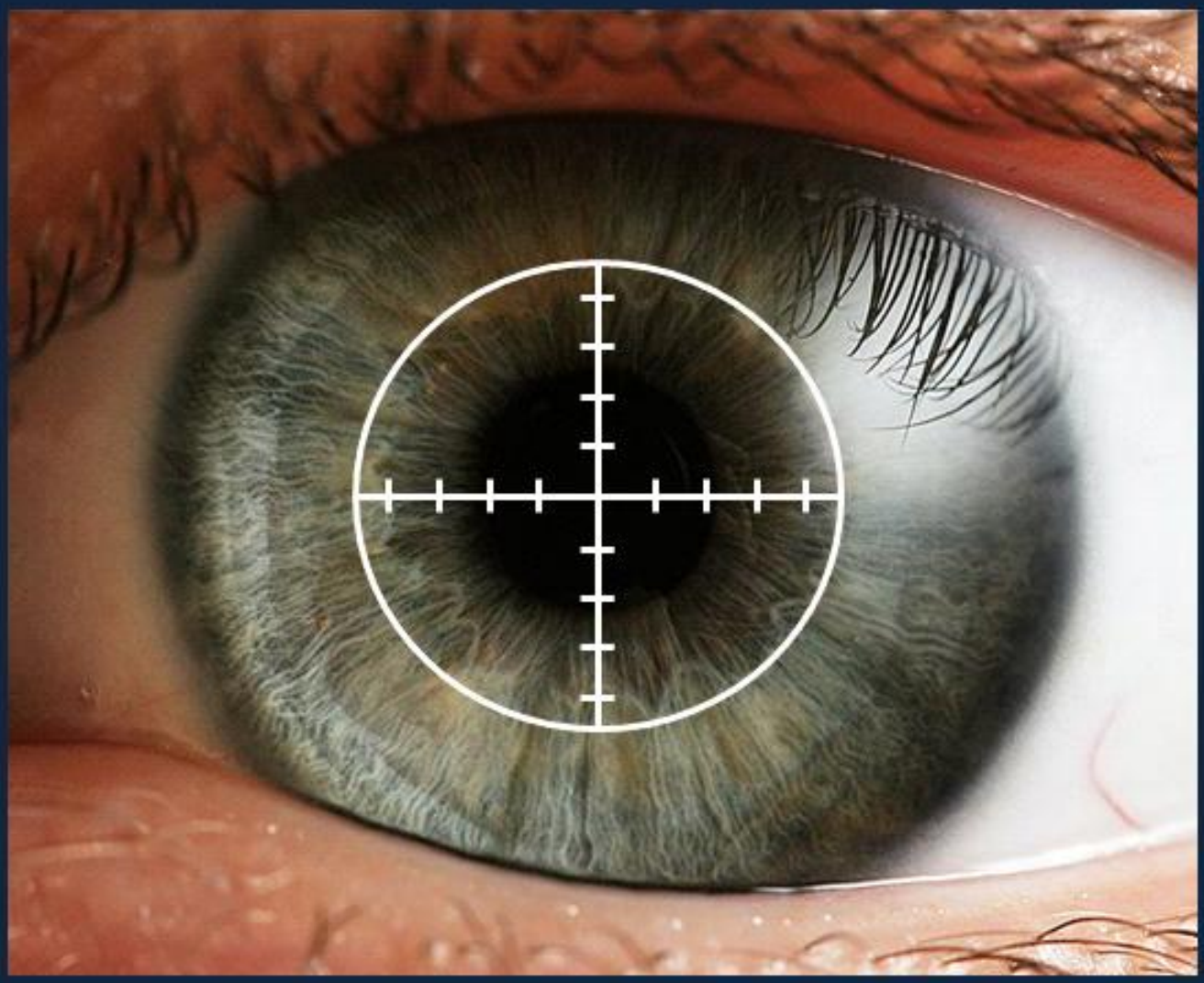
ROADMAP BEELDTECHNOLOGIE VEILIGHEIDSDOMEIN



In opdracht van
Politie Rotterdam-Rijnmond | Koninklijke Marechaussee | Nederlands Forensisch Instituut | Gemeente Utrecht | Voorziening Tot Samenwerking Politie Nederland | Nationaal Coördinator Terrorismebestrijding

Opgesteld door
DSP-groep

DSP - groep
Onderzoek – Advies – Management

Roadmap beeldtechnologie veiligheidsdomein

Behoeften en gewenste innovaties voor 'Veilig door innovatie'

Amsterdam, 20 december 2010

Sander Flight
Paul Hulshof

Met medewerking van:
Jolien Terpstra

Opgesteld voor contactgroep beeldtechnologie veiligheidsdomein
- Politie Rotterdam Rijnmond (voorzitter)
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (opdrachtgever)
- Ministerie van Justitie
- Koninklijke Marechaussee
- Voorziening Tot Samenwerking Politie Nederland
- Gemeente Utrecht
- Nederlands Forensisch Instituut
- Nationaal Coördinator Terrorismebestrijding

DSP – groep BV
Van Diemenstraat 374
1013 CR Amsterdam
T: +31 (0)20 625 75 37
F: +31 (0)20 627 47 59
E: dsp@dsp-groep.nl
W: www.dsp-groep.nl
KvK: 33176766 A'dam

Inhoud

Management samenvatting

Beelden spelen een steeds grotere rol in het veiligheidsdomein. Van kleine incidenten tot grote rampen zijn beelden beschikbaar en de instanties die in Nederland waken over onze veiligheid, zoals de politie, het Openbaar Ministerie en de douane krijgen dagelijks beeldmateriaal binnen. De beeldenstroom groeit snel, denk maar aan de beelden van de rellen bij Hoek van Holland of van de paniek bij de dodenherdenking op de Dam. De verwerking van al die beelden leidt tot problemen. Het ministerie van BZK heeft in het kader van het kabinetsprogramma 'Veilig door innovatie' DSP-groep opdracht gegeven een roadmap voor beeldtechnologie in het veiligheidsdomein op te stellen. De roadmap geeft aan waar we in 2020 willen staan en via welke mijlpalen in 2015 we daar kunnen komen. Tevens zijn enkele nieuwe aandachtspunten geformuleerd voor toekomstige innovaties.

Grenzen bereikt

Bij het verwerken van de 'tsunami aan beelden' lopen we aan tegen financiële, menselijke, organisatorische en juridische grenzen. Voor partijen in het veiligheidsdomein wordt het steeds moeilijker om relevante beelden te selecteren. Daar komt bij dat veel beelden gemaakt door derden (bewakingscamera's van particulieren, webcams of mobiele telefoons van burgers) niet passen in de eigen systemen. Er wordt daarom veel geïnvesteerd in onderzoek en innovaties op het vlak van beeldtechnologie: om de aansluiting op systemen van anderen te vergemakkelijken en om beter te worden in het selecteren van de relevante informatie in eigen en andermans beelden.

Vraag en aanbod

Voor dit soort onderzoek en innovatie is een budget beschikbaar in het kabinetsprogramma 'Veilig door innovatie'. Bij de beoordeling van de onderzoeksvoorstellen blijkt dat aanbod en vraag niet goed op elkaar aansluiten. Het blijkt moeilijk te bepalen welke voorstellen een kans verdienen en welke niet. Instanties binnen het veiligheidsdomein worden soms verleid om mee te doen aan experimenten, waarvan eigenlijk niet duidelijk is welk probleem ze precies zullen oplossen. Tegelijkertijd is het voor producenten van beeldtechnologie niet altijd duidelijk welke behoeften het veiligheidsdomein heeft.

Geen 'business as usual'

	Geen behoefte	Wel behoefte
Wordt niet ontwikkeld	Niet investeren	**Investeren**
Wordt al ontwikkeld	Stoppen	'Business as usual'

In elk geval zou er vanaf nu alleen nog moeten worden geïnvesteerd in innovaties en onderzoek waar a) behoefte aan bestaat en die b) niet vanzelf tot stand komen (business as usual). Niemand weet echter wat de behoeften van het totale veiligheidsdomein zijn. Deze roadmap maakt een behoefteninventarisatie onder meer dan veertig representanten van organisaties in het veiligheidsdomein. Een tweede punt is dat niemand weet welke innovaties en onderzoeken er al lopen. Dat is natuurlijk ook onmogelijk, maar het blijkt wel mogelijk de belangrijkste trends en ontwikkelingen te beschrijven. Ook dat gebeurt in deze roadmap. Door de behoeften vervol-

gens met de trends en ontwikkelingen te contrasteren, wordt duidelijk waar de komende jaren extra investeringen nodig zijn.

Drie trends
De tientallen experts die meewerkten aan deze roadmap onderscheiden twintig technische, organisatorische en maatschappelijke trends voor beeldtechnologie en veiligheid (hoofdstuk 2). Drie trends springen eruit:

1 *Meer beelden*
Per jaar groeit het aantal beelden met ongeveer 15%. Dat betekent dat de hoeveelheid beeldmateriaal in 2020 vier keer zo groot zal zijn als in 2010 en in 2030 zelfs tien keer zo groot. In het veiligheidsdomein is zelfs sprake van een jaarlijkse verdubbeling, aldus deskundigen. De rellen in Hoek van Holland leverden een stroom beelden op, vooral van mobiele telefoons, die veel groter was dan bij vergelijkbare incidenten enkele jaren eerder.

2 *Meer hits*
Door beelden te koppelen aan andere databases, zoals kentekens, paspoorten of mobiele telefoons, neemt het aantal *hits* exponentieel toe. *Hits* zijn brokjes informatie die interessant zijn voor instanties in het veiligheidsdomein. De enorme technische mogelijkheden leiden ertoe dat partijen overspoeld kunnen worden door informatie waar ze wat mee kunnen, willen en soms zelfs móeten doen.

3 *Veiligheidsdomein moet investeren*
De partners binnen het veiligheidsdomein willen kunnen werken met beelden van anderen. Omdat die anderen steeds meer en steeds betere apparatuur kopen, zullen de partijen in het veiligheidsdomein voortdurend moeten investeren in hardware, software en verbindingen om bij te blijven. Ook investeringen in deskundigheidsbevordering en organisatorische aanpassingen zijn continu nodig. Er hoeven geen wielen te worden uitgevonden, maar de wielen die door anderen worden uitgevonden moeten wel kunnen draaien.

Aandachtspunten voor onderzoek en innovatie
Alleen innovaties die voorzien in een behoefte *en* die niet vallen in de categorie 'business as usual' moeten worden gestimuleerd. Daar zijn selectiecriteria voor nodig. In de diverse subarena's worden al criteria gehanteerd die door de contactgroep worden onderschreven. In aanvulling daarop zijn enkele aandachtspunten geformuleerd. Onderzoeksvoorstellen die gaan over beeldtechnologie in het veiligheidsdomein komen eerder in aanmerking als ze expliciet ingaan op deze punten. Deze aandachtspunten staan in hoofdstuk 4. De aandachtspunten zijn bedoeld voor de indieners van onderzoeksvoorstellen én voor de beoordelaars.

Roadmap beeldtechnologie veiligheidsdomein

De roadmap zelf wordt hieronder gepresenteerd in de vorm van een strategisch doel voor 2020 en drie mijlpalen voor 2015. Onderzoek en innovaties die de komende jaren nodig zijn om mijlpalen en strategisch doel te halen, worden in het onderste deel van de roadmap benoemd.

2020 – Strategisch doel

Relevante beelden kunnen vinden
In 2020 kunnen partijen in het veiligheidsdomein onafhankelijk van de lokatie waar ze zich bevinden, en zowel *live* als achteraf, relevante beelden vinden in verschillende bronnen van beeldinformatie en deze op een voor de veiligheidsketen zinvolle wijze weergeven, bewerken, bewaren en analyseren.

2015 - Mijlpalen

Objecten en subjecten volgen
In 2015 kunnen partijen in het veiligheidsdomein objecten en subjecten (terug)vinden en volgen over verschillende bronnen van beeldinformatie.

Reconstructie incidenten
In 2015 kunnen partijen in het veiligheidsdomein op basis van beelden gebeurtenissen en incidenten reconstrueren, zodanig dat bruikbare informatie wordt geleverd aan de veiligheidsketen.

Metadata toevoegen
In 2015 worden beelden automatisch geannoteerd met metadata of ‘tags’ waardoor de bruikbaarheid en uitwisselbaarheid in de keten wordt vergroot.

2011 – 2015 Onderzoek & innovatie

Techniek
Objecten en subjecten volgen
Reconstructie achteraf
Relevante beelden filteren
Standaarden voor beeldmateriaal
Metadata standaard toevoegen
Beelden elders ontsluiten
Kwaliteit camera’s omhoog
Goedkoop/veilig beeldtransport
Authenticiteit garanderen

Organisatie
Deskundige observanten
Gebruikers koppelen aan producenten
Schaalbare systemen
Waarborgen persoonsgegevens, toezicht

Aanbevelingen

1. Meer uitwisseling en samenwerking
   Er blijkt bij veel partijen in het veiligheidsdomein, zowel bij afnemers van innovaties en de aanbieders, grote behoefte te bestaan aan samenwerking en uitwisseling van ervaringen over innovaties. Wat wordt elders al ontwikkeld? Wat levert dat op? Is het ook toepasbaar in andere sectoren?De deelnemers aan deze roadmap vonden de workshops nuttig en het was een eyeopener om te zien wat anderen in het veiligheidsdomein al doen. De prille samenwerking moet worden bestendigd: niet door weer een nieuwe groep op te richten, maar door actief aansluiting te zoeken vanuit de contactgroep bij bestaande groepen en overleggen. De contactgroep wil als een kring van ambassadeurs gaan werken: ze houden onderling contact en delen de informatie die ze krijgen met hun achterban. .

2. Vraaggestuurd
   Innovaties zouden moeten worden gestuurd door eindgebruikers en niet, zoals nu vaak gebeurt, door aanbieders. Gebruikers moeten worden betrokken bij alle innovaties en ze moeten zelf ook voorstellen kunnen indienen.

3. Eenvoudige procedures
   Subsidietrajecten kosten vaak veel tijd en papierwerk. Sommige interessante (markt)partijen haken om die reden af. Het is verstandig de aanvraag van subsidies en de verantwoording achteraf overzichtelijker, gemakkelijker en sneller te maken. Overigens geldt dit niet zozeer voor 'Veilig door innovatie' maar meer voor Europese subsidies zoals het Kaderprogramma 7[1].

4. Behoeften periodiek opnieuw inventariseren
   In een paar jaar kan veel veranderen. Daarom moeten de behoeften van het veiligheidsdomein periodiek worden geïnventariseerd. Dat maakt het mogelijk om te bepalen aan welke innovaties behoefte bestaat bij een groot aantal partijen in het veiligheidsdomein. .

