Integrale Veiligheid
Kampweg 5
3769 DE Soesterberg
Postbus 23
3769 ZG Soesterberg

www.tno.nl

T +31 88 866 15 00
F +31 34 635 39 77
infodesk@tno.nl

TNO-rapport

TNO-DV 2012IN064

Thema Integrale Veiligheid
Vraaggestuurd programma 2011-2014
Voortgangsrapportage 2011

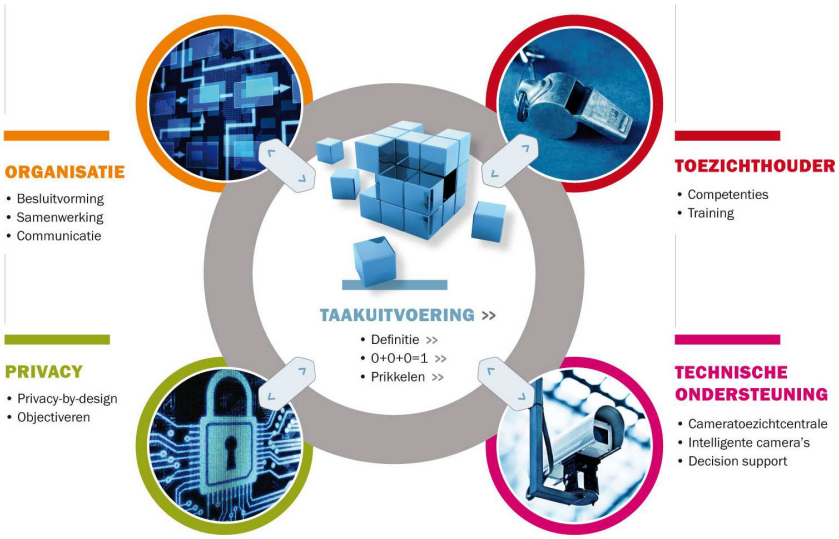
Datum	maart 2012
Auteur(s)	Dr.ir. J.A. Don (programmamanager)
Regievoerend departement	Ministerie van Veiligheid en Justitie
Projectnummer	053.01011/01.02
Rubricering rapport	Ongerubriceerd
Titel	Ongerubriceerd
Samenvatting	Ongerubriceerd
Rapporttekst	Ongerubriceerd
Aantal pagina's	30
Geautoriseerd door	Drs. H.G. Geveke
Handtekening	

Samenvatting

In 2011 is het TNO-Meerjarenonderzoeksprogramma Maatschappelijke Veiligheid 2011-2014 van start gegaan. Daarbij gaat het tegelijkertijd om het realiseren van impact op de toekomstige veiligheidssituatie in Nederland en het versterken van de basiskennispositie bij TNO. Dit rapport biedt voor het TNO-management en het regievoerend departement Veiligheid en Justitie een rapportage van de voortgang in 2011.

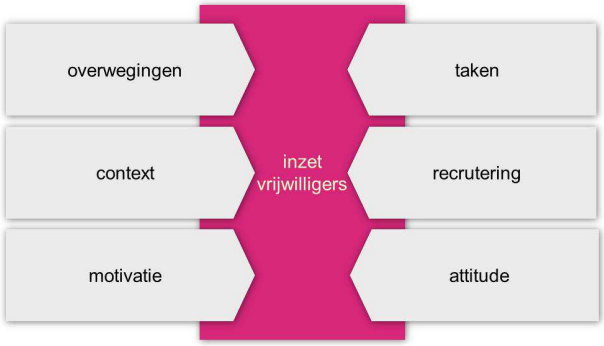
Op de vijf topics binnen het programma zijn in 2011 als belangrijkste resultaten bereikt:

- *Topic 1. Herkennen afwijkend gedrag*
  Er is een basismodel ontwikkeld om toezichtsorganisaties optimaal te ontwerpen:



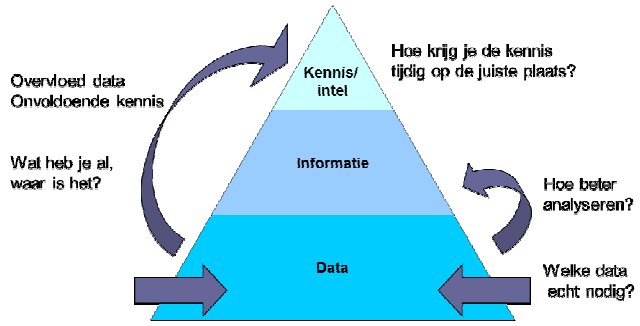
  Daarnaast is een video analyse tool ontwikkeld, waarbij men in het scherm benoemd ziet welke gedraging in beeld te zien is. Ook is er kennis opgebouwd over het prikkelen van mensen door beveiligingsmedewerkers om hun eventuele kwade intenties beter te onderscheiden.

- *Topic 2. Activering van burgers*
  Een belangrijk vraagstuk bij de activering van burgers voor veiligheid is de matching van competenties, motivatiebepalende factoren en te leveren bijdrage aan de veiligheid van henzelf en hun omgeving. Voor deze vraagstelling is het volgende analyse-kader opgesteld:

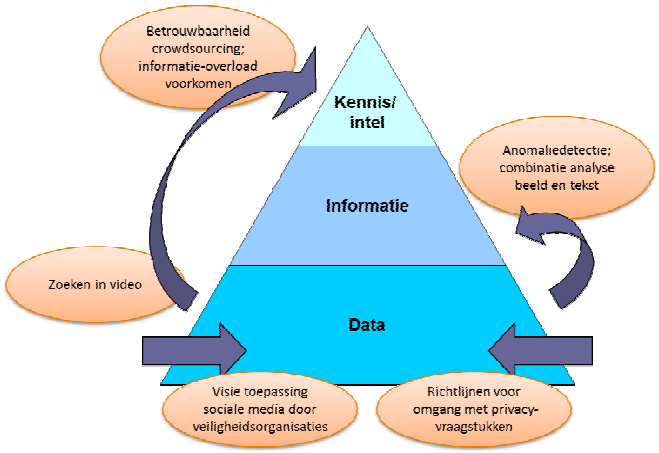


Daarnaast is experimenteel onderzocht hoe communicatie naar de burgers via social media geoptimaliseerd kan worden.

- *Topic 3. Slimmer omgaan met grote hoeveelheden informatie*
  Met name op het gebied van anomaliedetectie (op internet/open bronnen) en op gebied van zoeken in video zijn een aantal nieuwe zoekmethoden (door-) ontwikkeld. Deze worden ingezet in diverse nationale en internationale projecten.

