Kampweg 5
Postbus 23
3769 ZG Soesterberg

www.tno.nl

T +31 34 635 62 11
F +31 34 635 39 77
info-DenV@tno.nl

TNO-rapport

TNO-DV 2010 C274

Thema Integrale Veiligheid
Vraaggestuurd Programma 2011-2014
VP Veilige Maatschappij

Datum	september 2010
Auteur(s)	dr. ir. J.A. Don
Regievoerend Departement	Ministerie van Binnenlandse Zaken en Koninkrijkrelaties
Projectnummer	032.09009
Rubricering rapport	Ongerubriceerd
Titel	Ongerubriceerd
Samenvatting	Ongerubriceerd
Rapporttekst	Ongerubriceerd
Aantal pagina's	1

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

Handtekening

Samenvatting

In het Strategisch Plan 2011-2014 van TNO is het Thema Integrale Veiligheid gericht op een veiliger samenleving. De twee innovatiegebieden binnen dit Thema zijn:

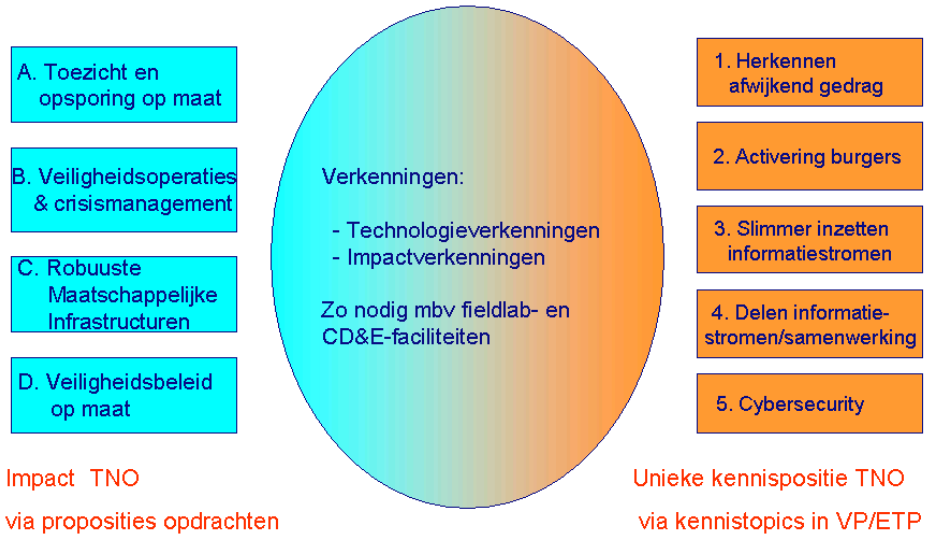
1. Wereldwijd inzetbare krijgsmacht.
2. Veilige Maatschappij.

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 dit Meerjarenprogramma 2011-2014 voor het Thema Integrale Veiligheid wordt alleen het Innovatiegebied Veilige Maatschappij verder uitgewerkt.

Veiligheid heeft zich ontwikkeld van een verzameling ad-hoc reacties op incidenten tot een samenhangend complex van maatregelen en effecten. De potentiële impact en het domino-effect van incidenten, maar ook de maatschappelijke kosten/baten van veiligheidsmaatregelen vereisen een integrale op risico en effect gebaseerde aanpak en regie. Perceptie en acceptatie spelen een grote rol in de keuze van oplossingen.
TNO gaat deze uitdagingen aan door te focussen op de volgende vier proposities:

A. Toezicht en opsporing op maat
B. Professionele veiligheidsoperaties & Crisismanagement
C. Robuuste maatschappelijke Infrastructuren
D. Veiligheidsbeleid op maat

Onder regie van BZK zijn in nauw overleg met behoeftestellers prioritaire kennis-topics gekozen voor het Vraaggestuurd Programma Veilige Maatschappij 2011-2014. Elk van deze kennistopics is van belang voor meerdere proposities:



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

Het voorliggende plan bevat een samen met stakeholders ontwikkelde focus voor de onderzoeksvragen in de jaren 2011-2014. De plannen voor 2011 en een roadmap per kennistopic zullen voor 1 november 2010 worden uitgewerkt.

Inhoudsopgave

1 Inleiding thema Integrale Veiligheid

1.1 Plaats van het Meerjarenprogramma 2011-2014

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

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

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

1.2 Beschrijving van het thema Integrale Veiligheid

In het Strategisch Plan 2011-2014 van TNO is het Thema Integrale Veiligheid gericht op een veiliger samenleving. Veiligheid èn het gevoel van veiligheid zijn meer dan ooit onderhevig aan bedreigingen die voortkomen uit de verdeling van welvaart, botsende opvattingen en toenemende schaarste aan grondstoffen. Wereldwijd zetten defensie, overheden, hulpdiensten en industrie zich in om ons te beschermen tegen steeds minder eenduidige en zichtbare bedreigingen. TNO ondersteunt innovaties om deze activiteiten slimmer, efficiënter en beter beschermt te doen.

Binnen het Thema Integrale Veiligheid heeft TNO twee innovatiegebieden gevormd:

1. WERELDWIJD INZETBARE KRIJGSMACHT
   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:
   - Kosteneffectief Opereren Krijgsmacht;
   - Information Superiority;
   - As Safe As Reasonably Affordable;
   - Meer Presteren met Minder Mensen.
2. VEILIGE MAATSCHAPPIJ
   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 vier onderwerpen:

- Toezicht en opsporing op maat;
- Professionele veiligheidsoperaties & Crisismanagement;
- Robuuste maatschappelijke Infrastructuren;
- Veiligheidsbeleid op maat.

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 dit Meerjarenprogramma 2011-2014 voor het Thema Integrale Veiligheid wordt alleen het Innovatiegebied Veilige Maatschappij verder uitgewerkt.

1.3 Doelstelling en resultaten 2011-2014 voor het Innovatiegebied Veilige Maatschappij

Binnen de vier geselecteerde onderwerpen – of proposities - initieert en faciliteert TNO innovaties. De kennisinvesteringen en de contractresearch zijn gericht op impact en daarvoor benodigde resultaten:

1. *Toezicht en opsporing op maat*
   Te bereiken impact: Kosteneffectief toezicht waar nodig en acceptabel.
   Te realiseren resultaten: innovatieve concepten voor toezicht, handhaving en opsporing waarbij op basis van afbakening in omgeving, tijd en middelen maximaal kosteneffectieve toezichts- en opsporingsresultaten kunnen worden bereikt en het implementeren hiervan met partners;
2. *Professionele veiligheidsoperaties & crisismanagement*
   Te bereiken impact: Meer veiligheid met minder mensen.
   Te realiseren resultaten: Concepten en componenten voor het revolutionair anders inrichten van de uitvoeringscapaciteit voor het effectiever, efficiënter en veiliger optreden van de operationele veiligheidsdiensten bij incidenten en calamiteiten en grootschalige crises. Een uitdaging is het risicogestuurd kunnen combineren van professionals van publieke en private organisaties en burgers in de verschillende fasen van de veiligheidsketen (pro-actie, preventie, preparatie, respons evaluatie en nazorg).
3. *Robuuste maatschappelijke infrastructuren*
   Te bereiken impact: Betere garantie van maatschappelijke dienstverlening.
   Te realiseren resultaten: Beslissingsondersteunende instrumenten en monitoringssystemen voor het zodanig inrichten van maatschappelijke infrastructuren (zoals woonwijken, bedrijventerreinen, mainports, openbaar vervoer, vitale infrastructuur voor ICT, water & energie, logistieke en industriële systemen) dat veiligheidsproblemen op een afgewogen manier kunnen worden voorkomen, opgevangen of opgelost en dat (veiligheids)organisaties in staat zijn om te leren en zich kunnen blijven aanpassen aan de dynamiek van maatschappij en markt.
4. *Veiligheidsbeleid op maat*
   Te bereiken impact: Beter Rendement uit Veiligheidsbeleid.
   Te realiseren resultaten: Modellen, beslissingsondersteunende instrumenten en ontwerp informatie-infrastructuur voor ontwikkeling en evaluatie van

beleidsopties en ondersteunen van implementatie van veiligheidsdoelstellingen op verschillende schaalniveaus (gemeente, regio, nationaal, internationaal). Uitdagingen zijn de bepaling van maatschappelijke ambitie en richting, het in kaart brengen van onzekerheden en de houding van verschillende groepen ten opzichte ervan, het ex-ante en ex-post kunnen bepalen van effecten van maatregelen/oplossingen in relatie tot kosten/baten, en het uitzetten van communicatie- en implementatietrajecten;

1.4 Overzicht Vraaggestuurde Programma's en relatie met ETP's

In het Vraaggestuurde Programma Veilige Maatschappij zijn de investeringen gericht op kennis die direct van belang is voor aan veiligheid gerelateerde vraagstellingen. Een aantal relevante kennisontwikkelingissues is veel breder van belang. De zogenaamde Enabling Technology Programma's van TNO zijn met name gericht op fundamentelere kennisontwikkeling die de kennisbasis voor meerdere thema's essentieel versterken. Van de zeven ETP-programma's in de periode 2011-2014 zijn er drie direct van belang voor het VP Veilige Maatschappij:

