdlijnen.

2.4 Aansturing van VP Security vanuit Roadmapteam Security

Het VP Security wordt begeleid door het door de topsector benoemde roadmapteam Security, bestaande uit Thales als industrieel boegbeeld, VenJ, Defensie, NLR, STW/NWO en TNO. Het Roadmapteam heeft hieraan als leden toegevoegd: NIDV en de Gemeente Den Haag. Het ministerie EZ heeft een eigen vertegenwoordiger aan het Roadmapteam toegevoegd.

In 2012 en 2013 is het kader van de topsectoren-ontwikkeling en de samenwerking van bedrijfsleven met TO2-instituten, universiteiten en overheden verder vormgegeven. Zo is door het team voor de roadmap Security initiatief genomen tot:

- Concretisering van ambities voor via NWO en STW uit te zetten onderzoek.
- Structurele verbindingen met de publieke veiligheids-organisaties als Nationale Politie, Brandweer, Veiligheidsregio's, KMar en Defensie.
- Publiek-private samenwerkingsinitiatieven voor innovatie en implementatie van vernieuwingen op de deelterreinen.

Vanuit het roadmapteam wordt als bredere ambitie benadrukt dat er een uitbouw moet plaatsvinden van de launching customer rol van alle partners uit overheid en bedrijfsleven. En dat zijn er vele, afhankelijk van het gekozen risicoscenario: te noemen zijn: Defensie, VenJ, de andere departementen, de Veiligheidsregio's, grote gemeenten, politie regio's, waterschappen, GHOR, brandweer, de beveiligers, de vitale sectoren, etc. Om de samenwerking te versterken wordt vanuit de Hague Security Delta een Nationaal Innovatiehuis Veiligheid opgezet. In 2013 is in dit kader structurele samenwerking van de regio's Den Haag eo, Twente en Eindhoven/Tilburg gerealiseerd. Met het VP sluit TNO op een aantal van de ontwikkelde initiatieven aan.

2.5 Oordeel TNO-Management over de uitvoering

Na de indiening van de HTSM-Roadmap Security in december 2011 zijn de LOI-partners geconsulteerd en de uitdagingen voor ontwikkelingen die passen in het vraaggestuurde onderzoekprogramma bij TNO geconcretiseerd. In 2012 zijn een drietal projecten opgestart voor hoofdlijnen binnen de roadmap. Over de voortgang is in maart 2013 een rapport uitgebracht. In mei 2013 volgde een actualisering van de roadmap. Het voorliggende rapport over de voortgang in 2013 geeft een goed beeld van de resultaten qua samenwerking en inhoudelijke kennis.

De samenwerking in de driehoek Overheid-Bedrijfsleven-Kennisinstellingen voor kennisontwikkeling en innovatie op het gebied van Security is substantieel uitgebouwd. De betrokkenheid van de gemeente Den Haag gaf via de vormgeving van The Hague Security Delta hieraan nog een aparte dimensie. De diverse door TNO georganiseerde workshops en zgn. "challenges" leveren ook een wezenlijke bijdrage hieraan.

De vier hoofddelen van de roadmap zijn Systems-of-systems, Cybersecurity, Passieve sensoren en Actieve sensoren en blijken een goede basis voor verder initiatief. Kritische succesfactor voor het gestand doen van de uitgesproken investeringsintenties van bedrijven is het perspectief op marktomzet cq. Launching customership voor de deelnemende bedrijven bij publieke veiligheidsorganisaties. Voor de drie eerstgenoemde deelroadmaps is dit concreter geworden, maar mede

door de reorganisaties bij de overheid en de financiële crisis moet hier nog wel het nodige gebeuren. Mede dankzij de door TNO in dit VP genomen initiatieven en ontwikkelde kennis kunnen de in de roadmap geformuleerde ambities voor de komende jaren realistisch genoemd worden. Voor de deelroadmap Actieve sensoren is er al jarenlang sprake van een goed functionerende “Gouden Driehoek”; uitbreiding met een civiele dimensie is wel een kans.

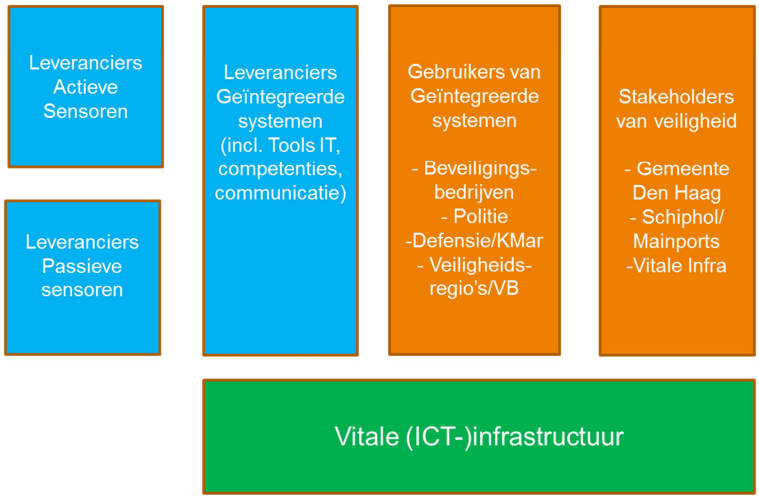
Samenvattend: Het VP Security heeft in 2013 in de context van het topsectorbeleid en met steun van het roadmapteam een verdere uitbouw van de driehoek Overheid-Bedrijfsleven-Kennisinstellingen gerealiseerd.

3 Vraaggestuurd Programma Security

3.1 Beoogde Impact en Doelgroep

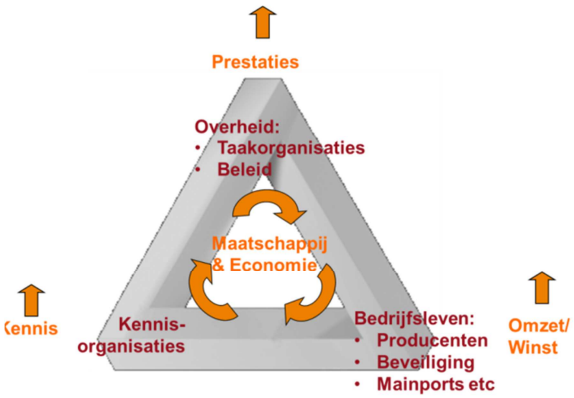
De ontwikkelingen in het VP Security zijn gericht op de volgende impact:

1. Versterken van de concurrentiekracht van het Nederlandse bedrijfsleven met betrekking tot systemen, IT-producten en sensoren en voor veiligheid.
2. Effectiever/efficiënter optreden van publieke en private veiligheidsorganisaties door innovatie van informatievoorziening, meldkamers, besluitvorming, doctrines, materieel, uitrusting en competenties.
3. Vergroten van veiligheid in verschillende maatschappelijke sectoren (waaronder de vitale infrastructuur en de topsectoren Logistiek en Water) en beter kunnen afwegen van de maatschappelijke en economische effecten van risico beperkende maatregelen.
4. Verbetering van de resilience van de maatschappij tegen cyberrisico's en van de bestrijding van de cybermisdaad.



Figuur 4 Waardeketen voor roadmap Security.

In het kader van de roadmap is het versterken van innovatie-initiatieven door de samenwerking in bovenstaande waardeketen voor veiligheid een kerndoel.
Dit betreft zowel gezamenlijke projecten als infrastructuur voor validatie van nieuwe opties en launching customership. In het VP Security wordt dit ook integraal aandacht gegeven om de doorlooptijd van innovatietrajecten te verkorten en de kans op implementatie te vergroten. De gouden driehoek van bedrijfsleven, overheid en kennisinstellingen heeft in de security-sector bijzondere betekenis doordat de overheid niet alleen een beleidsbetrokkenheid heeft maar ook uitvoerende taken in bedrijfsmatig gerunde organisaties.



Figuur 5 Gouden driehoek voor Security is Economie & Maatschappij.

Van bijzonder belang voor het participerende bedrijfsleven is het optimaal gebruik maken van de kennis die internationaal ontwikkeld wordt en aansluiting op internationaal in ontwikkeling zijnde praktijk van veiligheidsorganisaties. Interoperabiliteit en standaardisatie zijn ook in het Europese kaderprogramma belangrijke aspecten. Vanuit de stakeholders van de roadmap Security zullen initiatieven genomen worden om dit te versterken. De al bestaande sterke deelname van TNO in de Europese arena is hier een goede uitvalsbasis.

3.2 Focus van de inhoud van het VP Security

3.2.1 Aansluiting op lopende VP's bij TNO

De vier onderdelen van het VP Security sluiten alle aan op onderdelen van al lopende Vraaggestuurde Programma's bij het TNO-thema Integrale Veiligheid. In onderstaande tabel wordt dit verder gespecificeerd:

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

Tabel 1

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.
Voor versterking van de aansluiting op de defensieprogramma's zijn in 2013 initiatieven genomen; hierbij geldt de strikte confidentialiteit voor Defensie als een randvoorwaarde.

3.2.2 Ontwikkeling projectenportfolio 2013

Van het totale TNO-budget voor het VP Security in 2013 is budget gealloceerd voor projecten gekoppeld aan de deelroadmaps Systems-of-Systems, Cybersecurity en Passieve sensoren. Daarnaast zijn de verplichtingen in lopende projecten die relevant zijn voor de vier deelroadmaps in het programma opgenomen.

Voor elk van deze drie deelroadmaps zijn de meest betrokken bedrijven in januari/februari 2012 gevraagd naar specificatie van hun ambities voor nieuwe samenwerkingsprojecten in het kader van de roadmap en een indicatie van daarbij horende in-kind- of cash-bijdragen. Uit deze bilaterale contacten zijn door TNO in overleg met het Roadmapteam kennisinvesteringsplannen (zgn. KIP's) opgesteld. Daarbij is zo goed mogelijk rekening gehouden met de kansen op toepassing bij de uitvoerende veiligheidsorganisaties. Ook is rekening gehouden met de door TNO geambieerde sterktes qua expertise.

In 2013 is prioriteit gegeven aan het ontwikkelen van samenwerkingsrelaties met de uitvoerende veiligheidsorganisaties. Dit betreft zowel de nationale politie (onder andere met betrekking tot RTIC's, de nationale meldkamer, het platform sensing) en de Kmar (met name op de Schiphol-locatie) als de veiligheidsregio's (crisismanagement en preparatie op overstromingsdreigingen). Daarnaast is op 13 juni een bijeenkomst In Focus georganiseerd met 80 deelnemers uit bedrijven en overheidsorganisaties.
(https://www.tno.nl/content.cfm?context=overtno&content=nieuwsbericht&laag1=37&laag2=2&item_id=2013-07-04%2010:59:12.0)
Ook zijn presentaties gegeven bij het congres "Veilig door innovatie" op 10 oktober en de NIDV-Tentoonstelling op 21 november 2013. Met betrekking tot cybersecurity zijn een aantal initiatieven met bedrijven genomen, waarbij ook financieel commitment is gerealiseerd. Ook op dit terrein is de aansluiting met publieke en private spelers ontwikkeld door contacten naar aanleiding van presentaties op bijeenkomsten. Een trend hierbij is dat ontwikkelingen voor systems-of-systems en cybersecurity geïntegreerd worden; dit is ook bij het project voor BKWI verder geconcretiseerd.

4 Resultaten van het VP Security in 2013

4.1 Deelroadmap Systems of systems

4.1.1 Doelstelling

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

In antwoord op deze maatschappelijke uitdaging, zien we de rol van informatiesturing toenemen binnen de veiligheidsketen. Informatiesturing binnen bijvoorbeeld politie, brandweer en GHOR in het veiligheidsveld, maar ook met gemeenten en beveiligingsbedrijven. En vooral ook in de *samenwerking* tussen de partijen. In een netcentrisch samenspel, dat je als een systeem van deelsystemen kunt beschouwen: een System -of-systems. Niet alleen 'traditionele' systemen maken deel uit van het System-of-systems. Want veiligheid is al lang niet alleen meer iets van de fysieke wereld. Ook de virtuele wereld van internet en social media speelt een steeds belangrijker rol. En daarmee komt de burger als onderdeel van het 'systeem' ook in beeld.

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

Dat betekent concreet bijvoorbeeld dat bij een brand de juiste blusmiddelen tijdig beschikbaar zijn, dat bij een overval de meest waarschijnlijke vluchtroutes zijn afgezet en dat surveillerende politiemensen precies weten wat er waar speelt. Particuliere Alarm Centrales vormen een vast onderdeel binnen het totale veiligheidssysteem. 'First time right' maakt het veiligheidsoptreden goedkoper en effectiever, met een hogere heterdaadkracht.

