Maatschappelijke Innovatie Agenda Veiligheid

BIJLAGEN

Nederland Ondernemend Innovatieland

Maatschappelijke Innovatie Agenda Veiligheid

Uitgave juni 2008

BIJLAGEN

Bijlagen

Bijlage I: Swot-Analyse van de vraag

ALGEMEEN

Wat zijn de dominante problemen en thema's op het gebied van veiligheid en voor de daarbij betrokken partijen? Deze bijlage geeft een goed overzicht waar de relevante vraagstukken liggen die door het innovatieprogramma (deels) opgelost kunnen worden. Het oplossen van knelpunten en problemen door innovatie, brengt ver-betering aan in de veiligheidssituatie in Nederland. Daarmee draagt het innovatieprogramma rechtstreeks bij aan het helpen verwezenlijken van veiligheidsdoelstellingen van het kabinet.

Hoewel de internationale ontwikkelingen van belang zijn om te zien wat de dominante thema's zijn binnen Europa, zijn voor het nationale innovatieprogramma veiligheid vooral de ontwikkelingen op het beleidsterrein van de departementen Justitie, Defensie en BZK van belang. Een overzicht van die terreinen en daarna de vergelijking ervan, moeten inzicht geven in wat ons bindt en wat niet. Wat ons bindt, bepaalt de zogenaamde 'common ground' waar succesvolle samenwerking en gemeenschappelijke programmering mogelijk is. Dit hoofdstuk eindigt dan ook met de omschrijving van de "common ground".

Er past nog één kleine kanttekening. In de intensieve gesprekken die plaatsvinden tussen de departementen, blijkt dat er soms voor verschillende initiatieven gelijke woorden bestaan maar andersom is ook het geval. Het Defensie 'Network Enabled Capabilities' blijkt bijvoorbeeld een civiele tegenvoeter te kennen: Informatie Gestuurd Optreden. Het conceptuele denken dat ten grondslag ligt aan beiden, is soortgelijk. Tegelijkertijd liggen er wel inhoudelijke nuances in de uitvoering en toepassing. Dus als er in het onderstaande begrippen worden gehanteerd die niet over-een komen, is daarmee nog niet gezegd dat er geen inhoudelijke overeenkomsten zijn. In de (toekomstige) samenwerking zal ook worden getracht te komen tot een gemeenschappelijk discours. In tussentijd zullen voorbeelden gemeenschappelijkheid achter verschillende begrippen moeten verduidelijken.

INTERNATIONALE ONTWIKKELINGEN

In Europa is het 7e kaderprogramma van start gegaan met voor het eerst ook 'veiligheid' als één van de aandachtsgebieden. De opzet van het European Security Research Programme (ESRP) is op advies van de European Security Research Advisory Board (ESRAB) ook vraaggestuurd ingericht ('Meeting the challenge: the European Security Research Agenda' (ESRAB rapport oktober 2006)).

Voor de opzet van het programma is uitgegaan van zogenaamde 'missies' ('missions') die voor de uitvoering bepaalde 'kunde' ('capabilities') vereisen. En vanuit de kennis wat je moet kunnen om je missie goed uit te voeren, volgt de behoefte aan technologie en innovatie. En gezamenlijk geeft het voorgaande richting aan de vulling van het programma. ESRAB heeft geadviseerd om voor veiligheid vier missiegebieden te definiëren:

- bescherming tegen terrorisme en georganiseerde misdaad
- grensbewaking
- bescherming van kritische/vitale infrastructuur
- herstel van veiligheid in geval van crises

Voor de komende jaren wordt binnen het ESRP onderzoek en ontwikkeling voorzien op het gebied van onder andere toegepast forensisch onderzoek, detectiesystemen (zowel gedrag als goederen), crisismanagement en multidisciplinair optreden en verbetering van uitrusting en materieel van de 'First responder'. Initiatieven waar Nederland naar verwachting zowel veel aan heeft als aan kan bijdragen, hangen samen met simulatoren, serious gaming en network enabled capabilities op het gebied van crisisbeheersing en gedrags- en persoonsherkenning en identificatie en versterking van het optreden op het plaats delict voor het verbeteren van de opsporing en handhaving.

NATIONALE ONTWIKKELINGEN

Defensie

Trends:

Groeiende verwevenheid tussen interne en externe veiligheid.

Vrijwel alle bedreigingen van onze samenleving hebben een internationale dimensie. Grote delen van de wereld zijn instabiel. Deze instabiliteit leidt tot tal van problemen die ook ons aangaan. Niet alleen zijn wij van oudsher oprecht begaan met het lot van andere mensen, maar het welvarende Europa ondervindt ook zelf de problemen in de vorm van onbeheersbare migratiestromen en de omvangrijke handel in drugs, wapens en mensen. Vooral zwakke staten vormen een aanwijsbare bron voor dergelijke veiligheidsrisico's. Zo hebben in een maatschappij waar de staat vrijwel afwezig is terroristische organisaties vrij spel. De recente geschiedenis van Afghanistan heeft dat wel bewezen. Mede om te voorkomen dat dat land opnieuw een uitvalsbasis voor terroristen wordt, levert Nederland er in Navo-verband een aanzienlijke bijdrage aan de stabilisering en versterking van het gezag. En ook al is in een land de staat aanwezig, dan functioneert zij lang niet altijd in dienst van de bevolking. Ook dit blijft niet zonder gevolgen. Politiek en religieus extremisme vinden hier namelijk een voedingsbodem.

Groeiende defensiebijdrage aan veiligheid binnen de landsgrenzen.
De samenwerking met civiele autoriteiten voor de nationale veiligheid is de afgelopen jaren sterk geïntensiveerd. De oprichting van de Kustwacht Nederland en de Dienst Speciale Interventie zijn voorbeelden hiervan en ook de Kustwacht Nederlandse Antillen en Aruba verdient vermelding. Niet alleen de omvang, maar ook de aard van de defensiebijdrage aan de nationale veiligheid is veranderd. In aanvulling op de algemene ondersteuning met personeel en materieel stelt Defensie ook hoogwaardige en specialistische capaciteiten beschikbaar. Door de veelvuldige inzet in het buitenland beschikt Defensie over capaciteiten en ervaringen die ook voor nationale inzet relevant zijn, bijvoorbeeld op het gebied van explosievenopruiming of de bestrijding van luchtvaartterrorisme. Daarnaast levert de Koninklijke marechaussee waardevolle bijdragen aan de nationale veiligheid. Het project "Intensivering civiel-militaire samenwerking" (ICMS) behelst afspraken over capaciteiten die Defensie gegarandeerd binnen vastgestelde termijnen aan civiele autoriteiten beschikbaar stelt. Defensie heeft zich ontwikkeld van een 'vangnet' voor de civiele autoriteiten tot een veiligheidspartner van de politie, de brandweer en de geneeskundige hulpverlening bij ongevallen en rampen. ICMS toont een alternatieve benadering om de slagkracht van de overheid te vergroten. De afgelopen periode zijn de handen op centraal niveau ineen geslagen. De komende tijd moeten de afspraken in de praktijk worden gebracht en moet de samenwerking ook op decentraal niveau worden verankerd. Civiele vertegenwoordigers in de veiligheidsregio's en de regionale militaire commandanten moeten elkaar snel weten te vinden en samen moeten zij de samenwerking in de dagelijkse bedrijfsvoering gestalte geven. Defensie heeft hiertoe de grenzen van de regionale militaire commando's aangepast aan die van de veiligheidsregio's. Ook zorgt Defensie ervoor dat iedere veiligheidsregio over een vaste militaire adviseur beschikt. Ten slotte neemt Defensie deel aan gezamenlijke oefeningen om de samenwerking verder te verbeteren.

Beleidskader Defensie:
Het defensiebeleid dient te zijn gestoeld op een gedegen begrip van de ontwikkelingen in onze nationale en internationale omgeving en van hun gevolgen voor de veiligheid van ons land en voor onze belangen en waarden. Dat Nederland een open land is in een wereld die alsmaar kleiner lijkt te worden, vormt daarbij een centraal gegeven. Onze openheid heeft ons onder meer een hoog levenspeil gebracht en wij moeten haar daarom zien te behouden. Onze openheid maakt ons evenwel ook kwetsbaar. Bedreigingen voor onze veiligheid hebben onmiskenbaar een mondiaal karakter. Juist een open samenleving als de Nederlandse moet in een tijdperk van vergaande mondialisering daarom haar weerbaarheid op peil houden.

In het regeerakkoord en het daaropvolgende beleidsprogramma van dit kabinet is tot uitdrukking gebracht welke gevolgen hieruit worden getrokken. Voorop staat dat Nederland in internationaal verband een actieve en constructieve partner wil blijven. De meeste vraagstukken waarmee Nederland wordt geconfronteerd, kunnen immers niet worden opgelost zonder een internationaal georiënteerde aanpak. Dat geldt ook voor onze veiligheid. Ons land draagt bovendien van oudsher de bevordering en de handhaving van de internationale rechtsorde hoog in het vaandel. Het kabinet hecht hieraan groot belang. Nederland investeert uit overtuiging in versterking van de internationale samenwerking en van de internationale rechtsorde en in duurzame ontwikkeling waar armoede heerst. Het motto van dit kabinet - "samen leven, samen werken" - reikt nadrukkelijk over de landsgrenzen heen. Zonder de actieve betrokkenheid van landen als Nederland bij internationale vraagstukken zou de wereld onveiliger en onrechtvaardiger zijn. Wij mogen alleen daarom al niet weglopen voor onze verantwoordelijkheid, ook niet als daarbij aanzienlijke risico's worden gelopen. Deze betrokkenheid - ook die van militaire aard - geeft ons in internationaal verband bovendien recht van spreken. Om uitvoering te geven aan een actief, geïntegreerde buitenlands beleid moet ons land blijven beschikken over een moderne, snel inzetbare en kwalitatief hoogwaardige krijgsmacht. Bovendien levert de krijgsmacht ook binnen de landsgrenzen op tal van manieren een wezenlijke bijdrage aan onze veiligheid.

Bij het verder gestalte geven aan de krijgsmacht hebben wij ons terdege rekenschap gegeven van de ontwikkelingen in onze omgeving en van de bij operaties opgedane ervaringen. Deze ontwikkelingen en ervaringen zijn vorig jaar in kaart gebracht in de Actualiseringsbrief ("Nieuw evenwicht, nieuwe ontwikkelingen", van 2 juni 2006, kamerstuk 30 300 X, nr. 127), mede op grond van gesprekken met vertegenwoordigers uit het bedrijfsleven, de wetenschap en de cultuur en van de resultaten van een serie werkconferenties. De Adviesraad Internationale Vraagstukken leverde eveneens een waardevolle bijdrage aan de discussie met een advies over de relatie tussen maatschappij en krijgsmacht.

Hoofdtaken Defensie:
Defensie heeft drie hoofdtaken:
1. De bescherming van het eigen en bondgenootschappelijke grondgebied, inclusief de Nederlandse Antillen en Aruba, zo nodig met alle beschikbare middelen;
2. Een actieve bijdrage aan het geïntegreerde buitenlandse beleid van ons land. Het gaat hierbij om:

- Kwalitatief en technologisch hoogwaardige militaire bijdragen aan internationale operaties in alle delen van het geweldsspectrum, ook in de beginfase van een operatie. Dit betreft:

Een bijdrage aan het ambitieniveau van de Navo. In verband hiermee zal de krijgsmacht tevens een continue bijdrage van wisselende omvang leveren aan de NATO Response Force;

- Een bijdrage aan het ambitieniveau van de Europese Unie. In verband hiermee zal de krijgsmacht tevens een periodieke bijdrage leveren aan de snelle reactiecapaciteiten van de Unie, de EU Battlegroups;
- Een bijdrage aan de Stand-by High Readiness Brigade (Shirbrig) van de Verenigde Naties;
- Deelneming gedurende maximaal een jaar aan een operatie in het hogere deel van het geweldsspectrum met een brigade van landstrijdkrachten, twee squadrons jachtvliegtuigen of een maritieme taakgroep;
- Gelijktijdige deelneming gedurende langere tijd aan maximaal drie operaties in het lagere deel van het geweldsspectrum met taakgroepen van bataljonsgrootte of, bij luchtoperaties en maritieme operaties, equivalenten hiervan;
- Het optreden bij landoperaties als lead nation op brigadeniveau en, samen met andere landen, op legerkorpsniveau, bij maritieme operaties als lead nation op taakgroepniveau en bij luchtoperaties met bijdragen op gelijkwaardige niveaus als de brigade;
- De uitvoering van speciale operaties, met inbegrip van evacuatieoperaties en contraterrorisme operaties;

- Deelneming aan politiemissies, waaronder die van de Europese Gendarmerie-eenheid, met functionarissen en eenheden van het Commando Koninklijke marechaussee en aan kleinschalige missies met een civiel-militair karakter;
- Beschikbaarstelling van militaire deskundigen ten behoeve van de training en advisering van veiligheidsorganisaties in andere landen;
- Verlening van internationale noodhulp op verzoek van civiele autoriteiten.

3 Bijdragen binnen de grenzen van het Koninkrijk aan de veiligheid van onze samenleving, onder civiel gezag. Het gaat hierbij in het bijzonder om:

- De uitvoering van nationale taken, zoals de grensbewaking door het Commando Koninklijke marechaussee en de kustwacht;
- Militaire bijstand bij de strafrechtelijke handhaving van de rechtsorde evenals de handhaving van de openbare orde en veiligheid, zoals met bijzondere bijstandseenheden en de explosievenopruiming;
- Militaire bijstand bij de bestrijding van rampen en zware ongevallen.

Bij de verdere uitwerking van deze analyse zijn vooral de behoeften voortkomend uit invulling van de tweede en de derde hoofdtaak relevant.

Behoeften Defensie:
Om succesvol ingezet te kunnen worden, dient het militair vermogen goed aan te sluiten bij de essentiële functionaliteiten die Defensie ambieert te vervullen. Innovatie van het militaire vermogen zal dan ook vooral plaatsvinden naar aanleiding van veranderingen in deze beoogde functionaliteiten. Het ministerie van Defensie heeft deze functionaliteiten vertaald naar de volgende zeven Essentiële Operationele Capaciteiten.

- vermogens die nodig zijn om ervoor te zorgen dat eenheden tijdig beschikbaar zijn (EOC1);
- vermogens die nodig zijn om toegang tot gevalideerde inlichtingen te realiseren (EOC2);
- vermogens die zijn nodig om ontplooibaarheid en mobiliteit te verzekeren (EOC3);
- vermogens die nodig zijn voor effectieve inzet (EOC4);
- vermogens die nodig zijn voor een adequate bevelvoering (EOC5);
- vermogens die nodig zijn voor een goede logistieke ondersteuning (EOC6); en
- vermogens die nodig zijn om de veiligheid en zelfbescherming te waarborgen (EOC7).