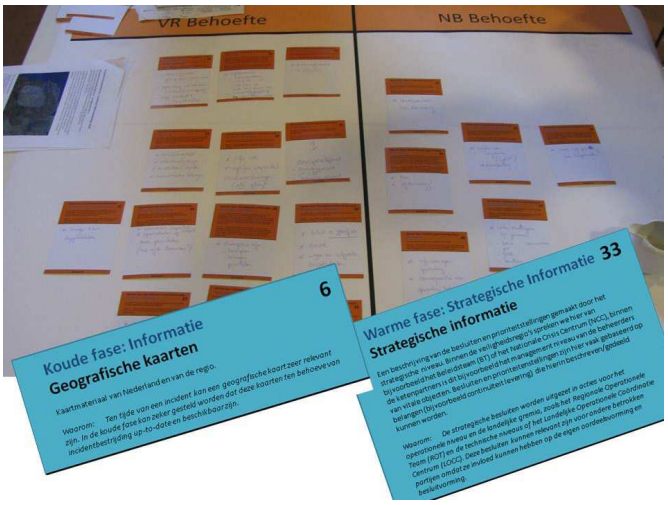


Figuur 1. De Informatiepiramide: data wordt verrijkt tot kennis



Figuur 2. De onderwerpen van topic 3 in 2011

- *Topic 4. Beter benutten van informatiestromen en samenwerking*
  Informatieaanbod voor samenwerkende professionals in de veiligheidsketen. Collaboration awareness vertelt je wat je moet weten van je crisispartners. Na de analyse in 2011 onderzoeken we in 2012 wat er in de koude fase èn wat er in de warme fase moet gebeuren om samenwerking te verbeteren. Dit moet ook leiden tot een training voor multidisciplinaire samenwerking.



- *Topic 5. Cybersecurity*
  In 2011 was een belangrijke onderzoeksvraag hoe misbruik van huidige en toekomstige mobiele platformen (Smart Phones) tijdig gedetecteerd kunnen worden op een wijze die effectieve opsporing en vervolging mogelijk maakt. Het in het onderzoek opgestelde overzicht van de trends in het mobiele domein geeft inzicht in dreigingen ten aanzien van de verschillende stakeholders. Verder is in kaart gebracht, aan de hand van interviews, welke rol smartphones hebben in misdaad/misbruik en in welke mate de overheid hierop is voorbereid. Twee conclusies waren dat traditionele opsporingsmiddelen afnemen in effectiviteit en dat detectie van grootschalig misbruik integraal inzicht vereist. De resultaten van het onderzoek zijn gepresenteerd voor de Telecom-ISAC.
  Een andere onderzoeksvraag was hoe *Security by design* kan worden ingebed in een op ICT gebaseerde vitale infrastructuur? De ontwikkelingen rond smart grid security zijn daarom in kaart gebracht met een overzicht van de belangrijkste factoren die de security van de vitale op ICT-gebaseerde infrastructuur bepalen. Het betreft hier niet alleen technische factoren, maar ook organisatorische maatregelen zowel over organisaties heen als binnen een enkele organisatie, en aanpassingen in de gebruiksmogelijkheden. Tevens is bijgedragen aan een EU-taakgroep rond smart grid security. Een deel van de resultaten van het onderzoek is in dit kader getoetst.

TNO heeft in 2011 in samenwerking met private en publieke stakeholders bijgedragen aan de ontwikkeling van gezamenlijke visies op gewenste ontwikkelingen voor vergroting van veiligheid in de maatschappij. Dit is vastgelegd in een aantal documenten en door TNO gepubliceerde White papers:

- De Nationale Cyber Security Research Agenda
- De Roadmap *Security* in het kader van de Topsector High Tech Systems & Materials
- White paper *Social media, burgerparticipatie en sociale veiligheid*
- White paper *Crowdsourcing in de opsporing*
- White paper *Van situation awareness naar collaboration awareness*
- R&D mapping of *Projects/products/methods and techniques for various crisis management tasks* (Europees project ACRIMAS)

Een belangrijke uitdaging voor 2012 is het stroomlijnen van de ontwikkelingen in het kader van de Roadmap security en het VP Veilige Maatschappij Daarbij is optimaal samenspel nodig tussen overheidsorganisaties met veiligheidstaken (als politie,

brandweer, GHOR, Defensie en KMar), bedrijfsleven en andere kennisinstellingen. Een aparte dimensie is de ontwikkeling van een Europese onderzoeksagenda in het kader van *Horizon 2020*.

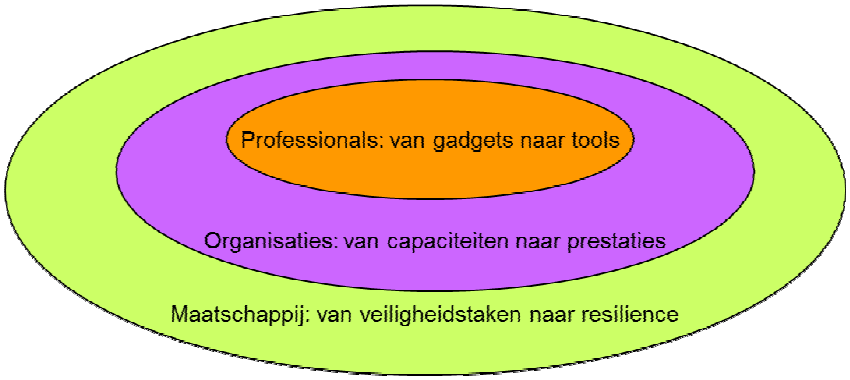
Inhoudsopgave

1 Inleiding

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 zeven impactdoelen:

- Nationale Veiligheid en crisismanagement
- Efficiënt en effectief toezicht
- Community resilience
- Opsporing en handhaving
- Secure mass transport & aviation
- Veilige gebouwen terreinen en infrastructuur
- Cybersecurity

Voor de ontwikkeling van de strategie en de programmering van het Vraaggestuurde onderzoek voor het Innovatiegebied Wereldwijde Krijgsmacht, vindt de afstemming tussen de overheid en TNO plaats onder regie van het Ministerie van Defensie. In deze voortgangsrapportage van het Meerjarenprogramma 2011-2014 voor het Thema Integrale Veiligheid wordt alleen het Innovatiegebied Veilige Maatschappij behandeld.