Veilig door innovatie

Deze roadmap is tot stand gekomen onder de vlag van het kabinetsprogramma 'Veilig door innovatie' (2006). Onderzoek en innovatie op het gebied van maatschappelijke veiligheid worden hierdoor gestimuleerd. Het maakt deel uit van het overheidsprogramma met als doel Nederland kennis- en innovatieland nummer één van Europa te maken.

In het kader van 'Veilig door innovatie' kunnen partijen onderzoeksvoorstellen indienen voor onderzoek en innovaties. Dit gebeurt in subarena's op specifieke thema's, zoals terrorisme en radicalisering of veiligheid van netwerken. Veel van de ingediende kennisbehoeften en onderzoeksvoorstellen bleken over beeldtechnologie te gaan. Daarom is een contactgroep voor beeldtechnologie opgericht die opdracht gaf een roadmap specifiek voor beeldtechnologie op te stellen. Met deze roadmap hebben de subarenda's nu een richtsnoer voor de onderzoeks- en innovatieagenda van de komende jaren.

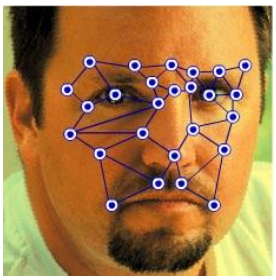
Noot 1 http://www.senternovem.nl/egl/

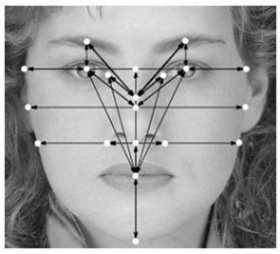
Uitgelicht: Video Content Analyse

Een mens kan maximaal een paar beeldschermen tegelijk bekijken, terwijl computers met behulp van Video Content Analyse veel beeldenstromen tegelijk kunnen 'bekijken'. Voor simpele taken werkt dit al goed: voor bewegingsdetectie en perimeterbeveiliging op parkeerterreinen en bedrijventerreinen bijvoorbeeld. Bij de meer geavanceerde toepassingen in gebieden met veel menselijk verkeer is het succes van video content analyse tot op heden veel kleiner. We gaan hier in op twee toepassingen: gezichtsherkenning en herkennen van afwijkend gedrag.

Gezichtsherkenning

De laatste decennia wordt al gewerkt aan automatische gezichtsherkenning op basis van camerabeelden. Er zijn diverse problemen met deze techniek. Ten eerste blijkt dat toepassing 'op straat' nauwelijks haalbaar is. Computers slagen er niet goed in gezichten uit een menigte te filteren voor analyse. Dat komt doordat mensen niet recht in de camera kijken, maar ook doordat gezichten worden afgeschermd door allerlei objecten of andere voorbijgangers. Een tweede probleem is dat het systeem alleen alarm kan slaan als er een 'hit' is. Dat vereist een bestand met recente (pas)foto's van alle personen die herkend moeten worden, zoals potentiële terroristen of criminelen. Dat soort bestanden bestaan niet of ze zijn onvolledig. Ten derde blijkt het bijna onmogelijk om beelden van verschillende camera's (bewakingscamera's, telefoons en foto's) onderling te vergelijken, waardoor er vaak geen match tot stand komt. De kans dat investeringen door de Nederlandse overheid deze problemen zullen oplossen is klein. Het lijkt daarom verstandiger te wachten op de resultaten van buitenlands onderzoek. Gezien de huidige stand van de techniek is het niet reëel te verwachten dat gezichtsherkenning in straatsituaties in 2015 zal werken en zelfs een horizon van 2020 is volgens veel deskundigen nog te optimistisch.





Herkennen afwijkend gedrag

Een andere vorm van Video Content Analyse is het automatisch herkennen van afwijkend gedrag. Ook op dit vlak zijn de resultaten beperkt. De regiopolitie Amsterdam-Amstelland concludeerde na het project *Smart Watch* in elk geval: 'Het automatisch herkennen van verdacht gedrag is buitengewoon moeilijk en op dit moment niet reëel'.[2]

Noot 2 B. van Diemen en L. van Mourik (2008), *Evaluatierapport project Smart Watch*, Politie Amsterdam-Amstelland.

Ten eerste is er enorm veel rekencapaciteit nodig voor het *real time* analyseren van gedrag. In een project met vijftig camera's die elk 25 beelden per seconde maken, moet een computer per seconde zo'n 600 megabyte aan data analyseren. Er zijn nauwelijks computers die daartoe in staat zijn. Ten tweede wordt menselijk gedrag vaak vereenvoudigd, bijvoorbeeld tot de routes die mensen afleggen. Afwijkende routes kunnen daarmee wel worden herkend, maar al het afwijkende gedrag dat geen verplaatsing is, zoals gejaagd om je heen kijken, een dreigende houding aannemen of zenuwachtig gedrag vertonen, valt daarmee buiten de analyses. Ten derde blijkt dat een groot aantal afwijkende gedragingen nooit automatisch te herkennen zal zijn omdat het gedrag pas wordt vertoond in reactie op iets anders. Volgens onderzoek van TNO voor de Nationaal Coördinator Terrorismebestrijding gaat het om de helft van alle verdachte gedragingen. Voor vijftig procent van het afwijkende gedrag *en* voor het beoordelen van door computers gedetecteerde hits, zal dus altijd menselijke interpretatie nodig blijven. Kortom: afwijkend gedrag zal voor een deel nooit worden automatisch worden herkend. Voor het deel dat wel herkenbaar is door computers, gaat de term 'business as usual' op: de Nederlandse overheid is niet de aangewezen partij is om hierin te investeren.

Investeer in mensen

Beide voorbeelden hierboven laten zien dat de mens achter de lens belangrijker is dan de computer. De grootste uitdaging op dit moment is ervoor te zorgen dat observanten niet alleen kijken naar beelden, maar vooral ook *zien* wat er gebeurt. Aan observanten in het veiligheidsdomein zullen steeds hogere eisen worden gesteld qua opleiding, competenties en bevoegdheden. Observanten zullen steeds vaker moeten werken met beeldinformatie van plekken die ze zelf nog niet kennen. Ook moeten ze de competenties en bevoegdheden hebben om politiemensen, hulpverleners, bewakers en beveiligers aan te sturen vanachter het beeldscherm. Dit betekent dat er in de komende jaren fors geïnvesteerd moet worden in de training en opleiding van observanten en de samenwerking tussen observanten en andere partijen in het veiligheidsdomein.

Uitgelicht: Opslagcapaciteit

De hoeveelheid beelden zal in 2020 vier keer zo groot zijn als in 2010. Veel instanties die zich met veiligheid bezighouden krijgen beelden binnen van anderen, dus vragen zij zich af of ze moeten investeren in opslagcapaciteit voor al die beelden. Die vraag kan hier niet beantwoord worden, omdat het geen innovatie, maar beheer betreft. Wel zijn er een aantal innovaties mogelijk die de benodigde opslagcapaciteit kunnen verkleinen. Daarom wordt dit onderwerp hier apart uitgelicht.

Opslagcapaciteit

In 2012 zal naar schatting van IMS Research 3.3 exabyte aan extra opslagruimte nodig zijn louter voor de nieuwe toepassingen van beeldtechnologie.[3] Dit soort hoeveelheden kunnen niet door afzonderlijke partijen in het veiligheidsdomein worden opgeslagen en beheerd. De trend is dan ook om dit soort data gespreid en dicht bij de bron op te slaan. Als partijen in het veiligheidsdomein beelden van anderen willen gebruiken, moeten ze die zoveel mogelijk bij de bron analyseren, selecteren en daarna pas transporteren. Dat heeft als voordeel dat meerdere geautoriseerde partijen gebruik kunnen maken van beelden, zonder dat elke partij die beelden zelf hoeft op te slaan. Gespreide opslag heeft overigens niet alleen kostenvoordelen, maar verkleint ook het risico op storingen en calamiteiten.

Dit model vergt een nieuwe manier van denken en werken. Er is behoefte aan onderzoek en innovatie om grote hoeveelheden beeldmateriaal van anderen slim te benaderen, te doorzoeken en – indien nodig – te gebruiken. De verwachting is dat zoekmachines steeds beter zullen worden in het doorzoeken van (streaming) video en het is dan ook niet nodig hier als Nederlandse overheid extra in te investeren via Veilig door innovatie. Toch zijn er twee innovaties die wél relevant zijn voor het veiligheidsdomein en die worden hier uitgelicht: metadata en standaarden.

Metadata

Het doorzoeken, opvragen en gebruiken van beeldmateriaal van derden wordt enorm versneld als er brokjes extra informatie in het beeldmateriaal zitten, zogenaamde metadata. Het gaat dan vooral om kenmerken als datum, tijdstip en locatie. Ook het toevoegen van echtheidskenmerken is zinvol: daaruit blijkt dat de beelden daadwerkelijk afkomstig zijn van een bepaalde partij en ook dat ze achteraf niet zijn gemanipuleerd. Dit soort informatie kan door de meeste moderne systemen al automatisch aan beelden worden toegevoegd, maar veel gebruikers kiezen er niet voor deze mogelijkheid aan te zetten. Voorlichting en actieve begeleiding van partners vanuit het veiligheidsdomein zou daar een positieve stimulans aan geven.

Noot 3 1 exabyte = 1 miljoen terabyte = 1 miljard gigabyte.

Standaarden

Zodra instanties uit het veiligheidsdomein proberen aan te haken op bestaande beeldsystemen van anderen gaat dit vaak mis. Het eerste probleem is dat de hardware en software die nodig zijn om de beelden te kunnen bekijken vaak niet beschikbaar zijn bij de partijen in het veiligheidsdomein. Veel politiemensen nemen bijvoorbeeld dvd's met beelden van bewakingscamera's mee naar huis, omdat ze op hun werkplek niet de software kunnen (laten) installeren die nodig is om de beelden te bekijken.

Er zijn twee mogelijke oplossingen voor dit probleem: zorgen dat het veiligheidsdomein alle beeldformaten kan inlezen of zorgen dat derden beelden maken die voldoen aan de standaarden binnen het veiligheidsdomein. Velen in het veiligheidsdomein geven de voorkeur aan de tweede optie, maar het afdwingen van een standaard blijkt al vrijwel onmogelijk binnen het veiligheidsdomein, laat staan daarbuiten.

Buiten het veiligheidsdomein is een standaard niet afdwingbaar, waardoor alleen op basis van vrijwilligheid aan kwaliteitseisen en standaardformats kan worden gewerkt. In de komende jaren zal er dus geïnvesteerd moeten worden in innovaties die koppelingen achteraf technisch mogelijk maken. Dit vereist niet alleen technische innovaties, maar ook organisatorische innovaties. Partijen die gebruik willen gaan maken van elkaars beelden moeten op basis van standaardautorisaties toegang kunnen krijgen en dit moet vooraf geregeld worden, niet achteraf. Ook moet er door voorlichting en samenwerking voor worden gezorgd dat camera's op de juiste plek worden opgehangen en optimaal worden ingesteld. Ook hier is nog veel winst te boeken door op innovatieve wijze de kennis en ervaring toegankelijk te maken voor partners in het veiligheidsdomein en actief aan deskundigheidsbevordering te werken.

Binnen het veiligheidsdomein valt ook winst te boeken door te investeren in de kwaliteit van beeldsensoren die door het veiligheidsdomein zelf worden aangeschaft. Zo zou bijvoorbeeld moeten worden gestimuleerd dat verouderde toezichtcamera's tijdig worden vervangen of weggehaald. Net als bij de partijen buiten het veiligheidsdomein geldt ook hier dat er veel winst te behalen valt door actief samen te werken in de fase waarin beeldsystemen worden aangeschaft en geïnstalleerd en niet achteraf.

1 Inleiding

In 2006 is het kabinetsprogramma 'Veilig door innovatie' van start gegaan: een nationaal stimuleringsprogramma voor innovatie op het vlak van maatschappelijke veiligheid. Het doel is het opbouwen van kennis, het stimuleren van innovatie en het ontwikkelen van producten, systemen en diensten die de veiligheid vergroten. Deze roadmap is opgesteld voor het overkoepelende thema beeldtechnologie in het veiligheidsdomein.

1.1 Programma ´Veilig door innovatie´

Nederland moet veilig zijn, veilig blijven en inwoners moeten zich veilig voelen. Continu dienen zich nieuwe veiligheidsvraagstukken aan door ontwikkelingen als globalisering, vergrijzing en nieuwe technologieën. Om voorbereid te zijn op de toekomst heeft het ministerie van Binnenlandse Zaken en Koninkrijksrelaties een nationaal onderzoeksprogramma 'Veilig door innovatie' opgezet. Dit programma heeft als doel:

- innovatieve oplossingen te ontwikkelen voor de aanpak van maatschappelijke veiligheidsproblemen (zoals bijv. het bestrijden van criminaliteit en het versterken van de crisisbeheersing)
- het presterend vermogen van de veiligheidsketen te vergroten (meer kunnen doen met hetzelfde aantal mensen)

In het onderzoeksprogramma wordt samengewerkt met de politie, brandweer, gemeenten, andere departementen, het bedrijfsleven en andere partners uit de veiligheidsketen (zie: www.veiligdoorinnovatie.nl).

Contactgroep beeldtechnologie
Binnen het programma 'Veilig door innovatie' kunnen partijen onderzoeksvoorstellen indienen in acht verschillende subarena's:

Terrorisme en radicalisering	Versterking opsporing en handhaving
Dreigings- en risicoherkenning en analyse	Geïntegreerde systemen
Veelvoorkomende criminaliteit en overlast	Uitrusting en materieel
Veiligheid van netwerksystemen	Opleiden en oefenen

In alle subarena's kwam beeldtechnologie veelvuldig aan bod: veel onderzoeks- en innovatievoorstellen gingen hierover. Ook blijkt dat veel innovaties en ontwikkelingen mono-disciplinair worden opgepakt, terwijl er vaak – met een aantal kleine aanpassingen – mogelijkheden zijn om meer multidisciplinair te werken. Op die manier kunnen meerdere partners in het veiligheidsdomein profiteren van innovaties. Daarom is een overkoepelende contactgroep beeldtechnologie ingesteld, voorgezeten door commissaris Hijmering, politie Rotterdam-Rijnmond. De contactgroep bestaat verder uit vertegenwoordigers van politie, justitie, NCTB, NFI en de marechaussee[4].

Noot 4 Zie bijlage 1.

De contactgroep is bedoeld om op het overkoepelende thema van beeldtechnologie in het veiligheidsdomein te zorgen voor afstemming van onderzoeksvoorstellen en uitwisseling van kennis en ervaring te stimuleren. De leden van de contactgroep kunnen worden beschouwd als ambassadeurs: zij delen informatie met elkaar en met hun achterban. Ook voor marktpartijen is het prettig als de 'vraag' naar innovaties in beeldtechnologie gezamenlijk wordt geformuleerd en onderling afgestemd.