De behoeften van Defensie zijn gericht op het versterken van deze capaciteiten. Hieronder worden de voor het innovatieprogramma relevante prioriteiten uit de beleidsbrief "Wereldwijd dienstbaar" gepresenteerd:

VERSTERKING VAN HET OPTREDEN IN NETWERKEN

Modern militair optreden vereist dat uiteenlopende wapensystemen, sensoren en Commandovoering-systemen te land, op zee en in de lucht zodanig met elkaar in verbinding staan dat snel, doeltreffend en met de nodige flexibiliteit kan worden opgetreden. Deze systemen en sensoren vormen gezamenlijk als het ware een netwerk, waarvoor in bondgenootschappelijk verband de aanduiding *Network Enabled Capabilities wordt gebruikt*. Doordat systemen en sensoren met elkaar in verbinding staan, kan een beter gemeenschappelijk beeld worden opgebouwd van de situatie in een operatiegebied. Ook kan zo bij een gewapend treffen de escalatiedominantie van onze militairen worden gewaarborgd, aangezien in een 'netwerk' snel een gecoördineerd beroep kan worden gedaan op extra middelen. Te denken is bijvoorbeeld aan de ondersteuning van gevechtsvliegtuigen of gevechtshelikopters van eenheden op de grond. Het vermogen systemen en sensoren in een netwerk samen te brengen, komt zowel de effectiviteit van de missie als de veiligheid van

de eigen eenheden ten goede. Complexe operaties zoals in Afghanistan vergen bovendien dat dit vermogen niet uitsluitend op hogere niveaus maar ook lager – dat wil zeggen bij kleinere eenheden en verbanden – aanwezig is. Investeringen in *Network Enabled Capabilities* bevorderen voorts het vermogen om samen met bondgenoten en partners op te treden.

VERSTERKING VAN DE INLICHTINGENKETEN

Het belang van een goede inlichtingenpositie is voor Defensie de afgelopen jaren onmiskenbaar toegenomen. De groeiende complexiteit van operaties en de mondialisering van de inzet van de krijgsmacht stellen bovendien hogere eisen aan de inlichtingenvoorziening. Wat leeft er in een operatiegebied onder de bevolking? Wat zijn de tegenstanders van een missie van plan en hoe moet daarop worden gereageerd? Betrouwbare en tijdige inlichtingen zijn niet alleen voorwaarden voor effectief militair optreden maar ook voor de veiligheid van onze militairen. Deze ontwikkelingen vergen een wezenlijke versterking van de inlichtingenketen bij Defensie.

VERBETERING VAN DE BESCHERMING VAN PERSONEEL OP UITZENDING.

De bescherming van uitgezonden personeel staat bij Defensie hoog op de agenda. Alleen goed beschermd personeel is in staat de missie te volbrengen. Ook uit het oogpunt van goed werkgeverschap voelt Defensie zich verplicht alles in het werk te stellen om de risico's te minimaliseren. De operationele ervaringen in vooral Afghanistan en Irak hebben duidelijk gemaakt dat hiervoor aanvullende maatregelen nodig zijn. Zo worden onze militairen vaker dan voorheen geconfronteerd met op afstand bediende explosieven, die in het militaire jargon *improvised explosive devices* (IED's) worden genoemd. Deze vormen een belangrijke bedreiging en vergen snelle tegenmaatregelen. Dergelijke maatregelen zijn niet alleen gericht op het vinden en het uitschakelen van de explosieven, maar ook op het uitschakelen van het achterliggende netwerk van de tegenstander. Er wordt een reeks maatregelen getroffen om onze eigen eenheden beter te beschermen. Inmiddels is een IED-taakgroep (*Taskforce "Countering IED"*) opgericht. De personele en materiële capaciteit om IED's te detecteren en te neutraliseren wordt uitgebreid. Operationele concepten worden aangepast en militaire kampementen worden versterkt. Het inlichtingenwerk en de opleiding en de training van militairen besteden aandacht aan de dreiging van aanslagen.

INVESTEREN IN KWALITEIT VAN PERSONEEL

De kwaliteit van het defensiepersoneel, zowel in de uitvoering als in de ondersteuning en zowel militair als burger, is bepalend voor het welslagen van ieder militair optreden. Een goede selectie van personeel bij instroom en doorstroom en een goede opleiding en training dragen rechtstreeks bij tot de inzetbaarheid van de krijgsmacht. Ook de bescherming van personeel tijdens operaties is sterk afhankelijk van strenge selectie, goede beheersing van militaire vaardigheden en intensieve trainingen die de realiteit van de inzet zo dicht mogelijk benaderen (*train as you fight, fight as you train*).

Technologiegebieden Defensie:

Op basis van de beschreven behoeften kunnen voor Defensie de volgende essentiële technologiegebieden worden geïdentificeerd:

- Materialen;
- Sensoren/sensorsystemen;
- Beeldverwerking;
- ICT;
- Electrotechniek;
- Regel- en computertechniek;
- Milieu- en veiligheidstechniek;
- Electronica en mechatronica;
- Werktuigbouwkunde;
- Medische technologie (Biologisch);
- Bouwkunde;
- Aandrijving, energiesystemen;
- Mechanica, hydraulica;
- Nanotechnologie.

BZK

Trends

Nederland wordt geconfronteerd met een veiligheidssituatie die sterk in beweging is. De veiligheidssituatie en de beleving daarvan wordt beïnvloed door:

- De opkomst van internationale criminaliteit en terrorisme. Het samenwerken met de USA, de veelheid aan internationale organisaties die in Nederland zijn gevestigd en de spilrol die Nederland speelt in financiële, logistieke en personele stromen, maken Nederland een potentieel doelwit.
- De sterke toename van aantal, aard aanleiding en uitwerking van zowel security als safety incidenten, waarbij de kwetsbaarheid van onze maatschappij zowel op collectief niveau als individueel niveau steeds groter wordt.
- Een sterke toename van complexe risico's door intensief ruimtegebruik en de integratie van woon-, werk-, transport- en recreatieactiviteiten.
- Europese samenwerking en regelgeving op het gebied van terreur-, criminaliteits- en calamiteitbestrijding speelt Europese regelgeving in toenemende mate een rol.
- Snelle technologische ontwikkelingen: de ontwikkelingen op het gebied van onder andere de communicatietechnologie hebben gezorgd voor globalisering en flexibilisering van de maatschappij. Zowel "specialistische" technologie als "consumenten" technologie zijn op grote schaal beschikbaar voor criminele en terroristische groeperingen.

- Door de samenstelling van de Nederlandse bevolking en de toenemende radicalisering is Nederland in toenemende mate kwetsbaar voor deelname aan internationale conflicten van politieke, nationale en religieuze aard.
- Er worden successen geboekt (terugdringen criminaliteit en overlast) maar die vertalen zich lang niet altijd in een veiliger gevoel bij de burger.

Bovenstaande ontwikkelingen vragen om een herwaardering van de bestaande organisatie en het zoeken naar andere manieren om criminaliteit-, terrorisme- en calamiteitbestrijding.

Beleidskader BZK

We willen een samenleving waarin mensen zich veilig, vertrouwd en met elkaar verbonden voelen. Een samenleving waarin wederzijds respect de norm is, waarin we elkaar geen overlast bezorgen en waarin geweld een uitzondering is, net als diefstal, vernieling en andere vormen van criminaliteit. Zo'n samenleving kan alleen worden bereikt als het streven daarnaar breed wordt omarmd, niet alleen in woorden maar ook in daden. Burgers en ondernemingen kunnen daarin veel betekenen op grond van hun eigen verantwoordelijkheid. Van de overheid mag worden verwacht dat zij weet op te treden wanneer de veiligheid in de knel komt. Alleen dan is onze samenleving een rechtsstaat in de volle zin van het woord. [missie pijler 5 van het beleidsprogramma]

Samenwerken in vertrouwen, over de bestuurslagen heen: dat is ons uitgangspunt binnen de overheid. Alleen zo kunnen maatschappelijke uitdagingen met succes worden opgepakt. Dat is niet vanzelfsprekend. De overheid bestaat uit veel afzonderlijke onderdelen, organisaties en autonome bestuurslagen. Het is nodig dat al deze onderdelen samenwerken om tot een goed presterende overheid te komen ook voor het thema veiligheid.

Politie, brandweer, ambulancediensten, marechaussee, centrale overheid, gemeenten, maatschappelijke organisaties, bedrijven en burgers hebben ieder hun verantwoordelijkheden in het handhaven van de openbare orde en veiligheid. Bedreigingen van onze veiligheid veranderen en raken steeds meer met elkaar verweven. Het antwoord op bedreigingen kan steeds minder door één organisatie worden geformuleerd en uitgevoerd. Om de veiligheid van burgers te kunnen waarborgen is het noodzakelijk dat deze partners in veiligheid goed met elkaar samenwerken, zowel in lokaal, regionaal, nationaal als internationaal verband, zodat er minder slachtoffers en schade optreden en de veiligheid van de hulpverleners beter gewaarborgd kan worden. Om goed te kunnen samenwerken, moeten de partners in veiligheid kunnen beschikken over voldoende kennis en expertise, zodat goed gehandeld kan worden onder wisselende maatschappelijke omstandigheden.

Een integrale aanpak van het veiligheidsbeleid is daarom noodzakelijk. Centraal staat het oplossen van de problemen waarmee mensen worden geconfronteerd. Voor veel van deze problemen richten zij zich in eerste instantie tot de decentrale overheid, zoals de gemeente. Juist op lokaal niveau wordt de veiligheid en het veiligheidsgevoel van de burger bepaald. De decentrale overheid moet dan ook meer ruimte en vrijheid krijgen om invulling te kunnen geven aan hun taak: het oplossen van maatschappelijke problemen voor hun burgers.

Voorop staat hierbij het voorkomen en bestrijden van onveiligheid en criminaliteit. Ook hier verdienen de decentrale besturen en organisaties, zoals de regiokorpsen van politie, het vertrouwen van het Rijk. Samenwerking moet de normale praktijk zijn. Het accent ligt daarbij op preventie.

Taken

Bij de uitvoering van het veiligheidsbeleid is een aantal taken specifiek[1] van belang:

- *Politietaken*
- *Brandweertaken*
- *Geneeskundige hulptaken bij ongevallen en rampen*

POLITIETAKEN

De politietaken worden uitgevoerd door – uiteraard – de Nederlandse politiekorpsen maar ook door de Koninklijke Marechaussee. Voor de Nederlandse politie zijn die taken nader geduid in artikel 2 van de politiewet. De politie heeft tot taak (in ondergeschiktheid aan het bevoegde gezag en in overeenstemming met de geldende rechtsregels) te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die dat behoeven. De daadwerkelijke handhaving van de rechtsorde, wordt meestal nader geduid als "opsporen en handhaven".

De Koninklijke Marechaussee heeft krachtens artikel 6 van de politiewet ondermeer taken opgedragen gekregen die samenhangen met het waken voor de veiligheid van de leden van het Koninklijk Huis, de uitvoering van de politietaak ten behoeve van Nederlandse en andere strijdkrachten, de uitvoering van de politietaak op ondermeer de luchthaven Schiphol, het verlenen van bijstand bij de bestrijding van grensoverschrijdende criminaliteit, grensbewaking en vreemdelingentoezicht.

BRANDWEERTAKEN

De brandweertaken worden uitgevoerd door (regionale) brandweerkorpsen onder verantwoordelijkheid van het bevoegd gezag. De brandweertaken zijn ondermeer het

[1] We beperken ons hier tot de belangrijkste taken. En dan ook nog op hoofdlijnen. "handhaving van de rechtsorde", bijvoorbeeld impliceert een groot aantal specifieke taken. Maar het voert te ver om al die taken in detail hier te benoemen.

voorkomen, beperken en bestrijden van brand, het beperken van brandgevaar, het voorkomen en beperken van ongevallen bij brand.

Daarnaast zijn de (regionale) brandweerkorpsen belast met de voorbereiding van de bestrijding van rampen en zware ongevallen in de gemeente en bevorderen zij in het bijzonder het houden van oefeningen en de totstandkoming van afspraken, die nodig zijn voor een doelmatige bestrijding van rampen en zware ongevallen.

GHOR-TAKEN

Geneeskundige hulpverlening bij ongevallen en rampen wordt uitgevoerd onder coördinatie van de GHOR organisatie. De taken van de GHOR behelzen onder meer het instellen en in stand houden van een centrale post voor het ambulancevervoer en het instellen en in stand houden van een organisatorisch samenwerkingsverband gericht op geneeskundige hulpverlening. De geneeskundige hulpverlening zelf bestaat uit een heel stelsel van (medisch/geneeskundige) zorgverleners.

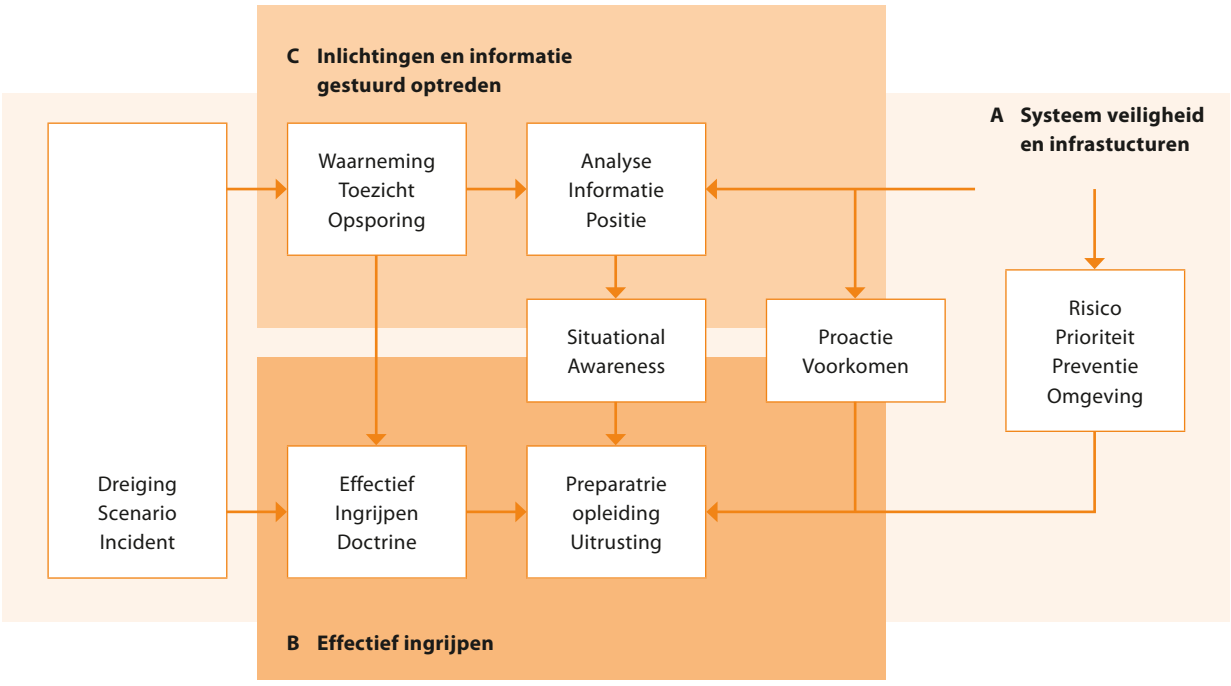
Behoeften

Binnen het brede veld van veiligheid zijn vele stakeholders en vanuit hun doelstellingen actuele behoeften. Een analyse van de behoeften van de uitvoerende overheidsorganisaties, lagere overheden en bedrijfsleven heeft geresulteerd in een driedeling:

- Systeembenadering veiligheid en infrastructuren; In dit deel wordt aandacht besteed aan dreigingen, scenario's en incidenten enerzijds en aan de risico's, prioriteitsstelling en preventieve omgevingsmaatregelen anderzijds.
- Effectief en veilig ingrijpen; Hierbinnen wordt aandacht besteed aan preparatie, opleiding, uitrusting en doctrine.
- Inlichtingen en informatie gestuurd optreden. In dit deel wordt aandacht besteed aan waarneming, toezicht en opsporing, de opbouw van een informatiepositie (en het faciliteren van situational awareness), pro-actief optreden en het voorkomen van incidenten.