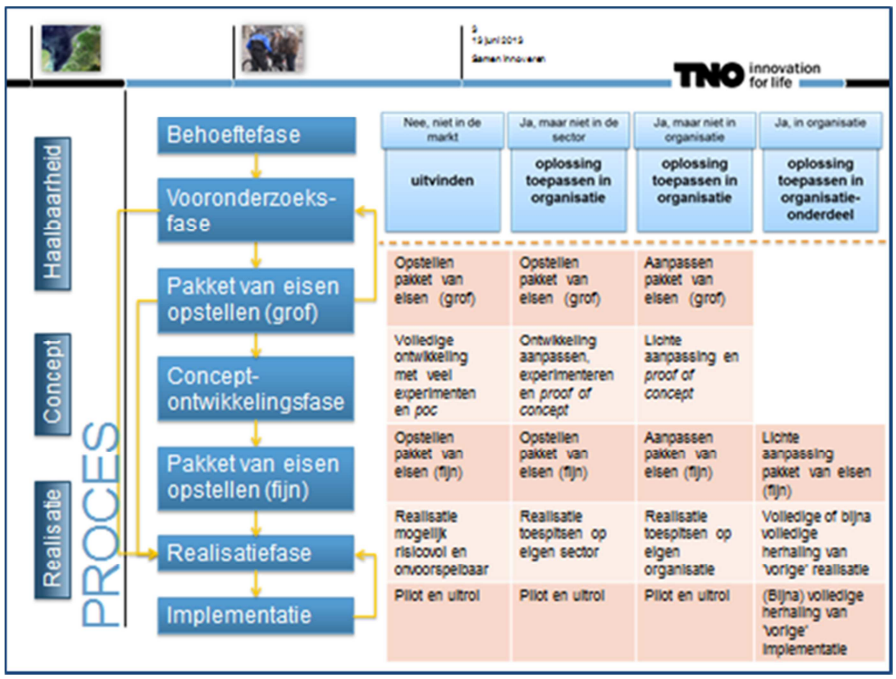
Het is de doelstelling van de deelroadmap Systems of Systems om door middel van action research sámen met bedrijfsleven en veiligheidspartners grenzen te verkennen van technologie, organisatie, processen en gedrag. Om in gezamenlijke ontwikkelprojecten nieuwe concepten te ontwikkelen en te beproeven om de Real Time Intelligence functie te versterken.
TNO zet haar kennis, ervaring en resources graag in om bij te dragen aan een betere informatie- en intelligencesturing binnen de politie en andere veiligheidspartners enerzijds, en aan economische kansen voor de deelnemende bedrijven in de vorm van nieuwe of verbeterde producten en diensten anderzijds.

4.1.2 *Gerealiseerde voortgang*

De reorganisatie van de Nationale Politie heeft een vertragend effect op het nader invullen van de samenwerkingsambities zoals geformuleerd eind 2012. Daarom is in 2013 gekozen voor diversificatie richting andere veiligheidspartners zoals Veiligheidsregio's, Koninklijke Marechaussee, gemeenten en waterschappen en internationale organisaties zoals Eurojust.

Innovatiemanagement

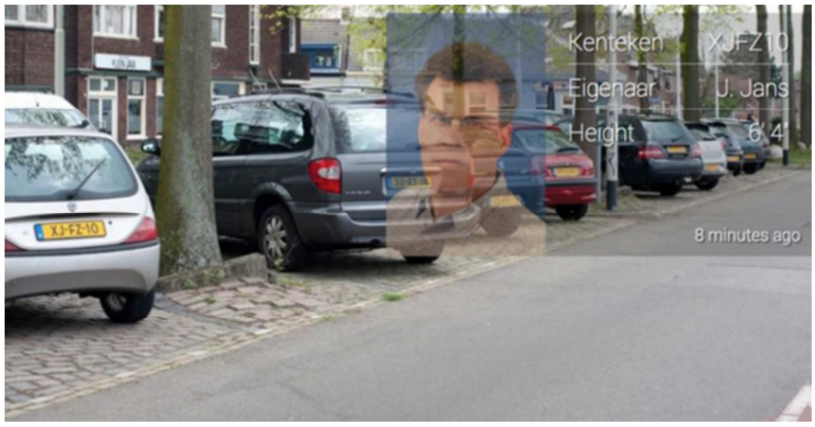
Anticiperend op een nauwe samenwerking met behoeftestellers in het kader van de topsectoren, is in het eerste kwartaal een zgn. 'Challenge' (geconcentreerde werkvorm) uitgevoerd om in beeld te krijgen welke wetenschappelijke en praktische kennis en ervaring er voorhanden is als kader en procesleidraad voor een samenwerking in de driehoek gericht op innovatie. De Challenge heeft geresulteerd in een praktisch toolbook en in een whitepaper *Innovatie Toolkit - Samen innoveren: politie, bedrijven en kennisinstellingen.*



Figuur 6 Generiek innovatieproces.

De toekomst van Real Time Intelligence - Situationeel beeld

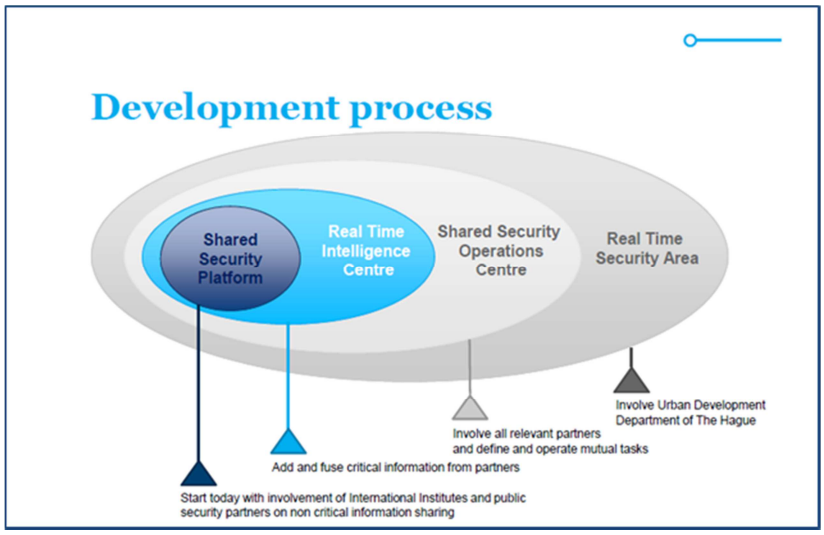
Om innovatieve producten en dienstconcepten te kunnen (helpen) ontwikkelen, is een integrerende verkenning uitgevoerd naar perspectieven op het opbouwen, onderhouden en delen van een situationeel beeld. Verschillende experts van binnen en buiten TNO (onder andere van de Politieacademie) hebben hiertoe hun kennis en ervaring ingebracht. Dit heeft geresulteerd in een visie op de wijze waarop Real Time Intelligence van waarde kan zijn voor de operationele man of vrouw op straat. Deze visie is opgetekend in het artikel *De toekomst van Real Time Intelligence.* Tevens is deze visie op diverse congressen en bijeenkomsten gepresenteerd en getoetst bij marktpartijen en veiligheidsorganisaties. De visie werd goed ontvangen.



Figuur 7 Impressie uit artikel 'De toekomst van Real Time Intelligence'.

Rondom Real Time Intelligence zijn een drietal clusters gevormd met bedrijfsleven en overheidsorganisaties. In deze clusters zal volgend jaar verder worden gewerkt in het kader van System of Systems: Rond de Internationale Zone in Den Haag, rond de Big Data en Veiligheid en rond Overstromingsdreiging.

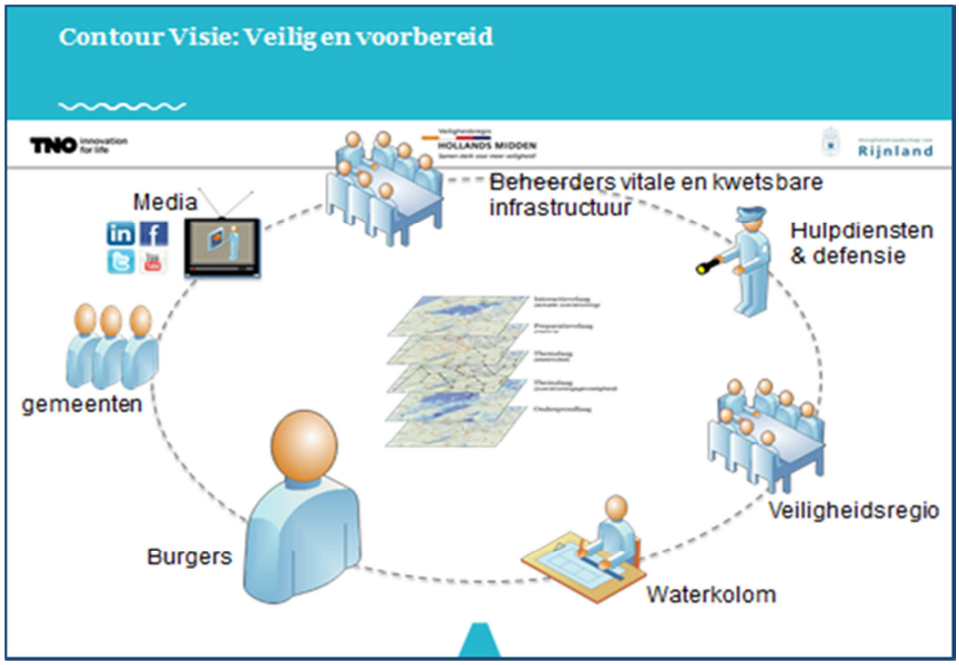
Beveiliging van de Internationale Zone Den Haag
In 2013 is in het kader van de 'Hague Security Delta' gestalte gegeven aan een veiliger Internationale Zone in Den Haag, met behoud van leefbaarheid in het gebied. Hiertoe hebben een aantal in Den Haag gevestigde Internationale Organisaties zoals Eurojust de handen ineengeslagen, en werken samen met TNO en een aantal leveranciers zoals Thales en Siemens aan de ambitie van een 'real time security area'. Vanuit Systems of Systems is bijgedragen aan het ontwikkelen van dit toekomstbeeld waarin de (beveiligers van) Internationale Organisaties nauw samenwerken, en informatie en resources in real time met elkaar en met de politie delen. In gezamenlijkheid is een roadmap ontwikkeld voor een steeds nauwere samenwerking in het beveiligen van de Internationale Zone (als een System-of-Systems). Het is de bedoeling om de samenwerking in dit kader te intensiveren in 2014, gebruikmakend van het nieuwe Real Time Intelligence lab dat in de nieuwe HSD-campus wordt gerealiseerd.



Figuur 8 Beoogd groeipad naar Real Time Security Area in de Internationale Zone Den Haag.

Omgaan met big data bij Burgerparticipatie voor handhaving en opsporing (RNIP)
Samen met TU-Delft, CGI en Nationale Politie is een voorstel ontwikkeld rond de ontwikkeling en integratie van systemen en processen voor burgerparticipatie bij handhaving en opsporing. Het betreft een R&D-project dat waarschijnlijk in 2014 zal starten.

Overstromingsrisico's
Het beperken van overstromingsrisico's is bij uitstek een uitdaging voor complexe samenwerkingen over de grenzen van organisaties heen. Samen met Veiligheidsregio Hollands Midden is gewerkt aan het inzichtelijk krijgen van zogenaamde 'cascade-effecten' bij overstromingen op bijvoorbeeld mobiliteit en energievoorziening. Met dergelijke kennis voorhanden kan in geval van overstromingen betere besluiten worden genomen ten aanzien van maatregelen en crisiscommunicatie. Helemaal als deze modellen gevoed kunnen worden met Real Time situationele data. Dan ontstaat Real Time Intelligence. Op basis van een overzicht van informatiebehoefte en informatie-eigenaren is in de laatste maand van 2013 een Challenge gehouden met als doel een aansprekend beeld te schetsen van een intelligent platform (kaart en kaartlagen) met meerwaarde voor besluitvorming in de complexe samenwerkingsrealiteit van een overstroming.
De ontwikkelde impressie van een oplossing, met bijbehorende voorwaardelijke roadmap voor samenwerking werd enthousiast ontvangen door de Veiligheidsregio's Hollands Midden en Zuid-Holland-Zuid, het Hoogheemraadschap Rijnland en het waterschap Hollandse Delta.