- Het ETP *Gedrag en Innovatie* gaat in op perceptie in relatie tot gedrag en beïnvloeding van actiebereidheid op micro-, meso- en macro-niveau. Een uitdaging is de onderscheiding van bevolkingsgroepen met karakteristieken, die verschillende mechanismen voor effectieve beïnvloeding vergen. Dit ETP is ook van belang voor de TNO-thema's *Gezond Leven* en *Mobiliteit.*
  In het VP Veilige Maatschappij zijn de aanknopingspunten voor dit ETP: het vroegtijdig herkennen van potentieel verdacht gedrag en zelfredzaamheid en burgerparticipatie.
- Het ETP *Sensoren* betreft de ontwikkeling van adaptieve multi-sensornetwerken, waarbij geminiaturiseerde low-cost sensoren en nieuwe inter-connecties tussen giga- hoeveelheden sensoren, netwerken en informatie leiden tot een golf van nieuwe toepassingsopties. Dit ETP is van belang voor al de zeven TNO-thema's.
  In het VP Veilige Maatschappij zijn de aanknopingspunten voor dit ETP: het vroegtijdig herkennen van potentieel verdacht gedrag en de informatievoorziening voor het gecoördineerd uitvoeren van veiligheidstaken.
- Het ETP *Modellen* betreft de ontwikkeling van methoden om giga hoeveelheden waarnemingen, data, relaties en op te werken tot beslissingsondersteuning en stuurinformatie voor actoren in beleid en operaties. Gebruikersspecifieke interfaces tot de informatieoceaan dienen gebruikers snel en juist interpreteerbare inzichten te geven die nodig zijn voor effectieve actie, coördinatie, gezamenlijke besluitvorming en communicatie. Dit ETP is ook van belang voor de TNO-thema's *Mobiliteit*, *Gebouwde omgeving*, *Energie* en *Informatiemaatschappij*.
  In het VP Veilige Maatschappij zijn de aanknopingspunten voor dit ETP: de activering van burgers in relatie tot veiligheidsorganisaties, informatiemining, de informatievoorziening voor het gecoördineerd uitvoeren van veiligheidstaken en cybersecurity.

1.5 Overleg met BZK als regievoerende Departement

BZK heeft als regievoerend departement het initiatief genomen om het VP in de strategieperiode 2011-2014 sterker te verankeren in de kennisbehoeften van de stakeholders. Tegelijkertijd is er strak vastgehouden aan de wens om de kennisontwikkeling te focusseren op een beperkt aantal topics.

De scherpere positionering van het VP kwam mede tot stand door betrokkenheid van trendsettende stakeholders, waarmee TNO in de voorgaande strategieperiode relaties heeft opgebouwd. Door de toename van nationale en internationale overheidsfondsen voor toepassingsgericht veiligheidsonderzoek is het perspectief op doorontwikkeling van in het VP ontwikkelde kennis naar concrete toepassing sterk verbeterd.

In het voorjaar van 2010 zijn door BZK een aantal bijeenkomsten georganiseerd, waarvoor uitgenodigd waren: Ministerie van Justitie, Ministerie van Defensie, AIVD, NCTb, NICC, ICTU, Veiligheidsregio Noord-Oost Gelderland, NVBR, Brandweer Amsterdam, LFR, vts-PN, KLPD, CIV, Politie-academie en CCV. In een interactief proces heeft dit geleid tot de keuze voor een vijftal topics en een overkoepelend onderdeel voor verkenningen:

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

Voor elk van deze topics zijn een aantal onderzoeksvragen geïdentificeerd en afgestemd, terwijl er een coördinerend behoeftesteller voor de begeleiding van de verdere uitwerking en uitvoering is aangewezen. Ook is afgesproken dat er twee keer per jaar een formeel voortgangsoverleg is tussen BZK, behoeftestellers en TNO.

De hierna te presenteren stand van zaken met betrekking tot de programmaontwikkeling zijn gebaseerd op een tiental door BZK georganiseerde werkbijeenkomsten met bijdragen van vele spelers. BZK heeft de uitkomsten geaccepteerd als basis voor de formele instemming met dit VP-plan. Verder zijn er afspraken gemaakt over het verdere proces om te komen tot gedetailleerde projectplannen voor 2011.

2 Vraaggestuurd Programma Veilige Maatschappij

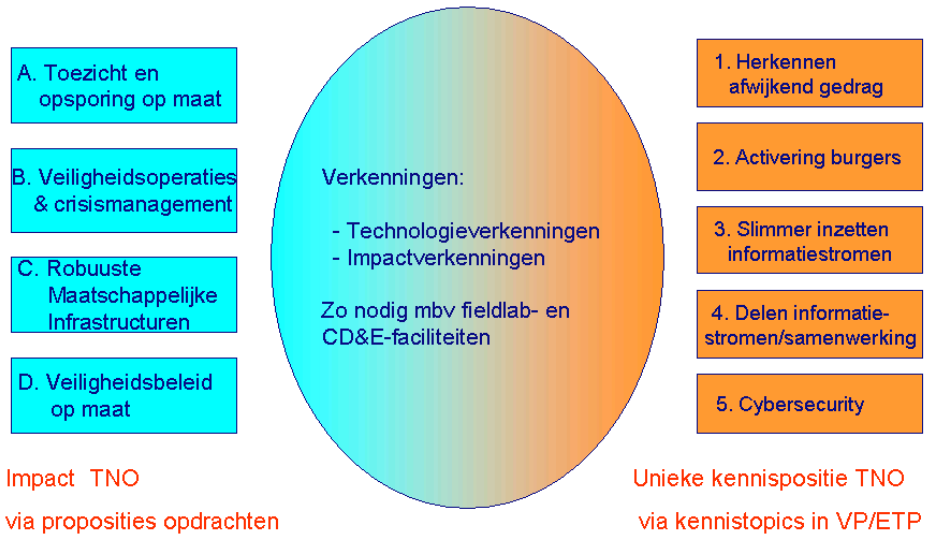
2.1 Beoogde Impact en Doelgroep

In het TNO-Innovatiegebied *Veilige Maatschappij* zijn de contractresearch en de kennisinvesteringen in de strategieperiode 2011-2014 gericht op de volgende impact:

1 Effectiever/ efficiënter optreden veiligheidsorganisaties door innovatie van doctrine, materieel, uitrusting en competenties;
2 Effectievere/ efficiëntere veiligheidsoperaties en rampenbestrijding door innovatie van informatievoorziening, besluitvorming en organisatie van de samenwerking tussen organisaties;
3 Vergroting veiligheid in openbare ruimte door effectief betrekken van burgers/bedrijven bij:
   - Preventie en veilig gedrag;
   - Waarnemingen bij incidenten en rampen/crises;
   - Eerste respons: zelfredzaamheid & community care;
   - Gestuurde inzet burgers bij veiligheidsincidenten (geformaliseerde burgerpanels, getrainde vrijwilligers in de wijk, ad hoc mobilisatie en instructie);
4 Beperking schade ten gevolge van rampen/crises (overstromingen, CBRNe-incidenten, uitval vitale infrastructuren) door snel en adequaat optreden en door kosteneffectieve pro-actieve maatregelen.

De in paragraaf 1.3 beschreven proposities van TNO zijn gericht op het bereiken van deze impact.

Onder regie van BZK zijn in nauw overleg met behoeftestellers prioritaire kennis-topics gekozen voor het Vraaggestuurd Programma Veilige Maatschappij 2011-2014. Elk van deze kennistopics is van belang voor meerdere proposities:



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

De belangrijkste doelgroepen waarop TNO zich richt met dit VP en hun aansluiting bij proposities en topics zijn:

Doelgroep	Belangrijke sectoren
Nationale overheid	- Veiligheid (BZK, Justitie, Defensie) - Economie (EZ) - Infrastructuur (EZ, V&W, VROM)
Decentrale overheid	- Veiligheidsregio's (brandweer, GHOR, meldkamers) - Gemeenten
Bedrijfsleven	- Veiligheidsbranche (industrie en diensten) - Vitale infrastructuur - Mainports
Veiligheidgerelateerde Instituten	- Onderzoek (NFI, CCV, Verweij-Jonker e.a.) - Opleiding (Politie-academie, NIFV e.a.)
Internationaal	- Overheden (EU, EU-lidstaten, DHS in VS) - Bedrijfsleven (Multinationals) - Complementaire kennisinstituten
Consortia voor publiekprivate samenwerking	- Veiligheid op luchthavens - Vitale infrastructuur - e.a.