SYSTEEMBENADERING VEILIGHEID EN INFRASTRUCTUREN

- Ontwikkelen van voorspellende modellen voor het genereren van een voorwaarschuwing voor mogelijke incidenten.
- Polarisatie en radicalisering lijken in Nederland in omvang, snelheid en intensiteit toe te nemen. Polarisatie en radicalisering kunnen de sociale samenhang en de onderlinge solidariteit in de samenleving bedreigen. Individuen en groepen zoeken de confrontatie met elkaar, keren zich af van de samenleving en kiezen mogelijk voor geweld. Het is noodzakelijk de achtergronden en oorzaken van polarisatie en radicalisering te kennen. Tevens is er behoefte aan kennis en middelen om de radicalisering op het internet en in radicale netwerken tegen te gaan.
- Versterking van de bescherming vitale infrastructuur. Voorkomen is beter dan genezen.



- Coördinatie tijdens crises, waarbij vele diensten zijn betrokken is cruciaal. Dit betreft zowel de afstemming met bestuurlijke partners, als de operationele afstemming tussen primair de hulpdiensten (brandweer, ambulance, politie en defensie).

EFFECTIEF EN VEILIG INGRIJPEN

- Verhogen van de fysieke veiligheid van specifieke locaties en voorzieningen inclusief de bescherming van gebouwen en personen tegen CBRN invloeden, explosies en wapengebruik.
- Verbetering van de opleiding en fysieke veiligheid van functionarissen, door het verbeteren van opleidings- en oefensituaties.
- Vergroten van het prestatievermogen (doeltreffendheid en doelmatigheid) van de verschillende hulpverleningsdiensten is een permanente behoefte.

INLICHTINGEN EN INFORMATIE GESTUURD OPTREDEN

- Beheersing van de openbare ruimte en vergroting van het toezicht, zowel "op straat" als "aan de grens" door zowel het gebruik van intelligente sensoren.
- Verbetering van de opsporing en delen van informatie, zowel tussen politie en inlichtingen organisaties enerzijds, maar ook in meer algemene zin tussen ketenpartners in de veiligheidsketen anderzijds.
- Inschakeling van de burger met als doel de informatie-uitwisseling te verbeteren en voorlichting te verbeteren, de burger actief te kunnen inzetten als "ogen en oren van de overheid" en de zelfredzaamheid van burgers bij incidenten te vergroten.
- Het is cruciaal dat de juiste persoon op het juiste moment op de juiste plaats over de juiste informatie beschikt. De veiligheidspartners dienen bij de uitvoering van hun veiligheidstaken hun informatie goed te kunnen uitwisselen door middel van een samenhangend geheel van basis voorzieningen.

Technologiegebieden BZK

Op basis van de beschreven behoeften kunnen voor BZK de volgende technologiegebieden worden geïdentificeerd:

- Geavanceerde materialen;
- Sensoren/sensorsystemen;
- Beeldverwerking;
- ICT;
- Biometrie;
- Simulatoren;
- Serious gaming.

Justitie

Trends

Voor het gehele beleidsveld van veiligheid, dus ook voor Justitie, geldt dat de maatschappelijke trends die reeds eerder zijn geïdentificeerd door het sociaal-cultureel planbureau (SCP), te weten: individualisering, informalisering, internationalisering en intensivering) van groot belang zullen zijn. Uit het beleidsprogramma van het huidige kabinet zijn verder de volgende trends te ontlenen:

REPRESSIE EN PREVENTIE

Er is de afgelopen jaren veel werk gemaakt van een stevige aanpak van de criminaliteit. Met name is veel geïnvesteerd in versterking van de politie, het Openbaar Ministerie en de rechtsprekende macht. Ook is het aantal cellen de afgelopen jaren fors uitgebreid. In toenemende mate is er nu aandacht voor het voorkómen van de criminaliteit. Door middel van preventieve maatregelen wordt voorkomen dat criminaliteit kans krijgt zich te ontwikkelen. Voorbeelden zijn de toepassing van cameratoezicht en de Keurmerken Veilig Wonen en Veilig Ondernemen. In het beleidsprogramma van het kabinet is deze ontwikkeling opgenomen in de vorm van het project Veiligheid begint bij Voorkomen. Hierbij is overigens een belangrijke rol weggelegd voor partijen als burger en bedrijfsleven.

KWANTITEIT EN KWALITEIT

Gelijktijdig is een ontwikkeling op gang gekomen die ziet op een toename van de kwaliteit van de aan Justitie gerelateerde organisaties. In het eerste Veiligheidsprogramma was met name een groot aantal maatregelen opgenomen die tot doelstelling hadden de kwantitatieve prestaties te verbeteren, zoals de afspraken met de politie en het Openbaar Ministerie over de extra instroom van verdachten. Met het Programma Versterking Opsporing en Vervolging is een ontwikkeling in gang gezet die juist de kwaliteit van onder meer de politie, het Openbaar Ministerie en het Nederlands Forensisch Instituut centraal stelt. Ook deze lijn naar kwaliteitsdenken is doorgezet in het beleidsprogramma van het huidige Kabinet. Zo staan de politieprioriteiten in het teken van het programmatisch werken, onder meer op terreinen als georganiseerde misdaad, cybercrime en financieel-econmomische criminaliteit. Deze prioriteiten zijn ook opgenomen in het Perspectief op 2010, het beleidsdocument van het Openbaar Ministerie.

ZICHTBARE EN MINDER ZICHTBARE VORMEN VAN CRIMINALITEIT

De derde trend bestaat uit een toenemende aandacht voor zogeheten minder zichtbare vormen van criminaliteit. Waar het Veiligheidsprogramma de nadruk legde op criminaliteit

en overlast in het publieke domein, staan in het beleidsprogramma van het huidige kabinet ook cybercrime, financieel-economische criminaliteit en georganiseerde misdaad op de agenda. De ontwrichtende werking die van deze ernstige vormen van criminaliteit uitgaat staat hierbij centraal.

Beleidskader
Ook het beleidskader voor Justitie wordt gevormd door het beleidsprogramma. Specifiek geldt dit voor de Vijfde Pijler (Veiligheid, Stabiliteit en Respect). Deze Pijler bevat de doelstelling te komen tot een reductie van de criminaliteit met 25% in 2010 ten opzichte van 2002 door:

- 19% minder geweldsdelicten
- 5% minder vermogensdelicten
- verbetering opheldering spercentage met 15%
- daling criminaliteit tegen ondernemingen met 25%
- daling recidive met 10%-punt.

De maatregelen en de projecten in het kader van het Innovatieprogramma Maatschappelijke Veiligheid leveren een bijdrage aan deze doelstellingen. Onderdeel van de Vijfde Pijler is het project Veiligheid begint bij Voorkomen. Ook in het project komen maatregelen bijeen die een bijdrage moeten leveren aan het doel de criminaliteit en de overlast substantieel te verminderen. Het project kent een integrale werkwijze, met acties van het lokaal bestuur én rijksoverheid, de burger en het bedrijfsleven.

Taken
Justitie heeft de taak de orde in onze samenleving te bevorderen zodat rechtvaardigheid, veiligheid en saamhorigheid voorop staan. Daaronder vallen de volgende terreinen:

WETGEVING
Om goed te kunnen functioneren, heeft een maatschappij duidelijke kaders nodig. Regels en wetten moeten zekerheid bieden over rechten en verplichtingen, tussen burgers onderling en tussen overheid en burger. Deze regels en wetten moeten bruikbaar zijn. Ze moeten bevorderen dat burgers zelf keuzes maken en hun verantwoordelijkheid dragen, zodat zij afzonderlijk en gezamenlijk een bijdrage kunnen leveren aan een vreedzame en welvarende samenleving.

CRIMINALITEITSPREVENTIE
Het ministerie van Justitie werkt aan een veiliger samenleving. Justitie is niet alléén verantwoordelijk voor de veiligheid. Het is belangrijk dat burgers, bedrijven en andere overheidsinstellingen zelf zoveel mogelijk maatregelen nemen om criminaliteit te voorkomen of te verminderen. Het ministerie stimuleert het nemen van zulke maatregelen door samenwerking te zoeken met allerlei instanties.

JEUGDBESCHERMING
Ieder kind moet zich op een gezonde en evenwichtige manier kunnen ontwikkelen tot een zelfstandige volwassene. Helaas groeit niet ieder kind op in een omgeving waarin dat vanzelfsprekend is. Soms worden kinderen ernstig beschadigd of dreigen zij dat te worden. Het ministerie van Justitie kan dan ingrijpen. In sommige situaties moet het zelfs. Dat is in de wet geregeld. Het kind staat daarbij op de eerste plaats. Dat geldt ook als een minderjarige een strafbaar feit heeft gepleegd. Justitie zal daar op reageren, maar wel zo dat de ontwikkeling van het kind wordt omgebogen in een goede richting.

RECHTSHANDHAVING
Een rechtvaardige en veiliger samenleving: daar steekt Justitie veel energie in. Bijvoorbeeld door het ontwerpen en uitvoeren van wetten. Maar de samenleving wordt alleen veiliger als burgers en bedrijven die wetten ook naleven. Ook de handhaving van wetten behoort tot de taken van Justitie.

RECHTSPLEGING EN RECHTSBIJSTAND
Onze samenleving wordt steeds ingewikkelder. Daardoor neemt de vraag naar recht en rechtspraak toe. De rechterlijke organisatie krijgt het steeds drukker. Toch moet er kwaliteit geleverd blijven worden. Daarom krijgt de verbetering van de bedrijfsvoering bij de rechterlijke organisatie veel aandacht. Want de rechtspraak in ons land is onafhankelijk en moet toegankelijk en slagvaardig blijven.

SLACHTOFFERZORG
Jaarlijks worden veel mensen slachtoffer van een strafbaar feit. Het kan soms lang duren voordat zij weer vertrouwen in de samenleving krijgen. Het is belangrijk dat zij goed worden geïnformeerd, opgevangen en, als ze daar behoefte aan hebben, begeleid. Hoe beter de opvang is, des te eerder mensen weer vertrouwen krijgen in de wereld om hen heen én in politie en Justitie. En hoe hun gevoel voor rechtvaardigheid, dat soms ernstig is aangetast, weer herstelt.

UITVOERING VAN STRAFFEN
Wie iets doet wat niet mag moet gestraft worden. Het ministerie van Justitie levert een bijdrage aan de veiligheid van de samenleving door bijvoorbeeld vrijheidsstraffen en vrijheidsbenemende maatregelen uit te voeren. Justitie zorgt ervoor dat dit rechtvaardig, consequent en effectief gebeurt.

VREEMDELINGENBELEID

Vreemdelingen komen om allerlei redenen naar Nederland. Bijvoorbeeld voor werk of studie. Sommigen komen als toerist, anderen voor gezinshereniging of om asiel te vragen. Veel vreemdelingen dienen een verzoek in om tot Nederland toegelaten te worden, om hier te blijven wonen of om Nederlander te worden (naturalisatie). Het ministerie van Justitie behandelt deze verzoeken.

INTERNATIONALE SAMENWERKING

Of het nu gaat om samenwerking tegen de misdaad, om opvang van vreemdelingen of om drugsbeleid: op vrijwel alle terreinen werkt het ministerie van Justitie internationaal samen. Problemen stoppen niet bij grenzen. Daarom worden die grenzen bij het zoeken naar oplossingen ook steeds minder belangrijk.

Behoeften

Bijdrage aan effectiviteit

Algemeen kan worden gesteld dat er behoefte bestaat om de effectiviteit van de werkzaamheden van Justitie verder te vergroten, en een bijdrage te leveren aan de hierboven weergegeven doelstellingen. Specifieke aandacht gaat hierbij uit naar de mogelijkheden van technologische toepassingen bij de preventie en de bestrijding van criminaliteit. Er wordt aangesloten bij de prioriteiten die zijn opgenomen in het beleidsprogramma.

In het beleidsprogramma worden meerdere terreinen expliciet benoemd waar het de mogelijkheden van technologie betreft:

- Versterking van het forensisch-technisch onderzoek.
  Het beleidsprogramma vermeld op dit punt: 'Er komen 500 'forensische assistenten' bij de politie, die vooral bij inbraken in woningen en bedrijven sporenonderzoek doen. Daardoor zullen meer daders worden gevonden, bijvoorbeeld wanneer zij DNA achterlieten op de plaats van het delict. Doelstelling is het ophelderingspercentage te verhogen met 15% in 2010'
- Monitoring ter voorkoming en bestrijding van criminaliteit.
  Uit het beleidsprogramma: 'De laatste jaren is het aantal fietsendiefstallen flink verminderd. Toch blijft het huidige niveau van zo'n 750.000 gestolen fietsen per jaar onaanvaardbaar hoog. Dit vraagt om extra preventieve maatregelen, zoals meer en veilige stallingmogelijkheden, benutting van het landelijke registratiesysteem van gestolen fietsen en technische beschermingsmethoden ('tags')'.
- Identificatie en observatie in de justitiële keten.
  Het beleidsprogramma: 'Een eenduidige vaststelling van de identiteit van personen in de justitiële keten is van groot belang. Belangrijke voorwaarde daarvoor is de echtheid en controleerbaarheid van de gegevens op documenten.'

Daarnaast zal ook de preventie en bestrijding van minder zichtbare vormen van criminaliteit als de georganiseerde misdaad, financieel economische criminaliteit en cybercrime voordeel kunnen hebben bij de toegenomen mogelijkheden van technologie. Deze prioriteiten bieden nader inzicht in de technologiegebieden die voor Justitie zouden voorzien in een behoefte.

TECHNOLOGIEGEBIEDEN

In meer algemene zin zijn drie technologiegebieden te onderscheiden die voor Justitie relevant zouden kunnen zijn: Nanotechnologie, Biotechnologie en Informatietechnologie. Met name de laatstgenoemde technologie kent reeds veel toepassingen. De verwachting hierbij is overigens dat juist een combinatie van de soorten technologieën (convergentie) in de toekomst een grote rol zal gaan spelen.

Deze ontwikkeling naar convergerende technologieën is op beperkte schaal reeds zichtbaar. Bij identiteitscontrole in de justitiële keten worden bijvoorbeeld meerdere technieken gebruikt zoals documentcontrole, dactyloscopie (vingerafdrukken) en foto's. Nieuw hieraan is dat deze technieken gecombineerd gebruikt worden en ook nieuw is dat de identiteiten "real-time" kunnen worden geverifieerd door het verbinden van de diverse registers bij politie en justitie. Bij de documentcontrole wordt gewerkt aan het verbeteren van de mogelijkheden om documenten te scannen en de elektronisch vastgelegde gegevens uit te lezen. Een belangrijke toevoeging volgt door documenten te controleren op echtheidskenmerken. Bij controle van een document wordt vastgesteld welke kenmerken het document heeft. Dit wordt getoetst aan de database met de image dna's. Op basis hiervan kan (met zekerheids en betrouwbaarheidspercentages) vastgesteld worden of een document 'echt' is.

Van deze ontwikkelingen mag worden verwacht dat de Nederlandse overheid en het bedrijfsleven hun internationale positie op het terrein van identiteitsmanagement kunnen versterken en uitbouwen en de integriteit van de informatie in overheidssystemen daardoor zal toenemen.