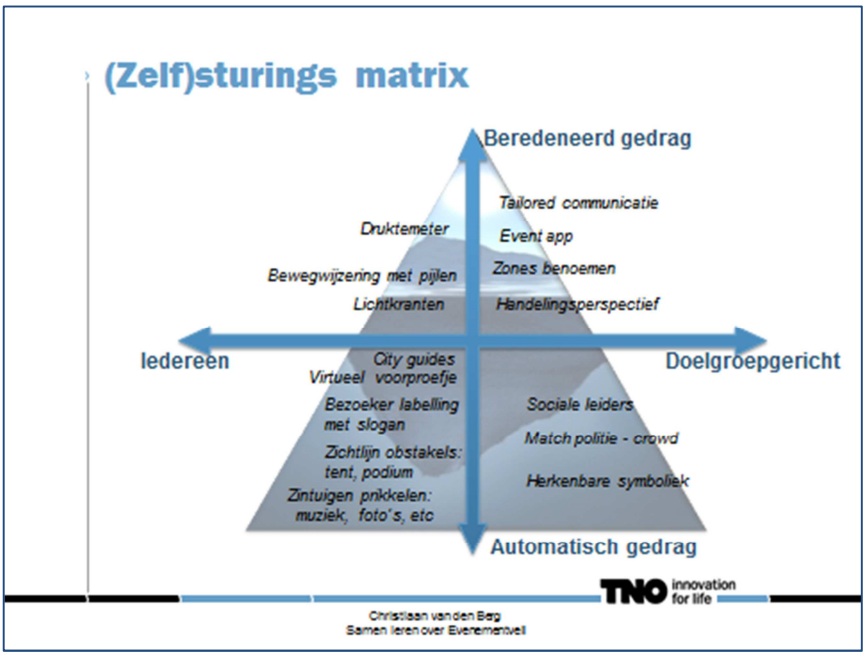
Figuur 9 Stakeholders bij (cascade-effecten van) overstromingen.

In 2014 zal verder worden ingezet op de gekozen richting, en zal met de nu al betrokken partijen een consortium worden uitgebouwd om rond Overstromings-dreiging tot een trendsettend project te komen.

Evenementenveiligheid

Voor 2013 is naast de focus op Real Time Intelligence ook gekozen voor een verkenning van mogelijkheden voor de Topsector HTSM op het gebied van Evenementveiligheid; de initiatie hiervan vond plaats in het roadmapteam. Hiertoe werd onderzoek gedaan naar behoeften van het opdrachtgevers- en aanbiedersveld, waaruit met name de behoefte naar voren kwam aan een betere instrumentarium voor het meten en beoordelen van drukte tijdens evenementen. In september 2013 is een Challenge uitgevoerd voor het Veiligheidsoverleg van de Nijmeegse 4-daagse in samenwerking met de roadmap Passieve Sensoren met medewerking van bedrijfsleven. De Challenge heeft aansprekende resultaten opgeleverd, die in 2014 nader kunnen worden uitgewerkt. Het betreft een nieuwe wijze van bemeten en voorspellen van (gevaarlijke) drukte in mensenmenigten enerzijds, en nieuwe wijzen van beïnvloeding van deze menigten met het oog op crowdmanagement anderzijds. Hiertoe moet een landelijk netwerk van lerende organisatoren en gemeenten worden opgezet, gefaciliteerd door een meerjarig onderzoeksproject.

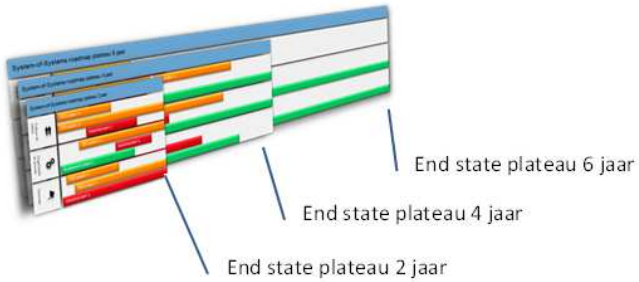
Figuur 10 Eén van de resultaten van de Challenge Evenementveiligheid rond het meten van drukte van menigten.



Figuur 11 Eén van de resultaten van de Challenge Evenementveiligheid rond gedragsbeïnvloeding.

Roadmapping voor System of Systems

Samen met het D-Cis lab van Thales is een eerste versie van een roadmap voor System-of-Systems opgesteld. Deze roadmap is behulpzaam bij het identificeren van nieuwe kansen voor onderzoek en ontwikkeling, en wordt gebruikt als discussiestuk in gesprekken met marktpartijen en behoeftestellers.



Figuur 12 Visualisatie van Roadmap System-of-Systems.

4.1.3 Publiciteit

- H. van den Broek en C.H. van den Berg, artikel De toekomst van Real Time Intelligence. Digitaal magazine Melding! en TNO.nl;
- A. de Vries, C. Broekman en C.H. van den Berg, artikel Drukte hoeft geen gedoe te zijn, in nieuwsbrief KCEV en op TNO.nl;
- H. van den Broek, W. Treurniet en J. Wevers, whitepaper Inzet intelligence capaciteit Defensie voor Civiele toepassing: Samen Slimmer;
- Hans van Vliet, Lotte de Groen, Marc Menkhorst, Pepijn Vos, Christiaan van den Berg, whitepaper: Innovatie Toolkit - Samen innoveren: politie, bedrijven en kennisinstellingen;

- Presentatie over Evenementveiligheid tijdens de Vierdaagse Feesten voor Politie-eenheid Nijmegen;
- C. van Dongen, D. Stolk, L. Weber, M. de Lange, Informatiepreparatie overstromingsrisico's en dominio-effecten, rapport van samenwerkingsproject van Veiligheidsregio's Hollands Midden, Hoogheemraadschap Rijnland en TNO
- Workshop Real Time Intelligence op Congres Veilig door Innovatie, 10 oktober 2013;
- Beursstand over RTI in relatie tot Overstromingsdreiging op NIDV-beurs 21 november 2013;
- Presentatie over RTI op CCR-summit - 2 oktober 2013;
- Presentatie over RTI en technologische ontwikkelingen op conferentie Meldkamer van de Toekomst, 14 november 2013;
- Presentatie over RTI en technologische ontwikkelingen voor het Dagelijks Bestuur Veiligheidsberaad, 29 november 2013.

4.2 Deelroadmap Cybersecurity

4.2.1 Doelstelling

Uit de inventarisatie van de ambities van de bedrijven die een intentieverklaring met belangstelling voor Cybersecurity hebben ondertekend, volgt grote belangstelling voor het gezamenlijk opzetten van innovaties voor het ontwerpen van veilige ICT infrastructuur en het adequaat detecteren van ICT-misbruik.

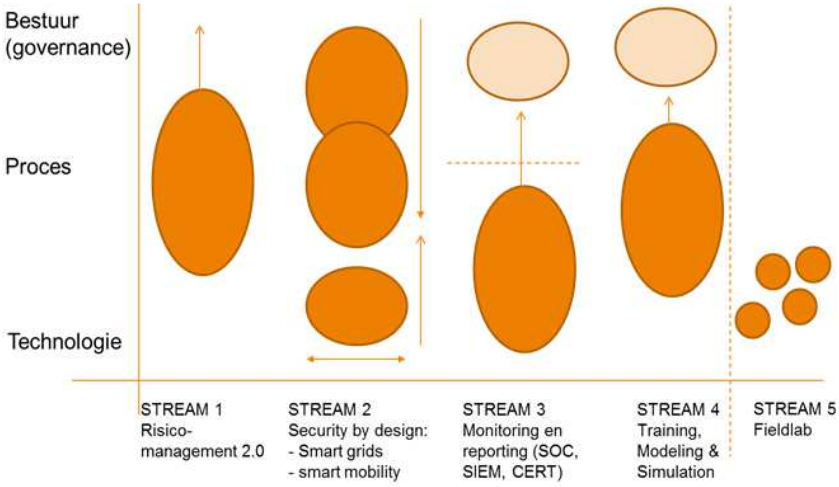
De snelle veranderingen in technologie, de toenemende verwevenheid van op ICT gebaseerde infrastructuren, de snelle introductie van nieuwe ICT-gebruiksmogelijkheden en de incoherentie van beschermingsmaatregelen over (ketens van) organisaties heen, zorgen voor nieuwe dreigingen en kwetsbaarheden. Een goede beheersing vereist steeds opnieuw risico-afwegingen en innovatieve maatregelen. Aangezien voorkomen van incidenten beter is dan genezen, is het wenselijk om al in het ontwerpstadium van ICT-infrastructuur en grootschalige op ICT-gebaseerde infrastructuur rekening te houden met bescherming (*security by design*). Hierbij richt het onderzoek zich op het opzetten van een referentiekader om risicofactoren van nieuwe technologie snel te kunnen inschatten en op het uitvoeren van technologiescans naar nieuwe ICT-ontwikkelingen. Voor de ontwikkeling van het referentiekader wordt gebruik gemaakt van een case studie naar een infrastructuur waarin grootschalige ontwikkelingen in de ICT-toepassingen gepland staan.
Voor de case studie is gekozen voor de smart grid ontwikkelingen in de energiesector, aangezien de ICT-ontwikkelingen daar sterke consequenties hebben in de besturingsmogelijkheden en maatschappelijke impact hebben voor de gebruikers.

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. Een belangrijke pijler binnen het onderwerp cyber security wordt gevormd door detectie van ICT-misbruik en bijbehorende mogelijkheden voor opsporing en vervolging. Voor ICT geldt dat zowel de overheid als het bedrijfsleven ieder voor zich maatregelen op dit gebied nemen.

Binnen het aanpalende Vraaggestuurde Programma Veilige Maatschappij onder regie van het ministerie VenJ wordt er specifiek aandacht besteed aan cyber-security voor de vitale infrastructuur. Dit betreft sectoren en voorzieningen waarvan

verstoring of uitval ernstige impact kan hebben op de samenleving in Nederland (en daarbuiten), zoals de energievoorziening, drinkwatervoorziening en de transportsector. Ook deze vitale sectoren zijn in steeds grotere mate afhankelijk van ICT.
De resilience van de cyberinfrastructuur in Nederland betreft niet alleen de vitale infrastructuur, maar heeft een breder belang voor het Nederlandse bedrijfsleven. Cybersecurity kan niet alleen door de overheid worden gerealiseerd. Dat is de focus van het project Cybersecurity in dit VP Security Het bedrijfsleven heeft nadrukkelijk een grote rol, als leverancier van (delen van de) hardware voor de infrastructuur, maar ook als 'ogen en oren' voor monitoring en detectie van, en bescherming tegen cyberdreigingen. Het Nationaal Cyber Security Centre (NCSC) heeft ook daarom als doelstelling geformuleerd om door middel van een samenwerkings-netwerk essentiële informatie uit te wisselen tussen (private) Security Operations Centers (SOC's), Security Incident and Event Monitoring (SIEM's) en Computer Emergency Response Teams (CERT's).

Doelstelling TNO-project Realiseren van cybersecurity in het bedrijfsleven
Onderstaand diagram geeft de vijf streams of werkpakketten in het project *Realiseren van cybersecurity in het bedrijfsleven* weer.



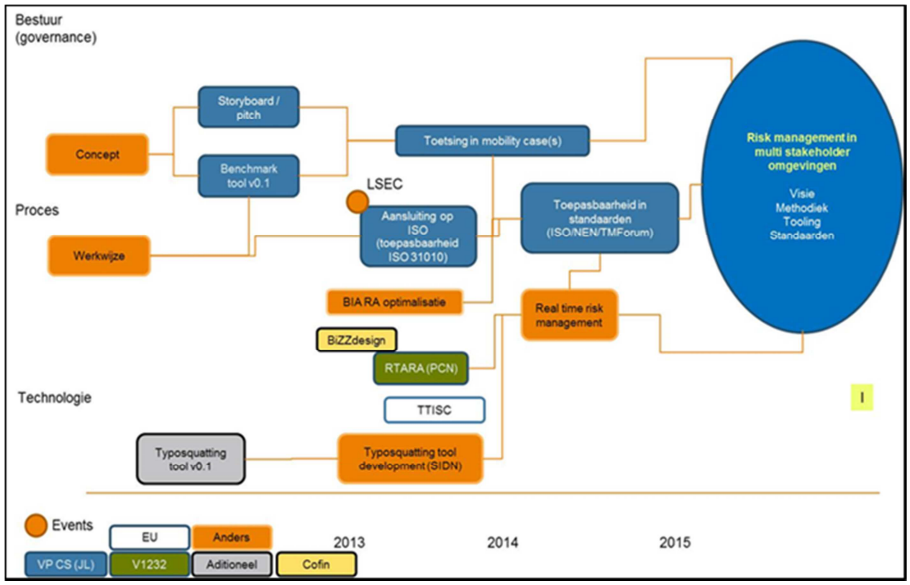
Figuur 13 Visualisatie van de uitdagingen voor vergroten van de cybersecurity in het bedrijfsleven.