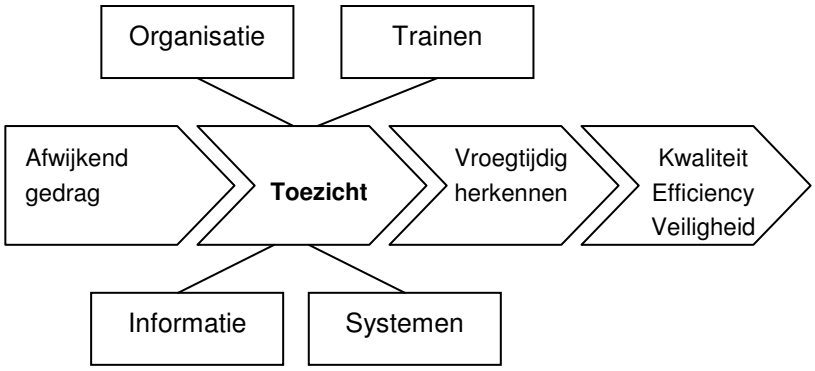
2.2 Focus van onderzoeksvragen en roadmap

Voor de vijf geselecteerde specifieke topics zijn de focus en de te beantwoorden onderzoeksvragen onderstaand uitgewerkt. In de komende periode tot 1 november 2010 zal per topic een projectplan voor 2011 en een roadmap voor 2011-2014 worden opgesteld. Naast de visie van betrokken stakeholders zullen ook de interne TNO gehanteerde roadmaps voor de vier proposities in het Innovatiegebied Veilige Maatschappij worden benut en zonodig geactualiseerd.

2.2.1 Vroegtijdig herkennen afwijkend gedrag

2.2.1.1 Omschrijving van het topic

Bij toezicht op de veiligheid in de (openbare) ruimte is het vroegtijdig herkennen van afwijkend gedrag een belangrijke sleutel om te komen tot verbetering van kwaliteit, efficiency en veiligheidsbeleving.



Deze verbeteringen zijn gericht op:
- hogere kwaliteit: effectief voorkómen van terrorisme, criminaliteit en veiligheidsincidenten, beperken van de gevolgen daarvan en opsporen van daders;
- betere efficiency: richten van de professionele capaciteit op de juiste prioriteiten en met minder inspanning effectief handhaven;
- optimale veiligheidsbeleving: burgers die zich veilig voelen, veilig handelen en mogelijk in de waarneming participeren.

Ontwikkelingen zijn tot nog toe overwegend geweest in het investeren van technische middelen:
- Vooral meer camera's, meer toezichtcentrales en als gevolg daarvan meer operators, geen heldere prestatie indicatoren;
- Het ontwikkelen van slimme uitkijksoftware, automatisch herkennen van bepaalde (afwijkende) gedragingen;
- Slimmer werken door netwerkverbinding te leggen tussen meldkamers en centrale.

Het onderwerp herkennen van *afwijkend gedrag* van potentieel kwaadwillenden staat nog in de kinderschoenen en omvat nu onder andere:
- Lijst met afwijkende gedragingen op basis van (beperkte) theorie en praktijkkennis (resultaat van TNO-onderzoek voor de NCTb);
- Gefragmenteerde kennis over afwijkende gedragingen uit praktijkervaringen als basis voor leren van best practises (o.a. gebruikt in Security Awareness Trainingen);
- Experimenten en kenniselicitatie van beveiligingsmedewerkers op beperkte schaal;
- Proeftuin bij uitkijkcentrale van CIV te Utrecht voor versnellen van innovaties voor multimodale waarneming;
- Proeftuin bij KLPD (o.a. experiment Amsterdam CS) voor (i) evaluaties van waarneming van afwijkend gedrag door agenten en marechaussee en (ii) combineren met ondersteuning in de waarneming via intelligente camera's;
- EU onderzoek naar optimaal gebruik camerasystemen en intelligente camera's (o.a. project ADABTS met deelname van TNO).

De behoefte om afwijkend gedrag vroegtijdig te herkennen vergt integrale beantwoording van de volgende vragen:
- Welke gedragingen, contextinformatie (van de ruimte) en andere relevante (intelligence) informatie kunnen voorspellende waarde hebben voor verdacht gedrag, terrorisme of criminaliteit?
- Welke proactieve handelingen kunnen beveiligingsoperators toepassen om afwijkend gedrag beter te kunnen interpreteren en eerder te kunnen waarnemen of dit potentieel verdacht is (prikkelen).
- Hoe gebruikt de menselijke beslisser (beveiligingsoperator) de informatie over (potentieel) verdacht gedrag en hoe beïnvloedt dat de kwaliteit van zijn of haar oordeelsvorming?
- Hoe en welke technologische ondersteuning (intelligente camera's, beslis-ondersteuning) kan gebruikt worden om tot een beter en vroegtijdiger oordeel te komen van afwijkend gedrag?
- Welke organisatie van taakuitvoering leidt tot optimaal toezicht en het vroegtijdig waarnemen van verdacht gedrag met daarin oog voor de samenwerkende beveiligingspartijen (w.o. politie, marechaussee, particuliere beveiligingsbedrijven, openbaar vervoer, burger), de mogelijkheden om netcentrisch te werken en de relatie te leggen tussen de verschillende informatiebronnen?
- Hoe wordt optimaal aangesloten op maatschappelijke randvoorwaarden als privacy en wettelijk kader?

Inzicht in bovenstaande vraagstukken is noodzakelijk voor het ontwikkelen van innovatieve integrale concepten voor toezicht van (openbare) ruimte in (camera)toezichtcentrales of genetwerkt (virtuele) toezichtorganisaties waarin alle relevante professionals (multiparty) en burgers gezamenlijk tot betere kwaliteit, efficiency en een verhoogde veiligheidsbeleving komen. In het VP zal basiskennis ontwikkeld worden met een focus zoals die onderstaand is uitgewerkt en afgestemd met de door BZK gecoördineerde begeleidingsgroep. Als vervolg op de kennisontwikkeling is doorontwikkeling in nationale en internationale innovatie-programma's voorzien gevolgd door vanuit stakeholders gefinancierde innovatietrajecten.

2.2.1.2 Focus van het topic

Waar gaat het precies over?	Vroegtijdig waarnemen en beïnvloeden van (potentieel) kwaadwillenden (niet corrigeren en handhaven) om terrorisme en criminaliteit te voorkomen.
Wie betreft het?	Alle partijen met (openbare) toezichttaken of partijen die daarvoor de (beleids)kaders opstellen: - BZK, NCTb, DJI; - Gemeenten; - Politie KLPD, Marechaussee; - Openbaar Vervoer, mainports; - Beveiligingsbedrijven.
Waarom is het onderzoek van belang?	- Veiligheid in het openbaar vervoer (issues groepsgedrag jeugd, gedragsbeïnvloeding reizigers/bestuurders, crowd management evenementen); - Veiligheid in gevangenissen (monitoren gevangenen en bezoekers); - Toezicht in winkels en winkelcentra (preventie diefstal, vandalisme); - Toegangscontrole (Schiphol, rechtbanken, voetbalstadions).
Waarmee kunnen we dit doen? (Focus)	- Met een ontwerp- en evaluatie-instrument voor de ontwikkeling en toets van effectieve en efficiënte toezichtorganisaties; - Waarnemen, vroeg interpreteren en beïnvloeden van afwijkend gedrag (weak signals, prikkelen individuen/groepen); - Optimale samenwerking tussen toezichthouders, gebruikmakend van alle beschikbare bronnen en informatie die afwijkend gedrag kunnen signaleren en duiden; - Intelligente sensornetwerken (spot, track & trace, intelligente camera's); - Ontwikkeling van in de surveillancepraktijk bruikbare risicoprofielen van een gebied, groepen en personen op basis van tijd, plaats, omgevingskenmerken, eigenschappen; randvoorwaarde: privacywetgeving; - Concept development & experimentation faciliteit, Livinglab in stedelijke omgeving/ Fieldlab in winkelcentrum;
Wie begeleidt?	Behoefstellers: Subarena Geïntegreerde Systemen (CIV), NCTb, AIVD.
	Klankbord: CCV, NCTb , Ministerie van Justitie.
TNO-team	Peter Rasker (trekker)

2.2.1.3 Met BZK en stakeholders afgestemde onderzoeksvragen

Vraag 1: Basismodel voor toezichtorganisatie in openbare ruimte
Hoe leidt het vroegtijdig herkennen van verdachte gedragingen afhankelijk van de context in verschillende (openbare) ruimten (openbaar vervoer, wijk, winkelcentra, luchthaven, enzovoort) tot een verhoogde kwaliteit, efficiency en veiligheidsbeleving bij het voorkomen van overlast en verloedering, kleine en grote criminaliteit en terrorisme en wat is het effect op het toezichtproces, de organisatie en de ondersteuning daarvan?

Focus op:
- Herkennen van verdacht gedrag;
- Relatie tussen gedragingen, omgeving, toezichtproces en prestatie-eisen;
- Professionalisering van toezicht in de (openbare) ruimte;
- Model waaruit men eisen kan afleiden voor het toezichtproces afhankelijk van het te herkennen verdacht gedrag, omgeving en prestatie-indicatoren.

Beschrijvend, voorspellend.

Vraag 2: Door professionals herkennen van (potentieel) verdacht gedrag
Welke gedragingen, contextinformatie en andere relevante (intelligence) informatie hebben voorspellende waarde (profiling) voor het voorkomen van overlast, kleine en grote criminaliteit en terrorisme?

Focus op:
- Breed perspectief gedragingen: personen in de ruimte maar ook informatie over personen in gegevensbestanden en andere informatiebronnen;
- Relatie met opsporing en proactief voorkomen van criminaliteit en terrorisme;
- Profiling: op basis van kenmerken extrapoleren van informatie om verdacht gedrag vroegtijdig te herkennen.