Sterktes, zwaktes, kansen en bedreigingen

Sterktes

De overheid is een grote speler en belangrijk als eerste klant
Voor een aantal taken heeft de centrale overheid een monopolistische positie in de vorm van politie, defensie en veiligheidsdiensten. Voor een ander deel heeft de regionale en lokale overheid een belangrijke rol, zoals bijv. de politie en brandweer. Hierdoor is de Nederlandse overheid vaak degene die de belangrijkste klant is voor een nieuw product of dienst. De overheid kan als 'launching customer' dus een belangrijke rol spelen bij het sneller ontwikkelen en toepassen van innovatieve oplossingen.

GEZAMENLIJKE VRAAGARTICULATIE BIJ PUBLIEKE GEBRUIKERS

Op het veiligheidsdomein zijn veel verschillende publieke en private gebruikers te onderscheiden. Traditioneel hebben de verschillende gebruikers diverse wensen ten aanzien van kennis en technologie. Door het initiatief Arena Maatschappelijke Veiligheid vindt een bundeling plaats van gebruikerswensen in het publieke domein (politie, brandweer, GHOR, marechaussee). De hieruit resulterende gezamenlijke gearticuleerde vraag zorgt voor een groter toepassingsgebied met meer vraagmassa. Het toepassingsgebied veiligheid wordt daardoor een aantrekkelijker focusgebied voor kennisinstellingen en bedrijven.

MEER AANDACHT VOOR KWALITEITSEISEN

Er is de laatste jaren groeiende aandacht voor het meten van en werken aan kwaliteit. Steeds meer gegevens worden bijgehouden en (openbaar) gerapporteerd. Elke sector werkt aan het ontwikkelen en toepassen van kwaliteitsindicatoren. Binnen de sector Veiligheid wordt gewerkt aan kwaliteitseisen zodat alle burgers in Nederland op een bepaald niveau van veiligheid kunnen rekenen.

NEDERLAND BESCHIKT OVER STERKE BOEGBEELDEN (MAINPORTS) ALS POTENTIËLE PROEFTUIN VOOR VEILIGHEIDSTOEPASSINGEN

Nederland is als dichtbevolkt land en belangrijke doorvoerhaven voor personen en goederen in Europa een ideaal testgebied voor innovaties op het veiligheidsdomein.
Het Nederlandse imago als 'Nederland transportland' met de bijbehorende mainports zoals luchthaven Schiphol en de haven van Rotterdam geven ons land hiervoor een sterke uitgangspositie.

Bedreigingen

VASTHOUDEN AAN VEROUDERDE KENNIS

Verouderde kennis blijft vaak te lang in gebruik, bijv. de brandweer en politie hechten sterk aan ingesleten manieren van werken. De keerzijde van de professionele houding is een vasthouden aan de traditionele autonomie. Professionals binnen de veiligheidssector worden vaak als eigenwijs gezien, niet geneigd om nieuwe dingen snel over te nemen ("not-invented here", eilandjes) en weerstand tegen standaardisatie.

KOSTEN EN BATEN VAN INNOVATIES BIJ VERSCHILLENDE STAKEHOLDERS

De kosten en opbrengsten van innovaties liggen vaak niet in één hand bij de eindgebruiker. Hierdoor is het soms moeilijk om partijen te overtuigen van de voordelen van samenwerking, omdat die elders neerslaan.

BEPERKTE DOORSTROOM VAN KENNIS NAAR TOEPASSING

Het onderzoeksgeld wordt verbrokkeld verdeeld over de kennisketen. Er is geen vloeiende doorgeleiding van resultaten van fundamenteel onderzoek naar toegepast onderzoek en implementatie. Dit is ook te wijten aan de hoge investeringsrisico's die gemoeid zijn met het ontwikkelen van nieuwe producten en beperkte mogelijkheden voor onderzoekers om deze risico's te nemen.

WET- EN REGELGEVING SLUIT NIET ALTIJD AAN OP TECHNOLOGISCHE ONTWIKKELINGEN

De juridische dimensie in de vorm van harmonisatie van de wet- en regelgeving is, zeker in het domein van internationale samenwerking, van cruciaal belang. Soms is wet- en regelgeving nog niet technologieneutraal en zijn nieuwe technologische oplossingen niet toegestaan. Ook kan het zijn dat wet- en regelgeving niet voorzien in nieuwe technologische ontwikkelingen. Een voorbeeld is dat de Lucht- en Verkeerswet nog niet voorzien in het gebruik van onbemande vliegtuigen voor bijvoorbeeld surveillance doeleinden. Testvluchten beperken zich op dit moment tot testvluchten boven militair domein. Ook ten aanzien van het al dan niet vastleggen van eisen aan toezichtruimte in het kader van cameratoezicht moet nog bepaald worden of daarvoor een wettelijke basis wenselijk is.

Daarnaast maakt de huidige wet- en regelgeving het voor de overheid lastig om het aanbestedingbeleid zodanig aan te passen dat innovatie (bij voorkeur door het Nederlandse bedrijfsleven) wordt bevorderd.

GEBREK AAN STANDAARDISATIE

Voor veiligheidsproducten zijn er nog weinig open standaarden. Voor commerciële producten en met name voor ICT gebaseerde diensten is het wenselijk dat er meer (open) standaarden komen voor interoperabiliteit en interconnectiviteit. Dat maakt het dan mogelijk dat software deelsystemen van verschillende leveranciers met elkaar gekoppeld worden en dat, in de toekomst, ook gewisseld kan worden van leverancier zonder dat (deel)systemen vervangen hoeven te worden. Ook voor leveranciers biedt dit mogelijkheden doordat nieuwe deelsystemen relatief eenvoudig te integreren zullen zijn in combinatie met andere, bestaande systemen.

Kansen

GESTANDAARDISEERDE ICT INFRASTRUCTUUR

De Informatie Basisvoorziening Veiligheid, een samenhangend geheel van generieke multidisciplinaire ICT voorzieningen voor gebruik door Politie, Brandweer, GHOR en andere veiligheidspartners, levert een gestandaardiseerde ICT Infrastructuur voor het Veiligheidsdomein.

MEER OOG VOOR INNOVATIE BIJ EINDGEBRUIKERS

Er komt meer sturing op output of zelfs outcome. Daardoor wordt de innovatie belangrijker en komt er meer ruimte voor vernieuwende concepten, bijvoorbeeld om bepaalde gezondheidsresultaten te bereiken.

Ook kostenbesparing is een argument voor innovatie en samenwerking aan innovatie. Innovatie kan via procesinnovaties en organisatorische vernieuwingen resulteren in een grotere efficiëntie.

MEER OOG VOOR INTEGRALE BENADERING

De slagkracht van de overheid zal door een integrale benadering, door de betrokkenheid van alle partners in veiligheid, worden vergroot. Een intensieve samenwerking tussen departementen is noodzakelijk. Denk aan de samenhang tussen projecten als Veiligheid begint bij Voorkomen, Kansen voor Kinderen en de initiatieven rond Krachtwijken. Ook de intensivering van de civiel militaire samenwerking (ICMS) gaat hieraan een bijdrage geven. Behalve van de lokale- en rijksoverheid wordt ook van individuele burgers, maatschappelijk middenveld en bedrijfsleven een bijdrage verwacht.

VERBETERING INRICHTING INLICHTINGENKETEN

Het belang van een juiste en adequate inrichting van de inlichtingenketen in de meest brede zin van het woord wordt onderkend. Het is cruciaal dat de juiste personen tijdig over de juiste informatie kunnen beschikken en op basis daarvan de juiste acties kunnen ondernemen. Hier komen onder meer de strafrechtelijke keten, de veiligheidsketen en de zorgketen in toenemende mate bij elkaar.

BELANG VAN FYSIEKE BESCHERMING EN OPLEIDING

De mens is in vrijwel alle processen een cruciale factor. Dat wil zeggen dat fysieke bescherming en opleiding sleutelbegrippen zijn voor een adequaat ingerichte veiligheidsorganisatie.

INTERNATIONALE DIMENSIE VAN VEILIGHEID

De maatschappelijke veiligheid van onze samenleving heeft zowel een interne (nationale) als externe (internationale) dimensie. Bij de borging van veiligheid in onze samenleving zijn deze twee dimensies weliswaar goed te onderscheiden maar op het niveau van beleidsvorming en taakuitvoering niet tot nauwelijks te scheiden. Borging van veiligheid houdt daarom in dat wij niet alleen invloed moeten kunnen uitoefenen op interne ontwikkelingen (zoals radicalisering), maar ook op externe ontwikkelingen (zoals internationale criminaliteit, terrorisme, migratiestromen en de handel in drugs, wapens en mensen). Vrijwel alle bedreigingen van onze samenleving hebben een internationale dimensie en de meeste gerelateerde vraagstukken waarmee Nederland wordt geconfronteerd kunnen niet worden opgelost zonder een internationaal georiënteerde aanpak. Door de internationale samenwerking kan ook meer op het gebied van kennis en technologie worden samengewerkt.

Bedreigingen

Het huidige personeelstekort dreigt sterk op te lopen door vergrijzing, ontgroening van het personeelsbestand en door de toenemende vraag om veiligheid. Daarbij heeft de sector veiligheid last van een imagoprobleem waardoor het lastig is nieuw personeel aan te trekken en bestaande werkers te behouden.

GEMEENSCHAPPELIJKE GEBIEDEN

In paragraaf 3.3 zijn voor achtereenvolgens Defensie, Binnenlandse zaken en Koninkrijksrelaties en Justitie voor het domein van maatschappelijke veiligheid de trends, taken en behoeften in kaart gebracht. In deze paragraaf zullen deze aspecten in een synthese bij elkaar worden gebracht om gemeenschappelijke gebieden te identificeren. Vanuit deze gebieden zullen vervolgens de gemeenschappelijke technologiegebieden worden geïdentificeerd.

Uit de analyses in paragraaf 3.3 komt een aantal aspecten duidelijk naar voren:
Ten eerste wordt onderkend dat de (maatschappelijke) veiligheid van onze samenleving zowel een interne (nationale) als externe (internationale) dimensie heeft. Bij de borging van veiligheid in onze samenleving zijn deze twee dimensies weliswaar goed te onderscheiden maar op het niveau van beleidsvorming en taakuitvoering niet tot nauwelijks te

scheiden. Borging van veiligheid houdt daarom in dat wij niet alleen invloed moeten kunnen uitoefenen op interne ontwikkelingen (zoals radicalisering) maar ook op externe ontwikkelingen (zoals internationale criminaliteit, terrorisme, onbeheersbare migratiestromen en de omvangrijke handel in drugs, wapens en mensen). Vrijwel alle bedreigingen van onze samenleving hebben een internationale dimensie en de meeste gerelateerde vraagstukken waarmee Nederland wordt geconfronteerd kunnen niet worden opgelost zonder een internationaal georiënteerde aanpak.

Ten tweede wordt onderkend dat op nationaal niveau een integrale benadering, door de betrokkenheid van alle partners in veiligheid, de slagkracht van de overheid zal vergroten. Een intensieve samenwerking tussen departementen is noodzakelijk. Denk aan de samenhang tussen projecten als Veiligheid begint bij Voorkomen, Kansen voor Kinderen en de initiatieven rond de Krachtwijken. Ook de intensivering van de civiel militaire samenwerking (ICMS) gaat hieraan een bijdrage geven. Behalve van de lokale- en rijksoverheid wordt ook van individuele burgers, maatschappelijk middenveld en bedrijfsleven een bijdrage verwacht.

Ten derde wordt het belang onderkend van een optreden in netwerken in de meest brede betekenis van het woord. Het is cruciaal dat de juiste personen tijdig over de juiste informatie kunnen beschikken en op basis daarvan de juiste acties kunnen ondernemen. Hier komen onder meer de strafrechtelijke keten, de veiligheidsketen en de zorgketen in toenemende mate dichter bij elkaar.

Ten vierde wordt onderkend dat de mens in vrijwel alle processen een cruciale factor is. Dat wil zeggen dat fysieke bescherming en opleiding sleutelbegrippen zijn voor een adequaat ingerichte veiligheidsorganisatie.

In de navolgende paragraaf zullen de hierboven genoemde gemeenschappelijke gebieden verder worden uitgewerkt.

1) Opereren in netwerken (NEC)

BESCHRIJVING

Het met meerdere partijen (kunnen) opereren in netwerken is één op één gerelateerd aan Network Enabled Capabilities (NEC). Met NEC wordt gedoeld op al die functionele mogelijkheden die samen een netwerk vormen waarmee snel, effectief en flexibel kan worden opgetreden. Onder netwerk worden onder andere sensor-, data-, informatie- en communicatienetwerken verstaan. De elementen van dit netwerk kunnen zich zowel te land, op zee als in de lucht bevinden, in het operatiegebied of op (grote) afstand daarvan.

Door informatie die is opgebouwd met behulp van gekoppelde sensorsystemen snel te verspreiden in het netwerk ontstaat een beter gedeeld beeld van de omgeving (shared situational awareness) en neemt de effectiviteit en snelheid van de besluitvorming toe. NEC kan door operationele netwerkcapaciteiten de communicatie en samenwerking tussen de militaire en civiele autoriteiten versterken.

INVULLING

Binnen de betrokken departementen wordt het opereren in netwerken op verschillende manieren opgepakt. Enkele voorbeelden zijn:

BZK: Bij crisismanagement is sprake van mono- en multidisciplinair optreden op verschillende niveaus en met een veelheid aan partijen. Een en ander is afhankelijk van de aard en omvang van het ongeval, het incident, de crisis of de ramp. Maar zelfs bij een relatief klein incident of ongeval is betrokkenheid van verschillende diensten en instanties een feit. NEC is van grote betekenis voor effectief optreden bij crisismanagement en operationeel optreden.

Defensie: Modern militair optreden vereist dat uiteenlopende wapensystemen, sensoren en commandovoeringsystemen te land, op zee en in de lucht zodanig met elkaar in verbinding staan dat snel, doeltreffend en met de nodige flexibiliteit kan worden opgetreden. Deze systemen en sensoren vormen gezamenlijk als het ware een netwerk, waarvoor in bondgenootschappelijk verband de aanduiding *Network Enabled Capabilities wordt gebruikt*. Doordat systemen en sensoren met elkaar in verbinding staan, kan een beter gemeenschappelijk beeld worden opgebouwd van de situatie in een operatiegebied. Ook kan zo bij een gewapend treffen de escalatiedominantie van onze militairen worden gewaarborgd, aangezien in een 'netwerk' snel een gecoördineerd beroep kan worden gedaan op extra middelen. Te denken is bijvoorbeeld aan de ondersteuning van gevechtsvliegtuigen of gevechtshelikopters van eenheden op de grond.
Het vermogen systemen en sensoren in een netwerk samen te brengen, komt zowel de effectiviteit van de missie als de veiligheid van de eigen eenheden ten goede. Complexe operaties zoals in Afghanistan vergen bovendien dat dit vermogen niet uitsluitend op hogere niveaus maar ook lager – dat wil zeggen bij kleinere eenheden en verbanden – aanwezig is. Investeringen in *Network Enabled Capabilities* bevorderen voorts het vermogen om samen met bondgenoten en partners op te treden.

Justitie: Een effectieve preventie en bestrijding van criminaliteit is alleen mogelijk bij een goede samenwerking en informatie-uitwisseling tussen betrokken partijen. Voor Justitie zijn met het opereren in netwerken daarom voordelen te behalen bij de preventie en bestrijding van jeugdcrimi-

naliteit en de aanpak van veelplegers (hierover vindt reeds overleg plaats in het veiligheidshuis en het casusoverleg), maar ook bij de preventie en de bestrijding van georganiseerde en financieel-economische criminaliteit en terrorisme (denk aan mogelijke voordelen van datamining en het koppelen van bestanden). Uiteraard dient hierbij rekening te worden gehouden met de mogelijkheden die de wet- en regelgeving biedt. Bij de identificatie in de strafrechtelijke en vreemdelingenketen is het van groot belang dat de ketenpartners over dezelfde informatie beschikken zodat een integer en integraal persoonsbeeld ontstaat. Ook hier kan dat optreden in netwerken een voordeel bieden.