Management oordeel over de uitvoering
Het jaar 2011 is het eerste jaar van de uitvoering van het Meerjarenonderzoeks-programma 2011-2014 Veilige Maatschappij. Dit jaar was voor dit VP ongekend turbulent:

- TNO ging per 1 januari 2011 in een nieuwe organisatiestructuur van start.
- Het regievoerende departement Veiligheid en Justitie maakte een grootschalige reorganisatie door, waardoor alle contactpersonen voor het VP Veilige Maatschappij werden vervangen door nieuwe begeleiders.
- De veiligheidsregio's zijn druk bezig met de invoering van de nieuwe Wet op de Veiligheidsregio's, terwijl de politie zwaar bezet is met de voorbereiding van de invoering van de nationale politie.
- Het innovatiebeleid van het Ministerie Economie, Landbouw en Innovatie werd op een nieuwe leest geschoeid, waardoor medio september duidelijk werd dat het VP-budget voor 2012 met 50% gereduceerd zou zijn.

Ondanks bovengeschetste dynamiek is de uitvoering van de VP-projecten soepel verlopen. De nieuwe organisatie van TNO bleek ook gunstig voor het inzetten van medewerkers uit afdelingen, die tot 1 januari 2011 in meerdere kerngebieden werkten. Verder hebben vrijwel alle begeleiders met grote betrokkenheid bijgedragen aan het op stoom krijgen van de uitvoering.

Bij de uitvoering van het project voor topic 4 (Beter benutten van informatiestromen en samenwerking) bleken de ambities rond lessons learned en collectief geheugen niet haalbaar. Dit heeft geleid tot bijstelling van het plan in overleg met de begeleiders vanuit VenJ.
De uitvoering van de verkenningen bleek een duidelijke toegevoegde waarde te hebben door een nieuwe opzet met directe interactie met stakeholders van VenJ, politie en brandweer. Door de budgetreductie van het VP in 2012 dreigden de ontwikkelingen niet met de gewenste snelheid tot stand te komen. VenJ heeft echter acties genomen om dit op andere wijze alsnog te realiseren.

Het ministerie VenJ heeft in 2011 het belang van het VP met daden erkend door:

- het faciliteren van de koppeling van de VP-inhoud aan actuele en toekomstige behoeften van overheid en bedrijfsleven.
- het betrekken van TNO bij het opstellen van een Strategische Innovatie-agenda voor VenJ zelf. Dit document wordt ingebracht in de discussie binnen VenJ hoe innovatie in de nieuwe organisaties moet worden verankerd; uitdaging is om na het vervallen van de pijlerfondsen innovatie zo in te bedden dat het niet meer een de facto-kostenpost is, maar een renderend investeringsfonds, dat leidt tot meer effectiviteit, efficiency en veiligheid.
- naar aanleiding van de invoering van het (economische) topsectorenbeleid de verankering van Security in de topsectoren bij EL&I krachtig te bepleiten. VenJ heeft bovendien de schade, als gevolg van de budgetreductie van het lopende programma, met een financiële injectie van 1 M€ beperkt. Tegelijk vindt nu mede dankzij de steun van VenJ de opbouw plaats van een nieuw VP Security in de topsector High Tech Systems & Materials.

2 Vraaggestuurd programma Veilige Maatschappij

2.1 Vragen waar het programma zich op richt

Het regievoerend departement Veiligheid en Justitie (VenJ, destijds Binnenlandse Zaken) heeft voor focussering van de Meerjarenprogramma 2011-2014 de volgende organisaties geconsulteerd: Ministerie van Defensie, AIVD, NCTb, NICC, ICTU, Veiligheidsregio Noordoost Gelderland, NVBR, Brandweer Amsterdam, LFR, vts-PN, KLPD, CIV, Politieacademie en CCV. In een interactief proces heeft dit geleid tot de keuze voor een vijftal topics en een overkoepelend VP-onderdeel voor verkenningen:

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

2.2 Uitvoering in 2011

2.2.1 Begeleiding van de topics

- Beschrijving van de uitvoering van de onderdelen van het programma in relatie tot de gestelde planning en doelen. Benoem ook evt. tegenvallers, belemmeringen etc.
- Verloop van het overleg in kennisarena's en met stakeholders of andere gremia.
- Overzicht van mate van participatie in (inter)nationale onderzoeks-programma's en netwerken.
- Initiatieven met betrekking tot kennisontwikkeling met bedrijfsleven, kennisinstellingen of overheden.

Voor elk van deze topics is een coördinerend behoeftesteller voor de verdere uitwerking en uitvoering is aangewezen. Elke coördinerend behoeftesteller heeft vervolgens een begeleidingsteam gevormd en het kennisontwikkelingsplan voor 2011 opgesteld.

VP-topic (TNO-projectleider per 31.12.2011)	**Coördinerend behoeftesteller (per 31.12 2011)**
1. Herkennen afwijkend gedrag (Maaike Lousberg)	Desiree Geerts (VenJ, DG-NCTV)
2. Activering burgers (Gerard Veldhuis)	Marjan Heijman (NVBR)
3. Info-mining (Karin de Jong)	Bart Custers (VenJ, DG RR)
4. Infobenutting voor samenwerken (Josine van de Ven)	Jan Lavén (Centrum Innovatie en Veiligheid, Utrecht)
5. Cybersecurity (Marieke Klaver)	Jos Leenheer (VenJ, DG-NCTV)

Gedurende het jaar 2011 zijn er voor ieder topic minstens drie bijeenkomsten van het begeleidende team geweest. Verder zijn ook de coördinerend begeleiders drie maal bijeen geweest (maart, september, november).

Als gevolg van de reorganisatie van het departement Veiligheid en Justitie is de aansturing van het VP in juni 2011 overgedragen van Leo Nieuwenhuizen/ Michiel van der Duin en Sabine Geerdes naar Kees Lebon en Edmée Moojen.

2.2.2 Verkenningen

In december 2010 is er een viertal onderwerpen voor het uitvoeren van een verkenningen afgesproken, terwijl in juni het reservebudget bestemd is voor het ontwikkelen van een Europees initiatief voor validatie van security innovaties.

Titel verkenning (TNO-projectleider)	**Begeleider**	**Projectleider TNO**
Bestuurlijke drukte en infomanagement	Mony Adriaanse/ Roel Holvast (VenJ)	Hans van de Broek
Mijden groot gevaar	Marjan Heijman/ Ricardo Weewer (NVBR/NIFV)	Peter Petiet
Zelfgemaakte explosieven	Sven Hameling (VenJ)	Antoine van der Heijden
NLW-plus voor openbare ordehandhaving en bewaken en beveiligen	S. Keizers (VenJ) Otto Adang (PA)	Inge Wetzer Marike van der Horst
Europees platform voor validatie security innovaties	Geen; wel afgestemd met Michiel vd Duijn (VenJ)	René Willems