Voorspellend, verklarend.

Vraag 3: Prikkelen
Welke proactieve handelingen kunnen professionals toepassen om afwijkend gedrag beter te interpreteren en potentieel verdacht gedrag eerder te kunnen waarnemen (prikkelen)?

Focus op:
- Afwijkende gedragingen snel interpreteren;
- Bieden van handelingsperspectief aan professionals.

Beschrijvend, verklarend.

Vraag 4: Intelligente systemen
Welke verdachte / afwijkende gedragingen zijn met intelligente systemen beter te signaleren, en welke door mensen? Welke technologische ondersteuning kan worden ingezet om tot een beter en vroeger oordeel te komen? Hoe is een signalering door intelligente systemen zó te representeren dat een operator snel een juiste interventie kan doen?

Focus op:
- Systemen en automatisering van herkenning van verdachte gedragingen;
- Evaluatie in praktijk met professionals;
- Optimaliseren van rendement door optimale mens-systeem interactie.

Probleemoplossend, evaluerend.

2.2.2 Activering burger in relatie met veiligheidsorganisaties

2.2.2.1 Omschrijving van het topic

De professionele veiligheidsorganisaties zien als belangrijke uitdaging het betrekken van de burger bij het zorgen voor de veiligheid in de maatschappij. Daarbij gaat het om:

- Het invullen van de verantwoordelijkheid van burgers en bedrijven om te zorgen voor hun eigen veiligheid en bij te dragen aan de veiligheid van hun omgeving. Het gaat dan om preventieve maatregelen (rookdetectoren, inbraakpreventie etc.), voorbereiding op eventuele noodsituaties (bekendheid met vluchtmogelijkheden, vorming emergente groepen), zelfredzaamheid bij veiligheidsincidenten en rampen, en hulp aan medeburgers vóór de professionele veiligheidsorganisaties ter plekke zijn.
- Het benutten van de competenties van burgers en in de omgeving aanwezige professionals (buschauffeurs, verpleegkundigen, winkeliers, etc. etc.) voor het effectief en efficiënt realiseren van veiligheidsdoelstellingen.
  Dit is bv van belang voor toezicht op de openbare ruimte, opsporing van daders na incidenten, eerste acties na brandmelding, bijstand bij veiligheidsoperaties.

Rond burgerbetrokkenheid bij veiligheid zijn er vele initiatieven. In het kader van deze topic zal basiskennis ontwikkeld worden die bijdraagt aan:

- Het bevorderen van veiligheidsbewustzijn en actiebereidheid door nieuwe communicatieconcepten (bv inzet van sociale media, gaming).
- Effectievere inzet van burgers door informatievoorziening en communicatie gebaseerd op in zicht in de plaatsvindende psychologische processen.
- Methoden om groepen burgers als vrijwilliger te mobiliseren en hun competenties te vergroten door instructie, training en opleiding.

2.2.2.2 Focus van het topic

Waar gaat het precies over?	Zelfredzaamheid (betere preventie en preparatie van burgers en bedrijven op fysieke en sociale veiligheidsincidenten) en burgerparticipatie (benutting van competenties van burgers en bedrijven voor uitvoeren van veiligheidstaken).
Wie betreft het?	- Burgers; - Politie, brandweer en GHOR; - Veiligheidsregio's; - Gemeenten; - Bedrijven, waar veiligheid bijzondere aandacht krijgt i.v.m. risico's en/of hoeveelheid mensen.
Waarom is het onderzoek van belang?	Beïnvloeden veiligheidsbewustzijn. Verankeren van verantwoordelijkheid t.a.v. eigen veiligheid bij burgers en bedrijven. Handelingsperspectief en handelingsbereidheid van burgers en bedrijven Terugtredende overheid. Opbouwen community resilience.
Waarmee kunnen we dit doen? (Focus)	Communicatie voor beïnvloeding van perceptie en gedrag (incl. sociale netwerken). Leren en instructie van burgers en professionals voor optimale samenwerking (serious gaming). Stimuleren en belonen om motivatie voor participatie te bewerkstelligen. Organisatie van en infrastructuur voor burgerinzet.
Wie begeleidt?	Coördinerend behoeftesteller: NVBR. Overige behoeftestellers: BZK/programma dreigingen en capaciteiten, VTSPN, NCTB.
	Klankbord: SMVP, Politieacademie, CCV.
TNO-team	Gerard Veldhuis (trekker)

2.2.2.3 Met BZK en stakeholders afgestemde onderzoeksvragen

Vraag 1 Informatie keuze en vorm t.b.v. handelingsperspectief en -bereidheid
Welke informatie kan op welke manier beschikbaar worden gesteld aan burgers, bedrijven en organisaties; om het eigen handelingsperspectief en –bereidheid te vergroten? Welke incidenten, noodsituatie of rampen zijn te identificeren? Welke informatiebehoefte hebben burgers en bedrijven? Welke scenario's zijn er en hoe kunnen deze worden gemodelleerd?

Focus op:
- Type incident, ramp noodsituatie;
- De eigen veiligheid, de veiligheid van de omgeving en de ondersteuning van veiligheidsorganisaties;
- Type informatie en wijze beschikbaar stellen;
- Typen omgeving (o.a. woon-, werk-, recreëer-omgeving);
- Juridische consequenties;
- Verschillen tussen groepen (burgers: sociaal zwakkeren, sociaal sterkeren, semiprofessionals; bedrijven: bedrijfshulpverlening, bedrijfsbewakers).

Beschrijvend, evaluerend.

Vraag 2 Ondersteuning veiligheidsorganisaties
Hoe kunnen veiligheidsorganisaties worden ondersteund bij de uitvoering van hun taken door inzet van burgers en bedrijven? Welke methoden voor beoordeling informatie, meldingen incident en terugkoppeling zijn noodzakelijk? Wat zijn effectieve wijze van samenwerking en afstemming tussen burgers, bedrijven en veiligheidsorganisaties? Welke blokkades en knelpunten zijn er voor effectieve samenwerking? Hoe kunnen bevindingen worden verpakt zodat betrokkenen ervaren en leren hoe samenwerking effectief kan verlopen?

Focus op:
- Verkrijgen betrouwbare informatie en beoordeling ervan;
- Voorbereiden op en tijdens incident, ramp noodsituatie;
- Anticiperen op actiebereidheid ‘mentaliteit’;
- Informatie voor taken m.b.t. toezicht en opsporing;
- Communicatie naar directe omgeving bij incident, ramp noodsituatie;
- Fysieke inzet van burgers en bedrijven bij incident, ramp noodsituatie;
- Blijvende motivatie van burgers en bedrijfsleven ‘terugmelden’ communicatie.

Evaluerend, ontwerpend, probleemoplossend.

Vraag 3 Ingrepen gebouwen en gebouwde omgeving (in relatie tot gedrag van burgers)
Wat is het effect van ingrepen gericht op veiligheid en zelfredzaamheid in gebouwen en de gebouwde omgeving op het gedrag van burgers? Welke maatregelen zijn er in gebouwde omgeving en in gebouwen te nemen en welk effect is er te verwachten op het vergroten van de zelfredzaamheid? Wat is de relatie tussen maatregelen in de gebouwde omgeving en gebouwen en het optreden veiligheidsorganisatie Hoe kunnen deze relaties worden gevat in een kwalitatief relatiemodel?

Focus op:
- Veilig bouwen;
- Afhankelijkheid inzet professionele veiligheidsorganisaties;
- Decentrale middelen voor hulpverlening en organisatievormen;
- Mogelijke interventies en hun werking: actuele informatievoorziening bij incidenten, rampen noodsituaties voor vergroting zelfredzaamheid;
- Kwalitatief relatiemodel voor effectiviteit van verschillende ingrepen op eigen resilience.

Beschrijvend, evaluerend.

Vraag 4 Optimale samenwerking burgers en professionals
Op welke manier kunnen burgers en professionals bij incidenten en crises en rond sociale veiligheid samenwerken? Welke reële scenario’s gericht op samenwerking van burgers en professionals zijn er? Hoe kan disseminatie van samenwerkingsconcepten vorm krijgen?

Focus op:
- Vertrouwen en gezamenlijke verantwoordelijkheid;
- Type incident, ramp noodsituatie;
- Verhoging veiligheidsbeleving;
- Disseminatie, oefenen, gaming, middelen.

Beschrijvend, evaluerend, probleemoplossend.

2.2.3 Slimmer inzetten van informatiestromen voor veiligheidstaken (Verbreden van informatiestromen. Wat is er nodig? En wat kunnen we ermee?)

2.2.3.1 Omschrijving van het topic

Informatie en informatiegestuurd werken zijn van grote waarde binnen het veiligheidsdomein (lees: instanties verantwoordelijk voor toezicht, handhaving en opsporing). Zonder tijdige en juiste informatie op de juiste plaats kunnen de operationele taken niet goed worden uitgevoerd.
Er is een enorme hoeveelheid informatie beschikbaar op basis waarvan uitvoerende en sturende instanties hun activiteiten en beslissingen kunnen baseren. In de praktijk blijkt er echter vele malen meer informatie en informatiebronnen beschikbaar dan die door de mensen werkzaam in het domein tijdig en juist ontsloten kunnen worden.
De hoeveelheid beschikbare informatie neemt ook exponentieel toe. Dit leidt ertoe dat relevante informatie niet tijdig kan worden onderkend en verwerkt om mede input te vormen voor acties en besluitvorming bij operationele inzet. Een neveneffect hiervan is onrust bij de medewerkers en besluitvormers die achteraf verwijten krijgen als bepaalde beslissingen onjuist blijken te zijn. Zo van, “als jullie wat beter hadden gezocht in de beschikbare informatie hadden jullie vooraf kunnen weten dat ….”