TECHNOLOGIEGEBIEDEN

De bijbehorende technologiegebieden zijn:

- Sensoren / biometrie
- ICT
- Datamining en datafusie
- Geïntegreerd systeemontwerp en -ontwikkeling

2) Beschermen personen

BESCHRIJVING

Dit gebied beslaat in brede zin het gebied dat toeziet op de gezondheid, veiligheid en (fysieke) bescherming van het eigen personeel. Het thema wordt benoemd in het beleidsprogramma van het kabinet, dat inzet op de bescherming van hulpverleners in een publieke functie.

INVULLING

Voor alle drie de departementen is de bescherming van hulpverleners tegen fysieke dreiging een belangrijk thema. Enkele voorbeelden zijn:

BZK: Het uitvoeren van taken is voor brandweer, politie en geneeskundige hulp bij ongevallen en rampen niet zonder gevaar. Onze operationele mensen moeten zo goed mogelijk worden beschermd als zij (in extreme omstandigheden) hun werk moeten uitvoeren. Daarom is het belangrijk dat we daarbij vroegtijdig weten onder welke omstandigheden de taken moeten worden uitgevoerd, welk materiaal nodig is om die taken adequaat en veilig uit te voeren. Een brandweerman moet zo beschermd mogelijk brandende woningen kunnen binnentreden om slachtoffers te redden zonder zelf slachtoffer te worden. Politiemensen hebben ook bescherming nodig bij binnentreden van verdachte panden en bij het opereren in de publieke ruimte waar uiteenlopende gevaren schuilen voor lijf en leden. En hetzelfde geld voor overige operationele diensten. Kennis en monitoring van de situatie, adequate hulpmiddelen ter bestrijding van het gevaar en een uitrusting die daartegen optimaal beschermt, zijn belangrijk.

Defensie: De bescherming van uitgezonden personeel staat bij Defensie hoog op de agenda. Alleen goed beschermd personeel is in staat de missie te volbrengen. Ook uit het oogpunt van goed werkgeverschap voelt Defensie zich verplicht alles in het werk te stellen om de risico's te minimaliseren. De operationele ervaringen in vooral Afghanistan en Irak hebben duidelijk gemaakt dat hiervoor aanvullende maatregelen nodig zijn. Zo worden onze militairen vaker dan voorheen geconfronteerd met op afstand bediende explosieven, die in het militaire jargon *improvised explosive devices* (IED's) worden genoemd. Deze vormen een belangrijke bedreiging en vergen snelle tegenmaatregelen. Dergelijke maatregelen zijn niet alleen gericht op het vinden en het uitschakelen van de explosieven, maar ook op het uitschakelen van het achterliggende netwerk van de tegenstander. Er wordt een reeks maatregelen getroffen om onze eigen eenheden beter te beschermen.
Inmiddels is een IED-taakgroep (Taskforce "Countering IED") opgericht. De personele en materiële capaciteit om IED's te detecteren en te neutraliseren wordt uitgebreid. Operationele concepten worden aangepast en militaire kampementen worden versterkt. Het inlichtingenwerk en de opleiding en de training van militairen besteden aandacht aan de dreiging van aanslagen. Op wielvoertuigen wordt aanvullende bescherming aangebracht.

Justitie: In het beleidsprogramma van het kabinet is aangegeven dat de bescherming van werknemers in een publieke functie aandacht verdient. De 'frontlijnwerkers' van Justitie mogen rekenen op bescherming bij het uitvoeren van hun werkzaamheden. Innovatie en technologische ontwikkelingen kunnen hier een bijdrage aan leveren. Onder meer kan hierbij worden gedacht aan de bescherming van opsporingsambtenaren op straat door verbeteringen in de uitrusting en van medewerkers van de penitentiaire inrichtingen (onder meer van de Interne Bijstandsteams), parketten en rechtbanken door ontwikkeling en toepassing van verbeterde systemen rond toegangscontrole, identiteitsvaststelling en alarmering.

TECHNOLOGIEGEBIEDEN

- Sensoren
- Biometrie
- ICT
- Geavanceerde materialen

3) Opleiding en training

BESCHRIJVING

De kwaliteit van het personeel, zowel in de uitvoering als in de ondersteuning, is bepalend voor het welslagen van ieder optreden . Een goede selectie van personeel bij instroom en doorstroom en een goede opleiding en training dragen rechtstreeks bij tot de inzetbaarheid. Ook de bescherming van personeel tijdens operaties is sterk afhankelijk van strenge selectie, goede beheersing van vaardigheden en intensieve trainingen die de realiteit van de inzet zo dicht mogelijk benaderen . Het gebruik maken van simulatie en kunstmatige omgevingen bij het trainen van personeel wordt steeds belangrijker. Hierbij wordt steeds meer gebruik gemaakt van virtuele realiteit en "embedded" training.

INVULLING PER DEPARTEMENT

Voor alle drie de departementen is het opleiden en trainen van hulpverleners een belangrijk thema. Enkele voorbeelden zijn:

BZK: In veel gevallen komen crises en incidenten op het gebied van veiligheid niet veelvuldig voor. Maar het ongeval of de ramp plaatsvindt, moet de veiligheidsketen onmiddellijk goed functioneren. (Gelukkig) Slechts weinigen kunnen bogen op geoefendheid door ervaring in uiteenlopende soorten van ongevallen en rampen. Daarom is opleiden en blijven trainen voor uiteenlopende vormen van crises en incidenten door (levensechte) simulaties essentieel. Dit geldt voor de operationele diensten maar a fortiori voor de bestuurlijke structuur bij crises en rampen. Voor ministers en burgemeesters is leiding geven aan crisisbestrijding nu eenmaal geen dagelijkse bezigheid en hebben ze weinig tijd voor oefeningen. Een realistische virtuele oefening maakt het mogelijk om op ieder moment te oefenen en uiteenlopende scenario's te variëren.

Defensie: Veiligheid en bescherming worden niet alleen bepaald door het materieel, maar in sterke mate ook door de opleiding en training het van personeel. Goed opgeleid personeel is essentieel voor een effectieve krijgsmacht. Nieuwe vormen van oorlogsvoering, nieuwe logistieke concepten, nieuwe "operatietheaters" en nieuwe wapensystemen noodzaken tot training en testing in een gecontroleerde omgeving. Dat kan op de thuisbasis zijn maar in toenemende mate vindt training en simulatie ook plaats in het veld. Een voorbeeld hiervan is de nieuwe tactische *indoorsimulator* van het commando landstrijdkrachten.

Justitie: Ook voor justitie kan op dit punt gedacht worden aan verdere ontwikkeling en verbetering van E-learning en opleidingen. Verdere innovatie op dit gebied zou specifiek voordeel kunnen bieden voor de opleidingen op meer technologiegerelateerde terreinen van Justitie als de preventie en bestrijding van cybercrime. Simulatietrainingen kunnen onder meer een bijdrage leveren aan het optreden bij incidenten en aan het onderzoek rond de plaats delict (forensisch technisch onderzoek).

TECHNOLOGIEGEBIEDEN

- Simulatoren
- Serious gaming
- ICT

Subconclusies

De veiligheidssector presteert redelijk goed maar het kan beter. Op zowel de veiligheidsuitkomsten (bijv. criminaliteitscijfers, opheldering spercentages) als kwaliteit van de organisatie zijn verbeteringen mogelijk. De sector zal innovatiever moeten inspelen op de groeiende vraag om veiligheid en op handen zijde personeelstekorten.

Er zijn nog veel innovatie belemmerende regels, nog niet genoeg investeringsmogelijkheden en te weinig doorstroom van kennis naar toepassing. De uitwisseling van kennis tussen onderzoek en praktijk en tussen de verschillende sectoren is suboptimaal. Al wordt hier met de interdepartementale civiel militaire samenwerking en de arena maatschappelijke veiligheid, hard aan gewerkt.

Ondanks deze belemmeringen is er nog veel te winnen door innovatie. Veiligheid is zich meer en meer als een markt aan het ontwikkelen (als eerste klant en door gebruik te maken van mainports). Daarnaast zullen, door mogelijke personeelstekorten en toenemende risico's, nieuwe oplossingen gerealiseerd moeten worden.

De hoofduitdaging voor de Nederlandse Veiligheidssector voor de komende jaren is: hoe pakken we de groeiende vraag om veiligheid efficiënt en effectief aan, rekening houdend met een goede kwaliteit en toegankelijkheid?

Een vergelijking van de verschillende departementale behoeften leidt tot drie gemeenschappelijke thema's:

① *Opereren in netwerken;*
Het met meerdere partijen (kunnen) opereren in netwerken is één op één gerelateerd aan Network Enabled Capabilities (NEC). Met NEC wordt gedoeld op al die functionele mogelijkheden die samen een netwerk vormen waarmee snel, effectief en flexibel kan worden opgetreden. Onder netwerk worden onder andere sensor-, data-, informatie- en communicatienetwerken verstaan. De elementen van dit netwerk kunnen zich zowel te land, op zee als in de lucht bevinden, in het operatiegebied of op (grote) afstand daarvan.

Door informatie die is opgebouwd met behulp van gekoppelde sensorsystemen snel te verspreiden in het netwerk ontstaat een beter gedeeld beeld van de omgeving (shared situational awareness) en neemt de effectiviteit en snelheid van de besluitvorming toe. NEC kan door operationele netwerkcapaciteiten de communicatie en samenwerking tussen de militaire en civiele autoriteiten versterken.

② *Beschermen personen;*
Dit gebied beslaat in brede zin het gebied dat toeziet op de gezondheid, veiligheid en (fysieke) bescherming van het eigen personeel. Het thema wordt benoemd in het beleidsprogramma van het kabinet, dat inzet op de bescherming van hulpverleners in een publieke functie.

③ *Opleiding en training.*
De kwaliteit van het personeel, zowel in de uitvoering als in de ondersteuning, is bepalend voor het welslagen van ieder optreden . Een goede selectie van personeel bij instroom en doorstroom en een goede opleiding en training dragen rechtstreeks bij tot de inzetbaarheid. Ook de bescherming van personeel tijdens operaties is sterk afhankelijk van strenge selectie, goede beheersing van vaardigheden en intensieve trainingen die de realiteit van de inzet zo dicht mogelijk benaderen . Het gebruik maken van simulatie en kunstmatige omgevingen bij het trainen van personeel wordt steeds belangrijker. Hierbij wordt steeds meer gebruik gemaakt van virtuele realiteit en “embedded” training.

De verschillende technologiegebieden die ontwikkeld moeten worden om de gemeenschappelijk gedefinieerde thema’s te versterken, zijn: sensoren, ICT, Datamining en datafusie, geïntegreerd systeemontwerp en –ontwikkeling, biometrie, geavanceerde materialen, simulatoren en serious gaming.

Bijlage II: Swot-Analyse van het aanbod

ALGEMEEN

Waar is Nederland internationaal gezien sterk in op veiligheidsgebied? Welke clusters kunnen vanuit een toepassings- en een gebruikersperspectief onderscheiden worden? Op basis van gesprekken van met experts en vertegenwoordigers van stakeholders, en kwantitatieve analyses naar octrooiaanvragen, wetenschappelijke publicaties en de Nederlandse participatie in het Europese netwerken, wijst onze analyse op zeven sterke Nederlandse clusters. Dit zijn:

- Detectie, identificatie en authenticatie
- ICT-veiligheid
- Command & Control
- Fysieke bescherming van personen en goederen
- Situational awaremess
- Onbemande waarneming
- Simulatie, opleiding en training

In de volgende paragraaf lichten we deze zeven clusters uitgebreider toe. Hieronder gaan we eerst in op de criteria die we hebben gehanteerd bij het definiëren van deze clusters.

CRITERIA

De bovenstaande zeven sterke Nederlandse clusters zijn benoemd op basis van:

- Excellentie in de vorm van de positie in economisch opzicht, kennispositie en/of wetenschap-pelijke kwaliteit in internationaal perspectief.
- Samenhang en (internationale) samenwerking in de vorm van (potentieel) gemeenschappelijke basis voor de bedrijven en kennisinstellingen, samenwerking tussen bedrijven en kennisinstellingen en aansluiting op relevante internationale netwerken.

Door het kwalitatieve karakter van de analyse is het niet goed mogelijk een rangorde aan te geven voor deze clusters.

AANSLUITING OP ESRAB-CLUSTERS

Afhankelijk van de invalshoek zijn er heel veel verschillende clusters te benoemen. In de verschillende defensie studies is er sprake van meer dan veertig technologiegebieden. Het ESRAB-rapport hanteert elf clusters die qua abstractieniveau goed matchen met de sterke Nederlandse clusters. In het onderstaande figuur wordt aangegeven hoe de Nederlandse sterke clusters zich verhouden tot de ESRAB-clusters. Wat daarbij dan ook naar voren komt is dat Nederland niet op alle clusters sterk is. De zeven sterke Nederlandse clusters sluiten daarnaast aan op het NIID voorstel voor het innovatieprogramma Veiligheid. Hierbij worden vijf verschillende clusters onderscheiden: situational awareness, onbemande systemen, modern en veilig uitgerust personeel, opleiding, training en simulatie, en wetgeving en standaarden. Daarnaast sluiten de clusters tevens goed aan op de door TNO onderscheiden vijf belangrijke innovatiekansen voor het thema Veiligheid. TNO ziet de volgende innovatiekansen voor het Nederlandse bedrijfsleven: Detectie en identificatie van explosieve, chemische en biologische agentia, Intelligente sensornetwerken, Bescherming van personen en fysieke objecten, Ontwikkelen competenties van veiligheidspersoneel en -organisaties, en ICT-Security.

In de figuur komt tevens sterk naar voren dat Nederland niet in alle clusters sterk is. De clusters waar Nederland een

Tabel ESRAB-clusters en sterke Nederlandse clusters

ESRAB-clusters	Sterke Nederlandse clusters
Risk assessment, modelling and impact reduction	Simulatie, training en opleiding
Doctrine and operation	
Training and exercises	Simulatie, training en opleiding
Detection, identification and authentication	Detectie, identificatie en authenticatie
Positioning and localisation	
Situation awareness and assessment (surveillance)	Situational awareness
Information management	ICT veiligheid
Intervention and neutralisation	
Communication	
Command and control	Command en Control
Incident response	
	Fysieke bescherming van personen en goederen
	Onbemande waarneming

minder sterke positie inneemt, zijn: Doctrine and operation, Positioning and localisation, Intervention and neutralisation, Communication and incident response.

STERKE NEDERLANDSE VEILIGHEIDSCLUSTERS

De zeven sterke Nederlandse veiligheidsclusters worden hieronder aan de hand van de eerder genoemde criteria beschreven. Na een algemene omschrijving, waarin het cluster wordt afgebakend, wordt per cluster aangegeven welke raakvlakken met het met de andere clusters heeft. Vervolgens komen de belangrijkste technologieën aan bod. Aansluitend volgt een beschrijving van de excellentie van en de samenhang en samenwerking binnen het cluster. De clusterbeschrijving wordt afgesloten met het benoemen van de belangrijkste partijen. De clusters worden in willekeurige volgorde gepresenteerd, er is geen prioritering aangebracht.