2.2.3 Deelname in projecten met nationale of EU-funding

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

Project-naam	**Onderwerp**	**Bron Funding**	**Topic VP 2011-2014**
ADABTS	Herkennen afwijkend gedrag	EU	1
WPSS	Tracken en tracen van mensen	MIA-V	1
ARENA	Herkennen dreigingen voor mobiele assets	EU	1
Game Valley	Veiligheidscompetenties	PiD	2
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
VIRTUOSO	Intelligence uit open bronnen	EU	3
GATE pilot safety	Serious Gaming burgemeesters	FES	4
EULER	Software defined radio	EU	4
ACRIMAS	Crisismanagement systems of systems	EU	4
TOKO	Training&opleiding keten-samenwerking	MIA-V	4
Cyber attack Detector	Cyber-Monitoring voor detectie bedrijfsspionage	MIA-V	5
ETCETERA	Verkenning security technologie	EU	6
DITSEF	Uitrusting First Responders	EU	Vorig VP

FRESP	Adembescherming first responders	EU	Vorig VP
RSTV	Sensors voor rookanalyse brand	MIA-V	Vorig VP
SECUR-ED	Veilig stedelijk transport	EU	Vorig VP
EMPHASIS	Opsporing explosieven productie	EU	Vorig VP
PREVAIL	Precursors zelfgemaakte explosieven	EU	Vorig VP
SPIRIT	Bescherming gebouwde infrastructuur	EU	Vorig VP
PROTECTRAIL	Integrale security railinfra	EU	Vorig VP
COPRA	Bescherming luchtvaart	EU	Vorig VP
Good practices manual for CIP	Bescherming vitale infrastructuur	EU	Vorig VP
VITRUV	Resilience stedelijke omgeving	EU	Vorig VP
Den Haag show-room Veilig NL	Veiligheid in de stad	PiD	Vorig VP
PRACTICE	Resilience tegen CBRN	EU	Vorig VP
DECOTESSC 1	Demo CBRN-respons	EU	Vorig VP
TWOBIAS	Monitoring biodreiging	EU	Vorig VP
CREATIF	Testen en certificeren CBRE-detectoren	EU	Vorig VP
SAFIRE	Verminderen radicalisering	EU	Vorig VP
Forensic Fieldlab	3D-model van plaats delict	PiD	Vorig VP

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

2.3 Resultaten 2011

2.3.1 Resultaten topics

De in 2011 bereikte resultaten zijn vastgelegd in de KIP-verslagen en onderzoeksverslagen en publicaties. In tegenstelling tot vorige jaren is er geen programma-brede highlight-rapportage opgesteld, omdat uit de feed back vanuit de doelgroep bleek dat de kennisoverdracht via breed samengestelde boekjes niet optimaal is. Daarom is besloten:

- Gedurende de looptijd van het VP zal voor elk topic een diepte-publicatie worden uitgebracht die bovendien aansluit op actuele uitdagingen voor innovatie. In 2011 zijn in dit verband gepubliceerd:
  - #SM @OOV? Visie op Sociale media in de Openbare Orde en Veiligheid (topic 2 en 4)
  - Informatie die werkt! (topic3)
  - Samen door de crisis! (topic 4)
  - MIRROR: Multidisciplinair Interactie raamwerk, Programma Flood Control 2015 (topic 4)
- Voor elk topic worden bredere bijeenkomsten georganiseerd. Zo vond op 9 december 2011 een bijeenkomst plaats over het verbeteren van cameratoezicht door het herkennen van afwijkend gedrag. Deze bijeenkomst werd bezocht door ca.60 deelnemers uit bedrijfsleven en publieke organisaties als politie en KMar. In de eerste helft van 2012 staan bijeenkomsten voor topic 2 (Activering van burgers) en topic 5 (Cybersecurity) in de planning.

2.3.2 Highlights van de resultaten in 2011

In de bijlagen van dit voortgangsrapport wordt een drietal *highlights* toegelicht. Dit betreft:

A Highlight: Activering van burgers
B Highlight: Werken in netwerken
C Highlight: Security by design voor de energiesector

2.3.3 Output

De bereikte resultaten in 2011 zijn in het algemeen in lijn met de afgesproken doelstellingen in het goedgekeurde Meerjarenprogramma voor het VP. Onderstaande tabel geeft de output van het programma weer.

Vorm van output	**Aantal**
TNO-rapporten	14
Rapporten 'gefunde' projecten	57
Wetenschappelijke artikelen	8
Publicaties vaktijdschriften	6
Websites van projecten met TNO-bijdragen	18
Octrooiaanvragen	3
Presentatie bij congressen en workshops	42

In 2011 is er duidelijk een verschuiving in de output doorgezet van wetenschappelijke artikelen naar presentaties op bijeenkomsten en op websites. Daarnaast heeft TNO in samenwerking met private en publieke stakeholders bijgedragen aan de ontwikkeling van gezamenlijke visies op gewenste ontwikkelingen en dit vastgelegd in een aantal documenten en door TNO gepubliceerde White papers:

- De Nationale Cyber Security Research Agenda
- De Roadmap *Security* in het kader van de Topsector High Tech Systems & Materials
- White paper *Social media, burgerparticipatie en sociale veiligheid*
- White paper *Crowdsourcing in de opsporing*
- White paper *Van situation awareness naar collaboration awareness*
- R&D mapping of *Projects/products/methods and techniques for various crisis management tasks* (Europees project ACRIMAS)

In 2011 is ook voortgang geboekt bij de ontwikkeling van praktijkomgevingen voor experimentele beproeving van veiligheidsinnovaties:

- Samen met NFI is het Forensic Fieldlab in Den Haag doorontwikkeld. Hier is nu een Plaats Delict nagebouwd, waar verschillende nieuwe forensische technieken kunnen gevalideerd worden terwijl tevens simulaties voor training uitgevoerd worden.
- Samen met o.a. Politie Haaglanden, Gemeente Den Haag en de Haagse Hogeschool is een Livinglab in ontwikkeling voor het beproeven van nieuwe concepten voor veiligheid in de stad.
- In Utrecht is een aantal projecten voor toezicht in de gemeentelijke uitkijkcentrale opgestart.

3 Aansluiting bij beleidsinitiatieven van EL&I

3.1 Maatschappelijk Innovatie Programma Maatschappelijke Veiligheid

Dit Vraaggestuurde Programma sluit met name aan op het Maatschappelijke InnovatieProgramma Security, waarbij de ministeries EL&I, VenJ en Defensie structureel betrokken zijn. In juni 2008 werd voor de inkadering van dit programma de Maatschappelijk Innovatie Agenda Veiligheid gepubliceerd, met als prioriteiten de volgende thema's:

- Opereren in ketens en netwerken
- Simulatie, training en opleiding
- Fysieke bescherming

In 2012 loopt nog een beperkt aantal projecten door.