De vraag rijst hoe hier op een goede wijze mee om te gaan? Zijn er technologische, organisatorische of procesmatige innovatieve oplossingen te bedenken die het mogelijk maken om meer informatie op goede wijze te ontsluiten ter ondersteuning van de operationele taken? Zijn er effectieve manieren van werken te bedenken waarbij het niet beschikken over volledige informatie niet als belemmerend wordt ervaren? Hoe kan de relevante informatie worden ontsloten terwijl alle niet relevante informatie buiten beeld blijft? Wat is de rol van de nieuwe media in het tijdig kunnen beschikken over de benodigde informatie?

Dit is de kern waar dit onderzoek om draait. Omdat er al veel gebeurt aan onderzoek op dit gebied zowel nationaal als internationaal zal worden gezocht naar additionele benaderingen en/of het verbinden van onderkende best practices tot bruikbare methoden of werkprocessen.

2.2.3.2 Focus van het topic

Waar gaat het precies over?	Slimmer inzetten van breed beschikbare informatie en nieuwe (sociale) media voor operationele veiligheidstaken. Verwerking van grote hoeveelheden aanwezige informatie, waarnemingen en meldingen tot direct bruikbare informatie.
Wie betreft het?	Operationele diensten in veiligheidsregio's en politieregio's (hulpverlening, toezicht, handhaving) Justitie/NFI/politie (opsporing) KLPD, NCTb, AIVD (intelligence)
Waarom is het onderzoek van belang?	De beschikbaarheid van (openbare) bronnen en informatie neemt exponentieel toe. Nieuwe sociale media (twitter, discussiefora) en andere bronnen (SMSalert, youtube) kunnen zinvolle informatie leveren waarmee risicovolle situaties en dreigingen vroegtijdig kunnen worden onderkend en op basis waarvan de-escalerend kan worden opgetreden. In al bestaande, geëscaleerde dreigingen of crisis kan de informatie worden gebruikt voor een snelle en eenduidige opsporing en/of afhandeling.
Waarmee kunnen we dit doen? (Focus)	**Technologische innovatie gericht op informatie-ontsluiting**: datamining, koppelen van informatiebronnen, videocontentanalyse, realtime vs. offline. **Procesinnovatie gericht op informatiegestuurd optreden**: risicoprofilering voor analyse van grote informatiestromen en koppeling van bronnen (kredietregistratie, kenteken, onroerend goed, …), burgerparticipatie. **Kwalitatieve en kwantitatieve analyse** van multimodale (burger-) meldingen op eigen initiatief cq. n.a.v. oproepen (meldkamer, twitter, website voor registratie van meldingen etc.), analyse van sociale media.
Wie begeleidt?	Coördinerend behoeftesteller: Ministerie van Justitie. Overige behoeftestellers: AIVD, NCTb, VTSPN, NICC.
	Klankbord:nader in te vullen.
TNO-team	Karin de Jong (trekker)

2.2.3.3 Met BZK en stakeholders afgestemde onderzoeksvragen

Vraag 1. Ontwikkelingen, methoden en technieken voor ontsluiting van nieuwe media (en wat kunnen we ermee?)
Bij deze onderzoeksvraag ligt de focus op de technologie voor mining van informatie uit nieuwe en bestaande bronnen. Invalshoeken zijn:

- Welke informatiebronnen leveren (de meeste) zinvolle informatie?
  Hoe verhouden de kosten en baten zich hiervan? Welke kwaliteit hebben ze (betrouwbaarheid, actualiteit, juistheid)? ***(Beschrijvend/vergelijkend)***
- Hoe kunnen verschillende soorten informatiebronnen optimaal bij elkaar worden gebracht? (beeld, spraak, data, video,…) T.b.v. analysedoeleinden en operationele inzet? ***(Probleemoplossend)***
- Te veel informatie is zowel voor de privacy als voor het veiligheidsapparaat een slechte zaak: Hoe kun je op voorhand bepalen of bepaalde informatie relevant zal zijn; hoe pas je het "select before you collect" doelmatig toe?
  [anoniem rechercheren / revocable privacy] Hoe kun je tegelijkertijd de (maatschappelijke) veiligheid verhogen en de privacy beter beschermen door

systemen zo in te richten dat je alleen informatie over overtreders te zien krijgt. ***(Probleemoplossend)***

- Hoe kunnen (de in ontwikkeling zijnde) technieken voor efficiënte data verrijking, semantic annotation (web 3. 0 technieken (o.a. het semantische web), collaborative tagging en rating) goed worden ingezet in het maatschappelijke veiligheidsdomein? ***(Beschrijvend, Evaluerend, Probleemoplossend)***
- Kun je afwijkende informatiepatronen in openbare bronnen (twitter, discussiefora, etc…) herkennen en hieruit mogelijke dreigingen/risico's en opportunities afleiden (afwijkend gedrag in informatiestromen). Hieronder valt ook het opstellen van profielen en normen, trends, indicatoren (kwalitatief en kwantitatief) ***(Testcases/ experimenteren)***
- Hoe ontwikkelen de sociale media zich de komende 10 jaar? Welke impact heeft dit op de samenleving en veiligheidsbeleving? ***(Beschrijvend/ Voorspellend)***

Vraag 2. Ontwikkeling van betere informatievoorzieningsystemen voor ondersteuning en sturing van veiligheidstaken

Bij deze onderzoeksvraag ligt de focus op het matchen van de behoefte aan informatie voor het uitvoeren van operationele veiligheidstaken met de potentieel te verkrijgen informatie uit nieuwe en bestaande bronnen. Invalshoeken zijn:

- Waar is potentieel hoge meerwaarde voor operationele veiligheidstaken te verwachten van het simultaan analyseren van (meer) reguliere informatiesystemen, actueel binnenkomende meldingen/waarnemingen en nieuwe media. Wat zijn bruikbare producten voor crisismanagement en voor meer heterdaads bij opsporing? **(Evaluerend)**
- Op welke wijze moeten informatiebronnen (intern, extern, intern + extern, beeld – tekst –geluid) worden gekoppeld om te leiden tot informatieverrijking bruikbaar voor operationele diensten (1+1 =3)? ***(Probleemoplossend)***
- Op welke wijze kunnen open en gesloten databronnen worden gecombineerd? Hoe kunnen informatiegebruikers/analisten tools en databronnen naar eigen inzicht koppelen? ***(Probleemoplossend)***
- Hoe kun je een proces inrichten dat automatisch relevant materiaal crawlt en vastlegt op een wijze die forensisch onderzoek faciliteert? ***(Probleemoplossend)***
- Op welke wijze kan kennis over afgesloten zaken en de effectiviteit van de interventies die daarin gebruikt zijn beschikbaar gemaakt worden voor een beslissingsondersteunend systeem ***(Evaluerend)***
- Verkenning van noodzakelijke vernieuwingen/ innovaties bij operationele veiligheidsdiensten om optimaal gebruik te kunnen maken van de nieuwe informatie-analysebenaderingen (training/opleiding personeel/ soort personeel, aanpassing van proces, organisatie, technologie etc…) **(Probleemoplossend/ Voorspellend)**

Vraag 3. Hoe kunnen privacy en vertrouwelijkheid de vereiste aandacht krijgen bij de nieuwe informatieanalyse-methoden voor ondersteuning van veiligheidstaken?

Bij deze onderzoeksvraag ligt de focus op de randvoorwaarden en belemmeringen bij het benutten van potentieel te verkrijgen informatie uit nieuwe en bestaande bronnen voor het uitvoeren van operationele veiligheidstaken met de. Invalshoeken zijn:

- Wat zijn de verwachte ontwikkelingen op gebied van privacy en welke impact heeft dit voor het gebruik van sociale media, burgerparticipatie etc… in operationele veiligheidstaken ***(Voorspellend)***
- Bij het verzamelen en combineren van allerlei gegevens worden profielen van personen, groepen en locaties opgebouwd. Op basis van deze profielen worden

verwachtingen over eventueel maatschappelijk ongewenst gedrag geformuleerd, waarop eventueel weer acties worden ondernomen (bv. preventief surveilleren, volgen, hinderen, vastzetten). Hoe ver moet/mag je hierin gaan? Wat is het morele kader ***(Evaluerend),*** welke gevolgen heeft dat voor de maatschappij ***(Evaluerend)*** en op welke manier zou dit via wetgeving vormgegeven kunnen worden ***(Probleemoplossend)***?