Detectie, identificatie en authenticatie

Het cluster Detectie, identificatie en authenticatie vindt zijn toepassing in een nieuwe vorm van waarneming. Deze informatie is vervolgens input voor zowel command & control management in meldkamers als op het ondersteunen van operationeel personeel op locatie. Voor een deel betreft het ook de 'vervanging' van 'blauw op straat' door camera's. Het heeft betrekking op ontwikkelingen in de vorm van (intelligent) cameratoezicht waarbij beeldanalyse wordt toegepast, zowel decentraal in de camera als centraal in de meldkamer. Ook combinaties met andere detectoren en sensoren, inclusief toepassingen als biometrie (in essentie beeldanalyse, maar dan gericht op het herkennen van personen of persoonskenmerken) vallen onder dit cluster.

- **Andere clusters** die raakvlakken hebben met dit cluster zijn Command & Control met betrekking tot het interpreteren van de (beeld)informatie en het nemen van operationele beslissingen. Met Situational awareness zijn er raakvlakken op het gebied van het vertalen van informatie naar de operationele werksituatie van veiligheidsmedewerkers.
- **Technologisch** betreft het onderwerpen als optiek, sensoriek, ICT-systeemintegratie, beeldverwerking en circuitboards. Daarnaast behoren ook ontwikkelingen op het gebied van biometrie of through-the-wall radar tot dit cluster.
- De **excellentie** van dit cluster op het gebied van beeldverwerking komt ook naar voren in de octrooien, waarvoor Nederland een sterkere positie inneemt dan gemiddeld het geval is voor Nederland. Uit het literatuuronderzoek van het informatiecentrum van EZ blijkt dat acht Nederlandse universiteiten (RUG, UT, TU/e, TUD, UL, UM en UvT) deelnemen in onderzoeksgroepen die zich toeleggen op onderzoek verwant aan dit cluster. Ook TNO en het Centrum voor Wiskunde en Informatica participeren hierin. In de periode 2005-2007 zijn er 32 publicaties op dit clustergebied verschenen. Op **internationaal** vlak blijkt uit de analyse van PASR dat in 2005 TNO, de Technische Universiteit Derft en het Korps Landelijke Politiediensten participeerden in toegewezen projecten op dit gebied. In 2006 namen UC Technologies, TNO en het Ministerie van Financiën deel aan gehonoreerde PASR projecten. Uit de eerste Security-tender van het Zevende Kaderprogramma blijkt dat TNO, de Universiteit van Amsterdam, het Havenbedrijf Rotterdam en Uniresearch succesvol waren op dit gebied.
- Qua **samenhang en samenwerking** is er een sterke basis in de vorm van de partners in het IOP Beeldverwerking, het MultimediaN programma en het daaruit voorkomende initiatief 'Maatschappelijke Veiligheid in beeld'. In deze initiatieven participeren vrijwel alle universiteiten en kennisinstellingen op dit gebied. Ook een groot aantal bedrijven neemt hieraan deel.
- **Belangrijke partijen** zijn TNO, Thales, Bosch (voormalig Philips), de Vrije Universiteit, Universiteit Utrecht, DECIS-lab, NFI, NEDAP, Astron, maar ook kleinere partijen als Sentient, Observision, Sound Intelligence, Vicar Vision, VDG-security en VCS-observation, Bioclear en C-it. Innovatieve starters binnen dit cluster zijn onder andere I-optics, Virus Free Air (spin-off TU Delft), IQ Corporation Announces, C&N, C2V, OpenFortress Digital Signatures, Uniqkey Biometrics en Utellus (starters via Technopartner).

ICT veiligheid (veiligheid-van-ICT)

Het cluster ICT-veiligheid richt zich op de veiligheid van de ICT-infrastructuur en op de beveiliging van de informatie zelf. Het gaat hierbij niet om de inhoud van de informatie. Met betrekking tot communicatienetwerken als het internet gaat het om onderwerpen als SPAM, virussen, identificatie-fraude en en phising. Ten aanzien van informatiebeveiliging gaat het verder om onderwerpen als encryptie of virtual private netwerk ontwikkelen (VPN). De veiligheid-van-ICT is ook een aspect (en dat maakt ook het onderscheid) dat veel breder voor onze economie en maatschappij van belang is.

Belangrijk is het dan ook om voor dit cluster onderscheid te maken tussen:

- **Veiligheid-van-ICT** dat zicht richt op de veiligheid van ICT als communicatiemedium (zowel qua infrastructuur als qua informatiebeveiliging) waar dit cluster zich dus op richt; en
- **ICT-voor-veiligheid** waarbij het gaat om de **toepassing** van ICT in de vorm van beeldverwerking, intelligent cameratoezicht, ICT-integratie van sensoren, fly-by-wire, datamining, systeemintegratie etc.

ICT-veiligheid is heel herkenbaar in de vorm van cybercrime op internet. Door de Europese Commissie is over dit onderwerp eerder gepubliceerd. Hierin maakt de Commissie het onderscheid tussen drie soorten cybercrime: traditionele criminaliteit (maar nu via internet), criminaliteit met betrekking tot de inhoud, zoals kinderporno, en criminaliteit tegen het internet zelf, in de vorm van virussen, Worms etc. In het Europese stimuleringsprogramma 'Prevention of and fight against crime' krijgt de Europese samenwerking op het gebied van cybercrime nader vorm. Cybercrime is ook een onderwerp voor het Nederlandse overheidsbeleid. Dit betreft niet alleen de strafrechtelijke kant. Ook de bedreiging van de vitale infrastructuur, waarbij er sprake is van een grote mate van afhankelijkheid van internet en elektronische communicatie valt hieronder. De verantwoordelijkheid van de overheid is in 2006 onderwerp geweest van studie door de interdepartementale projectgroep 'Herijking ICT-veiligheidsbeleid'. De analyse van de projectgroep is in mei 2007 aan de Tweede Kamer aangeboden. Andere aspecten die van belang zijn voor het benoemen van dit cluster zijn:

- Dit cluster heeft raakvlakken met vrijwel alle **andere clusters**. Bij vrijwel alle andere clusters is er immers sprake van communicatie die kwetsbaar is. Alleen voor het cluster fysieke bescherming van personen is die link er in mindere mate. Echter, de link is ook niet geheel afwezig. In de vorm van een nieuw brandwerend pak voor veiligheidsdiensten is de ontwikkeling immers dat in het pak ook communicatiemiddelen geïntegreerd worden.
- **Technologisch** gaat het om ontwikkelingen op het gebied van informatie- en ICT-architectuur, meer wiskundige versleutelingstechnieken voor encryptie en programmeertechnieken (die programma's opleveren die minder gevoelig zijn voor virussen etc.).
- Qua **excellentie** is er met betrekking tot de octrooien een redelijke positie, maar die kan niet heel concreet worden vertaald naar dit cluster geziene de wat ongrijpbare definities van ICT en computertechnologie. Het literatuuronderzoek van het informatiecentrum van EZ wijst uit dat er 20 lopende onderzoeken zijn die gerelateerd zijn aan dit gebied. Hierbij zijn zeven universiteiten betrokken (RU, RUG, TU/e, TUD, UT, VU en de UvT). Ook TNO is actief op dit gebied. Het literatuuronderzoek wijst op één publicatie in 2007 van de TU/e en de UvT gerelateerd aan dit cluster. Uit de analyse van de PASR projecten blijkt dat op **internationaal** vlak de Radboud Universiteit in 2005 participeerde in een gehonoreerd project gerelateerd aan dit cluster. De uitkomst van de eerste tender op de thematische beleidsprioriteit Security binnen KP7 geeft aan dat Europol, NORTT Nederland en TNO participeren in met succes ingediende projecten.
- De basis voor dit cluster is de **samenwerking** binnen het Sentinelsprogramma en het daarop aansluitende initiatief 'Veilig Verbonden' waarin vrijwel alle universiteiten en kennisinstellingen op dit gebied participeren, samen met een groot aantal kleine en grote bedrijven.
- **Belangrijke partijen** zijn de universiteiten van Twente, Utrecht en Nijmegen, TNO CWI, Telematica Instituut, Philips, Capgemini en LogicaCMG. Qua kleinere bedrijven kan gedacht worden aan Fox-FT, Kahuna, Securecomm, Mermedia security technology. Innovatieve starters via Technopartner op dit gebied zijn: Borg Identity, com-Connect Security en SMS4sure.

Command & Control

Dit cluster richt zich op het operationele management bij toezicht en bij incidenten, rampen en crises. Het is een cluster dat ook in het kader van niet-criminele veiligheid van belang is. Incidenten, rampen en crisis kunnen immers ook het gevolg zijn van een ongeluk als het ontsporen van een trein, of een natuurramp in de vorm van overstromingen of wat kleinschaliger een incident als brand als het gevolg van kortsluiting of blikseminslag. Wat bij Command & Control een belangrijk aspect is, is de centrale aansturing vanuit één locatie waar alle relevante informatie samen komt. Ook een onderwerp als intelligent cameratoezicht behoort tot dit cluster met als meerwaarde dat het in meldkamers leidt tot informatiereductie.

Naast de technologische kant is de human factor van belang. Hoe kan informatie op een passende wijze worden aangeboden, hoe moeten meldkamers optimaal ingericht worden. Bij crises en rampen spelen aspecten als werkdruk en stress een rol. Deze aspecten kunnen tot gevolg hebben dat niet alle informatie ook daadwerkelijk aandacht krijgt of goed wordt geïnterpreteerd.

- De relatie met de **andere clusters** is dat detectie en identificatie van informatie en onbemande systemen input kunnen zijn voor command- en controlsystemen. Daarnaast kan er sprake zijn van informatie-uitwisseling met situational awareness. In de vorm van simulatie kan de operationale uitvoering van Command & Control worden geoefend en getraind.
- **Technologisch** heeft het betrekking op aspecten als systeemintegratie in de vorm van het combineren van informatie en gegevensbestanden, datamining, decision support en communicatie.
- De **excellentie** van dit cluster kan niet duidelijk uit het uitgevoerde onderzoek van Octrooicentrum Nederland worden afgeleid. Het literatuuronderzoek van EZ wijst op drie onderzoeksgroepen waarin de Universiteit Twente, de Technische Universiteit Delft, Universiteit Wageningen,

TNO en de KNAW participeren. Er zijn uit 2005 en 2006 drie publicaties bekend van de Technische Universiteit Delft, TNO en het COT. **Internationaal** gezien blijkt uit de analyse van de PASR projecten dat in 2005 het Korps Landelijke Politiediensten, het NLR, TNO en 42 Solutions BV participeerden in twee met succes ingediende projecten. In 2006 namen Europol en TNO deel aan gehonoreerde projecten op dit gebied. De eerste tender van KP7 op het gebied van Security wijst uit dat het SCP, Sogeti Nederland, TNO, het Instituut Sociale Studies en de Vrije Universiteit participeren in met succes ingediende projecten.

- Samenwerking vindt momenteel vooral plaats op projectbasis (zie bovenstaande alinea). Binnen de NIID is er een platform Command, Control and Technologie, waar bedrijven zich hebben verenigd. Daarnaast is het netwerk rond het IOP Mens-Machine Interactie relevant voor dit cluster.
- **Belangrijke partijen** zijn TNO en Thales. Ook systeemintegrators zoals Imtech en CapGemini zijn hier belangrijke partijen.

Fysieke bescherming van personen en goederen

De fysieke bescherming van personen en goederen heeft betrekking op het beschermen van personeel en materieel bij incidenten, aanslagen en ander geweld in bedreigende situaties. Het betreft toepassingen als kogel- en steekwerende vesten voor politie en militairen, brandwerende vesten, explosiebestendig straatmeubilair (prullenbakken), catering trolleys voor vliegtuigen, etc.

- Dit cluster is gerelateerd aan de **andere clusters** als het cluster wordt beschouwd als een bredere, geïntegreerde toepassing van de verschillende technologieën, in plaats van enkel gericht op de fysieke bescherming van personen en goederen. In het geval van de bredere benadering heeft het cluster raakvlakken met Detectie, identificatie en authenticatie, Command & Control en Situational awareness.
- **Technologisch** gaat het om geavanceerde materialen voor toepassingen als kogelvrije vesten en brandwerende pakken.
- De Nederlandse **excellentie** op het terrein van geavanceerde materialen is uitgebreid beschreven door SenterNovem in het kader van het nieuwe innovatieprogramma rond materialen. Qua octrooien doet Nederland goed mee op enkele specifieke materiaalgebieden (bijvoorbeeld vezels). Sterke spelers zijn DSM, Akzo Nobel, Teijin Twaron, Ten Cate, Corus en Stork. Aan drie technische universiteiten en TNO wordt internationaal erkend onderzoek verricht. Het literatuuronderzoek dat in 2005 en 2006 een viertal publicaties zijn verschenen van de Technische Universiteit Delft en TNO gerelateerd aan dit cluster. Internationaal gezien blijkt uit de bekeken PASR projecten dat Active Space Technologies in 2006 deel uitmaakte van een consortium dat met succes een project heeft ingediend binnen deze regeling. TNO is daarnaast succesvol gebleken bij het indienen van een projecten binnen KF7 op dit gebied.
- Op het gebied van geavanceerde materialen is de **samenwerking en samenhang** in Nederland goed, maar nog in ontwikkeling. Bedrijven en kennisinstellingen zijn al jarenlang verenigd in diverse IOP's en het TTI NIMR. Het nieuwe innovatieprogramma M2i op het gebied van materialen is breed van karakter en wordt ook breed gedragen. Veiligheid als toepassingsgebied is binnen dit M2i-initiatief echter maar minimaal aanwezig.
- **Belangrijke partijen** op het gebied van geavanceerde materialen zijn TNO, de drie technische universiteiten, de Erasmus en Wageningen universiteit, NIFV-Nibra, NDVIR, DSM, Ten Cate, Dijkstra, Corus, Havenbedrijf Rotterdam, NEDAP en Futura Composites. Kleinere partijen zijn onder andere: Detail Repair, Ecotax, Eefting Inbraakpreventie, HBD Total Security, Heras Mobile Fencing & Security, Infraspecials, Norm Safety Products, Prefire, Safeworks en Securitech. Innovatieve starters zijn Quintech en TANIQ (spin-off TU-Delft).

Situational awareness

Het toepassingscluster situational awareness is gericht op het operationeel ondersteunen van veiligheidspersoneel op straat en in het veld. Niet alleen als zij te voet zijn, maar ook in of rond voertuigen. Het betreft mobiele en draadloze toepassingen die informatie verstrekken om beter voorbereid te zijn op incidenten waar men mee geconfronteerd zal worden. Maar ook de terugkoppeling van informatie naar de meldkamer en/of commandopost in het kader van Command & Control is van belang. Ontwikkelingen hebben betrekking op toepassingen als PDA's. Hiermee kunnen op snelle en eenvoudige wijze gegevensbestanden geraadpleegd worden. In de vorm van de PDA's of beeldtelefoons kan verder visuele informatie over de plaats van delict, waar men naar op toe is, worden aangeboden (die bijvoorbeeld via camerasystemen beschikbaar is). Daarnaast zijn ontwikkelingen op het gebied van geografische informatie in de vorm van kaarten en precieze plaats-locatie-informatie verbonden met dit cluster.