Op de horizontale as zijn de uit gesprekken met LOI-partners geselecteerde vijf ontwikkelingsuitdagingen voor cybersecurity aangegeven. Op de verticale as is met drie lagen aangegeven dat ontwikkelingen op verschillende hiërarchische niveaus liggen: technologie (de hardware en individuele competenties), proces (organisatie en samenwerking) en bestuur (governance, beleid).
De plaats en grootte van de ovalen geeft aan op welk niveau de inhoudelijke onderwerpen gewoonlijk zijn geplaatst binnen organisaties. Risicomanagement is bijvoorbeeld meestal te vinden op procesmatig niveau, met ISO of COBIT als standaarden. Monitoring en reporting daarentegen heeft meestal een sterk technologische inslag, met enige procesmatige rapportagevormen op IT-management niveau.
De lichtgekleurde ovalen geven de 'witte vlekken' aan. Steekhoudende rapportages over cybersecurity waarmee sturing mogelijk is bereiken zelden het bestuurlijk

niveau (o.a. gebrek aan KPI's) en de bestuurslaag is zelden opgeleid om cybersecurity dreigingen te kunnen inschatten of aanpakken. De pijlen geven aan waarheen de inhoudelijke onderwerpen idealiter zouden moeten bewegen.
Op de snijvlakken tussen de streams en de organisatorische niveau's zitten de mogelijkheden voor publiek-private samenwerking; daar zijn de activiteiten gepositioneerd binnen dit project.

4.2.2 Gerealiseerde voortgang in 2013

Met behulp van de opgebouwde resultaten en inzichten van 2012 zijn bij de start van 2013 voor de vier inhoudelijke streams roadmaps ontwikkeld (zie figuur 14 voor een voorbeeld). Deze zijn daarna getoetst in contacten met het bedrijfsleven, overheden en uitvoeringsorganisaties. Hierbij zijn pitches gebruikt om in gesprekken te kunnen focussen op onderzoeksvragen. Vervolgens is richting gegeven aan de invulling van de projecten in de verschillende streams; naar aanleiding van de behoeftes van de geraadpleegde partijen zijn enkele deelprojecten geïntensiveerd, terwijl er ook een aantal is getemporiseerd.

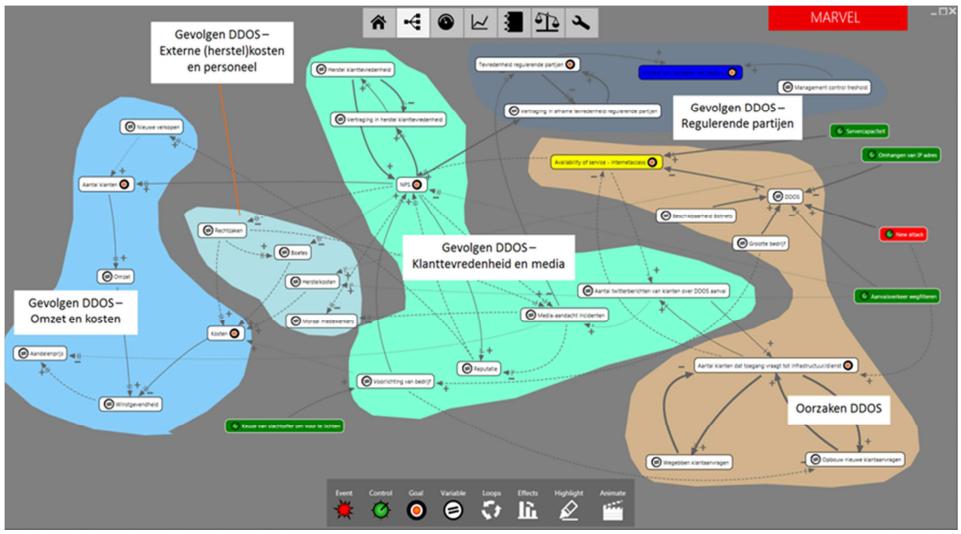


Figuur 14 Roadmap van stream 1. Advanced Risk Management.

Stream 1 Advanced Risk Management
In deze stream is onderzocht hoe Cybersecurity ondergebracht kan worden in bestaande risicoprocessen van organisaties.

Het eerste deelproject in deze stream betreft *de gevolgen van cyberincidenten*. Als input voor risicomanagement 2.0 is het inzichtelijk maken daarvan essentieel. Het gaat dan zowel om materiële als immateriële schade, zoals verlies van continuïteit van bedrijfsvoering, geloofwaardigheid of klantverlies. Samen met een afstudeerder van de Erasmus Universiteit Rotterdam (EUR) is een causaal model ontwikkeld waarmee bedrijven een afweging kunnen maken of een cyberdreiging relevant is, en of het risico aanvaardbaar is of niet. Op basis van de TNO Marvel tool zijn enkele Cyber aanvalsscenario's generiek gemodelleerd om de impact op de bedrijfsvoering te kunnen duiden. Dit zijn: DDOS aanvallen, hacking en Advanced Persistant Threats (APTs). Met zo'n model kan een beoordeling worden gemaakt voor een specifiek bedrijf, een bedrijfstak of een overheid om rekening te

houden met de tijdsduur van een aanval, de frequentie, de intensiteit of het lekken van data. Op 1 oktober 2013 is het DDOS model gepresenteerd bij de opening van het TNO Cyber Security Lab (CSL) aan 46 bedrijven die actief zijn in de procesindustrie. In onderstaande figuur staat een voorbeeld voor de impact van een DDOS aanval op een bedrijf uit de telecom sector.



Figuur 15 Model voor beoordeling van de gevolgen van een DDOS-aanval op een telecom-bedrijf.

In zo'n semi-kwantitatief model is betrekkelijk snel zicht te krijgen op zowel de aanvalsvector als de impact van een specifieke cyberaanval op een bepaalde sector. Ook het effect van tegenmaatregelen is hierin goed te modelleren. Met de resultaten is het mogelijk om de (niet gekwantificeerde) impact van een enkelvoudige cyberaanval (eenmalig, één type aanval) op bedrijfsdoelstellingen en het effect van tegenmaatregelen hierop te laten zien.

Verder is aan de hand van de modellering goed te bepalen wat wel of niet zinvol is om te monitoren. In de praktijk is dit van belang voor het opstellen van de 'policy' voor het gebruik van reguliere monitoring tools. Zo is bij een DDOS aanval, zoals verwacht, het monitoren van het inkomende dataverkeer relevant (directe detectie), maar ook het monitoren van Twitter blijkt zinvol te zijn, omdat uitingen en het sentiment op Twitter van invloed zijn op de te nemen maatregelen om de DDOS aanval tegen te gaan (indirecte detectie).

Door het identificeren van bedrijfs- of sectorale kenmerken zijn indicaties mogelijk van specifieke dreigingen van cyberrisico's. Voor de inschatting van de kwetsbaarheid zijn gegevens verzameld uit enkele (vertrouwelijke) databases met security incidenten, aangevuld met interviews met security specialisten.

In een tweede deelproject is onderzoek gedaan naar *Typosquatting.* Door het (legaal) registreren van domeinnamen die sterk lijken op de domeinnaam van het slachtoffer, kan bijvoorbeeld snel en nagenoeg ongemerkt gevoelige informatie worden ontvreemd; ook kan een sterk gelijkende website worden misbruikt voor phishing. In samenwerking met de Stichting Internet Domeinregistratie Nederland

(SIDN) is in 2013 onderzocht of het mogelijk is om een tool te ontwikkelen, waarmee kan worden ingeschat of een specifieke internet domeinnaam kwetsbaar is voor misbruik, omdat de naam sterk lijkt op andere domeinnamen.

Er zijn twee geavanceerde typosquat modules ontwikkeld. Eén module is gebaseerd op ‘fuzzy matching’, terwijl een andere module een combinatie van domein-classifiers gebruikt. Samen met SIDN is de technische werking en de performance van de modules geëvalueerd. De twee modules vormen het hart van de 'Tracker'. Op basis van informatie die gegenereerd wordt met Tracker, kunnen rechtmatige domeinnaamhouders zelf het risico op misbruik van gelijkende domeinnamen beter inschatten en zo nodig actie ondernemen om hun belangen te beschermen ('Brand protection').
De resultaten van het deelproject Typosquatting zijn door SIDN samen met een klankbordgroep (Rabobank, NCSC) geëvalueerd en positief beoordeeld.

Een derde deelproject van deze stream betreft het ontwikkelen van een *Verplichtingen-Verwachtingen model*. Hierbij is samengewerkt met enkele uitvoerende organisaties van de overheid (BKWI, UWV) en de Gemeente Utrecht. Met cofinanciering van BKWI zijn in een representatieve praktijksituatie de door TNO ontwikkelde concepten voor Advanced Risk Management getoetst. Onderling vertrouwen van de ketenpartijen (de uitvoeringsorganisaties of 'manifestpartijen', BKWI en de gemeentes) in SUWI-net is cruciaal voor deze vitale overheids-infrastructuur. Door de grote complexiteit van de keten, gecombineerd met een sterk toegenomen dynamiek in het ontstaan van risico's, zijn bestaande methodes voor risicomanagement minder efficiënt en effectief geworden. Gegevensbronnen en gegevensafnemers hebben daarbij regelmatig sterk tegengestelde belangen.

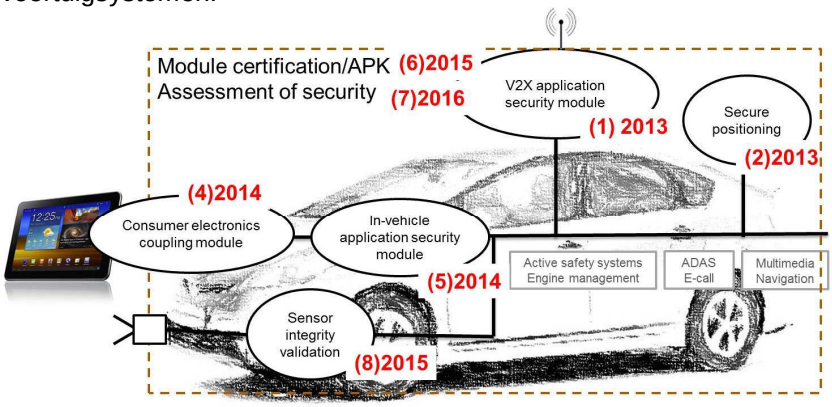
Het experiment heeft duidelijk aangetoond dat risicomanagement op basis van verplichtingen en verwachtingen beter werkt dan traditionele methodes. Voordelen zijn ondermeer:

- Risico's zijn direct gekoppeld aan bedrijfsdoelstellingen.
- Verschillende aspecten van risicomanagement worden op het juiste bestuurlijke niveau geadresseerd.
- Zwakke organisatorische plekken (inherent een bron van risico's) worden zichtbaar.

De Security officer van BKWI heeft laten weten dat hij heel blij is met de TNO methode en de bereikte resultaten.
Naar aanleiding hiervan heeft TNO een boekje uitgebracht waarin Advanced Risk Management wordt beschreven en hoe het toegepast kan worden. De Taskforce BID heeft inmiddels belangstelling getoond en er zijn ook contacten met de bankensector gelegd (ING, RABO). In Q4 2013 heeft ook de CIO van PostNL zijn belangstelling uitgesproken.

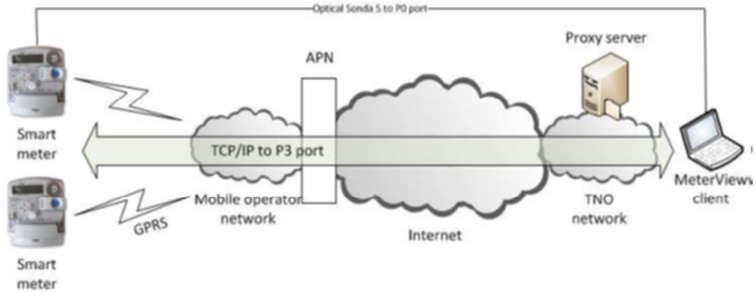
Stream 2: 'Security-by-Design' in (vitale) ICT-infrastructuren
In deze stream wordt onderzocht hoe toekomstige grootschalige ICT-infrastructuren al vanaf de designfase veilig gemaakt kunnen worden volgens security-by-design en privacy-by-design principes.