3.2 EL&I-cofinanciering

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

In 2011 zijn twee projecten opgestart om het herkennen van menselijk gedrag door toezicht-houdend personeel te verbeteren. Het gaat daarbij zowel om surveillanten als operators van uitkijkcentrales.

Verder is met Imtech als co-financier een EL&I-cofinancieringsproject opgestart voor de ontwikkeling van indoor lokalisatie met radar tags. Met name voor bewakingsdoelen worden hier toepassingen voorzien (o.a. monitoring gedetineerden in gevangenissen).

3.3 Verankering Security in de topsectoren

Het nieuwe innovatiebeleid van het ministerie EL&I heeft geleid tot een halvering van het budget voor het VP Maatschappelijke Veiligheid in 2012 en volgende jaren. Parallel daaraan is dankzij een krachtsinspanning van de Nederlandse industrie (o.a. NIDV) en de ministeries VenJ en Defensie in het kader van de topsector High Tech Systems & Materials een roadmap ontwikkeld voor het opbouwen van een structurele samenwerking in een zogenaamde Gouden driehoek van overheid-bedrijfsleven-kennisinfrastructuur. Hierbij wordt voortgebouwd op de MIA-V, de Nationale Cyber Security Research Agenda en de Security-paragraaf van de Point One-roadmap. Meer informatie over deze roadmap is te vinden op de website www.htsm.nl.

Daarnaast is veiligheid een apart onderkend issue in de innovatiecontracten van de topsectoren Water (zgn. businesscase Flood Control 2100), Logistiek (roadmap voor risk based security controle van goederenstromen) en de sector overschrijdende innovatie-agenda voor ICT.

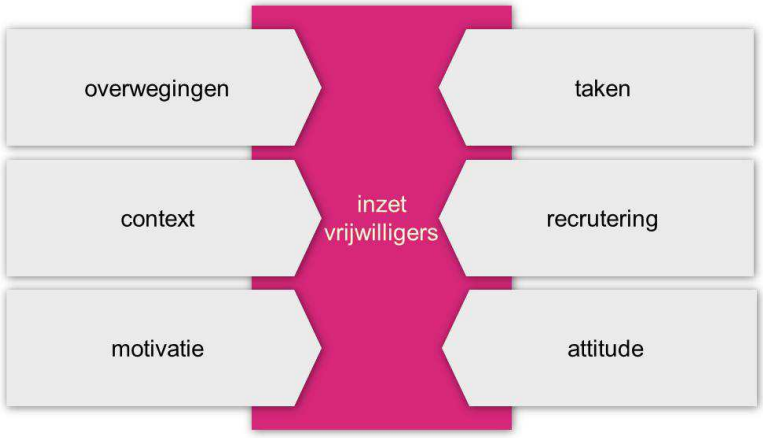
A Highlight: Activering van burgers

Na jaren van beïnvloeding van onze samenleving met de slogan “Duurzaam…. begin bij jezelf” is het tijd om voor veiligheid een zelfde benadering te kiezen. De sterke toename van beschikbare informatie en nieuwe communicatiemogelijkheden maakt de empowerment van burgers en de vraaggestuurde inzet van vrijwilligers mogelijk. De ontwikkeling van Burgernet met maar liefst 600.000 verbonden burgers biedt een uitdagende basis voor verder initiatief.

In het topic “Activering van burgers” van het VP Veilige Maatschappij is in 2011 een structurele aanpak van de burgerbetrokkenheid in de steigers gezet.

1. Ontwikkeling van model voor matching burgercompetenties en veiligheidstaken

Na de oriëntatiefase is een vragenlijst voorbereid en uitgezet bij vrijwilligers die betrokken zijn bij diverse organisaties (Brandweer, Politie, KNRM, Oranje en Rode kruis, Natres en de Reddingsbrigade). De uitkomsten leiden tot een overzicht van beweegredenen van mensen om zich als vrijwilliger bij de betreffende organisaties aan te melden. Daarnaast wordt er gekeken binnen organisaties die vrijwilligers inzetten welke taken zij laten uitvoeren, hoe de matching tot stand komt en welke ondersteuning wordt geboden. Daarvoor zijn interviews gehouden met experts om het model compleet te maken en te achterhalen op welke wijze binnen betreffende organisaties wordt omgegaan met de inzet van burgers. De opgebouwde kennis is voor betrokken organisaties van belang om effectiever en beter met hun mensen om te gaan, maar biedt ook inzicht op welke aspecten ‘type’ organisaties en vrijwilligers verschillen of overeenkomen.

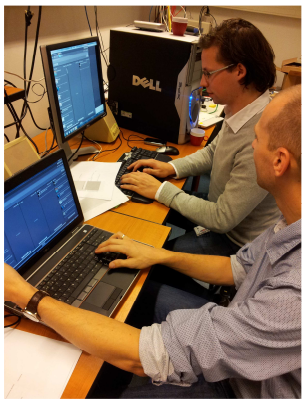


Concept model burgercompetenties en eigenschappen in relatie tot vrijwilligerstaken

2. Rol van social media tijdens veiligheidsincidenten

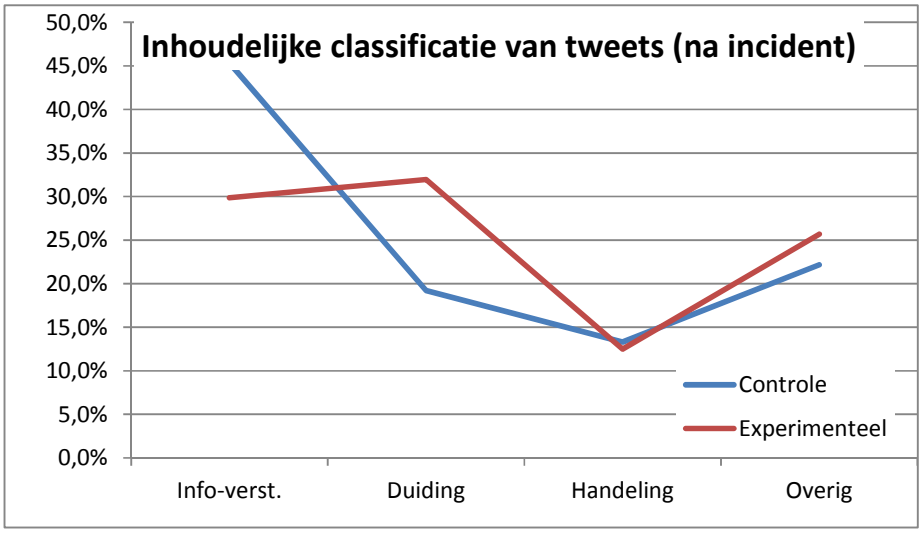
Er is een experiment uitgevoerd met een viertal groepen burgers bij een in scène gezet concert. Tijdens het evenement valt de stroom uit en zijn er diverse voorvallen. Het is een korte trial van 25 minuten. De verschillende groepen aanwezigen krijgen via moderatoren over het incident andere type informatie (standaard proces informatie

versus standaard proces informatie & antwoord op de eigen vragen) en kunnen ook met behulp van hun twitter account zelf informatie genereren of gebruiken. Er is geanalyseerd op welke wijze het gebruik van twitter helpt bij het grip krijgen op de situatie en welke invloed de soort informatie heeft op de gemoedstoestand van de burgers. In een groepsdiscussie is verkend op welke wijze gebruikers met informatie ondersteund willen worden. Ook is er gekeken naar het type bijdrage dat men levert en de ontwikkeling in emotie tijdens het voorval. Uit de eerste resultaten blijkt dat in het algemeen de emoties na het incident een negatievere lading hebben gekregen.