De roadmap beeldtechnologie in het veiligheidsdomein die u nu leest is het eerste product dat onder verantwoordelijkheid van de contactgroep beeldtechnologie in het veiligheidsdomein verschijnt. Onafhankelijk onderzoeks- en adviesbureau DSP-groep heeft de opdracht gekregen de roadmap op te stellen. Bij de voorbereiding is overlegd met meer dan dertig vertegenwoordigers van diverse partijen in het veiligheidsdomein.

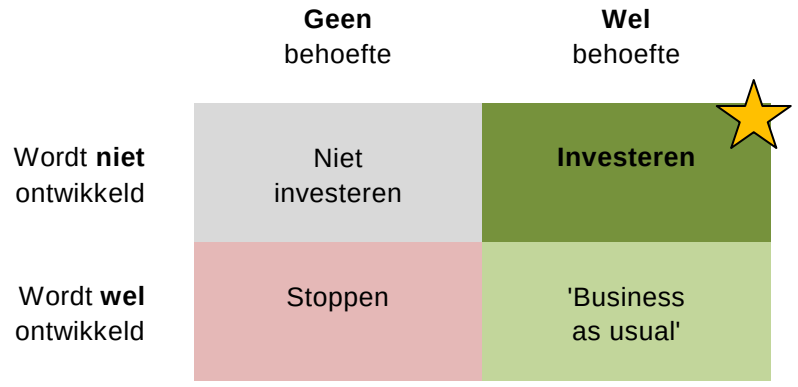
Tijdpad

December 2009	Startbijeenkomst contactgroep
Februari 2010	Eerste ronde workshops in drie groepen en interviews
Maart 2010	Terugkoppeling workshops in contactgroep
April 2010	Tweede ronde workshops drie groepen en interviews
Mei 2010	Terugkoppeling workshops in contactgroep
November 2010	Definitieve roadmap vastgesteld
December 2010	Publicatie roadmap

1.2 Behoeften en ontwikkelingen

Deze roadmap moet duidelijk maken aan welke innovaties op het gebied van beeldtechnologie in het veiligheidsdomein behoefte is. Om dat te kunnen bepalen is eerst een inventarisatie gemaakt van de huidige trends en ontwikkelingen in beeldtechnologie. Vervolgens zijn de behoeften van diverse partijen in het veiligheidsdomein in kaart gebracht. Door de ontwikkelingen in beeldtechnologie en de behoeften van het veiligheidsdomein vervolgens aan elkaar te koppelen, wordt duidelijk waar extra investeringen nodig zijn.

Figuur 1.1 Behoeften en ontwikkelingen



De roadmap moet ertoe leiden dat er vanuit 'Veilig door innovatie' alleen wordt geïnvesteerd in innovaties waar werkelijk behoefte aan bestaat én die niet tot stand zouden komen zonder stimulering vanuit de overheid. De drie andere categorieën zijn, om verschillende redenen, geen extra investeringen waard. Vooral de categorie 'business as usual' is interessant: dit zijn innovaties waar wel behoefte aan is, maar die nu al door (en vaak voor) anderen worden ontwikkeld. Het is niet de bedoeling dat het programma 'Veilig door innovatie' in dergelijke innovaties investeert, omdat ze er vanzelf wel zullen komen. Het moet gaan om innovaties die zonder overheidssteun niet gerealiseerd zouden worden.

De grenzen bepalen en bewaken
Niemand beschikt over een overzicht van alle innovaties waar momenteel aan wordt gewerkt. Hoe kan je dan bepalen of een onderzoeksvoorstel 'business as usual' is? Ook is het niet altijd duidelijk wat precies de behoeften zijn van het veiligheidsdomein. Hoe kan je dan bepalen of er wel behoefte aan een bepaalde innovatie is?

Deze roadmap voorziet in die behoefte. Voor het eerste punt, een overzicht van de *ontwikkelingen*, is een overzicht opgesteld van de relevante trends en ontwikkelingen in beeldtechnologie in het veiligheidsdomein (hoofdstuk 2). Daaruit blijkt welke zaken als 'business as usual' kunnen worden beschouwd en dus geen extra steun nodig hebben. Deze inventarisatie is echter niet onbeperkt houdbaar. Kennis, informatie en ervaringen moeten onderling worden gedeeld door alle partijen in het veiligheidsdomein. In deze roadmap staan aanbevelingen voor kennisuitwisseling.

Ook voor het tweede punt, een overzicht van de *behoeften* van het veiligheidsdomein, kunt u in deze roadmap terecht. In hoofdstuk 3 staan de technische en organisatorische behoeften van het veiligheidsdomein zoals die op dit moment zijn. Ook de behoeften ontwikkelen zich in de loop der tijd. Als deze roadmap in 2000 zou zijn opgesteld met als horizon 2010, zouden er inmiddels ook andere behoeften zijn geweest. In 2000 leefden Pim Fortuyn en Theo van Gogh nog en waren de terroristische aanslagen in New York, Madrid en Londen nog niet gepleegd. Die gebeurtenissen en hun consequenties hebben de behoeften van het veiligheidsdomein in relatief korte tijd flink veranderd. Vandaar ook de aanbeveling in deze roadmap om de inventarisatie van behoeften periodiek te herhalen.

1.3 Veiligheidsdomein moet behoeften bepalen, niet de aanbieders

Deze roadmap is bedoeld om richting te geven aan onderzoeks- en innovatietrajecten. Waar willen we over tien jaar staan en wat moeten we doen om daar te komen? Uit de workshops bleek dat partijen in het veiligheidsdomein zich soms laten verleiden tot technologische experimenten waarvan niet duidelijk is welk probleem ze oplossen.
Er is op zich natuurlijk niets mis met experimenteren. Maar het is wel de vraag welke experimenten de overheid zou moeten financieren. Zoals op het Innovatiecongres Veiligheid 2010 door een brandweercommandant werd opgemerkt: 'In het veiligheidsdomein komt innoveren vaker neer op slim jatten, dan op slim bedenken'. Dit kwam ook vaak terug in de workshops en discussies die wij voerden met partijen voor deze roadmap. Innovatie is geen doel op zich, maar een middel om een doel te bereiken. Pas als dat doel helder is, kan worden beoordeeld welke innovaties nodig zijn. Ook

wordt dan duidelijk of het gaat om het bedenken van nieuwe ideeën en producten of het slim overnemen en implementeren van ideeën en producten van anderen. In elk geval is duidelijk dat de partijen in het veiligheidsdomein die beeldtechnologie aanschaffen de behoeften moeten bepalen en niet de aanbieders. Overigens geven de leveranciers waar wij mee spraken aan dat ook zij prijs zouden stellen op een heldere behoeftenformulering vanuit de vraagzijde, zodat zij hun aanbod beter kunnen afstemmen op de vraag.

Privacy en wetgeving

Het was oorspronkelijk niet de bedoeling in deze roadmap een fundamentele discussie te voeren over wet- en regelgeving en privacy. Toch kwamen deze onderwerpen keer op keer aan bod in de workshops, interviews en gesprekken. Mensen op de werkvloer worstelen bijna dagelijks met vraagstukken rondom privacy en met de opslag, verwerking en uitwisseling van persoonsgegevens.

Er is grote behoefte aan heldere wet- en regelgeving. Deze roep om wettelijke kaders veronderstelt echter een helder beleidskader. Het moet eerst duidelijk zijn welk beleid (met welke instrumenten) is geformuleerd voor welk maatschappelijk probleem. Voorgestelde beleidsinstrumenten moeten worden beoordeeld op de bestaande wettelijke grondslag. Er is vervolgens behoefte aan jurisprudentie om te bezien of wijziging van regelgeving nodig is.

Veel technologie is zo nieuw dat er geen specifieke wet- en regelgeving voor bestaat. De eerste gemeentelijke camera werd al in 1997 opgehangen, terwijl de Gemeentewet deze vorm van cameratoezicht pas in 2006 van een wettelijk kader voorzag. Als je met innovaties moet wachten totdat er een wet is die aangeeft hoe ver je precies mag gaan, komt er nooit iets nieuws tot stand.

Om deze redenen zijn gedachten over maatschappelijk draagvlak, privacy en wet- en regelgeving prominent aanwezig in deze roadmap: bij de behoeften (hoofdstuk 3) en bij de aandachtspunten voor nieuwe onderzoeksvoorstellen (hoofdstuk 4).

1.4 Totstandkoming roadmap

Deze roadmap voor beeldtechnologie is, zoals gezegd, het resultaat van een intensief traject met meer dan dertig vertegenwoordigers van allerlei partijen in het veiligheidsdomein[5]. Daarnaast is de contactgroep beeldtechnologie bij aanvang, halverwege en na afronding geïnformeerd en geraadpleegd. De voortgang van het project werd teruggekoppeld en het traject werd in de gewenste richting bijgestuurd.

Er is een zeer brede vertegenwoordiging van professionals uit allerlei delen van het veiligheidsdomein bij deze roadmap betrokken. Het was onmogelijk *alle* partners in het veiligheidsdomein te betrekken, dus er moest een selectie worden gemaakt. De tien leden van de contactgroep hebben gespreks-

Noot 5 In de bijlage staat een overzicht van alle personen die hebben meegewerkt.

partners voorgesteld. Dit leidde tot een lijst namen van personen van diverse partijen in het veiligheidsdomein, inclusief leveranciers van beeldtechnologie. In overleg met de contactgroep is besloten 32 deelnemers te selecteren voor deelname aan de workshops, waarbij de voorkeur uitging naar één persoon per organisatie.

Deelnemende organisaties roadmap

Politiekorpsen
Haaglanden
Rotterdam-Rijnmond
Amsterdam-Amstelland
Midden- en West Brabant

Gemeenten
Almere
Gouda
Utrecht

OV en transport
Connexxion
Arriva
Nederlandse Spoorwegen
Schiphol Group

Landelijk
Voorziening tot samenwerking Politie Nederland
Nederlands Forensisch Instituut
Nationaal Coördinator Terrorismebestrijding
Koninklijke Marechaussee
Korps Landelijke Politiediensten
Ministerie van Justitie
Ministerie van BZK
TNO

Leveranciers
IBM
Siemens
Bosch
ADT
Axis

Daarnaast zijn tien aanvullende gesprekken gevoerd met deskundigen van diverse instanties (zie bijlage 2).

Met vertegenwoordigers van al deze organisaties zijn twee workshops gehouden: eerst zijn de behoeften geïnventariseerd (workshop 1) en vervolgens zijn de criteria voor het honoreren van onderzoeksvoorstellen opgesteld (workshop 2). Om de groepen niet te groot te maken is ervoor gekozen de workshops te verdelen in drie ´soorten´ gesprekspartners: leveranciers van beeldsystemen, producenten van eigen beelden en gebruikers van andermans beeldmateriaal. Daarnaast zijn individuele gesprekken gevoerd met tien vertegenwoordigers van partijen in het veiligheidsdomein. Ongetwijfeld zouden de resultaten iets anders zijn geweest als wij met nog meer anderen hadden gesproken. Toch denken wij dat deze roadmap een goed beeld geeft van de behoeften van de meeste partners in het veiligheidsdomein.

2 Ontwikkelingen in beeldtechnologie

In dit hoofdstuk worden twintig trends in de wereld van de beeldtechnologie beschreven. Beeldtechnologie heeft in de afgelopen vijftig jaar een enorme ontwikkeling doorgemaakt. Bijna iedereen met een camera en een personal computer kan nu filmpjes maken en deze eenvoudig opslaan, bewerken en met anderen delen, bijvoorbeeld via internet. De innovaties volgen elkaar in zo'n hoog tempo op, dat het moeilijk te voorspellen is waar we over tien jaar zullen staan.

'Prediction is very difficult, especially if it's about the future' (Niels Bohr)
'If I knew where jazz was going, I'd be there already' (Humprey Lyttleton)

Trends: geen mega of micro, wel meso
Het gaat in deze roadmap over beeldtechnologie en veiligheid. De trends die hier worden besproken gaan over beide onderwerpen tegelijk. Maar dan nog blijven er enorm veel trends over die relevant zijn dus een selectie was nodig. Er is gekozen voor trends op mesoniveau en niet op mega- of microniveau. Megatrends als individualisering, globalisering en vergrijzing die decennia bestrijken zult u hier dus niet aantreffen. Ook microtrends blijven hier buiten beschouwing: geen 3D-camera's, infraroodtechniek of laserverbindingen. De trends die wij hebben uitgekozen bevinden zich tussen deze twee uitersten: mesotrends.
Voor een overzicht van trends op macroniveau verwijzen wij de lezer naar andere publicaties, bijvoorbeeld de megatrends van Siemens: demografische veranderingen, urbanisatie, klimaatverandering en globalisering[6]. Een overzicht van microtrends bestaat, voorzover bij ons bekend, nog niet.

Een andere interessante referentie is de roadmap voor geïntegreerde systemen[7]. In die roadmap staat een 'kort overzicht van lopend onderzoek' met een beschrijving van ruim zeventig actuele programma's, systemen, architecturen en oefeningen. Deze variëren van grote projecten, zoals C2000 en Burgernet, tot kleinere projecten als Catchken en @migo. Ook worden er acht fieldlabs in beschreven. Die publicatie geeft een goed beeld van de enorme diversiteit aan lopende ontwikkelingen in het veiligheidsdomein.

Bronnen
De informatie in dit hoofdstuk is afkomstig uit een aantal bronnen: internationale trendwatchers, zoals Gartner en IMS Research, wetenschappelijke publicaties en gesprekken met sleutelfiguren in workshops en individuele interviews. Volledigheid is onmogelijk: het is een overzicht dat de komende jaren up-to-date moet worden gehouden (zie de aanbevelingen voor beheer van deze roadmap aan het eind van dit rapport).

Noot 6 Siemens megatrends: http://www.it-solutions.siemens.com/b2b/it/en/global/about-us/profile/megatrends/Pages/megatrends.aspx.
Nederlandse macrotrends op maatschappelijke veiligheid: http://www.minbzk.nl/aspx/download.aspx?file=/contents/pages/85099/1000.pdf.

Noot 7 *Roadmap subarena geïntegreerde systemen*, M&I Partners, Gemeente Utrecht, 2009. Deze roadmap is beschikbaar op http://www.subarena-gs.nl (registratie vereist).