Het eerste deelproject betreft *Security in Collaborative Driving systemen ('Smart Mobility')*. Door de terughoudendheid van de consortiumpartners in DITCM (o.a. NXP, TomTom, Peek, Rijkswaterstaat) om deel te nemen in een gezamenlijk te financieren project hebben de werkzaamheden in 2013 zich beperkt tot het onderhouden van de contacten. Voor 2014 lijken er echter mogelijkheden te zijn voor een onderzoek naar vehicle-to-vehicle en vehicle-to-portal (V2X) security. Zie onderstaande figuur voor een impressie van V2X in verscheidene voertuigsystemen.



Figuur 16 Onderdelen waarin V2X security als onderwerp terugkomt.

In een tweede deelproject *Security in meet- en regelsystemen van energienetwerken* is samengewerkt met bedrijven uit de elektriciteitssector.

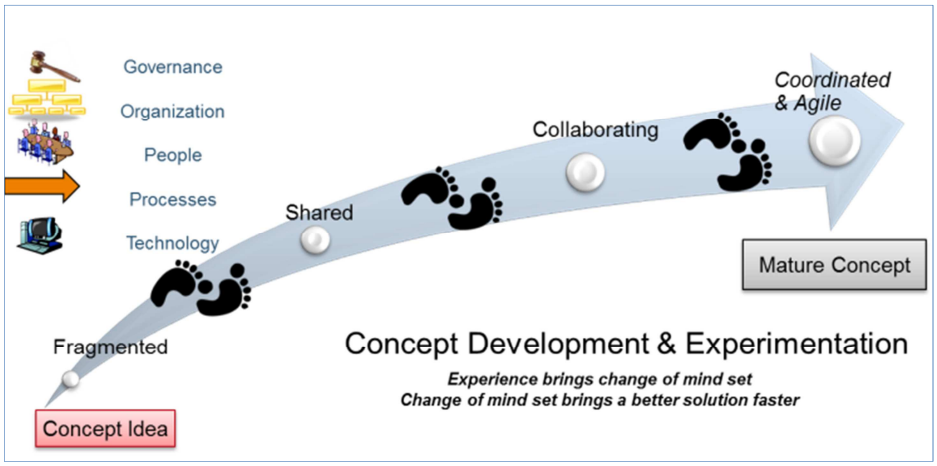


Figuur 17 Testopstelling slimme meter.

Als vervolg wordt met een ontwikkelingsonderzoek opgezet met participatie van de stakeholders. Naast de elektriciteitsproducenten zullen ook netbeheerders en componentenleveranciers zoals fabrikanten van smart meters betrokken worden

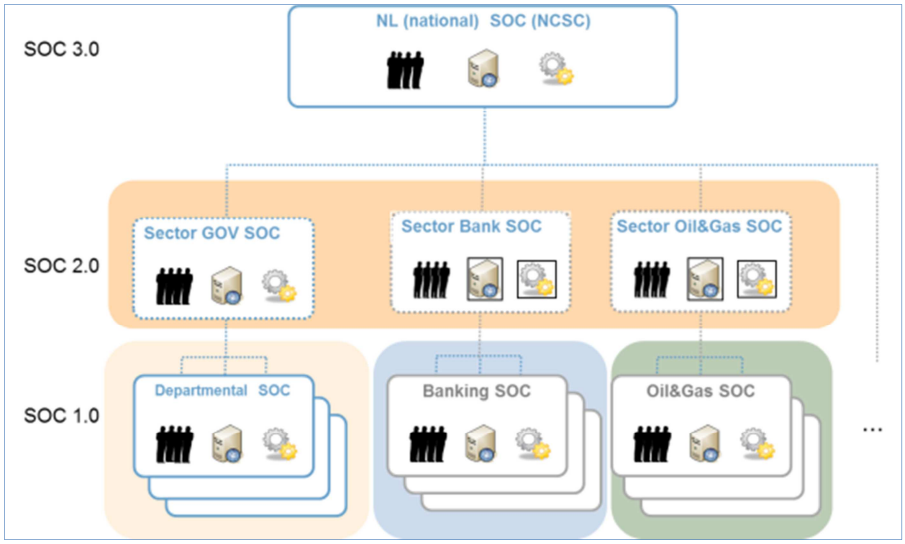
Stream 3 'Monitoring en Reporting'
Centrale vraag voor deze stream luidt: Hoe kunnen binnen grootschalige ICT-netwerken cyberdreigingen en -incidenten worden gemonitord?
Gangbare monitoring tools meten vooral op het niveau van de infrastructuur, maar door versleuteling, vermomming en het opgaan in de massale hoeveelheid (IP-)verkeer is het detecteren van cyberdreigingen en -incidenten steeds complexer geworden.

Het eerste deelproject van deze stream *Detectie en informatiefusie [Organisatorisch]* richt zich op het ontwikkelen van sensoren om Cyberdreigingen te kunnen detecteren, alsmede het onderling vergelijken van de capabilities van Security Operation Centers (SOC's). De visie van de Rijksoverheid is data sectorale SOC's uiteindelijk intersectoraal informatie zullen gaan uitwisselen.
De concretisering hiervan blijkt in de praktijk uiterst complex. TNO heeft via een Concept-development & experimentation-benadering (zie onderstaande figuur) een eerste concept uitgewerkt.



Figuur 18 Concept Development & Experimentation.

Een resultaat hiervan is een concretisering van de ontwikkeling van SOC 1.0 naar SOC 3.0:



Figuur 19 Ontwikkeling van SOC 1.0 naar SOC 3.0.

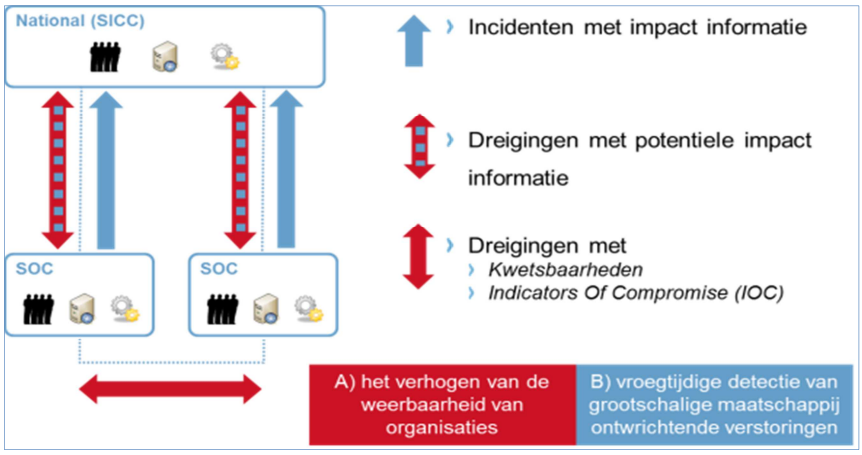
De resultaten zijn gedeeld met de Rijks Beveiligingsautoriteit (Rijks-BVA) en verscheidene marktpartijen: IBM, HP, Dell, Unisys, DataExpert en Compumatica. Inmiddels hebben enkele van deze partijen een investering gedaan of toegezegd (IBM, Compumatica, Dell, Data Expert) in het samenbrengen van hun apparatuur in het Cyber Security Lab van TNO voor testdoeleinden. Voor het versnellen van verdere ontwikkelingen dient de behoefte aan (nieuwe) sensoren verder ontwikkeld en gespecificeerd te worden om het vooruitzicht op marktkansen te vergroten.

Hiervoor zal verder gebouwd moeten worden aan het draagvlak voor de implementatie van de visie op de gewenste situatie in de toekomst in een samenwerking met NCSC, ICCIO, partijen uit de vitale sectoren, rijksoverheid, vendors, system integrators en telecombedrijven.

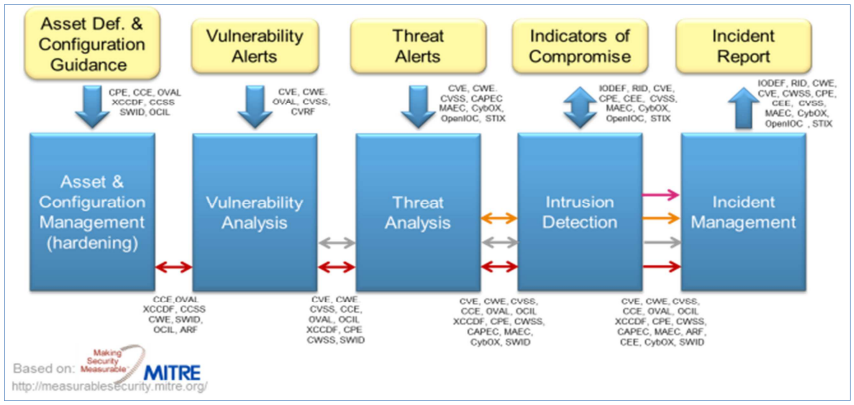
De doelstelling van het tweede deelproject in deze stream *Detectie en informatiefusie [Technisch]* is het ontwerpen van een technische infrastructuur om cyber incident informatie te kunnen delen over organisaties en domeinen heen, om zodoende vroegtijdig grootschalige incidenten te kunnen detecteren. Dit is een cruciale schakel in de beoogde samenwerking tussen SOCs. Vragen die hierbij beantwoord moeten worden, zijn:

1. Hoe ziet een dergelijke infrastructuur eruit?
2. Welke informatie moet worden uitgewisseld?
3. Welke protocollen en/of standaarden worden gebruikt of moeten worden ontwikkeld?

In 2013 zijn binnen dit project methoden en technieken onderzocht om Cyber-security informatie geautomatiseerd uit te wisselen tussen organisaties (lees: tussen SOCs) en over organisaties heen naar een ‘Security Intelligence & Coordination Centre’ (lees: organisatie als het NCSC of een NL SOC).
In samenwerking met het VP Security is een diepgaand onderzoek uitgevoerd naar de informatiestromen en protocollen (zie onderstaande figuren).



Figuur 20 Gegevensuitwisseling tussen SOC’s.



Figuur 21 Mapping van standaarden op security management.

De uitwisselingsstandaarden zijn nog volop in ontwikkeling. In het project is gebruik gemaakt van het 'Malware Information Sharing Platform' (MISP), de gestructureerde 'taal' voor uitwisseling van security incident informatie 'Structured Threat Information eXchange' (STIX) en het transport mechanisme voor security incident informatie 'Trusted Automated eXchange of Indicator Information' (TAXII). Zowel STIX als TAXII worden op dit moment gestandaardiseerd door het standaardisatie-orgaan MITRE. Met de opgebouwde kennis speelt TNO een belangrijke rol op het gebied van security informatie-uitwisseling; er is belangstelling van de Nederlandse banken omdat deze kennis zeer schaars is en nu door Amerikaanse firma's geleverd moeten worden. Bij het vervolg zijn diverse internationale bedrijven uit de ICT-sector betrokken.

Stream 4 Training, security awareness en opleidingstools (incl modellen/simulaties)
Naast de techniek, architectuur en governance is het gedrag van mensen van grote invloed op de kwetsbaarheid voor cybersecurity dreigingen. De mens blijkt telkens weer een zwakke schakel, zoals bij patching, phishing, social engineering, maar ook bij het toepassen van richtlijnen. De human factor, in termen van security awareness, opleiding, training en gebruik van simulaties of serious games is geïdentificeerd als factor van betekenis.

In het kader van deze stream is in 2013 door TNO in samenwerking met de TU Delft (Michel van Eeten), de TU Twente (Pieter Hartel en Marianne Unger) en NWO een voorstel gedaan om onderzoek te starten naar zogeheten 'Supertargets'. Dit is een aanduiding voor een deel van de bevolking, dat bovenmatig slachtoffer wordt van cybercriminaliteit, zoals phishing, hacking, malware, ramsomware, identiteitsdiefstal, etc. Het deelproject beoogt de meest kwetsbare internetgebruikers te vinden, deze gebruikers actief te helpen en herhaald slachtofferschap te doorbreken. De universiteiten willen dit voorstel graag in samenwerking uitvoeren, aangevuld met NWO budget voor een vierjarig onderzoeksprogramma, uit te voeren met AIO's.

Het ontwikkelen van samenwerking met potentiële partners voor dit onderzoek moet in 2014 verder vorm krijgen. Daarvoor is een pitch beschikbaar en gehouden bij SIDN, BZK en de banken. Op basis van de ze informatie hebben Rabobank en BZK toegezegd te willen participeren.