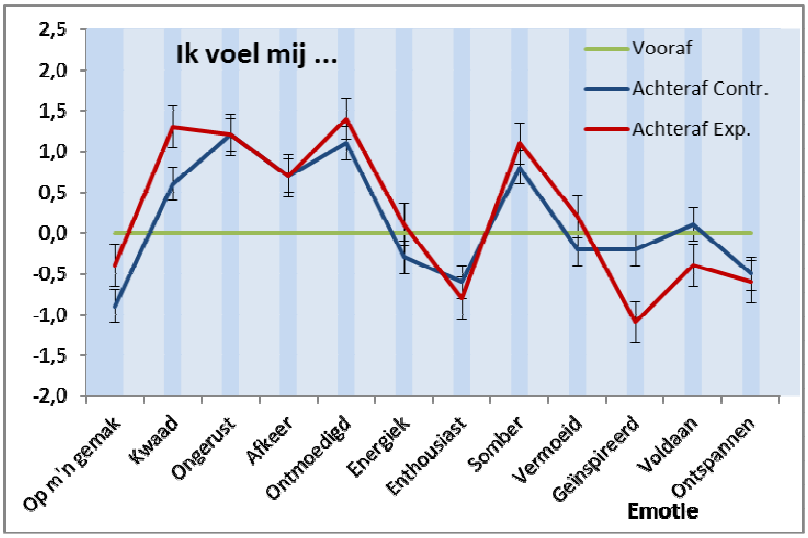
Tijdens het experiment wordt door de moderatoren gereageerd op tweets

De experimentele groep die van de moderatoren antwoord krijgt op door hun gestelde vragen, stelt duidelijk minder vragen over de gegeven informatie zelf. Toch stellen ze in totaal wel evenveel vragen, maar de inhoud verschuift naar duiding.



Burgers die via twitter antwoord krijgen op vragen (= de experimentele groep) gaan meer vragen stellen over wat de informatie betekent; de controle groep blijft vragen stellen over de informatie zelf.

De experimentele groep scoort achteraf over het algemeen extremer, wat aangeeft dat hun emoties sterker (negatief) beïnvloed zijn tijdens het experiment.
Verder valt op dat er een relatief groot verschil tussen de groepen zichtbaar is bij ‘Geïnspireerd’ en ‘Voldaan’.



Verschil in ervaren emotie bij de experimentele en de controle groep

Het experiment bevestigde een aantal verwachtingen:

- Mensen die betrokken zijn bij een incident reageren daar meetbaar emotioneel (negatief) op;
- Een plotselinge stijging van het aantal tweets geeft een goede indicatie dat er iets gebeurt. Dergelijke veranderingen kunnen gebruikt worden om automatisch te detecteren dat er iets gebeurt.
- Betrokkenen bij een incident hebben behoefte aan juiste informatie en snelle communicatie. Eén van beide, zonder de andere, is onvoldoende en geeft de betrokkenen het gevoel dat ze niet gehoord worden of dat de communicatie niet goed verloopt.

Er was ook een aantal verrassende conclusies:

- Wanneer mensen weinig informatie krijgen gaan ze vragen stellen, wanneer mensen veel informatie krijgen zoeken ze duiding;
- Hoe meer informatie er gegeven wordt, hoe sterker de emotionele reactie ; nog niet onderzocht is in hoeverre het geven van handelingsperspectief dit verschijnsel kan compenseren;
- Een bottleneck voor automatische interpretatie van tweets is het gebruik van ontkenningen en gebruik van humor.

In het gesprek achteraf gaven de deelnemers uit de experimentele groep aan dat zij voldoende, relevante informatie gekregen hadden, frequent genoeg (hoewel dit natuurlijk altijd beter kan). Ook wat betreft handelingsperspectief hadden zij voldoende handvatten gekregen; zij liepen zelf geen direct gevaar en de richtlijn om eerst afstand te houden van het podium en later de ruimte rustig te verlaten voldeed. Hier stelden de experimentele groep dan ook geen vragen meer over (in tegenstelling tot de

controlegroep). Wat overbleef waren de vragen naar duiding. Hieraan was in het scenario niet veel ruimte gegeven, zodat deze vragen bleven bestaan. Hieruit kan worden afgeleid dat tijdens een incident al kan worden geanticipeerd op de fase na het incident. Gerichte en betrouwbare informatie heeft invloed op de nafase. Hulpverleners doen hier al veel aan, wanneer bijdrages een meer specifiek karakter krijgen, voelen betrokkenen zich gehoord en serieus genomen.

B Highlight: Werken in Netwerken

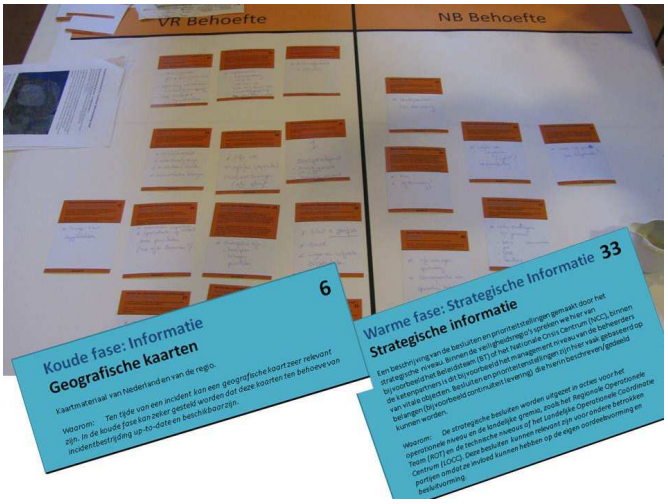
Bij veiligheidsincidenten en openbare orde zijn steeds meer organisaties betrokken. Denk bijvoorbeeld aan chemische ongevallen, wateroverlast of maatschappelijke onrust. De verwevenheid tussen partners uit het veiligheidsdomein en private en functionele partijen bij het bestrijden van incidenten groeit. Door innovatie kunnen de publieke en private sector beter op elkaar aansluiten. Uitdagingen zijn zich samen te ontwikkelen en gezamenlijk gebruik te maken van de aanwezige incident-informatie en kennis over capaciteiten en materieel. Dit betreft de hele veiligheidsketen, van proactie tot leren van evaluatie. Daarbij liggen er nog vele onbenutte capaciteiten van burgers en bedrijven. Zo kunnen bijvoorbeeld burgers bij incidenten als in Alphen aan de Rijn zichzelf en hun kinderen beter in veiligheid brengen door elkaar snel te informeren over vluchtroutes en schuilplaatsen. Voor de hulpdiensten wordt het initiëren, organiseren en coördineren van de betrokken partijen bij de incidentbestrijding dan steeds belangrijker.