2.1 Ontwikkelingen in techniek

Ontwikkelingen in techniek
Van analoog naar digitaal
Mega-pixel en datatransport
Closed circuit* wordt *open circuit
Mobiele toepassingen
Metadata
Slimme software
Externe opslag

Van analoog naar digitaal
De toekomst van beeldtechnologie is digitaal. Analoge camera's worden vervangen door digitale netwerkcamera's. In 2007 vormden netwerkcamera's al twintig procent van de totale verkoop en dit percentage steeg daarna elk jaar. Digitale camera's maken het makkelijker om beelden te transporteren, op te slaan en (met behulp van software) te analyseren. Camera's worden steeds kleiner. Hierdoor wordt het bijvoorbeeld mogelijk camera's te verwerken in de helmen van bikers van de politie. Sommigen voorspellen zelfs dat camera's in de komende jaren zo klein zullen worden, dat ze nog maar nauwelijks zichtbaar zijn.

Acht 'generaties' digitale camera's: links de oudere modellen, rechts de nieuwste

Mega-pixel en datatransport
Het aantal mega-pixel camera's stijgt, waardoor de beeldkwaliteit, en dus de bruikbaarheid van beelden voor opsporing en bewijsvoering, zal toenemen. Dit stelt weer extra eisen aan verbindingen: de bandbreedte die nodig is om beelden te transporteren moet groter worden. Dit zien we ook inderdaad gebeuren, vooral bij draadloze verbindingen.

Closed circuit wordt open circuit
De tijd dat elk apparaat zijn eigen draad had is voorbij. In plaats van een gesloten één-op-één verbinding tussen een beeldsensor en een centrale of opslagserver, wordt steeds vaker gekozen voor het versturen van beveiligde beeldinformatie over open, flexibele IP-systemen.

Mobiele toepassingen
Naarmate beeldsensoren kleiner worden en naarmate draadloze verbindingen beter worden, komen er steeds meer mobiele toepassingen van beeldtechnologie in het veiligheidsdomein. Zo worden er op dit moment bijvoorbeeld brandweerauto's, ambulances en politievoertuigen uitgerust met camera's. Ook krijgen bikers van politie een camera op hun helm[8]. In bussen, treinen, trams en metro's neemt het aantal camera's ook fors toe en die beelden worden ook vaak richting het veiligheidsdomein verstuurd. Hieraan gekoppeld is de groei in het aantal draadloze apparaten, zoals mobiele telefoons of PDA's, die beelden kunnen weergeven. Zo wordt het mogelijk beelden van een camera *real time* door te sturen, al dan niet via een toezichtcentrale, naar politie, brandweer of beveiliger 'op de grond'.

Metadata
Het wordt steeds eenvoudiger om extra informatie of metadata aan beelden te koppelen: tijdstip, lokatie (GPS) en dergelijke. Hierdoor kan eenvoudiger een koppeling worden gelegd tussen beelden uit verschillende systemen: je weet hoe laat de beelden zijn gemaakt en je weet waar ze zijn gemaakt. Daarnaast wordt het mogelijk beelden geografisch weer te geven op kaarten en plattegronden. Ook wordt het eenvoudiger om echtheidskenmerken toe te voegen aan de beelden, waardoor de authenticiteit beter kan worden vastgesteld[9].

Slimme software – Video Content Analyse
De behoefte om de interpretatie van beeldmateriaal te automatiseren blijft onverminderd groot, vooral omdat menselijk toezicht relatief kostbaar is. Mensen kunnen maximaal één beeld tegelijk interpreteren, computers kunnen er meerdere tegelijk 'bekijken' met kostenbesparing en tijdwinst als gevolg. Het ideaalbeeld van velen is dat alle ´schermen standaard op zwart´ staan en alleen aanspringen als er een aanleiding voor is.
In 2012 zal naar schatting veertig procent van alle netwerkcamera’s uitgerust zijn met een vorm van Video Content Analyse (VCA). Dit is software die de kwaliteit van beelden automatisch kan verbeteren of een bepaalde interpretatie aan de beelden kan geven. VCA gaat niet alleen om het interpreteren van beelden of het bieden van een handelingsperspectief; het is ook behulpzaam bij beeldverbetering (contrast, kleur), het vinden en volgen van objecten (nog voordat er een interpretatie aan wordt gegeven) en het combineren van verschillende beelden tot één geheel (*stitching*).
De meeste aandacht gaat op dit moment echter uit naar het automatiseren van de *interpretatie* van beelden en het bieden van een handelingsperspectief op basis van VCA, zonder dat er menselijk toezicht nodig is. In laboratoria worden onder gecontroleerde omstandigheden resultaten geboekt, maar zodra deze technieken worden toegepast in een werkelijke straatsituatie, vallen de resultaten vaak tegen. Toepassingen die nu al wel goed werken zijn de eenvoudiger toepassingen, zoals bewegingsdetectie of perimeterbeveiliging (een digitale 'trip-wire' die alarm slaat als een object een virtuele grens overschrijdt).

Noot 8 IMS Research voorspelt voor politievoertuigen een wereldwijde groei van 6,5 procent per jaar tot 2013: www.imsresearch.com.

Noot 9 Overigens blijkt dat veel systemen wel standaard ingebouwde mogelijkheden om locatiegegevens, tijdstippen of echtheidskenmerken aan beelden toe te voegen hebben, maar dat deze niet 'aan' staan.

Complexere zaken, zoals het herkennen van afwijkend gedrag, het volgen van subjecten over verschillende camera's of gezichtsherkenning, blijken erg moeilijk te automatiseren. Zelfs als we fors investeren in het automatisch herkennen van afwijkende gedragingen bijvoorbeeld, verwachten experts dat we over een paar jaar niet meer dan de helft van alle relevante afwijkende gedragingen automatisch kunnen detecteren. Dit bleek uit onderzoek door TNO in opdracht van de Nationaal Coördinator Terrorismebestrijding. Voor de overige vijftig procent *en* voor het beoordelen van de door computers gedetecteerde hits, zal altijd menselijke interpretatie nodig blijven.

Sommige experts waar wij mee spraken waren zeer kritisch over de gouden bergen die door sommige marktpartijen al jarenlang in het vooruitzicht worden gesteld. Sommigen betwijfelen nu zelfs of het buiten het laboratorium ooit zal lukken met slimme software afwijkende gedragingen te detecteren, laat staan te interpreteren. De regiopolitie Amsterdam-Amstelland concludeerde na het project *Smart Watch* in elk geval: 'Het automatisch herkennen van verdacht gedrag is buitengewoon moeilijk en op dit moment niet reëel'[10]. De consensus lijkt nu te zijn dat de menselijke interpretatie altijd nodig zal blijven in aanvulling op slimme software (zie 'de menselijke factor' in de volgende paragraaf).
Een probleem hierbij is dat er geen kwaliteitsstandaarden bestaan voor Video Content Analyse. Enkele deelnemers aan de workshops stelden voor om als eerste stap in de goede richting een dataset van beeldmateriaal op te bouwen waarmee ontwikkelaars hun producten kunnen ontwikkelen en testen. Daarmee kunnen aantoonbaar bruikbare toepassingen volgens objectieve criteria worden onderscheiden van toepassingen die nauwelijks meerwaarde opleveren.

Externe opslag
Het zal op termijn niet haalbaar zijn alle beeldinformatie in eigen beheer op te slaan. Dit geldt ook voor partijen in het veiligheidsdomein. Voor het jaar 2012 zal naar schatting van IMS Research 3.3 exabytes aan extra opslagruimte nodig zijn louter voor de nieuwe toepassingen van beeldtechnologie. Hoewel opslagcapaciteit steeds goedkoper wordt, zijn de partijen in het veiligheidsdomein toch van mening dat het niet wenselijk is dergelijke hoeveelheden allemaal in eigen beheer op te slaan[11]. De opslag kan beter gespreid worden over verschillende servers. De opslag van beeldmateriaal moet plaatsvinden dichtbij de bron en moet beschikbaar worden voor geautoriseerde andere partijen. Dat vereist goede afspraken over de uitwisseling van beelden tussen verschillende partijen: technisch, juridisch en organisatorisch. Overigens is gespreide opslag vanuit een oogpunt van redundantie en veiligheid volgens veel betrokkenen ook een wenselijke ontwikkeling.

Noot 10 B. van Diemen en L. van Mourik (2008), *Evaluatierapport project Smart Watch*, Politie Amsterdam-Amstelland.
Noot 11 1 exabyte = 1 miljoen terabyte = 1 miljard gigabyte.

2.2 Ontwikkelingen in organisatie

Ontwikkelingen in organisatie
De menselijke factor
Koppeling diverse gebruikers aan een beeldsysteem
Koppeling beeldsensoren aan andere sensoren
Koppeling beeldinformatie aan bestaande databases
Netcentrisch werken
Integratie publiek en privaat

De menselijke factor
'De mens achter de lens' zal de komende jaren nodig blijven. Dat bleek hierboven al (zie 'slimme software'), maar werd ook bevestigd door alle professionals waar wij mee spraken in het kader van deze roadmap. Observanten zullen altijd nodig zijn om beelden te interpreteren of om acties in gang te zetten – ook als beelden eerst door slimme software zijn beoordeeld.
Een belangrijke uitkomst van onderzoek is ook dat samenwerking tussen observanten en surveillanten belangrijk is voor het vroegtijdig signaleren van risicovol gedrag. Het blijkt namelijk dat sommige vormen van afwijkend gedrag pas zichtbaar worden als een surveillant 'op de grond' (bijvoorbeeld door iemand aan te spreken of langs te lopen) gedragingen kan versterken. Pas na menselijke interventie wordt duidelijk of er echt sprake is van een verhoogd risico. Ook in die zin is de menselijke factor in de toekomst dus onmisbaar.
Aan observanten in het veiligheidsdomein zullen steeds hogere eisen worden gesteld qua opleiding, competenties en bevoegdheden. Observanten moeten beter getraind worden in het interpreteren van grote hoeveelheden complexe beeldinformatie, ook van plekken die ze zelf nog niet kennen. Ook moeten ze in staat zijn, zowel qua competenties als bevoegdheden, anderen 'op de grond' (politiemensen, noodhulp, bewakers en beveiligers) aan te sturen.

Koppeling diverse gebruikers aan een beeldsysteem
De tijd dat elk beeldsysteem maar door één organisatie, de eigenaar van het systeem, werd gebruikt ligt achter ons. Toezichtcentrales en dataservers worden steeds groter en ze worden gecentraliseerd tot knooppunten in een netwerk met diverse gebruikers. Verschillende partijen kunnen, als leverancier of gebruiker van beeldinformatie, aansluiten op deze centrale knooppunten.
Dit leidt vaak tot problemen, doordat de beelden niet voldoen aan de eisen van de ontvangende partij. Een voorbeeld zijn de overzichtsbeelden van menigten die met het oog op openbare orde zijn gemaakt. Dit soort beelden zijn vaak slecht bruikbaar voor opsporingsdoeleinden. Bewakingscamera's die, met het oog op afschrikking, in een hoek van het plafond zijn gehangen, hebben te kampen met hetzelfde probleem: op dit soort beelden is het gezicht van bijvoorbeeld een overvaller vaak niet te zien. Om dit soort problemen te beperken, is behoefte aan standaarden, zowel voor de kwaliteit van het beeld zelf als voor de wijze waarop beeldsensoren worden geïnstalleerd door de eigenaar (zie ´technische behoeften´ in het volgende hoofdstuk).

Koppeling beeldsensoren aan andere sensoren
Steeds vaker worden beeldsensoren gekoppeld aan andere sensoren. Beelden bevatten vaak te weinig informatie om te dienen als bewijsmateriaal en

ze geven ook niet altijd aan wat de beste reactie is als een incident wordt waargenomen (of vermoed). De verrijking van beeldinformatie met informatie van andere sensoren verbetert dit.
Geluidsdetectie kan er bijvoorbeeld voor zorgen dat een observant achter de monitor onderscheid kan maken tussen een luidruchtige vriendenclub op straat en een groep vechtende mensen. Een ander voorbeeld is het antidiefstalsysteem (de poortjes) in een winkel die op het moment dat er gestolen goederen de winkel verlaten een camera 'triggeren' en ervoor zorgen dat het beeld van dat moment wordt doorgestuurd naar een toezichtruimte van bewakers, of bijvoorbeeld de regionale meldkamer.
Dit soort koppelingen zullen steeds meer worden gelegd, waardoor het aantal relevante beelden richting het veiligheidsdomein zal toenemen. Dat houdt in dat er ook meer capaciteit moet worden gereserveerd voor het adequaat reageren op dit soort verrijkte informatie.

Koppeling beeldinformatie aan bestaande databases
Steeds vaker wordt beeldinformatie gekoppeld aan andere databases. Kentekens die door camera's worden waargenomen (ANPR) worden bijvoorbeeld gekoppeld aan een database met gegevens over gestolen voertuigen. De markt voor ANPR groeit jaarlijks met ruim dertig procent, aldus IMS Research. Gezichtsherkenning of andere vormen van persoonsidentificatie op vliegvelden, in voetbalstadions, in kantoren en dergelijke kan automatisch worden gekoppeld aan databases met informatie over personen, zoals een lijst met gezochte terroristen, mensen met een stadionverbod, belastingontduikers, bepaalde werknemers, etcetera.
Dit soort koppelingen zorgen vaak voor een enorme toename van het aantal 'hits': gebeurtenissen waar vanuit het veiligheidsdomein een reactie op zou moeten volgen. De politie in Engeland bijvoorbeeld had na een uur kentekens scannen voldoende opsporingsinformatie om een team politiemensen maandenlang aan het werk te zetten voor het opsporen van gestolen voertuigen en het innen van nog openstaande boetes.

Netcentrisch werken
Beeldtechnologie wordt steeds vaker ingezet volgens het concept van netcentrisch werken, ook wel Network Enabled Capabilities genoemd. Dit houdt in dat informatieleveranciers, besluitvormers en eenheden op de grond in een geïntegreerd en interactief informatienetwerk samenwerken. De spil van de informatievoorziening is een gedeeld actueel operationeel beeld: iedereen moet over dezelfde actuele informatie kunnen beschikken[12].

Integratie publiek en privaat
Het streven naar schaalvoordelen leidt ertoe dat publieke en private partijen steeds vaker naar samenwerkingsmogelijkheden zoeken. Twee eigen camerasystemen en twee toezichtcentrales zijn nu eenmaal duurder dan één.
Deze tendens is al zichtbaar in diverse politieregio's in Nederland, met name in Utrecht, Brabant, Limburg, IJsselland en de drie noordelijke regio's. Ook op Schiphol is sprake van grootschalige samenwerking tussen publieke en private partijen: verschillende partijen werken hier samen in dezelfde uitkijkruimte en delen de camera's met elkaar. Het blijkt veel tijd en moeite te kos-

Noot 12 Netcentrisch werken is niet beperkt tot beeldtechnologie, maar gaat over het koppelen van informatie die door sensoren en mensen wordt gegenereerd. In de reeds genoemde *Roadmap subarena geïntegreerde systemen* wordt netcentrisch werken uitgebreider dan hier besproken.

ten om dit soort samenwerking daadwerkelijk te realiseren, maar de opbrengsten kunnen zeer groot zijn.