- Situational awareness is gerelateerd aan de **andere clusters** Detectie, identificatie en authenticatie, Command & Control en Fysieke bescherming van personen en goederen.
- **Technologisch** betreft dit een breed scala aan ICT-gebaseerde ontwikkeling. Ook een ontwikkelingen als

First responder, soldier modernization program of Verbeterd operationeel Soldaatsysteem (VOSS) passen binnen dit cluster.

- **De excellente positie** van dit cluster op het gebied van beeldverwerking komt ook naar voren in de octrooien, waarvoor Nederland een heel sterke positie inneemt dan gemiddeld het geval is voor Nederland. Uit het literatuuronderzoek van EZ komt naar voren dat er elf lopende onderzoeken zijn die gericht zijn op dit gebied. Binnen deze onderzoeken participeren zes universiteiten (RU, TU/e, UT, TUD, UM en VU). Daarnaast nemen TNO en het Holst centre hieraan deel. Er zijn verder een viertal publicaties uit 2005 van de technische universiteiten uit Delft en Eindhoven en TNO bekend die aan dit cluster gerelateerd zijn. **Internationaal** gezien blijkt uit de PASR projecten dat TNO in 2006 betrokken was bij twee met succes ingediende projecten gerelateerd aan dit cluster. TNO was daarnaast ook succesvol in KP7.
- De **samenwerking** in dit cluster vindt onder meer plaats via de programma's VOSS en SMP van het ministerie van Defensie.
- **Belangrijke partijen** op dit gebied zijn TNO, TomTom, de technische universiteiten Delft, Eindhoven en Twente, het Telematica Instituut, de Universiteit van Amsterdam. Een innovatieve starter binnen dit cluster (via Technopartner) is Ambient Systems.

Onbemande waarneming

Het deelcluster onbemande waarneming richt zich op de behoefte om verkenningen uit te kunnen voeren van incident locaties zonder dat men dit wil doen met vliegtuigen of helikopters of het inzetten van menselijke verkenners. Het betreft toepassingen als onbemande vliegtuigen, maar ook van robotachtige voertuigen.

- Het cluster onbemande waarneming is gerelateerd aan de **andere clusters**: Detectie, identificatie en authenticatie en Command & Control.
- **Technologisch** gaat het uiteindelijk om de toepassing van sensoren en als zodanig sluit het direct aan bij het cluster detectie, identificatie en authenticatie. De specifieke Nederlandse expertise richt zich vooral op de complexiteit en innovatie voor het realiseren van kleine vliegtuigjes en robotisering.
- De **excellentie** van dit cluster op het gebied van sensoren komt naar voren in de octrooien, waarvoor Nederland redelijke positie inneemt, die wel iets achterblijft maar waar wel een duidelijke groei waarneembaar is. Philips is ook hier de belangrijkste Nederlandse aanvrager (derde wereldwijd). Naast Philips zijn ASML, TNO en de Nederlandse vestiging van Mitsibushi de belangrijkste aanvragers. Het literatuuronderzoek van het informatiecentrum van EZ wijst op drie lopende onderzoeken waarin de technische universiteiten Delft en Twente, TNO en de Vrije Universiteit deelnemen. Uit de periode 2005-2007 zijn er een zestal publicaties gerelateerd aan dit cluster van de Universiteit van Amsterdam, het Holstcentre, de Technische Universiteit Delft en TNO bekend. Binnen PASR zijn er geen projecten bekend met een Nederlandse deelnemer gerelateerd aan dit cluster. Uit de eerste tender van KP7 blijkt **internationaal** gezien dat het Havenbedrijf Rotterdam en Uniresearch deelnemen aan consortia die met succes projecten hebben ingediend.
- De basis voor dit onbemande waarneming vormt de **samenwerking** in het kader van Netherlands Industrial MALE UAV Platform (NIMUP) waarin een tiental bedrijven al een groot aantal jaren samenwerkt met betrekking tot het realiseren van onbemande vliegtuigen. Mede geïnitieerd door deze verkenning (is dit cluster doende zich te verbreden tot ook onbemande voertuigen.
- **Belangrijke partijen** zijn onder meer Thales, TNO, Stork en het NLR. Qua materiaaltechnologie zijn ook DSM en Technische Universiteit Delft (vliegtuigbouw) belangrijke partners. Innovatieve starters zijn Delft Dynamics, ISIS BV (spin-off TU Delft) en Airborn (viaTechnopartner).

Simulatie, opleiding en training

Met de komst van steeds geavanceerdere oplossingen en systemen is er een toenemende behoefte aan training en opleiding. Dit cluster heeft daarnaast betrekking op simulatie en serious gaming gericht op het virtueel oefenen voor incidenten, rampen en crises. Juist door het voorbereid zijn op terroristische aanslagen is het belangrijk dat er meer operationele ervaring komt voor het goed kunnen optreden als een dergelijke situatie zich voordoet. Voor deze situaties zijn vormen van simulatie interessant, omdat dat training en opleiding voor situaties die in de praktijk niet tot nauwelijks voorkomen.

In het kader van het interdepartementale actieprogramma 'Maatschappelijke sectoren & ICT' (M&ICT, zie ook hoofdstuk 3) is door Dialogic een onderzoek uitgevoerd naar serious gaming. Deze studie begint met een literatuurstudie en internationale ontwikkelingen op het gebied van serious gaming. De studie gaat in op een aantal cases op het gebied van veiligheid: virtuele brandweer training, internetr gebaseerde simulatie voor de Politieacademie en e-learning voor het op pijl houden van juridische kennis voor de politie.

Dit cluster is nauw verbonden met het **cluster** Command & Control..

- **Technologisch** gaat het vooral om een breed scala aan software toepassingen uit een lopend van training en e-learning toepassingen tot complexe simulatoren en games. Voor simulatie toepassingen gaat het ook om de fysieke, werktuigbouwkundige realisatie van simulatoren in de vorm van vliegtuigcockpits, stuurhuis van schepen, interieur van auto's.
- Met betrekking tot de **excellentie** is het beeld niet helemaal duidelijk. In het kader van ICIS en GATE lijkt er een goede basis voor de toekomst. Volgens Dialogic en Slot zijn VS, Canada, Japan en Engeland sterker, maar blijft Nederland zeker niet achter, vooral als het gaat om serious gaming. In Nederland zijn er twee onderzoeksgroepen (RUG en TUD) bekend die zich toeleggen op onderwerpen gerelateerd aan dit cluster. Verder wijst het literatuuronderzoek van het informatiecentrum van EZ in de periode 2005-2007 op drie publicaties (TUD, RUG, NLR, UM en COT)**. Internationaal** gezien blijkt dat TNO participeerde in 2006 in een PASR project gerelateerd aan dit cluster. Er zijn geen met succes ingediende projecten binnen KF7 bekend.
- Ten aanzien van **samenhang en samenwerking** is er een sterke kern in de vorm van het DECIS-lab. In dit samenwerkingverband participeren vrijwel alle universiteiten en kennisinstellingen op dit gebied alsook een groot aantal grote als kleine bedrijven. Dit DECIS-lab geeft ook invulling aan het ICIS-project. Daarnaast is het GATE initiatief op het gebied van serious gaming relevant. Binnen het NIID bestaat ook het Nederlands Industrial Simulator Platform (NISP) waarin een 15-tal bedrijven geclusterd zijn rond simulatortechnologie. Dit cluster is doende zich uit te breiden met bedrijven die erg veel ervaring hebben en expertise hebben met virtual reality.
- **Belangrijke partijen** zijn TNO, Thales, Imtech, Technische Universiteit Delft, Hogeschool Utrecht, Xsnes, AGS en Trigion.

Sterktes, zwaktes, kansen en bedreigingen

STERKTES

In Nederland zijn een zevental sterke clusters met relevantie voor het toepassingsgebied veiligheid. Dit zijn:

- Detectie, identificatie en authenticatie
- ICT-veiligheid
- Command and control
- Fysieke bescherming van personen en goederen
- Situational awareness
- Onbemande waarneming
- Simulatie, opleiding en training

Op deze gebieden is een goede kennisbasis met economische potentie aanwezig bij kennisinstellingen (universiteiten en TNO, GTI's) en bij bedrijven. De nadruk hierbij ligt op kennis, er is relatief weinig productie veiligheidstoepassingen in Nederland.

ZWAKTES

Onvoldoende kruisbestuiving m.b.t. kennis tussen vraag en aanbod

Er is veel kennisontwikkeling, maar veel kennis blijft op de plank liggen. Er is mogelijk nog onvoldoende inzicht in de ontwikkelde kennis en technologie bij eindgebruikers binnen de verschillende sectoren. Recente initiatieven zoals de Interdepartementale civiel militaire samenwerking (ICMS) en de arenavorming maatschappelijke veiligheid, laten zien dat er op dit gebied ontwikkelingen zijn ingezet die zich overigens nog in de praktijk moeten bewijzen.

Aan de aanbodzijde is de kennis bij onderzoekers en technologie over het veiligheidsdomein voor verbetering vatbaar.

Veiligheid is geen technologie- maar toepassinggebied

Veiligheid is geen technologie- maar toepassingsgebied. Er is daardoor sprake van andere technologieën die ook toegepast kan worden voor veiligheid. Bijvoorbeeld sensoren, beeldverwerking, materialen, ICT etc. kunnen breed worden toegepast voor zowel milieu, duurzaamheid, medische systemen als ook voor veiligheid. Dit brengt als zwakte met zich mee dat veel bedrijven zich niet in eerste instantie op het toepassingsgebied veiligheid richten. Bovendien ontbreekt het daardoor aan historische samenwerkingsclusters van bedrijven en kennisinstellingen. Sinds een paar jaar zijn er echter wel ontwikkelingen in deze richting.

Aanbodzijde kenmerkt zich door weinig grote bedrijven en veel nichespelers
Het toepassingsgebied veiligheid kenmerkt zich aan de aanbodzijde door de aanwezigheid van slechts een paar grote bedrijven en een hele groep kleine bedrijven, veelal nichespelers. Als nadeel brengt dit met zich mee dat kleine bedrijven veelal weinig specifieke R&D capaciteit kunnen vrijmaken. De kleinere bedrijven zijn daarentegen wel flexibeler om in te spelen op nieuwe ontwikkelingen en kunnen daardoor innovatiever zijn.

KANSEN

Toepassingsgebied veiligheid is kansrijk voor Defensie Technologische en Industriële basis
Nederland heeft een Defensie en Technologische en Industriële Basis, die R&D intensief is en over economische potenties beschikt. Nationale veiligheid biedt als toepassingsgebied de grootste kansen voor civiele toepassingen van defensietechnologie. Er kan zelfs gezegd worden dat er vanuit het oogpunt van innovatie een integratie tussen defensie en nationale veiligheid gaande is. Vooral de defensietechnologieën rond de innovatiethema's "E-learning", "Intelligente logistiek", "High Performance/Special Purpose"-marineschepen, "Levensduurmanagement" en "Onbemande voertuigen" kunnen met relatief weinig aanpassingen naar het civiele domein worden vertaald. Hierbij bieden vooral de eerste drie goede kansen door de aansluiting bij de sterkten van de Nederlandse DGI. "Militaire informatie-expertsystemen", "Soldaat modernisering" en "Shared situational awareness" bieden eveneens kansen, maar vragen een relatief grote inspanning om ze te benutten;

Veel innovatieve starters
Bij de inventarisatie naar de sterke clusters in het veiligheidsdomein valt het aantal innovatieve starters in de verschillende clusters op. Alleen al in het cluster Detectie, identificatie en authenticatie, zijn de volgende innovatieve starters geïdentificeerd: I-optics, Virus Free Air (spin-off TU Delft), IQ Corporation Announces, C&N, C2V, OpenFortress Digital Signatures, Uniqkey Biometrics en Utellus. Door een groot aantal innovatieve starters, lijkt er tevens voor de komende jaren groeipotentieel te zijn.

Internationale kansen
Er liggen kansen voor globalisering en internationalisering: kennisuitwisseling over de grenzen heen wordt gestimuleerd doordat onder andere de EU middelen beschikbaar heeft (bijvoorbeeld in KP7) voor samenwerking.

BEDREIGINGEN

Tekort aan bèta's en technisch personeel
Het algemene knelpunt van een tekort aan bèta's en technisch personeel geldt in het bijzonder voor veiligheidsbedrijven, omdat sommige bedrijven (die zich op de defensiemarkt richten) alleen personeel uit NAVO-landen mogen aannemen en dus internationaal gezien ook op een krappere arbeidsmarkt zitten. Aan de andere kant staat het onderwerp veiligheid sterk in de belangstelling en trekt het veel aandacht. Er zijn verschillende nieuwe opleidingen van start gegaan, onder andere op het terrein van Forensic Science aan de UvA.

Gebrek aan private financiering
Er is gebrek aan private financiering van onderzoek bijvoorbeeld vanuit het bedrijfsleven, door te lage financiële rendementsverwachtingen en langdurige trajecten.

SUBCONCLUSIES

Er zijn zeven clusters geïdentificeerd, die kansrijk zijn voor Nederland als het gaat om innovatie rond Veiligheid. De clusters zijn gekozen op basis van samenhang, samenwerking en internationale excellentie. Bij het identificeren en benoemen van deze clusters is zoveel mogelijk aangesloten bij de 'capabilities' die door ESRAB benoemd zijn. Uit de vergelijking komt eveneens naar voren dat Nederland op verschillende 'capabilities' een minder sterke positie inneemt (doctrine and operation, positioning and localisation, intervention and neutralisation, communication and incident response). De sterke clusters zijn:

Detectie, identificatie en authenticatie
Dit cluster vindt zijn toepassing vooral in een nieuwe vorm van waarneming. Deze informatie is vervolgens input voor zowel command & control management in meldkamers als het ondersteunen van operationeel personeel op lokatie. Voor een deel betreft het de 'vervanging' van 'blauw op straat' door camera's. Dit cluster heeft betrekking op ontwikkelingen in de vorm van (intelligent) cameratoezicht waarbij beeldanalyse wordt toegepast, zowel decentraal in de camera als centraal in de meldkamer.

ICT-veiligheid
Dit cluster richt zich zowel op de veiligheid van de ICT-infrastructuur als op de beveiliging van de informatie zelf. Het gaat hierbij niet om de inhoud van de informatie. Met betrekking tot communicatienetwerken als het internet gaat het om onderwerpen als SPAM en virussen maar ook om aspecten als identificatie-fraude en phising. Ten aanzien van informatiebeveiliging draait het verder om onderwerpen als encryptie of virtual private netwerk ontwikkelen (VPN).

Command & Control
Dit cluster richt zich op het operationele management bij toezicht en bij incidenten, rampen en crises. Een belangrijk aspect is de centrale aansturing vanuit één locatie waar alle relevante informatie samen komt. Naast de technologische kant is ook de menselijke factor van belang; hoe kan informatie op een passende wijze worden aangeboden, hoe moeten meldkamers optimaal worden ingericht. Verder spelen aspecten als werkdruk en stress spelen een rol, omdat zij tot gevolg kunnen hebben dat niet alle informatie ook daadwerkelijk aandacht krijgt en of goed wordt geïnterpreteerd.

Fysieke bescherming van personen en goederen
Dit cluster heeft betrekking op het beschermen van personeel en materieel bij incidenten, aanslagen en andere geweldadige of bedreigende situaties. Het betreft toepassingen als kogel- en steekwerende vesten voor politie en militairen, brandwerende vesten, explosiebestendig straatmeubilair (prullenbakken), catering trolleys voor vliegtuigen, containers etc.