In het topic “Beter benutten informatiestromen en samenwerking” van het VP Veilige Maatschappij wordt de basis gelegd voor het soepel en succesvol samenwerken van partners in het veiligheidsdomein en de private partijen in tijdelijke netwerken voor het bestrijden van onveiligheid in de breedste zin van het woord.

Eerste resultaten

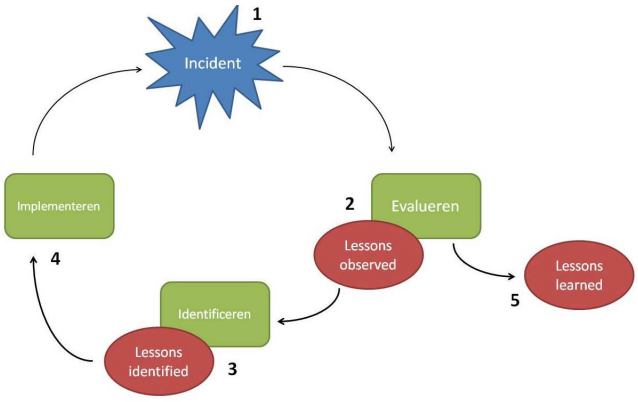
In 2011 is een viertal onderwerpen onderzocht op kansen en mogelijkheden tot aansluiting bij de ontwikkeling van netcentrisch werken zoals dat nu geïmplementeerd wordt in de praktijk:

1. Informatieaanbod voor samenwerkende professionals in de veiligheidsketen. Collaboration awareness vertelt je wat je moet weten van je crisispartners. Na de analyse in 2011 onderzoeken we in 2012 wat er in de koude fase èn wat er in de warme fase moet gebeuren om samenwerking te verbeteren. Dit moet ook leiden tot een training voor multidisciplinaire samenwerking.



Bij crisisbeheersing zijn vele organisaties betrokken. Het analyseren van de informatiebehoeften en het delen daarvan in de koude en de warme fase leidt tot nieuwe werkwijzen voor informatievoorziening en communicatie

2. Nieuwe generatie gebruikersinterfaces. Op basis van een informatiemodel met 3 lagen, bieden we gebruikers informatie aan over het incident. Elke laag bevat weer andere informatie, gericht op de taak: situatie schets, inzet eenheden, aanwezig materiaal.
3. Collectief geheugen en leren leren. Een collectief geheugen maakt lessons learned snel toegankelijk, waardoor samenwerken makkelijker wordt. Om aan die lessen te komen, moet je niet alleen evalueren, maar ook lessen identificeren en implementeren. En dat is in een multidisciplinaire omgeving moeilijker, want… wie is verantwoordelijk. In 2012 onderzoeken we de knelpunten voor multidisciplinair leren en komen met een proces om dit te ondersteunen.
4. Publiek-private informatievoorziening. Als crisispartners samenwerken willen ze wel graag informatie delen, maar vaak is onduidelijk waarom en tot welk doel. Met het in 2011 uitgebreide Raamwerk Informatiedeling Vitaal wordt duidelijk welke informatie gedeeld moet worden in de koude, de lauwe en de warme fase. In onderlinge afstemming komen partijen tot wederzijds begrip waarom juist die informatie nuttig is, en op welke manier de partner deze informatiebehoefte kan ondersteunen.



Het leren van ervaringen vergt meer dan waarnemen van fouten.

C Highlight: Security by design voor de energiesector

Ervaringen met bijvoorbeeld de OV-chipkaart en de slimme meter binnen de energiesector laten zien dat het van groot belang is om al in het begin van grote ontwikkeltrajecten security als expliciet aandachtspunt mee te nemen.

Nieuws

"Privacy slimme meter niet goed geregeld"

01-03-2011, 12:11 door Redactie

Vorige week ging de Eerste Kamer akkoord met de uitrol van de slimme energiemeter in Nederland, maar de privacy is nog altijd niet goed geregeld. Zo is de uitrol van de slimme meter een Europese eis. "Nederland is hierbij te klein om de specificaties van de slimme meter te bepalen en daarom wordt op Europees niveau al samenwerking gezocht. Privacy en beveiliging zijn hierbij echter compleet onderbelicht gebleven", zegt Frank Geerts van Atos in het FD.

Om strenge privacy- en beveiligingseisen in Nederland te kunnen doorvoeren bij het gebruik van de slimme meter, zijn Europese standaarden nodig. Het tweede obstakel dat Geerts ziet is dat er geen enkele proef is uitgevoerd om privacy- en beveiligingsproblemen te ontdekken.

Nieuws

"Nieuwe hacksoftware voor OV-chipkaart"