2.3 Ontwikkelingen in de samenleving

Ontwikkelingen in de samenleving
Meer beeldsensoren
Meer uitwisseling van beelden
***Realtime* beeldinformatie van overal**
De burger als partner in toezicht
Vervuiling in het informatietijdperk

Meer beeldsensoren
Camera's worden steeds beter en (relatief) goedkoper. Het aantal beeldsensoren zal de komende jaren stijgen, volgens een internationale groep experts met circa vijftien procent per jaar[13]. Bijna alle mobiele telefoons hebben inmiddels standaard een camera ingebouwd, laptops en personal computers hebben webcams en particulieren kopen in grote getale camera´s om hun eigendommen in beeld te brengen. In de ontwerpfase van nieuwe gebouwen, winkelcentra, stations en zelfs wooncomplexen worden camera's en de benodigde infrastructuur steeds vaker als algemene voorziening opgenomen. Dit gebeurt meestal zonder dat vooraf helder is met welk doel dit gebeurt en aan welke eisen het systeem moet voldoen om bruikbare beelden op te kunnen leveren als er een incident gebeurt.
Veel camera´s worden overigens helemaal niet met het oog op *safety* of *security* opgehangen: sommige zijn voor vermaak (zoals veel webcams), andere, bijvoorbeeld in het openbaar vervoer of op vliegvelden, voor overzicht over het aantal reizigers met als doel het bespoedigen van de doorstroom (hoeveel loketten moeten open?).
Het aantal beelden van ´derden´ dat richting het veiligheidsdomein wordt gestuurd, neemt nog sneller toe[14]. Partijen in het veiligheidsdomein vinden het onwenselijk als de overheid zou proberen de groei van het aantal beeldsensoren of het aantal beelden dat richting het veiligheidsdomein komt, in te dammen. De enig werkbare aanpak om *overload* te voorkomen, is het slimmer selecteren van beeldmateriaal waar het veiligheidsdomein mee aan het werk moet. Dat vereist technische innovaties om beeldmateriaal snel en goed te kunnen beoordelen op relevantie, door computers of door mensen. Maar techniek alleen is niet genoeg. Er moeten ook afspraken komen over de vraag in welke gevallen het veiligheidsdomein in actie wil komen op basis van beelden van anderen (zie ook de volgende hoofdstukken).

Meer uitwisseling van beelden
Ook het delen van beelden wordt steeds makkelijker, sneller en beter. Websites als Youtube maken het voor iedereen mogelijk beelden te publiceren op het internet. Het bedrijf Cisco schat in dat binnen drie jaar negentig pro-

Noot 13 Zie: ´Sensors Expo & Conference 2008´, in *Sensors & Transducers Journal*, Vol. 93, Issue 6.
Noot 14 Sommigen spreken zelfs van een 'tsunami' aan beeldmateriaal richting het veiligheidsdomein. Een goed voorbeeld is het incident bij Hoek van Holland. De hoeveelheid beeldmateriaal die daar beschikbaar werd gesteld, was volgens een betrokkene van de politie Rotterdam-Rijnmond, tien keer zo groot als bij het vorige vergelijkbare incident.

cent van al het dataverkeer op netwerken uit video zal bestaan[15]. Video over het netwerk blijft niet beperkt tot de zakelijke markt, maar wordt – net als de mobiele telefonie – ook door de consument omarmd. Mensen sturen elkaar over een paar jaar korte videoberichten in plaats van tekstberichten, is hun voorspelling. Dit leidt tot een enorme stroom aan beeldmateriaal en onvermijdelijk zal een deel daarvan ook relevant zijn voor het veiligheidsdomein.

Realtime beeldinformatie van overal

De introductie van de webcam en andere kleine en/of draagbare camera´s met een internetverbinding heeft grote gevolgen voor het veiligheidsdomein. Er zijn vaak grote hoeveelheden beeldmateriaal beschikbaar van incidenten. Voorbeelden hiervan zijn het dancefeest bij Hoek van Holland of bijvoorbeeld de aanslagen in Londen. Na deze incidenten kwamen grote hoeveelheden beeldmateriaal op het veiligheidsdomein af en uiteraard werd daar gebruik van gemaakt[16].

Maar ook als er geen incidenten gebeuren, worden er live beelden vanaf allerlei plekken op aarde weergegeven, bijvoorbeeld op internet. Google maps laat bijvoorbeeld *live* beelden van webcams zien – inmiddels honderden in Nederland. Deze camera´s kunnen in veel gevallen zelfs worden bediend (inzoomen, zwenken) door de bezoeker van de website. Ook gemeenten plaatsen webcams die op internet worden getoond, soms voor recreatieve doeleinden, soms met het oog op criminaliteitspreventie (zie hieronder 'De burger als partner').

In de toekomst wordt het wellicht mogelijk van elke plek waar een webcam staat, *realtime* de beelden naar een willekeurige computer toe te halen. Dat komt in feite neer op een *realtime* variant van Google Streetview. We zien geen foto´s meer van een paar maanden tot een jaar geleden, maar van een paar minuten geleden.

Als de dekkingsgraad hoog genoeg wordt, kunnen partijen in het veiligheidsdomein dat soort beelden gaan gebruiken en is het dus niet meer nodig eigen camerasystemen op te hangen. Ook wordt het in theorie mogelijk om, mits toegang kan worden verkregen tot opgenomen beelden, gebeurtenissen te reconstrueren.

De burger als partner

Steeds vaker blijkt dat burgers bereid en in staat zijn een rol te spelen in het veiligheidsdomein, ook bij beeldtechnologie. Er zijn voorbeelden van camerasystemen die niet worden bekeken door professionele observanten, maar door burgers. In Engeland bijvoorbeeld kunnen burgers beelden van bewakingscamera's via internet bekijken. Als zij een verdachte situatie waarnemen, kunnen ze een melding doen aan de politie die de beelden vervolgens zelf bekijkt en beoordeelt. Camerabeelden worden aangeboden en de deelnemers kunnen zelf niet bepalen welke camera ze willen bekijken. Burgers

Noot 15 Mondelinge presentatie door M. Knopert, product sales specialist Cisco op de *Safety & Security Conference*, 14 april 2010, Amsterdam.

Noot 16 Als het gaat om een belangrijke zaak, leidt dit vaak tot enorme tijdsinvesteringen. In het Verenigd Koninkrijk moest de politie voor het kunnen aanhouden van de *Brixton nail bomber* maar liefst vierduizend uur aan beeldmateriaal bekijken (drie manjaren) afkomstig van meer dan duizend camera's. Hoeveel uur er is besteed aan het bekijken van camerabeelden na de aanslagen van 2005 in Londen is niet bekend, maar waarschijnlijk ging het oo om vele manjaren. Alleen al de organisatie *Transport for London* beschikt over een systeem met tienduizend camera's in treinen, stations, wegen en bussen. De beelden van alle camera's in de buurt van de aanslagen zijn opgevraagd en bestudeerd.
Bron: http://www.timesonline.co.uk/tol/news/uk/crime/article5859923.ece.

die veel bruikbare tips doorgeven krijgen een financiële beloning[17]. Ook in Zoetermeer is het sinds kort mogelijk dat burgers beelden van bewakingscamera's bekijken via internet[18]. Een ander voorbeeld is de oproep van de minister van BZK aan burgers die getuige zijn van geweld tegen hulpverleners het incident te filmen en de beelden door te geven aan de autoriteiten. Maar ook ongevraagd blijken mensen steeds vaker opnames te maken van incidenten en deze beschikbaar te willen stellen aan justitie. Deze trend zal doorzetten, waardoor het aantal meldingen met beeldinformatie verder zal toenemen.
Een andere manier waarop burgers een rol spelen bij beeldtechnologie, is dat zij object van toezicht zijn. De Wet bescherming persoonsgegevens geeft burgers het recht op inzage, correctie, motivatie en verzet[19]. Ook moet de burger in principe altijd worden geïnformeerd over de gegevensverwerking. Burgers zijn dus belanghebbende van beelden waarop zij te zien zijn. Sommige partijen in het veiligheidsdomein zien het als een belangrijke trend dat burgers steeds vaker, terecht, zelf willen kunnen beschikken over hun persoonsgegevens.
Veiligheid is niet de exclusieve verantwoordelijkheid van de overheid. Het is waarschijnlijk dat participatie van burgers, zowel in de handhaving als in de opsporing, de komende jaren steeds meer zal worden gestimuleerd door de overheid. Burgerparticipatie kan bijvoorbeeld de heterdaadkracht versterken. In het veiligheidsdomein zal het particuliere gebruik van allerlei technologieën optimaal gebruikt moeten worden. Het voert voor deze roadmap te ver om hier al te gedetailleerd op in te gaan; het onderwerp verdient meer aandacht dan hier mogelijk is.

Vervuiling in het informatietijdperk
Steeds meer processen worden geautomatiseerd en bijna elk geautomatiseerd proces leidt tot dataproductie, bedoeld of onbedoeld. Een logboek, een database, een overzicht van transacties. In veel gevallen worden deze data bewaard – niet omdat het nodig is voor het gestelde doel, maar omdat het tijd en geld kost om te bepalen wat je wilt weggooien. Het is vaak goedkoper om alles maar gewoon te bewaren.
Hierdoor wordt de hoeveelheid data snel groter. Hierdoor wordt ook de kans op 'missers' bij de koppeling van informatie aan verouderde of inaccurate databases groter. Securityspecialist Bruce Schneier vergelijkt het huidige informatietijdperk met het industriële tijdperk een eeuw geleden. Volgens hem zullen toekomstige generaties zich verbaasd afvragen hoe wij zoveel data konden genereren, bewaren en kopiëren zonder iets te doen tegen de vervuiling die hierdoor wordt veroorzaakt.
Anderen zijn van mening dat het desondanks de voorkeur verdient alles te bewaren. Opslagcapaciteit is steeds minder een probleem. Daar komt bij dat algoritmes die data doorzoeken makkelijker te ontwikkelen zijn als de hoeveelheid data groter is. Een andere reden om alle data te bewaren is dat je nooit weet welke informatie later relevant kan worden ('cold cases'). Hoe

Noot 17 Zie: www.interneteyes.co.uk. Op het moment van schrijven van deze roadmap hadden circa 15.000 mensen zich aangemeld voor deze service.

Noot 18 Er zijn diverse gemeenten die webcams hebben geplaatst op de openbare weg, maar deze hebben geen openbare orde doelstelling. De camera's in Zoetermeer hebben dat wel. Het College Bescherming Persoonsgegevens heeft in een reactie laten weten geen actie te zullen ondernemen tegen deze vorm van cameratoezicht, maar heeft er wel moeite mee dat iedereen de beelden die via de camera's worden uitgezonden kan opnemen.

Noot 19 Dit geldt uiteraard niet als de beelden worden gebruikt voor opsporingsdoeleinden, maar in dat geval geldt niet de Wet bescherming persoonsgegevens, maar de Wet politiegegevens.

het ook zij: de hoeveelheid data groeit exponentieel en de hoeveelheid 'hooi' wordt dus steeds groter. De behoefte aan slimme technieken om daar de spelden in te kunnen vinden neemt daardoor toe (zie ook de behoeften en de aandachtspunten voor nieuwe onderzoeksvoorstellen hieronder).

2.4 Concluderend

Als we alle trends in beeldtechnologie op een rij zetten, kunnen drie voor het veiligheidsdomein relevante conclusies worden getrokken:

1 **Meer en betere beelden**
Bij een voorspelde groei van 15 procent per jaar, zal de hoeveelheid beeldmateriaal over tien jaar verviervoudigd zijn en over twintig jaar verzestienvoudigd ten opzichte van de huidige hoeveelheid. De hoeveelheid beeldmateriaal die interessant is voor partijen in het veiligheidsdomein groeit navenant. Indammen van deze groei ('het dichtdraaien van de kraan') is geen reële optie. De enige manier om werkelijk vooruitgang te boeken is door beter te worden in het vinden van relevante beelden in de totale beeldenstroom. In het volgende hoofdstuk zal blijken dat dit ook precies de grootste behoefte van partijen in het veiligheidsdomein is.

2 **Meer hits**
Beeldtechnologie en beelden worden geïntegreerd in een groot en complex netwerk. Beelden worden steeds vaker gekoppeld aan andere sensoren of databases. Hierdoor neemt het aantal relevante gebeurtenissen of ´hits´ exponentieel toe. Ook voor dit proces geldt dat het onmogelijk kan worden gestopt. Het is ook onwenselijk dit te doen: het is beter om op de hoogte te zijn van wat er gebeurt en geen actie te ondernemen, dan niet op de hoogte te zijn. In het slechtste geval wordt de stapel 'cold cases' groter, in het beste geval leidt het tot een betere informatiepositie waardoor partijen in het veiligheidsdomein goed gefundeerde prioriteiten in hun werk kunnen stellen. De uitdaging voor de komende jaren is beter worden in het onderscheiden van 'ruis' van 'relevant'.

3 **Veiligheidsdomein moet bijblijven**
Een derde conclusie is dat het veiligheidsdomein het zich niet kan permitteren achter te blijven bij de snelle ontwikkelingen in de rest van de samenleving. De meeste partijen in het veiligheidsdomein zijn nu nog niet in staat snel grote hoeveelheden relevant beeldmateriaal te ontvangen, te analyseren en te gebruiken. In de samenleving als geheel is het aantal beeldsensoren de afgelopen jaren veel harder gegroeid dan in het veiligheidsdomein. Die achterstand moet worden ingelopen. De apparatuur (hardware, software en verbindingen) en de organisatie achter de schermen (backoffice) in het veiligheidsdomein moeten up-to-date worden gebracht en worden gehouden. Want als er een ingrijpend incident gebeurt en er zijn beelden van, dan *moet* het veiligheidsdomein in staat zijn die beelden te gebruiken. Dat vereist voortdurende investeringen in apparatuur, deskundigheidsbevordering en aanpassingen in de organisatie[20].

Noot 20 Het is moeilijk om aan te geven welke groei nodig is om de achterstand in te lopen, maar volgens een expert van de politie is tot 2015 misschien wel een groei van 100% per jaar nodig zijn om op gelijk niveau met de rest van de samenleving te komen.