Stream 5. Cyber Security Lab (CSL)
Om tot een Secure Cyberspace te komen is veel onderzoek en innovatie nodig. Onze visie is om de uitdagingen in Cyber Security, integraal en multidisciplinair te benaderen. Aandacht voor de techniek maar ook voor de mens, processen, organisatie en de besturing. Een aanpak die experimenteel van aard is en waarin we de komende jaren stap voor stap tot een volwassen oplossing gaan komen.
De oprichting van een cyberlab past geheel bij deze visie. TNO biedt aan veelbelovende cyber security innovatieprojecten de technische faciliteiten en ruimte in haar cyberlab. Het TNO Cyber Security Lab is daarvoor een “Dedicated Facility” dat de werkruimte en technische faciliteiten biedt. Het is een plek waar TNO samen met partijen uit de gouden driehoek van overheid, bedrijfsleven en kennisinstituten projecten kan ondernemen.

Vanuit de deelroadmap Cybersecurity is vrijwel alle inhoudelijke technische expertise geleverd over de opzet en het technische design van het CSL.

Deze ontwerpen kunnen als deliverable worden beschouwd. Verder is expertise geleverd bij de opbouw van het lab, waaronder de virtualisatie van servers en de separate aansluitingen op het ongefilterde internet. Het CSL is op 21 mei 2013 geopend.

TNO wil in deze omgeving samen met andere partijen innoveren en voert daarom gesprekken met partijen zoals IBM, HP, Dell, Thales, UNISYS, Compumatica en Dataexpert IBM, HP en Thales Deze partijen zijn bereid equipment te leveren aan het CSL, alsmede gezamenlijke projecten op te zetten.
In 2014 zal dit in samenwerking met The Hague Security Delta verder gestalte krijgen. Een impressie van het lab bij de TNO-locatie in Den Haag geven onderstaande beelden.

Figuur 22 Het CyberSecurityLab bij TNO met de nieuwste, door grote ICT-bedrijven ter beschikking gestelde tools.

4.2.3 Publiciteit

- Advanced Risk Management, TNO-publicatie, André Smulders en Rieks Joosten, 2013;
- Business pitch 'Advanced Risk Management 2.0', TNO, André Smulders en Jeroen Laarakkers, 2013;
- Business pitch 'Cost of Cybersecurity', TNO, Eldine Verweij, Jeroen Laarakkers, 2013;
- Business pitch 'Visie op Virtual Government SOC', TNO, Jeroen Laarakkers en Robin de Haas, 2013;
- Business pitch 'Supertargets - De zwakste schakel - Human Factors in Cybersecurity, TNO; Carlijn Broekman en Jeroen Laarakkers, 2013;
- TNO-rapport Detectie en Informatiefusie, Tim Hartog en Frank Fransen, 2011;
- TNO-rapport Exploiting a replay vulnerability in Smart Meter communication, Hiddo Hut en Gerben Broenink, 2013.

4.3 Deelroadmap Passieve sensoren

4.3.1 Doelstelling

Veiligheid staat in Nederland hoog op de politieke en maatschappelijke agenda. De politiek stelt letterlijk dat het “veiliger moet worden op straten, in wijken en de openbare ruimte”. Men wil de straatterreur, overlast, intimidatie, agressie, geweld

en criminaliteit daadkrachtig aanpakken. Bovendien moet terrorisme zo veel mogelijk worden voorkomen. Vooral in de voor terroristische aanslagen kwetsbare openbare vervoersector. TNO heeft zich voor wat betreft de deelroadmap passieve sensoren geconcentreerd op toezicht ten behoeve van handhaving, beveiliging, bewaking en opsporing.
Toezicht gaat gepaard met grote investeringen in mensen en middelen van de overheid, de particuliere beveiligingsbranche en hun toeleveranciers. Verschillende toezichtsituaties stellen echter specifieke eisen aan de mate van toezicht, zoals de mate van professionalisering, technische ondersteuning, beschikbare informatie of de competenties van de toezichthouders. Het streven is voor elke toezichtsituatie de optimale mix te realiseren van organisatie, mensen en middelen, techniek, informatiebronnen, werkwijzen en competenties.

Succesvol veiligheidstoezicht in o.a. luchthavens, openbaar vervoer, beurzen, buitenwijken, musea, overheidsgebouwen, evenementen en grote winkelcentra vereist het vroegtijdig kunnen beoordelen of er sprake is van een op handen zijnde incident, vergrijp of delict. Dat is een complexe taak. Mensen zijn daarbij redelijk goed in het herkennen van subtiele afwijkingen, maar technische systemen hebben hun kracht in het combineren van grotere reeksen waarnemingen en het opslaan van grote hoeveelheden informatie. Om met zo weinig mogelijk mens- en machinekracht een zo groot mogelijk veiligheidseffect te bereiken is het inzetten van slimme sensoren en sensorsystemen van steeds groter belang. Een investering in sensoren, mits in het juiste toezichtconcept, kan leiden tot hogere efficiency en effectiviteit.

Binnen het aanpalende Vraaggestuurde Programma Veilige Maatschappij onder regie van het ministerie VenJ wordt er specifiek aandacht besteed aan de menselijke en organisatorische aspecten om afwijkend gedrag te kunnen herkennen voor toezicht in diverse situaties. Bij het project Passieve sensoren in dit VP security wordt met gebruikmaking van die resultaten van het VP Veilige Maatschappij een kennisbasis voor toezicht op maat ontwikkeld. De belangrijkste vraag in dit project is: welk type toezichtsysteem en in welke configuratie, is het meest geschikt in welke situatie en waarom? Het is dan cruciaal dat er evenwichtig met heel verschillende randvoorwaarden wordt omgegaan; denk aan: beschikbaar budget, dreigingsniveau, mate van gevoeligheid van waarop toezicht gehouden wordt, acceptatie van loze alarmen en intrinsieke structuur van het veiligheidsprobleem. De resultaten van dit project moeten bijdragen aan de mogelijkheden voor bedrijven om zich te profileren ten opzichte van andere bedrijven, en om beter aansluiting te vinden bij hun specifieke klantsegment.

Op de kruising van toezichttypen en toepassingsgebieden liggen de kansen.
In 2013 zijn voor vijf kruispunten in nauwe samenwerking met het bedrijfsleven verkenningen (zogenaamde “challenges”) uitgevoerd, waarbij de concrete vraagstelling van een probleemeigenaar vanuit het betreffende toepassingsgebied de uitdaging centraal stond. Bij deze challenges zijn in-kind bijdrages van bedrijfsleven en andere stakeholders geleverd om in een zeer kort tijdsbestek de meerwaarde van een mogelijke oplossing aan te tonen. De doelstelling was om voor minstens twee challenges vervolgonderzoek te doen om een ontwikkeltraject te initiëren.

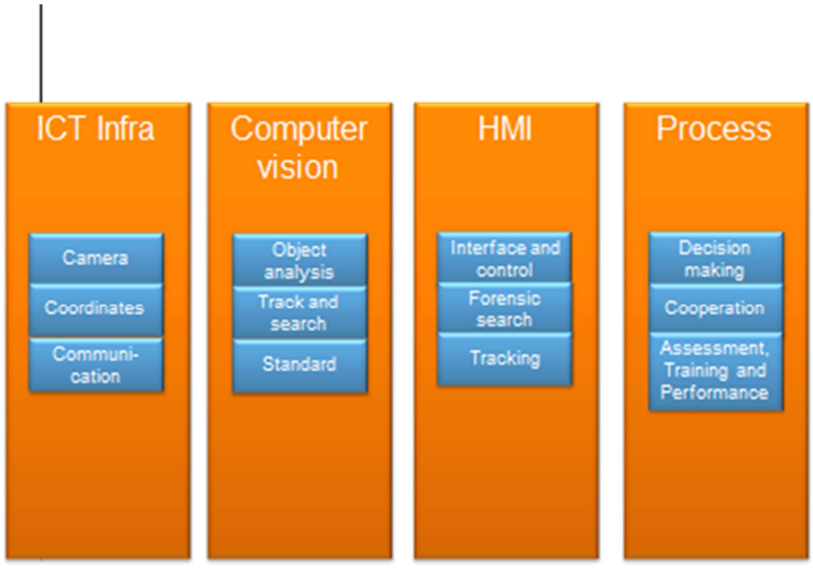
Verder is in 2013 gewerkt aan technologisch onderzoek voor twee specifieke onderwerpen die aansluiten bij de behoeftes van de LoI ondertekenaars; (middellang / lange termijn kennisontwikkeling voor bedrijven):

- afwijkend gedrag detectie op situatie-niveau middels combineren van losse activiteiten om tot ketens van gedrag te komen,
- activiteitsherkenning op signaal- en objectniveau middels wide baseline multi-viewpoint sensoren (camera's).

4.3.2 Gerealiseerde voortgang

Challenge 1. Volgen en Terugvinden van Personen

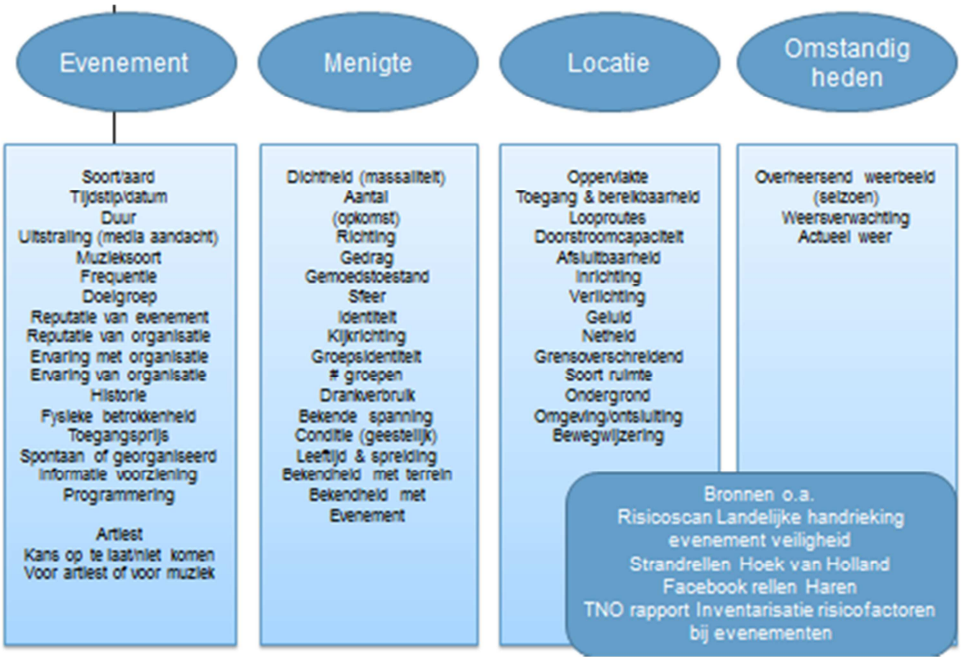
Schiphol is een van de meest uitdagende en prominente toezichtlocaties van Nederland. Als bedrijf en als nationale luchthaven heeft het te maken met diverse bedreigingen van de continuïteit en van haar imago. Om die dreigingen het hoofd te bieden werkt Schiphol samen met een groot aantal organisaties, waaronder KMar, Douane en veiligheidsdiensten. Deze uitvoerende organisaties maken o.a. gebruik van cameratoezicht en van toezicht op de werkvloer zelf. De KMar heeft TNO gevraagd om een oplossingsrichting te verkennen van diverse problemen zoals achtergelaten bagage en indringers in gesloten compartimenten.
Deze oplossingsrichting is het volgen en terugvinden van personen. In een challenge in mei heeft TNO in nauwe samenwerking met KMar, Schiphol en hoofdleverancier Bosch een roadmap geschreven voor het invoeren van deze oplossingsrichting. Deze roadmap ligt nu bij het GMI en bij het delegatieoverleg. In deze roadmap wordt beschreven hoe upgrades in ICT infrastructuur, video analytics, contextuele user interfaces en aanpassingen in werkprocessen kunnen leiden tot significante verbeteringen. Deze roadmap is ook als best practice ingebracht in Thematic Group on Surveillance & Video Analytics van de ERNCIP (European Research Network on Critical Infrastructure Protection)



Figuur 23 Vier pijlers van de ontwikkelde roadmap voor het volgen en terugvinden van personen op grote luchthavens.