04-12-2011, 13:12 door Redactie

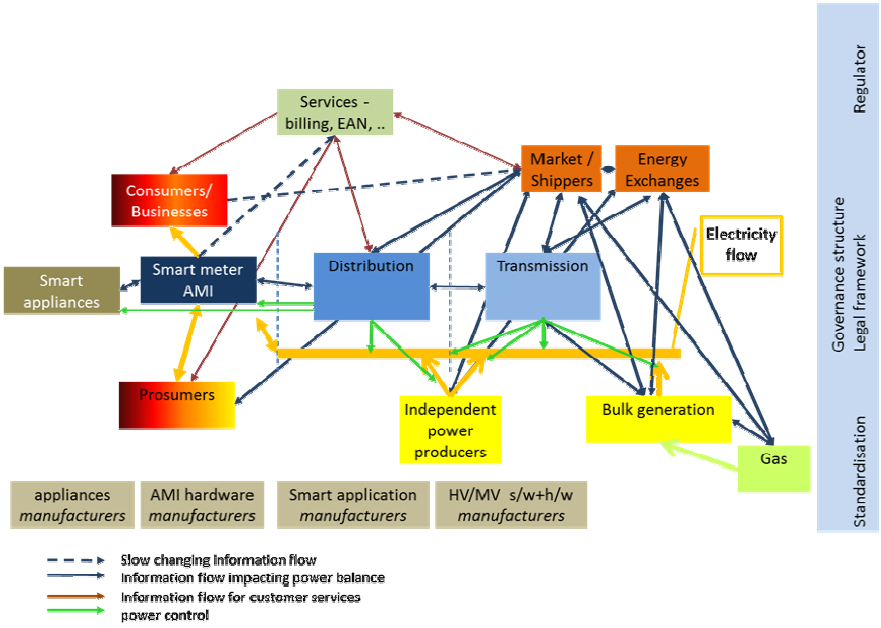
Op een weblog zou nieuwe software zijn verschenen om binnen tien seconden de OV-chipkaart te kraken, zonder dat hier externe apparatuur voor nodig is. Volgens het op Google gehoste "OVchipkaarthacken" blog, met als slogan "Hack binnen 10 seconden uw OV zonder externe apparatuur!", is het in zes stappen mogelijk om met de kaart te frauderen. Hierbij wordt op de kaart aangegeven op welk station men is ingecheckt, iets wat volgens het blog niet door een conducteur is te detecteren.

Het topic cyber security van het VP Veilige Maatschappij richt zich op methoden om in een vroegtijdig stadium van het ontwerp en de ontwikkeling van nieuwe grootschalige infrastructuur security in te bouwen, het zogeheten ‘security by design’.

Het onderzoek richt zich op het identificeren van de factoren die de inbedding van bescherming tegen ICT-dreigingen al in het ontwerpstadium van infrastructuur en grootschalige systemen mogelijk maken. Omdat deze vraagstelling breed is, wordt deze onderzoeksvraag allereerst onderzocht aan de hand van een case. Voor de case is gekozen voor de energiesector. Binnen de energiesector staat de komende jaren een groot aantal nieuwe ontwikkelingen gepland, waarbij ICT een grote rol speelt (‘smart grid’). Bovendien laat het Stuxnet-incident en recente digitale aanvallen op de energiesector zien dat de ICT-systemen binnen de vitale infrastructuur ook doelwit kunnen zijn van kwaadwillenden.

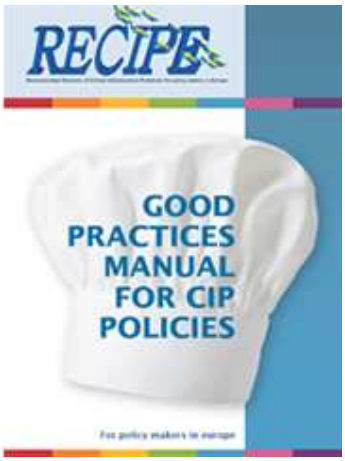
Binnen het onderzoek worden de ontwikkelingen op het gebied van smart grids in kaart gebracht en wordt een overzicht opgesteld van de belangrijkste factoren die zorgen voor de security van de vitale op ICT-gebaseerde infrastructuur. Het betreft hier niet alleen technische factoren, maar ook organisatorische maatregelen en aanpassingen in de gebruiksmogelijkheden. Per invloedsfactor wordt nagegaan wat het effect van de factor is, en welke mogelijkheden er zijn om deze factor te beïnvloeden. Zo wordt bijvoorbeeld ingegaan op de rol die standaarden en good practices kunnen spelen. Tevens wordt geïdentificeerd welke stakeholders een rol spelen bij de totstandkoming van de ICT-beveiligings- en veiligheidsmaatregelen.

Binnen de keten speelt een groot aantal partijen een rol, variërend van bijvoorbeeld leveranciers, distributie- en transmissie operators en eindgebruikers. Voor een veilige keten is bij elk van deze partijen inzicht in de informatiestromen en systemen en mogelijke risico’s noodzakelijk, bijvoorbeeld in de flow en beveiliging van persoonlijke informatie in verband met de privacy.



Bovenstaande figuur geeft een basismodel van het hier betrokken deel van de energiesector. Hiermee is het mogelijk te onderzoeken op welke wijze de stakeholders, elk met de eigen belangen en insteek, in een vroegtijdig stadium kunnen worden betrokken bij de risicobeoordeling en op welke wijze de basisprincipes van security by design het best voor het voetlicht kunnen worden gebracht. Ondersteunende modellen helpen bij het opbouwen van een gezamenlijk beeld van de partijen in de keten en ondersteunen zo een betere samenwerking en betere borging van de veiligheid van de keten. Deze ontwikkelingen sluiten aan bij de samenwerking met Alliander, KPN en KEMA binnen het European Network for Cyber Security (ENCS). Tevens is er bijgedragen aan een EU-taakgroep rond smart grid security en zijn een deel van de resultaten van het onderzoek in dit kader ingebracht en getoetst.
Daarnaast zijn CPNI.NL en TNO coördinator van een werkgroep op dit gebied in het kader van de Europese samenwerking binnen de European Reference Network for Critical Infrastructure Protection (ERNCIP). Het onderzoek draagt in belangrijke mate bij aan de internationale positionering van TNO op het gebied van smart grid security.

In mei 2011 zijn de resultaten van het door TNO geleide project ‘Recommended Elements for Critical Infrastructure Protection for policy-makers in Europe (RECIPE) gepresenteerd tijdens een internationale workshop in Rome. Hier waren de CIP coördinatoren uit de EU-lidstaten en ook enkele medewerkers van DG Home bijeen. Begin juni zijn de projectresultaten ook gepresenteerd in Boedapest tijdens de EU-USA/Canada topbijeenkomst. Het door EU-DG Home en VenJ gesteunde project heeft geleid tot een handboek met Good Practices voor beleidsmakers op het gebied van bescherming vitale infrastructuur (download: www.tno.nl/recipereport).



Samen met de projectpartners uit Oostenrijk, Slowakije en Estland zijn eerst de CIP-activiteiten in Europese landen en ook daarbuiten in kaart gebracht met behulp van interviews en een desk studie. Daarna is ingezoomed op een zestal thema's: identificatie van vitale infrastructuur (producten en diensten), afhankelijkheden (ketenuitval), publiek-private samenwerking (PPS), informatie delen, risicomanagement en crisismanagement. Met behulp van de in het VP Veilige Maatschappij ontwikkelde kennis is een diepgaande analyse gemaakt van een aantal succesvolle inspirerende CIP-activiteiten, maar ook van minder goed gelukte en gefaalde nationale activiteiten. Nederland heeft zich met de in het RECIPE boekje ingebrachte kennis goed op de Europese CIP-kaart gezet.