3 Roadmap beeldtechnologie veiligheidsdomein

In dit hoofdstuk wordt de roadmap beeldtechnologie voor het veiligheidsdomein gepresenteerd. De roadmap formuleert een strategisch doel dat in 2020 bereikt zou moeten worden. Om dat strategische doel te kunnen halen, moeten enkele tussenliggende mijlpalen worden bereikt in 2015. Om de mijlpalen te kunnen halen zijn allerlei kleine en grotere innovaties en investeringen nodig, niet alleen in techniek, maar ook in organisatorisch opzicht. Deze worden ook besproken.

2020 – Strategisch doel

Relevante beelden kunnen vinden
In 2020 kunnen partijen in het veiligheidsdomein onafhankelijk van de lokatie waar ze zich bevinden, en zowel *live* als achteraf, relevante beelden vinden in verschillende bronnen van beeldinformatie en deze op een voor de veiligheidsketen zinvolle wijze weergeven, bewerken, bewaren en analyseren.

2015 – Mijlpalen

Objecten en subjecten volgen
In 2015 kunnen partijen in het veiligheidsdomein objecten en subjecten (terug)vinden en volgen over verschillende bronnen van beeldinformatie.

Reconstructie incidenten
In 2015 kunnen partijen in het veiligheidsdomein op basis van beelden gebeurtenissen en incidenten reconstrueren, zodanig dat bruikbare informatie wordt geleverd aan de veiligheidsketen.

Metadata toevoegen
In 2015 worden beelden automatisch geannoteerd met metadata of ‘tags’ waardoor de bruikbaarheid en uitwisselbaarheid in de keten wordt vergroot.

2011 – 2015 Onderzoek & innovatie

Techniek
Objecten en subjecten volgen
Reconstructie achteraf
Relevante beelden filteren
Standaarden voor beeldmateriaal
Metadata standaard toevoegen
Beelden elders ontsluiten
Kwaliteit camera’s omhoog
Goedkoop/veilig beeldtransport
Authenticiteit garanderen

Organisatie
Deskundige observanten
Gebruikers koppelen aan producenten
Schaalbare systemen
Waarborgen persoonsgegevens, toezicht

Van opsporing achteraf naar preventie en heterdaad

Veel innovaties in beeldtechnologie voor het veiligheidsdomein richten zich op opsporing achteraf en reconstructie van incidenten op basis van opgenomen beelden. Dit komt doordat veel beeldmateriaal niet live wordt bekeken door partijen in het veiligheidsdomein, maar pas na incidenten aan het veiligheidsdomein wordt doorgegeven. De innovatieagenda moet ertoe leiden dat dit perspectief wordt uitgebreid met een meer pro-actieve insteek. Er is behoefte aan innovaties die eraan bijdragen dat de focus van opsporing en reconstructie achteraf wordt verlegd naar pre-ventie en meer heterdaadkracht (zie bijlage 4 over de beeldenketen).

Om het strategische doel en de mijlpalen te bereiken, is behoefte aan innovaties, zowel technisch als organisatorisch. De technische behoeften (3.1) en organisatorische behoeften (3.2) worden in dit hoofdstuk besproken.

3.1 Technische behoeften

Na een eerste brede inventarisatie van behoeften zijn acht primaire behoeften geselecteerd. Aan de deelnemers van de workshops is gevraagd hier een prioritering in aan te brengen. Elke deelnemer mocht (maximaal) drie punten toekennen aan elke behoefte. Deze drie punten mochten allemaal aan dezelfde behoefte worden toegekend of over verschillende behoeften worden verdeeld. Daar kwam de volgende prioritering uit (in de tabel staat het aantal gegeven punten per behoefte):

Technische behoeften	Prioriteit
Objecten, subjecten volgen + vinden en reconstrueren achteraf	24
Relevante beelden filteren	12
Standaard beelden	7
Metadata standaard toevoegen	5
Beelden elders ontsluiten	4
Kwaliteit camera´s omhoog + camera´s juiste plaats, aantal	3
Beelden goedkoop en veilig transporteren	3
Authenticiteit beelden gegarandeerd	1

Hieronder worden de acht behoeften nader toegelicht. Ze zijn gesorteerd op prioriteit met de belangrijkste behoeften bovenaan.

1 **Objecten en subjecten volgen + vinden en reconstrueren achteraf**
Objecten en subjecten moeten gevolgd kunnen worden. Dit moet mogelijk worden per camera, maar ook over verschillende camera's en zelfs verschillende beeldsystemen. Het moet dus bijvoorbeeld mogelijk worden, liefst geautomatiseerd, een koppeling te leggen tussen beelden gemaakt met mobiele telefoons en beelden van bewakingscamera's uit hetzelfde gebied.
Ook is er behoefte aan het vinden en reconstrueren van 'events', live en

achteraf. Wanneer zich een incident heeft voorgedaan, moet het mogelijk worden door samenvoegen en combineren van verschillende (typen) camerabeelden een reconstructie te maken.

2 **Relevante beelden filteren**
Relevante beelden moet snel en gemakkelijk kunnen worden gefilterd uit de totale hoeveelheid beeldmateriaal, zowel live als achteraf. Daarbij moet het mogelijk zijn 'events' te onderscheiden: zaken, personen of gebeurtenissen.
Een uitdaging voor veel partijen in het veiligheidsdomein is het verleggen van de huidige focus op opsporing en reconstructie achteraf naar preventie en vroegtijdig ingrijpen bij incidenten. Voorkomen is immers beter dan genezen. Het herkennen van afwijkend gedrag of afwijkende gebeurtenissen speelde in de discussies een belangrijke rol. Op basis van beelden moeten afwijkende gedragingen herkend kunnen worden, liefst geautomatiseerd. Het aantal observanten stijgt immers minder snel dan het aantal beeldsensoren (zie ook de tekst over de gewenste organisatorische innovaties in de volgende paragraaf).

3 **Standaard voor beelden**
Veel partijen in het veiligheidsdomein moeten werken met beelden die door anderen zijn gemaakt, zowel *live* als opgenomen beelden. Beelden van verschillende systemen hebben vaak ook verschillende kwaliteitsniveaus en werken met verschillende (industriële) standaarden. Dit leidt tot veel problemen bij de uitwisseling van beelden tussen partijen.
Er zijn twee oplossingsrichtingen aangedragen door de deelnemers aan deze roadmap. De eerste oplossingsrichting is het afdwingen van een gemeenschappelijke standaard. De tweede oplossing is het zoeken naar software en hardware die ons in staat stelt met verschillende standaarden om te gaan.
Het afdwingen van een standaard blijkt buitengewoon moeilijk te zijn, zelfs binnen het veiligheidsdomein. In 2008 is een poging gedaan om een standaard voor digitale camerabeelden af te spreken[21]. Een belangrijke bevinding tijdens dat traject was dat alleen binnen de strafrechtketen een standaard zou kunnen worden opgelegd via de Coördinatiegroep Informatievoorziening Strafrechtsketen en de Raad van Hoofdcommissarissen. Het is onmogelijk een standaard af te dwingen bij partijen buiten de strafrechtketen; daar kan alleen met richtlijnen worden gewerkt.
Er zijn normen beschikbaar in beoordelingsrichtlijnen, technisch forensische normen en NEN-normen[22]. Maar het bestaan van deze normen leidt er blijkbaar niet toe dat er werkelijk een standaardisatie tot stand komt. Dat komt voor een deel ongetwijfeld door onwil, onwetendheid of onkunde bij de partijen die camera's aanschaffen. Maar voor een ander deel komt het ook doordat leveranciers van beeldsystemen helemaal geen belang hebben bij dergelijke standaarden. Zij hebben juist baat bij differentiatie en producten die niet aansluiten op vroegere generaties[23].

Noot 21 Zie: *Standaarden camerabeelden* t.b.v. het project 'Cameratoezicht openbaar vervoer NCTb', Ministerie van Justitie, 2007/2008.
Noot 22 NEN-EN-501732-7 (NEN staat voor NEderlandse Norm).
Noot 23 Overigens gaven enkele grote spelers in de markt waar wij mee spraken desgevraagd aan dat dit geen bewuste strategie van hun bedrijf is. Het is volgens hen een logisch gevolg van de steeds veranderende behoefte in de markt. Deze bedrijven proberen een product te leveren waar de klant om vraagt en als daar nieuwe beeldformats voor nodig zijn, is dat geen bezwaar.

Daarnaast leert de ervaring dat standaarden in geval van nood makkelijk worden losgelaten. Als er beelden beschikbaar zijn van een groot incident, zoals een aanslag of een ramp, wordt in de praktijk al het beeldmateriaal geaccepteerd. Daarom is het waarschijnlijk realistischer om te investeren in het omgaan met verschillende standaarden, dan in het afdwingen van een standaard. Dit vereist niet alleen innovaties in technische voorzieningen, maar ook in de organisatie binnen het veiligheidsdomein (zie ook het volgende hoofdstuk).

Een hieraan gerelateerd onderwerp zijn afspraken over archivering en beheer van beelden. Nu worden beelden vaak op diverse plaatsen voor diverse doelen bewaard en beheerd. Dat bemoeilijkt het terugvinden van relevante beelden (*cold cases*). Ook hier is behoefte aan meer afspraken en samenwerking tussen partijen in het veiligheidsdomein.

4 **Metadata standaard toevoegen**
Om snel te kunnen bepalen of beeldmateriaal relevante beelden bevat (onderscheid maken tussen 'ruis' en 'relevant'), kan metadata zeer behulpzaam zijn. Metadata zijn brokjes informatie die als een soort label aan beelden kunnen worden gekoppeld. Andere relevante informatie (zoals tekst die aangeeft wat er te zien is op de beelden) moet ook eenvoudig kunnen worden toegevoegd, om het gebruik van beelden door derden te versnellen en vereenvoudigen. De belangrijkste voorbeelden van automatisch toe te voegen metadata zijn datum, tijdstip en locatie. Dit soort metadata kan door de meeste moderne camera's al automatisch aan beelden worden toegevoegd. Een probleem is alleen dat veel gebruikers deze optie niet aanzetten. Hier zou voorlichting en actieve begeleiding vanuit het veiligheidsdomein een bijdrage aan kunnen leveren.

5 **Beelden elders ontsluiten**
Voor partners in het veiligheidsdomein is het van belang beelden elders te kunnen weergeven, opslaan en/of bewerken. Dat betekent dat beelden in (al dan niet beveiligde) netwerken moeten worden gemaakt. Dit hangt overigens sterk samen met de behoefte aan goed en veilig transport van beelden en de behoefte aan een standaard beeldformat.

6 **Kwaliteit camera´s omhoog + camera´s juiste plaats, juiste aantal**
De kwaliteit van camera's en camerabeelden in het veiligheidsdomein moet omhoog. Het komt nog te vaak voor dat beelden korrelig, schokkerig of anderszins van te lage kwaliteit zijn. Hierdoor is het vaak onmogelijk objecten en subjecten te herkennen en identificeren, waardoor beelden onbruikbaar zijn bij opsporingswerk of reconstructies. Veel beeldmateriaal dat aan het veiligheidsdomein ter beschikking wordt gesteld is afkomstig van oude camera´s die niet voldoen aan moderne eisen.
De verbetering van beeldkwaliteit zelf hoeft niet door de overheid te worden gestimuleerd: dit is immers 'business as usual'. Ook als de overheid niets doet, zal de gemiddelde kwaliteit van beelden vanzelf beter worden. Sterker nog: de overheid kán geen eisen stellen aan kwaliteit, plaatsing en het aantal camera´s van derden (mobiele telefoons, webcams). Maar veel deelnemers aan de workshops vinden dat de overheid wel zou moeten investeren in de kwaliteit van beeldsensoren die door partijen in het

---

Er zijn overigens ook uitzonderingen. Axis Communications kiest voor cameratechnologie volgens een open standaard. Zie www.onvif.com.

veiligheidsdomein zelf worden aangeschaft. Camera's worden bijvoorbeeld vaak aangeschaft zonder dat rekening wordt gehouden met afschrijving binnen drie of vijf jaar, waardoor veel verouderde camera's jarenlang blijven hangen.
De wens om meer kwaliteit heeft overigens niet alleen betrekking op de beeldkwaliteit zelf (resolutie e.d), maar ook met de manier waarop camera's worden geïnstalleerd. Camera's moeten op de juiste plek worden opgehangen en met een juist aantal. Ook hier is nog veel winst te boeken door op innovatieve wijze de inzichten op dit terrein toegankelijk te maken en deskundigheid te bevorderen. Het uitwisselen van ervaringen met installateurs kan helpen de 'beunhazen' buiten de deur te houden.
Er is ook behoefte aan een overzicht van alle beeldsensoren die beschikbaar zijn. Het voorstel werd gedaan een digitale kaart te creëren waarop wordt aangegeven waar welke camera's staan, van wie deze camera's zijn en wat ze in beeld brengen. Dergelijke initiatieven vergen echter een lange adem, een slimme organisatievorm, goede projectleiding en wettelijke kaders om deelname aan het systeem af te kunnen dwingen[24].

7 **Beelden goedkoop en veilig transporteren**
Beelden dienen goedkoop en veilig getransporteerd te kunnen worden. Het transporteren van beelden is op dit moment nog altijd relatief kostbaar, vooral als het gaat om beelden van hoge kwaliteit. Voor een deel zal dat probleem vanzelf worden opgelost: ´business as usual´. De afgelopen decennia is het beeldtransport beter, sneller en goedkoper geworden en die trend zal ook zonder investering door de overheid wel doorzetten. Toch zijn de partners in het veiligheidsdomein van mening dat hierin extra zou moeten worden geïnvesteerd. De kwaliteit van verbindingen binnen de politie bijvoorbeeld loopt achter op die van andere partijen in de maatschappij en het blijkt soms bijzonder moeilijk middelen te vinden voor een verbetering van de infrastructuur. Regiokorpsen kiezen soms voor het aanleggen van 'blauw glas', maar dit gebeurt niet in elk korps en ook tussen korpsen zijn de verbindingen niet overal goed genoeg. Overigens moet ook goed worden onderzocht hoe met behulp van datacompressie winst kan worden behaald. Als het voor het signaleren van een incident of 'hit' niet nodig is de beelden op de hoogste kwaliteit binnen te halen, moet dat ook niet gebeuren. Achteraf kunnen beelden – nadat een 'hit' is waargenomen – alsnog op de hoogste kwaliteit naar het veiligheidsdomein worden toegehaald.
Goedkoop transport van beelden mag dan 'business as usual' zijn; betere beveiliging van datatransport tot het niveau dat door het veiligheidsdomein wordt gewenst, zal wel degelijk extra investeringen vergen. De benodigde veiligheid zal niet zonder grote druk vanuit het veiligheidsdomein gerealiseerd worden.