Challenge 2. Evenementenveiligheid (samen met deelroadmap System of Systems)
TNO is sinds 2005 betrokken bij de ontwikkeling van systemen voor crowd management bij voetbal (i.s.m. diverse MKB, gemeente Den Haag, ADO Den Haag en KNVB). Na een verkenning van het bredere onderwerp “evenementenveiligheid”. heeft TNO in juni 2013 een workshop georganiseerd op het netwerkevent InFocus. Daar resulteerde een stevige discussie tot het aanbod van de politie en de Vierdaagse organisatie in Nijmegen om samen met TNO mogelijkheden voor innovatie te concretiseren. Deze begin september uitgevoerde challenge heeft geleid tot de identificatie van een verzameling van zeven parameters van een menigte die het waard zijn om te observeren tijdens een evenement. Voor twee van deze parameters (sfeer en samenstelling) zijn zowel de operationele definitie als de meetmethode onvoldoende specifiek of bekend. Hier liggen kansen voor het bedrijfsleven en de wetenschap om tot innovatie te komen.

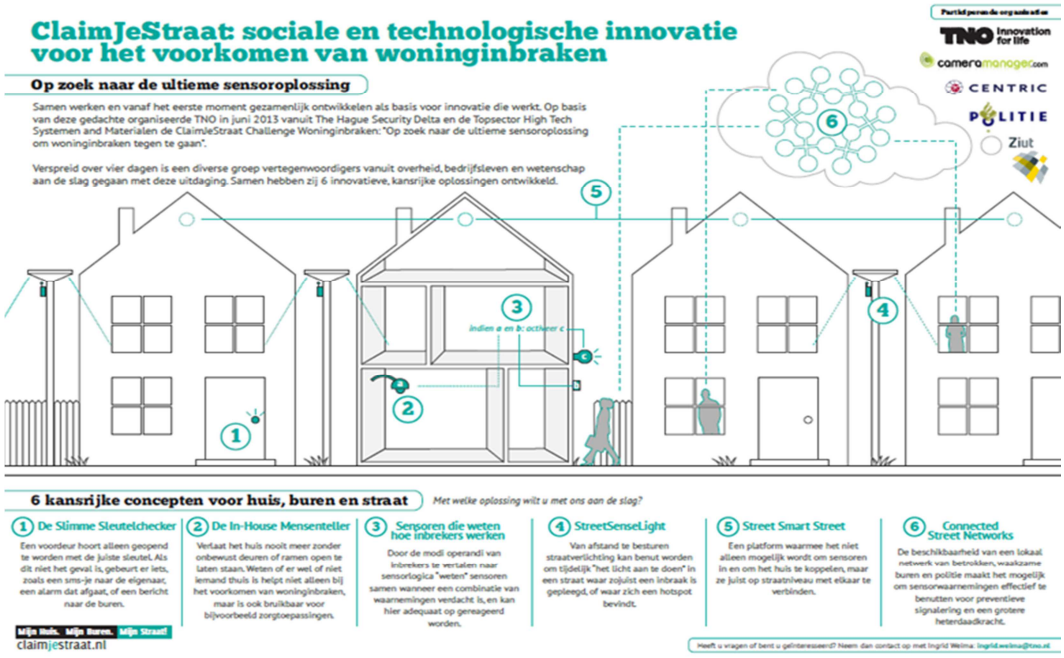
Naar aanleiding van de presentatie over het resultaat van deze challenge in oktober 2013 bij de CCR Summit te Kerkrade is er ook op strategisch niveau een initiatief voor evenementenveiligheid uitgewerkt: de CrowdAcademy. Doordat evenementen in locatie, tijd en organisatie strak afgebakende fenomenen zijn, is het lastig gebleken om ervaringen door te vertalen naar lessen voor de toekomst.
In de CrowdAcademy kan een geharmoniseerd model van evenementen worden ontwikkeld, waarop ieder evenement is te projecteren. Hierdoor wordt het mogelijk om de representativiteit van ervaringen op objectieve wijze zichtbaar te maken en zo een optimale aanpak bij nieuwe evenementen te realiseren. TNO is op zoek naar manieren om deze suggestie met het bedrijfsleven en (lokale) overheden nader uit te werken.



Figuur 24 CrowdAcademy: Interatief leren van evenementen.

Challenge 3. Woninginbraken & High impact Crime (i.s.m. the Hague Security Delta & ClaimJeStraat)
Woninginbraken en high impact crime raken de burger direct. Daarom is het een speerpunt van de Nationale Politie en van het Ministerie V&J om deze vorm van

criminaliteit significant terug te dringen. Voor het Nederlandse MKB liggen hier kansen indien gebruik wordt gemaakt van social media, domotica en passieve sensoren. Politiechef Frans Heeres, portefeuillehouder woninginbraken is als challenger opgetreden voor een vijftal MKB's die ambities hebben op dit gebied. De challenge is nog niet afgerond, maar de eerste resultaten worden wel al zichtbaar. Deze gaan in op de verschillende "schillen" rond een woning: de voordeur, de woning zelf, de woning en haar buren, en de straat voor de woning.



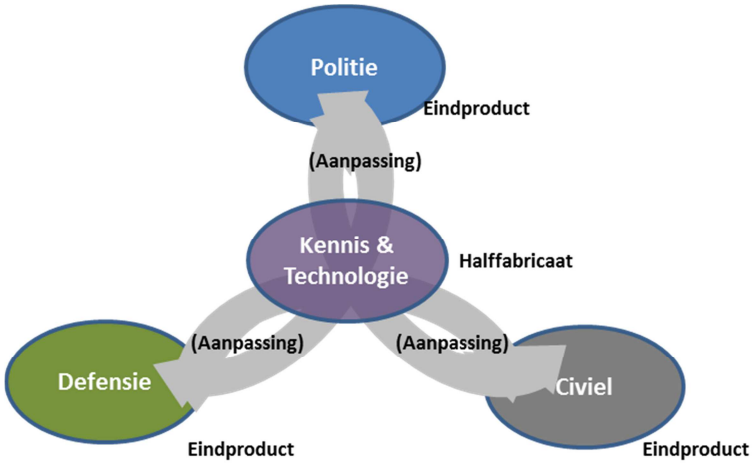
Figuur 25 Zes complementaire innovaties om woninginbraak en high-impact crimes in de woonwijk tegen te gaan.

Challenge 4. Crowd Management (in samenwerking met System of Systems)
Schiphol en andere grote OV-locaties hebben te maken met eisen en wensen vanuit safety en comfort in relatie tot de drukte en de doorstroming op hun locaties. Concrete risico's zijn het oplopen van vertraging in het vertrek van vliegtuigen of treinen door vertraagde passagiers, verdrukking en een slecht imago. In 2013 is een visie ontwikkeld op een crowdmanagement groeipad. Van monitoring van actuele drukte via voorspellen van drukte naar pro-actief optreden. In de herfstvakantie is een druktemeting uitgevoerd om een begin te maken met het kwantificeren van drukte, en met het vaststellen van de grootte van het probleem. De resultaten zullen binnenkort worden opgeleverd, en kunnen ook in het kader van de challenge evenementenveiligheid meerwaarde hebben.

Challenge 5 (in voorbereiding). Civiel militaire samenwerking bij innovatie-trajecten.
De ministeries van Defensie en Veiligheid en Justitie werken hard aan het ontwikkelen van verdergaande samenwerking tussen defensie en civiele veiligheidsorganisaties. TNO is door haar intensieve relatie met beide werelden bij uitstek in de positie om hier op een veilige en effectieve wijze aan bij te dragen. Ook voor innovatie-trajecten biedt civiel-militaire samenwerking perspectief.
Er rijzen dan wel een aantal vragen. Welke concrete voordelen zijn er dan voor de betrokken organisaties? Wat kan er tijdens het onderzoek en de ontwikkeling gedaan worden om eventuele nadelen te ondervangen? Welke concrete rollen

spelen TNO, het bedrijfsleven en de Nederlandse overheden daar in?
Aan het einde van 2013 is een beknopte verkenning gedaan naar de antwoorden op deze vragen. Dit heeft geleid tot een beknopte white paper die in Q1 2014 afgerond wordt.

Vervolgens zal worden onderzocht welke concrete producten, diensten of systemen voldoende kansrijk zijn om te investeren, bijvoorbeeld in een challenge.



Figuur 26 Civiel-militaire samenwerking is maatwerk.

Technologische ontwikkelingen

- *Detectie afwijkend gedrag te midden van normaal gedrag middels combineren van losse activiteiten om tot ketens van gedrag te komen.*
  Een goede dataset waarin zowel normaal, als afwijkend gedrag te zien is, ontbreekt. TNO is met het project WPSS (Watching People Security Services) in de positie om zo'n dataset wel te maken. In 2013 hebben we daarom 30 zakkenrolincidenten nagespeeld in winkelcentrum Kanaleneiland. Dit heeft een unieke dataset opgeleverd met daarin zowel normaal (van winkelende mensen) als afwijkend (van onze zakkenrol-acteurs) gedrag. Deze dataset is kwalitatief van hoog niveau omdat de camera's (met bijdrage van AXIS) en cameraposities optimaal zijn en omdat het aantal viewpoints op de scene hoger ligt dan normaal. Hierdoor is het mogelijk om zowel goede tracking, als goede gedragsdetectie te doen. De dataverwerking is nu nog aan de gang, maar er is vanuit diverse hoeken al interesse getoond in deze dataset. We moeten daarbij rekening houden met beperkingen vanuit de privacy en bescherming persoonsgegevens.
- *Activiteitsherkenning op signaal- en objectniveau middels wide baseline multi-viewpoint sensoren (camera's).*
  De algoritmes van het voor DARPA uitgevoerde project CORTEX en aanpalende projecten zijn typisch gericht op een enkele camera. In 2013 hebben we deze algoritmes uitgeprobeerd op een laboratorium dataset van IXMAS. Hier hebben we geleerd dat reeds het toevoegen van één extra gezichtspunt de prestaties flink verhoogd, tot 96,4%. In nog niet gepubliceerd werk hebben we ook verder gekeken naar het leren vanuit een gezichtspunt, en het detecteren vanuit een ander gezichtspunt. Deze kennis is uniek voor passieve sensoren zoals camera's, vanwege hun directionele aard. Met het werk over meerdere gezichtspunten lopen we vooruit op de trend van steeds meer camera's, en de hoge verwachtingen van Video Content Analysis (VCA).

Met het werk over “0+0=1” lopen we vooruit op de trend van meerdere modaliteiten zoals geluid, menselijke tags in combinatie met VCA.

De opgebouwde kennis over gezichtspunten samen met de gedragsherkenning uit het militaire domein van CORTEX zorgt dat zowel defensie als civiele toepassingen hier nut bij hebben.

Netwerkevent InFocus
In 2012 is vraagarticulatie als belangrijkste behoefte uitgesproken door de LoI-bedrijven. Hoewel dit in eerste instantie een zaak is tussen verwerver en aanbieder, kan TNO helpen om dit proces te stimuleren. Na de inventarisatie van de kennisbehoeften en innovatie-uitdagingen bleek er begin 2013 een gefragmenteerd beeld van de waarop Passieve Sensoren zich zou moeten concentreren. Naast de al ingezette challenge bij Schiphol werd daarom in juni het netwerk evenement “InFocus” georganiseerd om een breder gedragen ambities te ontwikkelen.
De bijeenkomst InFocus werd georganiseerd langs drie lijnen:
1) wat zijn de grote trends, met name de kansen en bedreigingen van informatieverwerking,
2) wat zijn concrete vragen in vier specifieke segmenten (transport & logistiek, toezicht openbare ruimte, bewaken & beveiligen en evenementenveiligheid),
3) welke samenwerkingen zijn nodig om op die vragen concrete impact te bereiken?

Middels plenaire sessies, workshops en veel vrije ruimte voor het leggen van contacten is daar invulling aan gegeven. Details zijn in een verslag vastgelegd.