- Hoe maak je het proces van burgerparticipatie controleerbaar/beheersbaar: in hoeverre sta je anonieme aangiftes toe? Welke risico's zijn er ten aanzien van zwartmaken van onschuldige personen? Welke informatie kan burgerparticipatie opleveren? Zijn er contexten waarbinnen burgerparticipatie juist wel of juist minder zinvol is? ***(Evaluerend)***

2.2.4 Delen en benutten van informatiestromen voor het samen uitvoeren van veiligheidstaken (Beter benutten van informatiestromen)

2.2.4.1 Omschrijving van het topic

De informatievoorziening in het veiligheidsveld staat voor de uitdaging om beschikbare gegevens, informatie, interpretaties en lesson learned beter te benutten over de grenzen van organisaties en onderdelen daarvan. De belangrijkste sleutels om daartoe te komen zijn samenwerking en het gebruik maken van de collectieve kennis en ervaring. Informatie kunnen verspreiden is niet genoeg. Delen (ook bewaren) en benutten van de informatiestromen zijn cruciale vervolgstappen.

Dit vraagt het tot stand brengen van een rolgericht (risico- en vraaggestuurd) informatieaanbod in de veiligheidsketen. (Kosten)effectiever samenwerken in ad hoc samengestelde keten en netwerken wordt dan mogelijk. Nu is veelal sprake van of een te klein, of een te groot aanbod van informatie. Informatie wordt beperkt gedeeld, of de gedeelde informatie wordt zonder rekening te houden met de gebruiker in grote hoeveelheden “op zijn of haar bordje gelegd”. Dit laatste met het risico van informatie overload en micromanagement. Basis voorwaarden om dit te veranderen zijn:

- vertrouwen;
- inzicht in elkaars competenties, verantwoordelijkheden en prioriteiten (organisational awareness);
- interoperabiliteit (technisch, semantisch en qua uitwisselingsbereidheid);
- gedeeld begrip; en
- samenwerking en afstemming op diverse niveaus voor wat betreft doelstellingen, planning en uitvoering.

Onderzoeksuitdagingen die daarmee gepaard gaan zijn:

- Hoe bereiken we dat genetwerkte organisatiedelen voldoende vertrouwen hebben in (bereid zijn afhankelijk te zijn van) elkaar en van techniek?
- Hoe kunnen we binnen een genetwerkte en dynamische organisatie een beeld onderhouden van de structuur van die organisatie en van de competenties, verantwoordelijkheden, activiteiten en prioriteiten van de verschillende organisatiedelen?
- Hoe zorgen we ervoor dat de verschillende deelorganisaties elkaar werkelijk begrijpen – overbruggen van semantische verschillen – welke beelden en handelingsperspectieven roept een situatiebeschrijving bij de verschillende deelorganisaties op?
- Welke rolgerichte gebruikersinterfaces zijn nodig voor het creëren van op elkaar afgestemde situational awareness en coördinatie van taken?

- Hoe creëren we een toegankelijk collectief geheugen en hoe kunnen we op basis daarvan voorspellend vermogen opbouwen? Het gaat dan zowel om locatiespecifieke historie als om lessons learned van soortgelijke incidenten in het verleden.

Niet alleen binnen de veiligheidsketen maar ook de samenwerking tussen publiek en privaat vereist structurele verankering in de informatievoorziening voor de uitvoering van veiligheidstaken. Netcentrisch werken komt binnen het veiligheidsveld op gang. Een volgende stap is publiek private netcentrische informatievoorziening, waarbij de vitale sectoren onderdeel worden van het (virtuele en fysieke) netwerk. Dit is een belangrijke vervolgstap op de afspraken zoals die nu tussen het veiligheidsveld en de private sector worden gemaakt.

Inzicht in bovenstaande vraagstukken is noodzakelijk om veiligheidstaken (kosten)effectiever uit te kunnen voeren. Technologische doorbraken spelen daarbij slechts een beperkte rol. Innovatie op het vlak van de mens (cultuur en opleiden/trainen/ oefenen), proces, organisatie en rond het juridisch kader zijn zeker zo belangrijk. In het VP zal basiskennis worden ontwikkeld met een focus zoals die onderstaand is uitgewerkt en afgestemd met de door BZK gecoördineerde begeleidingsgroep.
De basiskennis zal veelal tot stand worden gebracht binnen fieldlabs en in nauwe samenwerking met het veiligheidsveld zelf. Als vervolg op de kennisontwikkeling is doorontwikkeling in nationale en internationale innovatieprogramma's voorzien gevolgd door vanuit stakeholders gefinancierde innovatietrajecten. Voorbeelden hiervan zijn:

- Politie informatiesysteem (bijvoorbeeld in de vorm van PDA's);
- Alerteringsysteem Terrorismebestrijding (ATb) versie X.0;
- Crisis Management Systeem versie X.0;
- Vernieuwing meldkamers / meldkamerconcept;
- Mobiele Data Terminal (MDT) versie X.0;
- Hulpverlener InformatieManagement Systeem (HIMS) versie X.0;
- Vernieuwing uitkijkcentrales;
- Control rooms - samenwerkende teams;
- Daar waar voorspellend vermogen direct toegevoegde waarde heeft.

2.2.4.2 Focus van het topic

Waar gaat het precies over?	Delen en benutten van informatiestromen voor het samen uitvoeren van veiligheidstaken. Informatievoorziening als basis voor het verbeteren van de beeldvorming, oordeelsvorming, besluitvorming en evaluatie; zowel gericht op multi-kolom/-laag optreden als op optreden binnen kolommen en zowel gericht op repressie als op preventie en pro-actie).
Wie betreft het?	Brandweer, Politie, GHOR, Defensie, Gemeenten, Veiligheidsregio's, de waterkolom, de vitale sectoren, private beveiligingsorganisaties en burgers/bedrijfsleven (multi-kolom) - vanaf het lokale tot en met internationaal niveau (multi-laags)
Waarom is het onderzoek van belang?	Informatie- en risico-gestuurd en gedifferentieerd (preventief, pro-actief, of repressief) veiligheidsoptreden zijn essentieel voor een verdere doorgroei van het kwaliteitsniveau van dit optreden (*doing better things* versus *doing things better*). Dit type optreden valt of staat met het hebben van de juiste informatie op het juiste moment op de juiste plaats, en het hierop laten volgen van de juiste actie van de juiste actor(en).
Waarmee kunnen we dit doen? (Focus)	• Ontwikkeling behoefte- en risico gestuurd informatieaanbod dat het handelingsperspectief duidelijk maakt, incl. de middelen om dit aanbod te generen en de werkwijzen om met dit aanbod effectief op te treden; • Intuïtieve human interfaces die de gebruiker ondersteunen in zijn handelen; • Ontwikkeling collectief geheugen van effectiviteit van gerealiseerde operationele aanpak en simulatiemethoden voor het vergroten van het voorspellend vermogen bij voorbereiden en uitvoeren van operationele taken; • Inrichting van de informatie-uitwisseling tussen publiek en privaat (m.n. vitale sectoren).
Wie begeleidt?	Coördinerend behoeftesteller: subarena Geïntegreerde systemen (CIV). Overige behoeftestellers: NVBR, NCTB (alerteringssysteem terrorisme-bestrijding, VTSPN.
	Klankbord: COT, Politie-academie e.a.
TNO-team	Harold Bousché, Willem Treurniet (trekkers)

2.2.4.3 Met BZK en stakeholders afgestemde onderzoeksvragen

Vraag 1. Informatie-aanbod voor samenwerkende professionals in de veiligheidsketen

Hoe kan het aanbod aan informatie voor de professionals zo worden georganiseerd (zowel vraag als risico gestuurd) dat het handelingsperspectief duidelijk is voor alle betrokken niveaus van de samenwerkende organisaties en op basis daarvan effectief wordt geacteerd?

Focus op:

- Professionele gebruikerscategorieën, hun behoeften aan informatie, hun motivatie tot delen van informatie met anderen;
- Hergebruik en reorganiseren van informatie afhankelijk van risico en doel/behoefte gebruiker, verticaal (alle niveaus eigen keten) en horizontaal (tussen ketenpartners);

- Structuur van informatievoorziening afgestemd op de rollen van de samenwerkende gebruikers in de veiligheidsketen (databronnen, geautomatiseerde voorbewerking van gegevens tot snel interpreteerbare informatie, karakteristieke vraagstellingen van gebruikerscategorieën);
- Voorselectie van handelingsperspectieven op basis van risicoprofielen;
- Draaiboeken (werkwijzen) voor specifieke handelingsperspectieven; CD&E.

Type onderzoek: beschrijvend, evaluerend, probleemoplossend.

Vraag 2. Nieuwe generatie gebruikersinterfaces
Hoe kan beschikbare informatie zo worden gepresenteerd dat de situational awareness voor gebruikers maximaal is?

Focus op:
- Effectieve human interfaces met gebruikmaking van augmented reality (samensmeden van camerabeelden en andere gegevens uit de werkelijkheid met realistische modellen tot een geïntegreerd geheel, zodat de gebruiker een met gegevens verrijkte werkelijkheid voor zich ziet);
- Multimodale communicatie (zichtbare/hoorbare/tactiele alerteringssignalen, voorbewerkte beelden, instructies via beeldscherm/gesproken tekst, expliciteren van dilemma's waarover besluit urgent is).