Noot 24 Een goed voorbeeld is het Kabels en Leidingen Informatie Centrum (KLIC); een landelijke stichting ter voorkoming van schade aan kabels en leidingen. Als een 'grondroerder' ergens gaat graven, moet hij vooraf informatie over de graaflocatie opvragen en zorgvuldig werken. De aanvraag gaat naar alle deelnemende kabel- en leidingenbeheerders die in de omgeving eigendommen in de grond hebben. KLIC verwerkt jaarlijks 130.000 aanvragen en duizend deelnemende bedrijven dragen gezamenlijk de kosten. De wettelijke basis is gelegd in de Wet informatie-uitwisseling ondergrondse netten van 2008. Het Agentschap Telecom is aangesteld als toezichthouder op naleving van de wet. Zie: www.kadaster.nl/klic.

8 **Authenticiteit beelden gegarandeerd**
Van veel beelden die worden gebruikt door het veiligheidsdomein kan de authenticiteit nu niet worden vastgesteld. Zijn deze beelden daadwerkelijk met deze camera gefilmd en zijn ze later niet bewerkt? Vragen als deze zorgen ervoor dat veel beelden niet bruikbaar zijn als bewijsmateriaal. Het verdient daarom aanbeveling leveranciers van beeldsensoren te stimuleren standaard bepaalde echtheidskenmerken op te nemen waardoor dit soort verificatie, liefst geautomatiseerd, mogelijk wordt.

3.2 Organisatorische behoeften

Er zijn niet alleen technische, maar ook organisatorische innovaties nodig om de gestelde doelen te bereiken. Er zijn vier behoeften geformuleerd.

Organisatorische behoeften
Deskundige observanten
Gebruikers koppelen aan producenten
Schaalbare systemen
Waarborgen persoonsgegevens, stevig toezicht

Deskundige observanten
De mens is en blijft een cruciaal onderdeel van beeldtechnologie in het veiligheidsdomein. Beelden spreken namelijk nooit voor zich en 'slimme' software blijkt in de praktijk vaak niet aan de hooggespannen verwachtingen te voldoen. Zoals in het vorige hoofdstuk ook al werd gesteld is er daarom behoefte aan observanten met meer opleiding, competenties en bevoegdheden. Observanten moeten beter getraind worden in het interpreteren van grote hoeveelheden complexe beeldinformatie. Ook moeten ze in staat zijn, zowel qua competenties als bevoegdheden, anderen 'op de grond' (politiemensen, noodhulp, bewakers en beveiligers) aan te sturen.

Gebruikers koppelen aan producenten
Om te stimuleren dat de hoeveelheid relevante beelden groter wordt en de hoeveelheid ruis wordt verminderd, moet het ontwikkelen van beeldtechnologie plaatsvinden in interactie met gebruikers, bijvoorbeeld in *fieldlabs*. Dit geldt niet alleen voor hardware, maar ook voor software, zoals de programmatuur waarmee beelden kunnen worden bekeken, doorzocht of geannoteerd.
Ook moet in de fase van ontwerp en installatie al rekening worden gehouden met behoeften van andere gebruikers dan de directe opdrachtgever. Kwaliteit, aantal en plaatsing van beeldsensoren zal ook verbeteren door koppeling van eindgebruikers aan producenten. Dit vereist organisatorische afstemming: er moeten afspraken komen over de partijen die betrokken moeten worden bij de introductie van beeldtechnologie. Ook moeten afspraken worden gemaakt over de minimale standaard waar beeldsensoren aan moeten voldoen.
Een positief neveneffect van het koppelen van gebruikers aan producenten is dat gebruikers beter weten waar beeldsensoren door anderen zijn opgehangen, wat ze precies in beeld brengen en met welke kwaliteit. Dat voorkomt missers (er waren beelden, maar ze zijn niet gebruikt) en overbodig werk (er is wel gezocht, maar de beelden bleken niet bruikbaar).

Schaalbare systemen
Schaalbaarheid in beeldtechnologie gaat over het vermogen mee te groeien als het gebruik en het aantal gebruikers van beeldsensoren groeit. Beeldtechnologie is schaalbaar als zonder aanpassingen in plaats van tien gebruikers ook honderd of duizend gebruikers kunnen worden bediend.
Dit vereist niet alleen technische schaalbaarheid, maar ook organisatorische schaalbaarheid. Partijen die gebruik willen gaan maken van elkaars beelden moeten op basis van standaard autorisaties toegang kunnen krijgen en dit moet vooraf geregeld worden, niet achteraf. De kolommen die nog altijd bestaan in het veiligheidsdomein (bijvoorbeeld tussen defensie en politie of tussen de verschillende zwaailichten) moeten worden opgeheven.

Waarborgen persoonsgegevens, stevig toezicht
Bepaalde vormen van beeldtechnologie kunnen verregaande consequenties hebben voor de vrijheid van burgers. De voorzitter van het College bescherming persoonsgegevens (CBP) verwoordde dit in 2007 als volgt: ´De optelsom van nieuwe bevoegdheden in het veiligheidsdomein leidt ertoe dat het dagelijkse doen en laten van burgers diepgaand wordt onderzocht zonder dat een verdenking is geformuleerd. Zo kan het gebruik van de techniek van ‘data mining’ ertoe leiden dat burgers die niets strafbaars van plan zijn, toch als verdachte worden aangemerkt. En de commissie Brouwer-Korf, die het kabinet adviseerde over bescherming van veiligheid en de persoonlijke levenssfeer, schreef onder andere: 'Het wordt voor burgers steeds lastiger om te overzien wat er met persoonsgegevens gebeurt. Als er de afgelopen tien jaar op het gebied van informatie in het veiligheidsdomein iets fundamenteel is veranderd, is het wel de groei van het aantal databases, het aantal gegevens dat daarin is opgeslagen en de mogelijkheden om die databestanden te bevragen en te delen met andere instanties.'
Deze trend zal doorzetten en daarom moet er meer aandacht komen voor bescherming van persoonsgegevens. Het reeds aangehaalde rapport *Gewoon doen* van de commissie Brouwer-Korf doet hier een aantal voorstellen voor. Een concreet voorbeeld is de conclusie dat het onwenselijk is dat het College bescherming persoonsgegevens een toezichtstaak combineert met advisering, voorlichting en facilitering. De Commissie adviseert de ministers van Justitie en BZK zorg te dragen voor robuust extern toezicht op de naleving en handhaving van de regels voor het omgaan met persoonsgegevens door een sterke en onafhankelijke toezichthouder, die alleen is belast met ‘toezicht houden en handhaven’. Dit advies krijgt steun van veel deelnemers aan de workshops. Daarnaast geeft de commissie aan dat het essentieel is dat elke professional die met beeldtechnologie en/of privacy werkt een helder en richtinggevend kader aangereikt moet krijgen. De grondslagen voor een zorgvuldige omgang met persoonsgegevens worden als volgt beschreven:

- risicoanalyse voordat met gegevensverzameling wordt gestart,
- 'indien noodzakelijk voor de veiligheid moet je delen',
- een helpdesk voor professionals,
- lage administratieve lasten en ruimhartiger vrijstellingenbeleid voor bedrijven die kwalitatief goed beleid voeren,
- burger beter informeren over zijn eigen gegevens en over privaatrechtelijke en bestuursrechtelijke mogelijkheden,
- inzagerecht en klachtenregelingen.

De deelnemers aan deze roadmap onderschrijven de noodzaak voor sterk en onafhankelijk toezicht en steunen het advies. Ook zien zij meerwaarde in 'privacy by design': het principe dat er in een vroeg stadium nagedacht wordt over het goede gebruik van persoonsgegevens binnen een organisatie, de noodzaak van het gebruik van deze gegevens en de bescherming ervan. Door al bij het ontwikkelen van systemen privacy en bescherming van persoonsgegevens in te bouwen is de kans op het succes het grootst.

4 Aandachtspunten bij innovatie

Het programma 'Veilig door innovatie' verstrekt subsidie voor onderzoeksvoorstellen die de toepassing van beeldtechnologie in het veiligheidsdomein kunnen verbeteren. In deze roadmap is aangegeven aan welke innovaties behoefte bestaat. Maar hoe kan worden bepaald welke innovaties in die behoeften zullen voorzien? Met andere woorden: welke selectiecriteria voor onderzoeks- en innovatievoorstellen moeten worden gehanteerd? In dit hoofdstuk worden de huidige criteria opgesomd en aangevuld met een aantal nieuwe aandachtspunten.

4.1 Huidige criteria

Onderzoeksvoorstellen worden op dit moment alleen opgenomen in het Research & Development programma als ze aan een aantal criteria voldoen:

- er ligt een gedefinieerde operationele behoefte ten grondslag aan het onderzoek
- er is een duidelijk perspectief op het vergroten van de maatschappelijke veiligheid
- er is een duidelijk perspectief op het vergroten van het presterend vermogen
- er is sprake van innovatief onderzoek
- er wordt optimaal gebruik gemaakt van eerder opgebouwde kennis
- het onderzoek sluit aan bij het vigerend veiligheidsbeleid
- het onderzoek heeft maatschappelijke impact
- er is een duidelijke noodzaak om het onderzoek in het betreffende jaar te starten
- er is geen sprake van duplicering van onderzoek[25]

Daarnaast kunnen per subarena aanvullende criteria zijn opgesteld waar voorstellen op worden beoordeeld. Deze criteria worden onderschreven door de deelnemers aan de workshops voor deze roadmap en blijven ook in de toekomst van kracht.

4.2 Nieuwe aandachtspunten

In aanvulling op bovengenoemde criteria (of eisen) zijn enkele aandachtspunten geformuleerd. Onderzoeksvoorstellen die gaan over beeldtechnologie in het veiligheidsdomein zouden eerder in aanmerking moeten komen voor subsidie als ze expliciet ingaan op deze punten. Het zijn geen eisen, maar aandachtspunten. De aandachtspunten zijn bedoeld om de indieners van voorstellen te helpen betere voorstellen te schrijven én om de beoordelaars te helpen de beste voorstellen te selecteren.

Noot 25 Bron: https://www.navi-online.nl/services/Proxy/kennisbank/id/15

Research of Development
Er zijn twee soorten onderzoeksvoorstellen: research (onderzoek) & development (ontwikkeling). Research vergt een lange adem, richt zich op opbrengsten op de middellange of lange termijn en kan bij aanvang geen garanties geven over opbrengsten. Bij development gaat het meer om het ontwikkelen van producten of het toepasbaar maken en implementeren van goede ideeën uit ander onderzoek. Development richt zich meer op de korte termijn en van die voorstellen mag dan ook worden verwacht dat ze wel aangeven wat de resultaten zullen zijn.

Aandachtspunten
1. Aandacht voor juridische helderheid
2. Niet investeren in 'business as usual'
3. Bijdrage datareductie óf slim zoeken
4. Levert naar verwachting voldoende rendement op
5. Geen paniekvoetbal
6. Resultaat op korte termijn
7. Aandacht voor implementatie

Punten 4 tot en met 7 gelden alleen voor development en niet voor research.

1. **Aandacht voor juridische helderheid**
   Er is nog maar weinig wet- en regelgeving die specifieke kaders stelt voor innovatieve beeldtechnologie. De afgelopen jaren leren ons dat de wet de techniek volgt en niet andersom. Vaak is de wetgeving die geldt gebaseerd op het idee dat jurisprudentie moet uitwijzen waar de grenzen precies liggen. Daarom is het wenselijk als onderzoeksvoorstellen expliciet aandacht besteden aan juridische aspecten van de innovatie. In elk voorstel moet in elk geval worden aangegeven in hoeverre de huidige wettelijke grondslag toereikend is. De contactgroep beveelt ook aan om de principes van 'Privacy by Design' toe te passen.

2. **Niet investeren in 'business as usual'**
   Bij de afweging of een onderzoeksvoorstel wordt gehonoreerd, moet worden vastgesteld of de voorgestelde innovatie in de categorie 'business as usual' valt of er alleen maar zal komen als er subsidie aan wordt toegekend. Voorbeelden van 'business as usual' zijn betere beeldkwaliteit van camera's, meer opslagcapaciteit of betere verbindingen. Dat zijn ontwikkelingen die niet gestimuleerd hoeven te worden, omdat ze er 'vanzelf' ook wel komen. Camera's worden elk jaar beter, opslag wordt elk jaar goedkoper en verbindingen (en compressietechnieken) worden elk jaar beter. Daarmee is niet gezegd dat dit soort zaken geen investeringen vergen, maar 'Veilig door innovatie' is hier niet het geëigende platform voor.

3. **Bijdrage datareductie óf slim zoeken**
   Eén van de grootste problemen voor het veiligheidsdomein is de enorme hoeveelheid beelden die op dit moment door allerlei partijen worden geproduceerd zonder dat vooraf is nagedacht over het verwerken ervan. Voor het veiligheidsdomein is het daarom belangrijk dat onderzoeksvoorstellen die worden gehonoreerd ofwel bijdragen aan datareductie door middel van slim filteren bij de bron (minder hooi), ofwel aan het sneller en

slimmer doorzoeken van beelden ('meer spelden'). Voorstellen die feitelijk neerkomen op het produceren van meer hooi en niet bijdragen aan het genereren van 'hits' zouden alleen bij hoge uitzondering moeten worden gehonoreerd.

Voor voorstellen in de categorie development gelden ook de volgende aandachtspunten.

4. **Levert naar verwachting voldoende rendement op**
   Het verdient aanbeveling om in onderzoeksvoorstellen een kosten-baten analyse op te nemen die inzichtelijk maakt wat het verwachte rendement zal zijn. Daarbij hoeft het overigens niet alleen om het financiële rendement te gaan, maar kunnen ook opbrengsten worden meegewogen die niet in geld zijn uit te drukken. De kosten moeten eigenlijk binnen de looptijd van het project kunnen worden terugverdiend. Als dat niet haalbaar is, moet in elk geval worden aangegeven wanneer dit naar verwachting wel het geval zal zijn. Het is natuurlijk bijzonder moeilijk om vooraf te voorspellen wat de opbrengsten van innovaties zijn. Sommigen geven zelfs aan dat als dit mogelijk is, het geen echte innovatie meer is. Toch verdient het aanbeveling om vooraf aandacht te besteden aan de vraag waar precies rendement wordt verwacht en hoe groot dat zal zijn.

5. **Geen paniekvoetbal**
   Onderzoeksvoorstellen zouden zo min mogelijk moeten voortkomen uit maatschappelijke vragen die opkomen als gevolg van één opvallend incident. Een voorbeeld is de invoering van de bodyscanner op Schiphol naar aanleiding van de verijdelde aanslag op een vliegtuig vanaf Amsterdam in 2009. Het is volgens de deelnemers niet nodig vanuit ´Veilig door innovatie´ te investeren in dat soort innovaties, omdat dergelijke innovaties er toch wel komen en dus in de categorie 'business as usual' vallen. Dit stimuleringsprogramma zou zich moeten richten op innovaties die normaal gesproken en zonder extra investering niet gerealiseerd zouden worden.