4.3.3 Publiciteit

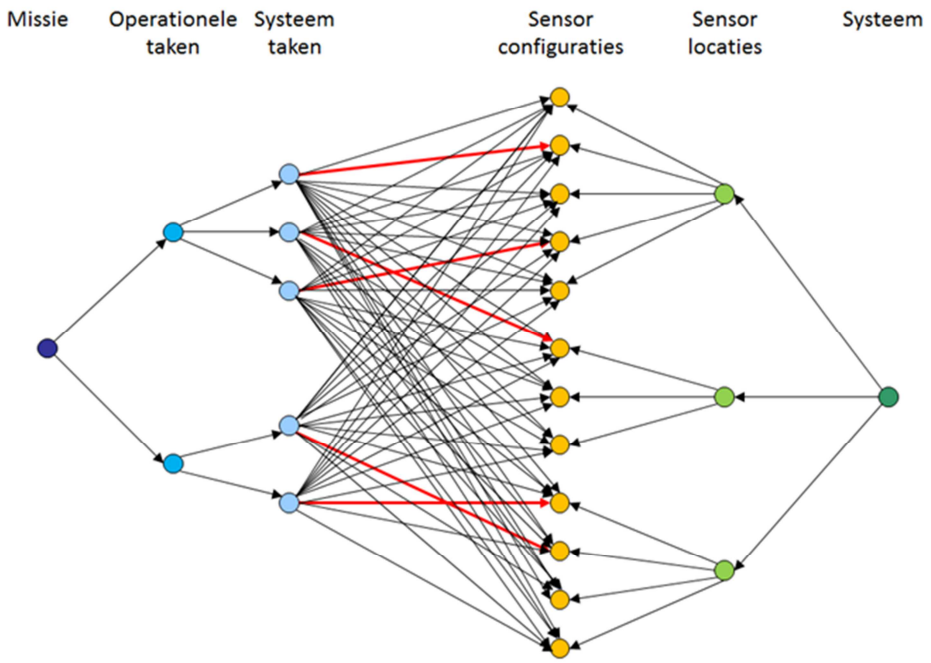
- van Rest, J., et al. "Requirements for multimedia metadata schemes in surveillance applications for security." Multimedia Tools and Applications (2013): 1-26.
- Bouma, Henri, et al. "Real-time tracking and fast retrieval of persons in multiple surveillance cameras of a shopping mall." SPIE Defense, Security, and Sensing. International Society for Optics and Photonics, 2013.
- Bouma, Henri, et al. "Behavioral profiling in CCTV cameras by combining multiple subtle suspicious observations of different surveillance operators." SPIE Defense, Security, and Sensing. International Society for Optics and Photonics, 2013.
- Diverse voordrachten bij InFocus, o.a. over de definities van afwijkend gedrag;
- Voordracht bij CCR Summit “Crowd Academy”.
- Onderhouden van BOIDS-patent over het automatisch bepalen van intenties van (groepen) mensen.

4.4 Deelroadmap Actieve sensoren

Voor de deelroadmap Actieve sensoren bestaat er al jaren een intensieve samenwerking tussen Defensie, Thales, TNO en TU-Delft. Er is hier sprake van een Gouden driehoek avant la lettre. In het kader van de Roadmap Security is er in 2012 naast de lopende defensieprogramma’s gewerkt aan het STARS-project en het DAISY-initiatief.
In het vervolg van het programma zal verkend worden welke toepassingen van actieve sensoren (technologie) aansluiten bij de behoeften in het civiele

veiligheidsdomein. Het is de ratio van STARS, en ook al is de tijdshorizon van laag TRL naar toepassing van STARs technologie nog meerdere jaren weg, er zijn toch potentieel waardevolle toepassingen. Er wordt bijvoorbeeld gedacht aan een miniradar als all weather/ pre alert node als aanvulling op slimme camera's en ook aan een mini radar netwerk (project Raebell) om kleine UAV's in een stedelijke omgeving te detecteren).
In het kader van deze deelroadmap zijn er drie meerjarenprojecten met substantiële bijdragen vanuit het bedrijfsleven in uitvoering:

1. *STARS (Sensor Technology Applied in Reconfigurable Systems)*
   Het STARS-programma is gericht op de ontwikkeling van nieuwe sensortechnologie, waarmee een dominante informatiepositie kan worden opgebouwd in een complexe, hoog dynamische omgeving. De kern van de innovatie in dit programma is het realiseren van sensoren en sensorsystemen die na hun installatie nog gereconfigureerd kunnen worden om bruikbaar te worden voor waarnemingsdoelen en –taken, die oorspronkelijk niet zo waren voorzien. Dit project wordt uitgevoerd door een consortium bestaande uit Thales NL, NXP Semiconductors, Recore Systems, TNO, TU-Delft en de Universiteit Twente.



Figuur 27 Voorbeeld van een decompositie van een missie in operationele taken en systeemtaken en een toewijzing van systeemtaken aan een systeem met herconfigureerbare sensoren op verschillende locaties.

2. *MAGNUS*
   Van belang is dat er binnen Europa een toegankelijke GaN supply chain is. Hieraan is in het kader van het EDA-project "KORRIGAN" gewerkt. In het kader van het huidige EDA project "MAGNUS" zal deze supply chain gebruikt worden om het praktische gebruik en de voordelen van op GaN technologie gebaseerde MMICs voor gebruik in phased array zend/ontvangst modules te demonstreren. Open vragen bij dit door Thales gecofinancierde project zijn: welke functies kunnen het best met behulp van GaN technologie gerealiseerd

worden en welke performance verbetering ten opzichte van bestaande technologie zijn hiermee mogelijk?
In 2013 zijn er schakelaar modellen ontwikkeld op basis waarvan X-band zend/ontvangst schakelaars met een vermogen van meer dan 40 Watt gerealiseerd kunnen worden. Hiermee wordt een aanzienlijke ruimte winst en kostenbesparing bereikt.
Ook zijn er robuuste GaN lage ruis versterkers gerealiseerd, die een 3 maal lagere DC dissipatie hebben dan de bestaande op GaN gebaseerde lage ruis versterkers.

3. *Solid state Transmitter & Receiver ICT (StrICt)*
   Er is vanuit de markt behoefte aan steeds verder geïntegreerde hoogvermogensversterkers, die zowel goedkoper zijn, meer efficiënt en een hoger uitgangsvermogen hebben. Een van de methoden om in deze behoefte te voorzien is de ontwikkeling van GaN MMIC technologie.
   Dit onderzoek met cofinanciering van Thales richt zich op de mogelijkheid om met een nieuwe ontwerpmethode zonder ingrijpende wijzigingen in de technologie toch versterkers te ontwikkelen die een hoog vermogen kunnen genereren of die goed met grote signalen om kunnen gaan. Marktpartijen die baat kunnen hebben bij deze ontwikkeling zijn sensorfabrikanten, microgolf systeem fabrikanten en componenthuizen.

4.5 Projecten met financiering van derden

De portefeuille van projecten met financiering van derden op het gebied van de roadmap Security heeft zich in 2013 goed ontwikkeld. Nieuwe projecten hebben een scoop die op de inhoud van de roadmap en de belangen van Nederlandse stakeholders zijn afgestemd. In het overzicht in Bijlage A is vermeld om welke projecten het gaat en welke Nederlandse partijen hierbij betrokken zijn.
Het portfolio van deze projecten vormt een substantiële basis voor uitbouw van de samenwerkende consortium voor de roadmap Security. De resultaten worden apart gerapporteerd aan de projectparticipanten en de fundingorganisaties. De vindplaats van gepubliceerde resultaten is ook in Bijlage A vermeld.

A Overzicht van projecten met matchende financiering van publieke en private stakeholders

Project	Deel-Roadmap Security	Projectdoel	Partners uit NL naast TNO	Verwijzing naar Rapportage/ publicatie
STARS	**Actieve sensoren**	Het binnen vier jaar ontwikkelen van de noodzakelijke kennis en technologie waarmee in Nederland reconfigureerbare sensoren en sensornetwerken kunnen worden gebouwd. Deze sensoren kunnen flexibel ingezet worden doordat de functionaliteit die opgesloten ligt in het systeem relatief eenvoudig en snel is te wijzigen.	Thales NL, NXP, Recore , TU Twente, TU Delft. Opengedeelte voor extra partners.	www.starsproject.nl/
Solid state Transmitter & Receiver ICT (StrICt; cofinanciering)	**Actieve sensoren**	Een ontwerpmethode voor versterkers die een hoog vermogen kunnen genereren en goed met grote signalen omgaan.	Thales	Vooralsnog vertrouwelijk i.v.m. patentbescherming
MAGNUS (cofinanciering)	**Actieve sensoren**	Demonstratie van het praktische gebruik en de voordelen van op GaN technologie gebaseerde MMICs voor gebruik in phased array zend/ontvangst modules.	Thales	Vooralsnog vertrouwelijk i.v.m. patentbescherming
ADABTS	**Passieve sensoren**	ADABTS aims to facilitate the protection of EU citizens, property and infrastructure against threats of terrorism, crime, and riots, by the automatic detection of abnormal human behaviour.	UvA, KLPD	www.informationsystems.foi.se/~adabts-fp7
TACTICS	**Passieve sensoren**	TACTICS seamlessly integrates new research results in the area of behaviour analysis, characteristics of the possible urban-based targets and situational awareness into a decision making framework comprising of a coherent set of tools and related processes, supporting security forces in responding more efficiently and effective to a given threat in order to actually prevent the attack or to limit its consequences.	KLPD, KMAR	net gestart
Watching people Security Service (Pijler 2)	**Passieve sensoren**	Combineren van verschillende mogelijkheden van tracking en detectie van afwijkende gedragingen en gebeurtenissen voor een mv toepassing	Vicar Vision, Eagle Vision Systems, Cameramanager.com, Noldus Information Technology, Borking Consultancy	www.vicarvision.nl/WPSS.html
Competentie-profiler	**Passieve sensoren**	Ontwikkelen van een competentieprofiel voor profilers die in het rijksmuseum afwijkend gedrag zullen moeten spotten en hierop kunnen reageren	Rijksmuseum, Van Gogh museum	http://www.tno.nl/content.cfm?context=overtno&content=nieuwsbericht&laag1=37&laag2=2&item_id=2012-10-17_09:43:35.0
Seabilla	**Passieve sensoren**	The SeaBILLA proposal aims at a cost-effective European Sea Border surveillance system	Thales NL, HITT	www.seabilla.eu
ARENA	**Passieve sensoren**	**A**rchitecture for the **R**ecognition of thr**E**ats to mobile assets using Networks of multiple Affordable sensors	TNO (Gebruikers Schiphol, KMar, Politie)	www.informationsystems.foi.se/~arena-fp7
SOBEK	**Passieve sensoren**	Hydrofoonarrays voor het detecteren van duikers en kleine bootjes in de omgeving van bedreigde objecten in havens	Aruba Ports Authority NV (Havenbedrijf Rotterdam), Douane, min v Defensie	www.tno.nl/downloads/TNO_%20SOBEK.pdf
PROTECT RAIL	**Systems-of systems**	A software based foresight system to imagine alternative long term developments for the future railway security system up to a range of 20 years	Prorail, NS, OV, Arriva, HTM, RET, GVB, veiligheidsregio Rijnmond via Klankbordgroep en Europese UETP	www.protectrail.eu
SECUR-ED	**Systems-of systems**	System architecture including sensor systems for CBRN-E detection for secured urban transportation	Prorail, NS, OV, Arriva, HTM, RET, GVB, veiligheidsregio Rijnmond via Klankbordgroep en Europese UETP	www.secur-ed.eu
XP-DITE	**Systems-of systems**	Development, demonstration and validation of a comprehensive approach to the design and evaluation of integrated security checkpoints for aviation security	TNO, Schiphol KLM, KMAR, NCTV	www.xp-dite.eu
COPRA	**Systems-of systems**	A roadmap for a comprehensive European approach to secure civil aviation.	KLM-AirFrance Schiphol, KMAR, NCTV	www.copra-project.eu/ Analysis of Future Threats to Civil Aviation within the Project COPRA, Proc future Sec Conf, 2012, 493
TrainingsOmgeving voor groot-schalig multidisciplinair KetenOptreden(TOKO,Pijler 2)	**Systems-of-systems**	Verbeteren van oefenen met ketenoptreden	Thales Nederland BV, System Navigator consultants BV, Bizz design BV, St. Novay	www.agentschapnl.nl/onderwerp/toko in 2013 eindrapportage
Informatie-preparatie overstromingen (cofinanciering)	**Systems-of-systems**	Real Time Intelligence en informatiepreparatie in samenwerking met ketenpartners en vitale infrastructuur	Universiteit Twente, NIFV Veiligheidsregio Hollands – Midden, HH Rijnland, Alliander	www.tno.nl/downloads/BOEKRAP_OVERSTROMINGSRISICOS_DEF.pdf
Advanced Risk management (cofinanciering)	**Cybersecurity**	Ontwikkelingen van een verplichtingen-verwachtingen model voor beheersing van de risico's van informatie-uitwisseling in complexe ketens van organisaties	TNO, BKWI, UWV; contacten met banken en PostNL	TNO-publicatie Advanced Risk Management