Type onderzoek: beschrijvend, evaluerend, probleemoplossend.

Vraag 3. Collectief geheugen en simulaties voor voorspellen
Hoe kunnen het collectieve geheugen en simulaties worden ingezet om voorspellend vermogen te creëren voor preventie, repressie en pro-actie?

Focus op:
- Consequenties per inzetfase;
- Ondersteuning besluitvorming over op- en afschaling;
- Ontsluiten en borgen van events en gebeurtenissen;
- Simulaties; CD&E;
- Nader te specificeren doelgroep.

Type onderzoek: ontwerpend, evaluerend.

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

Focus op:
- Ketenafhankelijkheidsanalyses;
- Koppelvlakken, zowel wat betreft systemen als processen;
- Selectie geschikte middelen;
- Type informatie;
- Simulatie van incidentontwikkeling met handelingsperspectief in verschillende scenario's;
- CD&E;
- Uitwerking voor een karakteristieke functie (suggestie: Alerteringssysteem Terrorismebestrijding).

Type onderzoek: beschrijvend, evaluerend, probleemoplossend.

2.2.5 Cybersecurity

2.2.5.1 Omschrijving van het topic

Het toenemend gebruik van ICT in alle delen van de maatschappij brengt naast kansen ook kwetsbaarheden met zich mee. Trendrapportages van organisaties als GovCERT en de nationale recherche laten zien dat misbruik van ICT sterk stijgt. Het gaat daarbij zowel om criminaliteit als het berokkenen van schade.
Dit topic richt zich op de bescherming van de cyberinfrastructuur tegen grootschalige dreigingen als opzettelijke verstoringen en misbruik.
Effectieve bescherming bestaat in het algemeen uit een evenwichtige verzameling maatregelen op het gebied van preventie, preparatie, detectie en respons. Zowel overheid als bedrijfsleven nemen reeds een groot aantal maatregelen op dit gebied.
De snelle veranderingen in de beschikbare technologie, de toenemende verwevenheid van infrastructuren, de snelle introductie van nieuwe gebruiksmogelijkheden en de incoherentie van maatregelen over organisaties heen zorgen echter voor nieuwe dreigingen en kwetsbaarheden en vergen steeds opnieuw risicoafwegingen en innovatieve maatregelen.
Om het onderzoek binnen dit topic vorm te geven is in een bijeenkomst met een aantal beleidsbepalende organisaties op het gebied van cybersecurity (waaronder NCTb, BZK/DGV, AIVD, Justitie, Defensie, vtsPN en NICC) een drietal onderwerpen benoemd waarop innovatie gewenst is.

Een belangrijke pijler binnen het onderwerp cybersecurity wordt gevormd door *detectie van misbruik* en bijbehorende mogelijkheden voor *opsporing en vervolging*. Er is behoefte aan methoden voor het analyseren van grote hoeveelheden gegevens, en ondersteunende analyse- en simulatiemodellen om misbruik vroegtijdig te herkennen. Hierbij richt het onderzoek zich niet op de afzonderlijke detectiesystemen, maar op het opbouwen van een gezamenlijk beeld uit een diversiteit aan informatiebronnen, zowel in aantal als type systemen. Speciale aandacht wordt besteed aan de toenemende functionaliteit van mobiele systemen, de hierbij komende risicofactoren en de mogelijkheden om hier in de opsporing op in te kunnen spelen.

Aangezien voorkomen van incidenten beter is dan genezen, is het wenselijk om al in het ontwerpstadium van systemen rekening te houden met security (‘*security by design’*). Hierbij richt het onderzoek zich op het opzetten van een referentiekader om risicofactoren van nieuwe technologie snel te kunnen inschatten en op het uitvoeren van technologiescans van opkomende technologieën.

Een speciaal aandachtsgebied wordt gevormd door *cybersecurity voor de vitale infrastructuur*. De vitale infrastructuur bestaat uit sectoren en voorzieningen waarvan verstoringen of uitval ernstige impact kunnen hebben op de Nederlandse samenleving, zoals de energievoorziening, drinkwatervoorziening en de transportsector. Ook deze vitale sectoren zijn in steeds grotere mate afhankelijk van ICT. Het risico van domino-effecten in de vitale infrastructuur ten gevolge van kwetsbaarheden in de cyberinfrastructuur vormt nationaal en internationaal een belangrijk aandachtspunt. Internationaal vindt samenwerking en gegevensuitwisseling plaats over dreigingen, kwetsbaarheden, maatregelen en onderliggende modellen. Binnen dit topic vindt op het de onderliggende modelvorming van cybersecurity intensieve internationale

samenwerking plaats. Om ook nationaal optimaal aan te kunnen sluiten bij de vraagstelling van de vitale sectoren wordt nauw samengewerkt met de Nationale Infrastructuur tegen Cybercrime (NICC). De goede samenwerking van de vitale sectoren binnen de informatieknooppunten van het NICC wordt gebruikt om de sectoroverstijgende onderzoeksvragen te identificeren en de onderzochte en bewezen oplossingsrichtingen zo direct mogelijk aan de vitale sectoren te kunnen terugkoppelen.

Het sector-overstijgende karakter van ICT zorgt ervoor dat dit topic relatie heeft met een aantal onderzoeksonderwerpen binnen andere TNO-thema's.

- binnen het TNO thema Informatiemaatschappij wordt aandacht besteed aan het ongeautoriseerd binnendringen van afzonderlijke computersystemen/ netwerken;
- het actief gebruik van cybermiddelen en het verstoren/bespioneren van communicatiesystemen valt onder het innovatiegebied Wereldwijd inzetbare krijgsmacht.

Tussen topic 5 en de genoemde onderzoeksonderwerpen binnen de overige thema's en innovatiegebieden zal nauwe afstemming plaatsvinden om onderzoeksonderwerpen af te stemmen en resultaten uit te wisselen.

2.2.5.2 Focus van het topic

Waar gaat het precies over?	Dreigingen t.a.v. cyberinfrastructuur/cybergebruik en pro-actieve bescherming daartegen. Het gaat hier met name om opzettelijk verstoren om schade te berokkenen en om misbruik.
Wie betreft het?	Ministerie BZK, Ministerie Justitie, NCTb, GovCERT, NICC, VTSPN, AIVD, KLPD, NFI, Logius, providers, VNO-NCW, Ministerie EZ, VNG, vitale sectoren, EU DG Home Affairs. (pm Defensie, KMar, EDA)
Waarom is het onderzoek van belang?	Misbruik van de cyberinfrastructuur door kwaadwillenden dient tegengegaan te worden door pro-actieve en preventieve maatregelen, terwijl het daadwerkelijk misbruiken zo vroeg mogelijk moet worden opgespoord en geëlimineerd. Daarnaast dienen opzettelijke verstoringen tot een zo gering mogelijke schade te leiden aan de cyberinfrastructuur zelf en de daarvan afhankelijke gebruikers.
Waarmee kunnen we dit doen? (Focus)	• Methoden voor vroegtijdig herkennen en opsporen van misbruik van de cyberinfrastructuur. • Ontwerp van de architectuur van de cyber-infrastructuur en gebruiksmodaliteiten die leiden tot vermindering van de mogelijkheid tot cybermisbruik (security by design). Methoden voor verminderen van de afhankelijkheid van de vitale infrastructuur-sectoren in de maatschappij van verstoringen in de cyberinfrastructuur.
Wie begeleidt?	Coördinerend behoeftesteller: n.t.b.
	Behoeftestellers: NCTb, BZK, Defensie, VTSPN, NICC.
TNO-team	Marieke Klaver (trekker)

2.2.5.3 Met BZK en stakeholders afgestemde onderzoeksvragen

Onderzoeksvraag 1: Vroegtijdig herkennen en opsporen
Hoe kan misbruik van de cyberinfrastructuur vroegtijdig worden herkend en opgespoord? Besteed hierbij speciale aandacht aan mobiele platformen.

Focus op:
- Instrumenten voor vroegtijdig herkennen van misbruik m.b.v. simulatie en modellen, rekening houdend met mogelijkheden voor opsporing en eliminatie;
- Welke dreigingen kunnen ontstaan door de toenemende functionaliteit van mobiele platformen en wat zijn adequate maatregelen daartegen.

Type onderzoek: beschrijvend, evaluerend, probleemoplossend.

Onderzoeksvraag 2: Voorkomen door security by design
Hoe is de schade door cybercrime tegen te gaan door security by design?

Focus op:
- Het opzetten van een referentiekader/-model van de cyberinfrastructuur voor een snelle beoordeling van potentiële additionele risico's van nieuwe ontwikkelingen (techniek, cybergebruik, dreigingen);
- Technology watch bescherming cyber-infrastructuur op architectuurniveau, inclusief gebruiksmodaliteiten die leiden tot vermindering van de mogelijkheid tot cybermisbruik;
- Simulatie en analyse van effecten van dreigingen en effectiviteit bescherming cyberinfrastructuur (meer-laagsbescherming, keten-afhankelijkheid, noodvoorzieningen e.d.).

Type onderzoek: beschrijvend, evaluerend, probleemoplossend.