Situational awareness
Dit cluster is gericht op het operationeel ondersteunen van veiligheidspersoneel op straat en in het veld. Niet alleen als zij te voet zijn, maar ook in of rond voertuigen. Het betreft mobiele en draadloze toepassingen die informatie verstrekken om beter voorbereid te zijn op incidenten waar men mee geconfronteerd zal worden. Maar ook de terugkoppeling van informatie naar de meldkamer en/of commandopost in het kader van Command & Control is van belang.

Onbemande waarneming
Dit cluster richt zich op de behoefte om verkenningen uit te kunnen voeren van incident locaties zonder dat men dit wil doen met vliegtuigen of helikopters of het inzetten van menselijke verkenners. Het betreft toepassingen als onbemande vliegtuigen, maar ook van robotachtige voertuigen.

Simulatie, opleiding en training
Met de komst van steeds geavanceerdere oplossingen en systemen is er een toenemende behoefte aan training en opleiding. Daarnaast heeft dit cluster betrekking op simulatie en serious gaming gericht op het virtueel oefenen voor incidenten, rampen en crises. Vanwege de wens om goed voorbereid te zijn op terroristische aanslagen is het belangrijk dat er meer operationele ervaring komt voor het goed kunnen optreden als een dergelijke situatie zich voordoet. Juist voor die situaties zijn vormen van simulatie interessant, omdat training en opleiding voor deze situaties in de praktijk niet tot nauwelijks voorkomen.

De veiligheidsmarkt kenmerkt zich door een aanbodzijde van slechts een paar grote bedrijven en veel kleine innovatieve starters. Daarbij biedt de veiligheidsmarkt kansen voor met name civiele toepassingen van defensietechnologie zowel nationaal als internationaal.

Het tekort aan bèta's en technisch personeel wordt binnen de veiligheidssector deels opgevangen doordat er verschillende nieuwe opleidingen van start zijn gegaan, onder andere op het terrein van Forensic Science aan de UVA. Zowel op het gebied van de kennisontwikkeling als op het gebied van de productontwikkeling is de veiligheidsmarkt een sterk opkomende markt.

Bijlage III: Match vraag en aanbod

GEMEENSCHAPPELIJKE MAATSCHAPPELIJKE THEMA'S

Een vergelijking van de verschillende departementale behoeften leidt tot drie gemeenschappelijke thema's:

1) Opereren in netwerken;
Het met meerdere partijen (kunnen) opereren in netwerken is één op één gerelateerd aan Network Enabled Capabilities (NEC). Met NEC wordt gedoeld op al die functionele mogelijkheden die samen een netwerk vormen waarmee snel, effectief en flexibel kan worden opgetreden.

Dit thema sluit aan op de onderstaande ontwikkelingen/ behoeften (zie hoofdstuk 3):
- Meer aandacht voor kwaliteitseisen;
- Gebrek aan standaardisatie (open standaarden) binnen het veiligheidsdomein;
- Gestandaardiseerde ICT-infrastructuur (de Informatie Basisvoorziening Veiligheid);
- Meer oog voor een integrale benadering door intensieve samenwerking tussen departementen;
- Het belang van verbeteren inrichting inlichtingenketen wordt onderkend;
- Versterking van het optreden in netwerken;
- Versterking van de inlichtingenketen;
- Er is grote behoefte aan inlichtingen- en informatiegestuurd optreden;
- Verschuiving van repressie naar preventie;
- Bijdrage aan effectiviteit.

2) Beschermen personen;
Dit gebied beslaat in brede zin het gebied dat toeziet op de gezondheid, veiligheid en (fysieke) bescherming van het eigen personeel. Het thema wordt benoemd in het beleidsprogramma van het kabinet, dat inzet op de bescherming van hulpverleners in een publieke functie.

Dit thema sluit aan op de onderstaande ontwikkelingen/ behoeften (zie hoofdstuk 3):
- Belang van fysieke bescherming en opleiding;
- Het huidige personeelstekort;
- Bescherming tegen terrorisme en georganiseerde misdaad;
- Bescherming van kritische/vitale infrastructuur;
- Verbetering van de bescherming van personeel op uitzending;
- De opkomst van internationale criminaliteit en terrorisme;
- De sterke toename van aantal, aard, aanleiding en uitwerking van zowel security als safety incidenten;
- Een sterke toename van complexe risico's door intensief ruimtegebruik en de integratie van woon-, werk-, transport- en recreatieactiviteiten;
- Effectief en veilig ingrijpen;
- Bijdrage aan effectiviteit.

3) Opleiding en training.
De kwaliteit van het personeel, zowel in de uitvoering als in de ondersteuning, is bepalend voor het welslagen van ieder optreden. Een goede selectie van personeel bij instroom en doorstroom en een goede opleiding en training dragen rechtstreeks bij tot de inzetbaarheid.

Dit thema sluit aan op de onderstaande ontwikkelingen/ behoeften (zie hoofdstuk 3):
- Belang van fysieke bescherming en opleiding;
- Meer aandacht voor kwaliteitseisen;
- Meer oog voor integrale benadering;
- Investeren in kwaliteit van personeel;
- Snelle technologische ontwikkelingen;
- Effectief en veilig ingrijpen;
- Bijdrage aan effectiviteit.

De verschillende technologiegebieden die ontwikkeld moeten worden om de gemeenschappelijk gedefinieerde thema's te versterken, zijn: sensoren, ICT, Datamining en datafusie, geïntegreerd systeemontwerp en –ontwikkeling, biometrie, geavanceerde materialen, simulatoren en serious gaming.

STERKE NEDERLANDSE CLUSTERS

Er zijn zeven clusters geïdentificeerd, die kansrijk zijn voor Nederland als het gaat om innovatie rond Veiligheid.
De clusters zijn gekozen op basis van samenhang, samenwerking en internationale excellentie. De sterke clusters zijn:

1) Detectie, identificatie en authenticatie
Dit cluster vindt zijn toepassing vooral in een nieuwe vorm van waarneming. Deze informatie is vervolgens input voor zowel command & control management in meldkamers als het ondersteunen van operationeel personeel op locatie.

2) ICT-veiligheid
Dit cluster richt zich zowel op de veiligheid van de ICT-infrastructuur als op de beveiliging van de informatie zelf. Het gaat hierbij niet om de inhoud van de informatie.

3) Command & Control
Dit cluster richt zich op het operationele management bij toezicht en bij incidenten, rampen en crises. Een belangrijk aspect is de centrale aansturing vanuit één locatie waar alle relevante informatie samen komt.

4) Fysieke bescherming van personen en goederen
Dit cluster heeft betrekking op het beschermen van personeel en materieel bij incidenten, aanslagen en andere gewelddadige of bedreigende situaties. Het betreft toepassingen als kogel- en steekwerende vesten voor politie en militairen, brandwerende vesten, explosiebestendig straatmeubilair (prullenbakken), catering trolleys voor vliegtuigen, containers etc.

5) Situational awareness
Dit cluster is gericht op het operationeel ondersteunen van veiligheidspersoneel op straat en in het veld. Het betreft mobiele en draadloze toepassingen die informatie verstrekken om beter voorbereid te zijn op incidenten waar men mee geconfronteerd zal worden.

6) Onbemande waarneming
Dit cluster richt zich op de behoefte om verkenningen uit te kunnen voeren van incident locaties zonder dat men dit wil doen met vliegtuigen of helikopters of het inzetten van menselijke verkenners.

7) Simulatie, opleiding en training
Met de komst van steeds geavanceerdere oplossingen en systemen is er een toenemende behoefte aan training en opleiding. Daarnaast heeft dit cluster betrekking op simulatie en serious gaming gericht op het virtueel oefenen voor incidenten, rampen en crises.

BENODIGDE TECHNOLOGIEGEBIEDEN BINNEN DE STERKE CLUSTERS

In de onderstaande tabel wordt aangegeven welke benodigde technologiegebieden binnen de sterke clusters kunnen worden opgepakt.

Bij het uitwerken van de drie gemeenschappelijke thema's, zullen de volgende technologiegebieden worden gestimuleerd: sensoren, ICT, geïntegreerd systeemontwerp, biometrie, geavanceerde materialen, geïntegreerd systeemontwikkeling, simulatoren en serious gaming.

VEILIGHEIDSMARKT IN ONTWIKKELING

De veiligheidssector presteert redelijk goed maar het kan beter. Op zowel de veiligheidsuitkomsten (bijv. criminaliteitscijfers, opsporingspercentages) als kwaliteit van de organisatie zijn verbeteringen mogelijk. De sector zal innovatiever moeten inspelen op de groeiende vraag om veiligheid en op handen zijde personeelstekorten.

Er zijn nog veel innovatie belemmerende regels, nog niet genoeg investeringsmogelijkheden en te weinig doorstroom van kennis naar toepassing. Innovatie wordt afgeremd in plaats van beloond. De uitwisseling van kennis tussen onderzoek en praktijk en tussen de verschillende sectoren is suboptimaal. Al wordt hier met de interdepartementale civiel militaire samenwerking en de arena maatschappelijke veiligheid, hard aan gewerkt.

Ondanks deze belemmeringen is er nog veel te winnen door innovatie. Veiligheid is zich meer en meer als een markt aan het ontwikkelen. Het (relatief) grote aantal innovatieve starters geeft aan dat zich hier steeds meer economische kansen (zowel nationaal als internationaal) voor het bedrijfsleven voordoen. Daarnaast zullen, door mogelijke personeelstekorten en toenemende risico's, nieuwe oplossingen gerealiseerd moeten worden.

	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5	Cluster 6	Cluster 7
Sensoren	X	-	-	X	X	X	-
ICT	X	X	X	X	X	X	X
Datamining	-	-	-	-	-	-	-
Datafusie	-	-	-	-	-	-	-
Geïntegreerd systeemontwerp	-	-	X	-	X	-	-
Geïntegreerd systeemontwikkeling	-	-	X	-	X	-	-
Biometrie	X	-	-	X	X	-	-
Geavanceerde materialen	-	-	-	X	-	-	-
Simulatoren	-	-	-	-	-	-	X
Serious gaming	-	-	-	-	-	-	X

AANBEVELINGEN

In deze paragraaf presenteren we een aantal aanbevelingen ten aanzien van het ontwikkelen van een (maatschappelijk) innovatieprogramma rond Veiligheid. Deze aanbevelingen volgen grotendeels uit de specifieke karakteristieken rond veiligheid (zoals beschreven in hoofdstuk 3 en 4) en uit de ervaring van SenterNovem met het opzetten en uitvoeren van innovatieprogramma's.

De aanbevelingen zijn:

- *Volg een integrale aanpak bij het benoemen en oplossen van knelpunten;*
  Een innovatieagenda is gekoppeld aan een visie en ambitie. De agenda beoogt die knelpunten op te lossen die het bereiken van deze ambitie in de weg staan. De ervaring met de innovatieprogramma's van het ministerie van Economische Zaken leert dat er veel verschillende typen knelpunten kunnen zijn die vragen om specifieke, per type knelpunt verschillende, aanpakken. Bij veiligheid spelen waarschijnlijk aspecten als gebrek aan standaardisatie, organisatorische en ethische factoren een rol. Het is aan te bevelen om bij het vaststellen van de innovatieagenda een integrale aanpak te volgen, waarbij alle relevante aspecten worden meegenomen.

- *Versterk de relatie tussen veiligheid en bestaande initiatieven en programma's;*
  Zoals al eerder gememoreerd: veiligheidstechnologie bestaat niet. Verschillende initiatieven en programma's zijn gericht op kennis en innovatie en hebben een potentiele link met het onderwerp Veiligheid. De overheid investeert al een aantal jaren flink in publiek-private technologie-ontwikkeling die uitstekend aansluit op de zeven sterke Nederlandse clusters. Om een aantal voorbeelden te noemen: Sentinels, Veilig Verbonden, de innovatieprogramma's Point One en M2i enz. Het verdient aanbeveling om de initiatieven en programma's die raakvlakken hebben met de zeven sterke Nederlandse clusters, te betrekken bij het ontwikkelen van de maatschappelijke innovatieagenda veiligheid.

- *Zorg voor coördinatie;*
  Het is belangrijk dat er een goede vraagarticulatie plaatsvindt met betrekking tot de maatschappelijke veiligheidsbehoefte, zodat aanbieders van kennis en oplossingen hierop kunnen inspelen. Een goede aanzet hiertoe is gegeven via de arena's Defensie en Maatschappelijke Veiligheid en via de Programmadirectie Kennis en Innovatie.
  Aan de andere kant betreft Veiligheid een breed toepassingsgebied waarop vele aanbieders actief zijn. Er vindt veel R&D en innovatie plaats op verschillende terreinen die voor Veiligheid relevant kunnen zijn. In deze verkenning is een eerste overzicht hiervan gemaakt. Het is strategisch belangrijk om dit overzicht actueel te houden en aan te vullen waar nodig.

- *Sluit aan op het zevende Kaderprogramma.*
  De Europese Commissie zet in het zevende Kaderprogramma strategisch in op Veiligheid. Veel van de onderwerpen die terugkomen zijn gerelateerd aan de innovatievraag van Defensie, BZK en Justitie en aan de zeven sterke Nederlandse clusters.

Bijlage IV: Criteria Maatschappelijke Innovatieagenda

Criteria Maatschappelijke Innovatieagenda

- De maatschappelijke innovatieagenda sluit aan op de probleemanalyses.
- De agenda gaat uit van interdepartementale samenhang en draagvlak. Dit resulteert in een samenhangende beleidsinzet op innovatie (dat wil zeggen logische samenhang met uitgaven uit de reguliere begroting en eventuele bijdragen uit andere enveloppen).
- Bij het opstellen van de agenda staat de bijdrage van kennis (onderzoek en onderwijs), innovatie en ondernemerschap aan de oplossing van maatschappelijke knelpunten centraal.
- Bij het vaststellen van ambities en doelstellingen is zowel de maatschappelijke als economische invalshoek relevant. Voor de economische invalshoek geldt dat wordt bijgedragen aan het stimuleren van innovatieve bedrijvigheid.
- De maatschappelijke innovatieagenda sluit aan bij technologieën en wetenschapsgebieden waarin Nederland sterk is of potentie heeft.
- De maatschappelijke innovatieagenda houdt rekening met regionale en internationale prioriteiten op het gebied van kennis, innovatie en ondernemerschap zodat de samenwerking met regionale en internationale partijen optimaal kan worden benut.
- Onderdeel van de agenda is de samenwerking tussen overheid, kennisinstellingen, maatschappelijke organisaties en bedrijfsleven (inclusief het MKB). Commitment van alle betrokken partijen is een essentiële voorwaarde voor de opzet van de agenda.

MEER INFORMATIE

Dit is een uitgave van de interdepartementale programmadirectie Kennis en Innovatie. Op de website www.kennis-innovatie.nl kunt u terecht voor meer informatie. Of u kunt bellen met 070 379 74 43.

NEDERLAND ONDERNEMEND INNOVATIELAND

Nederland Ondernemend Innovatieland verbindt het oplossen van maatschappelijke vraagstukken met het versterken van economische concurrentiekracht door het stimuleren van innovatie.
Nederland Ondernemend Innovatieland doet dit door te investeren in projecten die onderwijs, onderzoek en ondernemerschap stimuleren. Dit vraagt om een rijksbrede aanpak. En daarvoor is de programmadirectie Kennis en Innovatie in het leven geroepen, waarin vertegenwoordigers van verschillende ministeries samenwerken. Dit zijn op dit moment de ministeries van BZK, Defensie, EZ, Justitie, LNV, OCW, SZW, VROM, VWS en VenW.

Nederland Ondernemend Innovatieland