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

Focus op:
- Simulatie en analyse van effecten van dreigingen m.b.t. cyberinfrastructuur is de vitale infrastructuur (keten-afhankelijkheid, meerlaags-bescherming) – internationale samenwerking;
- Ontwikkeling generieke methoden en tools voor de beoordeling van de Cyberstatus van vitale sectoren – in samenwerking met de NICC.

Type onderzoek: beschrijvend, evaluerend, probleemoplossend.

2.2.6 Verkenningen
In het overleg met BZK is besproken dat de huidige portfolio van kennistopics en onderzoeksvragen in het Vraaggestuurde onderzoekprogramma ook bijgesteld moet kunnen worden als er nieuwe ontwikkelingen plaatsvinden. De opkomst van nieuwe technologieën of maatschappelijke ontwikkelingen kunnen een forse impact hebben op de benodigde aanpak van veiligheidsvraagstukken. Daarom is afgesproken een deel van het VP-budget te alloceren voor verkenningen met verschillende invalshoeken:

Technologieverkenningen	**Impactverkenningen**
Deze zijn gericht op het helder krijgen van de potentiële impact van opkomende technologieën die een dreiging of een kans met betrekking tot de veiligheid in de maatschappij kunnen vormen.	Deze zijn gericht op het verkennen van potentieel te ontwikkelen technologieën mogelijke oplossingen voor nieuwe vraagstellingen.
Bijv.: Wat kan "Augmented Reality"-technologie in het veiligheidsdomein betekenen? Hoe benutten we de potentiële meerwaarde van nieuw ontwikkelde technologie in het VP-deelprogramma Effectief en Veilig Ingrijpen 2007-2010?	Bijv.: Welke dreiging betekent het breed beschikbaar komen van nieuwe bioagentia? Welke technologieën kunnen bijdragen aan de wens om hulpverleners meer op afstand te houden van plaatsen met een hoog veiligheidsrisico?

Om de verkenningen optimaal te laten aansluiten bij de praktijkomstandigheden en wisselwerking tussen organisaties en stakeholders zullen zonodig activiteiten met inzet van een fieldlab of CD&E-faciliteiten worden uitgevoerd.

De in het kader van dit VP uit te voeren verkenningen zullen normaliter òf voortbouwen op ontwikkelde basiskennis òf potentieel kunnen leiden tot nieuwe onderzoeksvragen voor het VP. Om de investeringen niet onnodig te verdunnen zullen er jaarlijks ca 3-5 verkenningen plaatsvinden. Bovendien wordt door deelname in bredere Europees kader een continue scan van potentieel opdoemende nieuwe opties uitgevoerd. Huidige projecten waarin TNO participeert zijn follow-up initiatieven van ESRIF (European Security Research and Innovation Forum) en enkele EU-projecten (CRESCENDO en ETCETERA).

Mede in verband met de nog lopende kabinetsformatie is besloten de keuze voor de in 2011 uit te voeren verkenningen pas in december 2010 te maken.

2.3 Samenwerking

2.3.1 Kennispartners van kennisopbouw

Voor de kennisopbouw in het kader van dit VP zal optimaal worden aangesloten bij de expertise van nationale en internationale kennisinstellingen. Daarnaast zal zo goed mogelijk worden samengewerkt met nationale stakeholders in het veiligheidsdomein, die eigen kennis- of innovatie-afdelingen hebben. In onderstaande tabel zijn nu bekende opties voor samenwerking bij de uitvoering van dit VP geïnventariseerd.

VP-Topic	Nationale kennispartners	Internationale ambities
1. Vroegtijdig herkennen van afwijkend gedrag van (potentiële) kwaadwillenden;	Methodiek: Politie-academie, LOKKMar, KLPD-DKDB. Technologie: Thales (gezamenlijke R&D), TU Delft & NLDA, UTwente, UvA. CCV	Intern. kennispartners technologie: FOI, SAGEM, MORPHO. Gehonoreerde EU projecten: ADABTS (crowds), ARENA (transport). Voorstel EU project: TACTICS (anti-terreur strategieën in stedelijke omgeving). DARPA project met partners uit VS: CORTEX (technologie voor gedragsherkenning).
2. Activering van burgers in relatie met veiligheidsorganisaties	Methodiek: NVBR, NIFV, Stichting Impact, CCV, Politieacademie, VU (CrisisLab), HKV Lijn in Water, Universiteit Twente, NCTb, CENS2, Technologie: Thales	Invoegen bekende EU trajecten Dit jonge onderwerp komt op de agenda bij EU KP7. Onze ambitie is om een internationaal consortium te formeren met vooraan-staande kennisinstituten en operationele diensten)
3. Slimmer inzetten van informatie	n.t.b.	n.t.b.
4. Delen en benutten van informatiestromen voor het samen uitvoeren van veiligheidstaken	VU/ Frank van Harmelen (Knowledge Representation & Reasoning), UU/ J-J. Meyer et al (modellering van organisaties), Univ. Nijmegen/ Wessel Kraaij (Semantische Netwerken), Universiteit van Amsterdam, Hogeschool van de Kunsten Utrecht, vtsPN Research & Innovatie, …	n.t.b.
5. Cybersecurity	n.t.b.	n.t.b.
6. Verkenningen.	HCSS	EU-projecten

2.3.2 Samenwerking met partners voor implementatie

Nationaal en internationaal zijn er omvangrijke innovatiestimuleringprogramma's op het gebied van een veiligheid in de maatschappij. In het kader van deze programma's worden consortia gevormd die innovatieve concepten kunnen doorontwikkelen en doorbraken voor implementatie tot stand kunnen brengen. TNO heeft bij dit soort programma's een erkende positie en wil ook de in dit VP te ontwikkelen kennis vroegtijdig verbinden met kennispartners en stakeholders om versterking van de ontwikkelingen te realiseren. Potentiële partners en ambities voor de vijf topics zijn onderstaand nader gespecificeerd.

VP-Topic	Nationale publieke en private partners /stakeholders	Internationale ambities
1. Vroegtijdig herkennen van afwijkend gedrag van (potentiële) kwaadwillenden;	Partners technologie: Thales, Tafel veiligheid IIP Sensornetwerken, CIV, Noldus, Eagle Vision, Vinotion, ADT, VDG, Bosch, Siemens. Stakeholders: KLPD, vtsPN, KMar.	Intentie: samenwerking met IBM Watson Lab (afwijkend gedrag) Op zetten van een internationaal erkend fieldlab voor het beproeven van innovatie van toezichtconcepten door beter herkennen van afwijkend gedrag.
2. Activering van burgers in relatie met veilig-heidsorganisaties	NIFV, CCV, n.t.b.	n.t.b.
3. Slimmer inzetten van informatie	n.t.b.	n.t.b.
4. Delen en benutten van informatiestromen voor het samen uitvoeren van veiligheidstaken	vtsPN Research & Innovatie, Bureau Veiligheidsberaad, Bureau Veiligheidsmonitor	EU FP7 2011.4.1-1 Crisis management modelling tool (FOI, ELBIT, BAE, TNO, EADS, Thales France, University Modena, ISDEFE, ITTI Poland) met NIFV
5. Cybersecurity	n.t.b.	n.t.b.
6. Verkenningen.		Duurzame aanwezigheid in strategische netwerken voor strategie-ontwikkeling op het gebied van security

2.3.3 Benutting van bestaande verankering in nationale en internationale innovatie-stimuleringsprogramma's

Als resultaat van het Vraaggestuurde Programma Maatschappelijke Veiligheid 2007-2010 participeert TNO in een dertigtal projecten en initiatieven binnen nationale en internationale innovatiestimuleringsprogramma's. Kenmerk van deze stimulerings-programma's is dat alle partners een eigen investering meebrengen. Voor TNO zijn er daarom budgettaire verplichtingen, die gefinancierd moeten worden uit het vervolgprogramma 2011-2014. Gezien het belang van uitnutten van eerder gepleegde

investeringen in kennisontwikkeling heeft BZK toegestemd in allocatie van de benodigde middelen hiervoor. In juni is aan BZK een overzicht van de benodigde budgetten verstrekt.

2.4 Afspraken voor uitwerken van projectplannen voor 2011

Met BZK is afgesproken dat TNO voor 1 november 2010 per topic een projectplan maakt voor de in 2011 uit te voeren activiteiten en een roadmap 2011-2014 voor kennisopbouw en initiatie van implementatie van de resultaten. Voor de vijf benoemde specifieke topics is er een klein groepje van 3 tot 4 behoeftestellers met een coördinator benoemd. Elk projectplan zal met het groepje behoeftestellers in de eerste helft van november worden besproken; de uitvoering van een project kan pas starten na daar verkregen instemming.

Met BZK zullen eind november 2010 de conclusies van de vijf overleggen over de projectplannen worden besproken. Dan zal ook nader overleg plaatsvinden over de financiële planning. Verder zal dan op basis van geïnventariseerde opties en de dan waarschijnlijk bekende beleidsvoornemens van het nieuwe kabinet een invulling plaatsvinden van het generieke topic Verkenningen.

Tweemaal per jaar zal er een bijeenkomst zijn onder leiding van BZK met de meest betrokken behoeftestellers. In het voorjaar gaat het dan om de resultaten van het achterliggende jaar en in het najaar om de invulling van de plannen voor het komende jaar.