6. **Resultaat op korte termijn**
   Deze roadmap formuleert strategische doelen voor 2015 en 2020. Toch is het volgens veel partijen in het veiligheidsdomein verstandig om te investeren in onderzoeksvoorstellen die mikken op een (tussen)doel dat op termijn van één of twee jaar concrete resultaten oplevert. Het 'laaghangend fruit' moet worden geplukt. Dit voorkomt dat onbereikbare doelen worden nagestreefd en maakt tussentijdse bijsturing mogelijk. Ook zijn successen op de korte termijn nodig om teleurstelling en frustratie te voorkomen bij partijen die met het ontwikkelde product aan de slag willen. Nogmaals: dit geldt alleen voor development en niet voor research.

7. **Aandacht voor implementatie**
   Het blijkt dat veel innovaties na de ontwikkelfase 'op de plank' blijven liggen. Veel partijen in het veiligheidsdomein geven aan dat er op dit moment niet zozeer behoefte is aan nieuwe concepten, producten en diensten, maar aan innovatieve manieren om bestaande concepten, producten en diensten te implementeren. Onderzoeksvoorstellen die werken aan implementatie van bestaande innovaties verdienen de voorkeur boven andere voorstellen.

Bijlagen

Bijlage 1 Leden contactgroep beeldtechnologie

Rene Adegeest, Koninklijke Marechaussee
Seerp Bruinsma, Ministerie van Justitie
Peter Duin, voorziening tot samenwerking Politie Nederland
Ton Hijmering, Politieregio Rotterdam Rijnmond (voorzitter)
Paul de Kruijf, Politieregio Rotterdam Rijnmond
Jan Laven, Gemeente Utrecht
Roy Mente, Koninklijke Marechaussee
Arnout Ruifrok, Nederlands Forensisch Instituut
Adri Voermans, Ministerie van BZK (opdrachtgever)
Thomas Voskuil, Nationaal Coördinator Terrorismebestrijding

Bijlage 2 Deelnemers workshops

Gebruikers van beeldtechnologie
18 februari 2010 en 12 april 2010
Ministerie van Justitie
Nationaal Coördinator Terrorismebestrijding
Nederlands Forensisch Instituut
Politie Amsterdam-Amstelland
Politie Haaglanden
Politie Midden en West Brabant
Politie Rotterdam-Rijnmond
TNO
Voorziening tot samenwerking politie Nederland

Producenten van beeldtechnologie
23 februari 2010 en 13 april 2010
Connexxion
Gemeente Almere
Gemeente Gouda
Koninklijke Marechaussee
Politie Amsterdam-Amstelland
Politie Rotterdam-Rijnmond
Schiphol Group
Voorziening tot samenwerking Politie Nederland

Installateurs van beeldtechnologie
19 maart 2010 en 16 april 2010
ADT Fire & Security
Axis Communications
IBM
Royal Haskoning
Siemens

Individuele interviews

Arriva
Dienstencentrum Gemeente Utrecht
Korps Landelijke Politie Diensten
Nederlands Forensisch Instituut
Nederlandse Spoorwegen
Politie Rotterdam-Rijnmond (4x)
Sensor Universe

Bijlage 3 Definities

Roadmap
De term roadmap is afkomstig uit de wereld van de softwareontwikkeling. Daar wordt het ook wel een *technology roadmap* genoemd. Een roadmap is een plan met korte en lange termijn doelen voor technologische ontwikkelingen[26]. Maar roadmaps hoeven niet alleen te gaan over technologische ontwikkelingen; ze worden door grote organisaties ook gebruikt om te helpen bij het bereiken van consensus over behoeften. Deze roadmap is er voor beide doelen: het stimuleren van technologische ontwikkelingen én het inventariseren van behoeften.

Bronnen van beeldmateriaal
Het gaat in deze roadmap om beeldtechnologie in het veiligheidsdomein. De meeste mensen denken dan automatisch aan bewakingscamera´s en beelden zoals die in programma´s als *Opsporing Verzocht* worden vertoond. Maar er zijn veel meer bronnen van beeldmateriaal die relevant (kunnen) zijn voor het veiligheidsdomein. Denk bijvoorbeeld eens aan alle mobiele telefoons met een camera, of aan filmpjes die op Youtube worden gepubliceerd. Met bronnen van beeldmateriaal worden in deze roadmap alle apparaten bedoeld waarmee beelden kunnen worden gemaakt. Dus bewakingscamera´s, maar ook mobiele telefoons, webcams, fototoestellen en satellieten. Voor de leesbaarheid wordt in deze roadmap in plaats van de onbekende term 'bronnen van beeldmateriaal' of 'beeldsensoren' wel af en toe het woord *camera's* als verzamelnaam gebruikt.

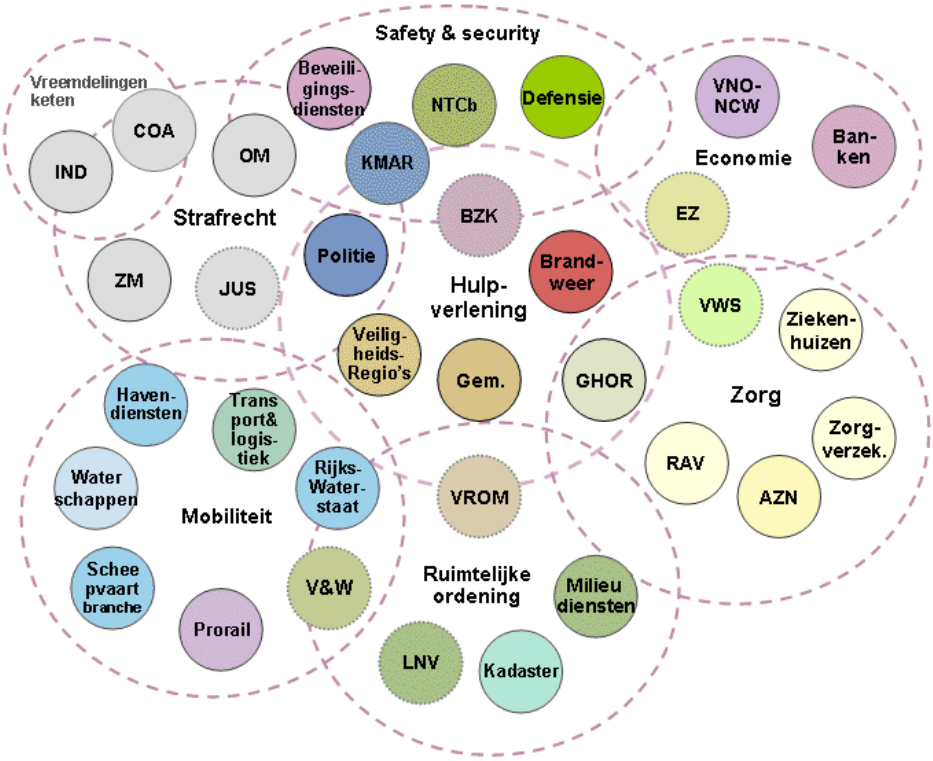
Sensoren
Naast beeldsensoren zijn er in het veiligheidsdomein allerlei andere sensoren, zoals microfoons, infrarooddetectie, satellieten en radar. Sensoren die het cameratoezicht ondersteunen kunnen een trigger zijn voor de centralist om specifiek naar bepaalde beelden te kijken en/of in te zoomen, maar vallen buiten deze roadmap. In deze roadmap ligt de focus op beeldtechnologie, maar een deel van de resultaten is ook relevant voor andere sensoren.

Het veiligheidsdomein
Het Nederlandse veiligheidsdomein bestaat uit alle organisaties die zich inzetten voor veiligheid in de breedste zin van het woord. Het is dus een grote groep organisaties die betrokken zijn bij het bewaken of vergroten van de sociale en/of fysieke veiligheid. Volgens de meesten gaat het daarbij in elk geval om ministeries (BZK, Justitie en Defensie), gemeenten (openbare orde en veiligheid), de zwaailichtensector (politie, brandweer en GHOR), douane en Koninklijke Marechaussee.
Velen vinden daarnaast dat ook de particuliere beveiligingsbranche erbij hoort, omdat hier veel publiek-private samenwerkingsverbanden mee bestaan. Ook openbaar vervoer bedrijven en vliegvelden horen volgens de meesten in dit domein thuis, evenals kennisinstellingen, zoals TNO en universiteiten.
Er waren ook deelnemers die vonden dat eigenlijk alle bedrijven en burgers ook tot het veiligheidsdomein behoren. Dat zou betekenen dat iedereen tot

Noot 26 Zie: http://en.wikipedia.org/wiki/Technology_roadmap.

het veiligheidsdomein behoort, waardoor de definitie geen doel meer dient. Een inperking is dus, al was het maar om praktische redenen, gewenst.

Onderstaand overzicht geeft een goede indruk van het aantal partijen dat tot het veiligheidsdomein kan worden gerekend.



Bron: M&I Partners, *Roadmap subarena geïntegreerde systemen*, in opdracht van Gemeente Utrecht (2009).

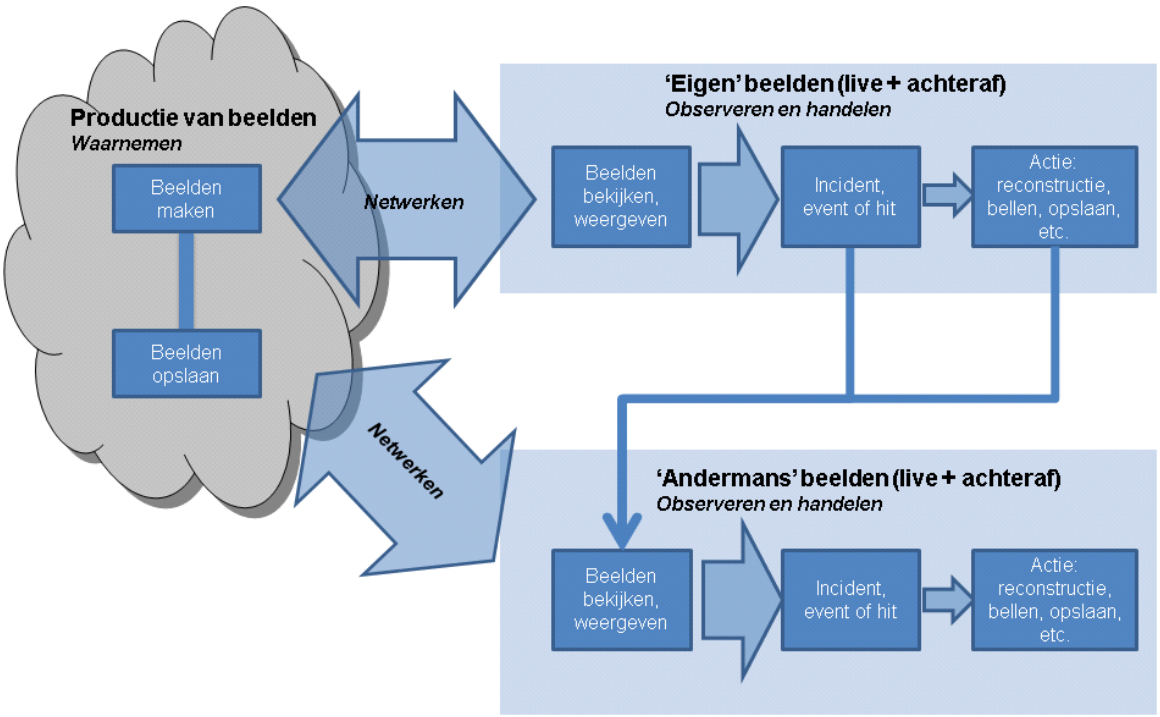
Bijlage 4 Beeldenketen

Beeldtechnologie kan op allerlei manieren worden beschreven. In technische zin moeten, onder andere, de volgende onderdelen worden onderscheiden:

- creatie,
- visualisatie,
- detectie,
- compressie,
- bewerking,
- overdracht,
- analyse en interpretatie,
- opslag en archivering,
- beheer.

De beeldenketen

Een andere manier om beeldtechnologie te beschrijven is door onderscheid te maken tussen beeldproducenten en beeldconsumenten. Dit leverde onderstaand schema op. Zoals elk schema is het een versimpeling van de werkelijkheid: het doel is echter niet volledigheid, maar overzichtelijkheid. Ook biedt het schema de mogelijkheid alle onderzoeksvoorstellen die tot nu toe zijn gehonoreerd een plek te geven.



Deze beeldenketen is gebaseerd op de wijze waarop beelden zich door het veiligheidsdomein verplaatsen. Eerst worden ze geproduceerd en, meestal, opgeslagen. Daarna kunnen er drie dingen met de beelden gebeuren: de producent van de beelden gaat er zelf mee aan de slag of een andere partij ontvangt de beelden van de producent (of haalt ze naar zich toe). De derde optie is overigens dat er niets met de beelden gebeurt en dat ze de 'wolk' nooit verlaten.

Productie van beelden
In het schema geeft de grijze beeldenwolk aan waar beelden worden geproduceerd. Hier bevinden zich bijzonder veel partijen uit het veiligheidsdomein, van politie en burgers tot beveiligingsbedrijven en ambulances.

Bekijken of weergeven
Op het moment dat er ook echt iets met de beelden wordt gedaan, wordt het beeld getransporteerd naar een plek waar het kan worden weergegeven. Dit valt zoals gezegd uiteen in twee soorten: 'eigen beelden' (live en achteraf) en 'andermans beelden' (live en achteraf).
Bij het gebruik van eigen beelden gaat het bijvoorbeeld om gemeentelijke camera's waarvan de beelden op bepaalde uren *live* worden uitgekeken in een gemeentelijke toezichtcentrale. Van gebruik van andermans beelden is bijvoorbeeld sprake wanneer de politie beelden opvraagt of aangeboden krijgt van een incident. De beelden worden bekeken, al dan niet geautomatiseerd met behulp van video content analyse.

Incident, event of hit
Bij een deel van de beelden kan sprake zijn van een incident, event of een andere relevante constatering, kort gezegd: een ´hit´. Als dit gebeurt in het deel van de keten waar men met eigen beelden werkt, wordt op dat moment vaak verbinding gelegd (live of achteraf) met een andere partij in het veiligheidsdomein. Wanneer bijvoorbeeld op de beelden van een NS-camera, die normaal alleen worden gebruikt om te zien hoe druk het op het station is, te zien is dat iemand wordt beroofd ('event'), kunnen deze beelden worden doorgestuurd naar de politie.

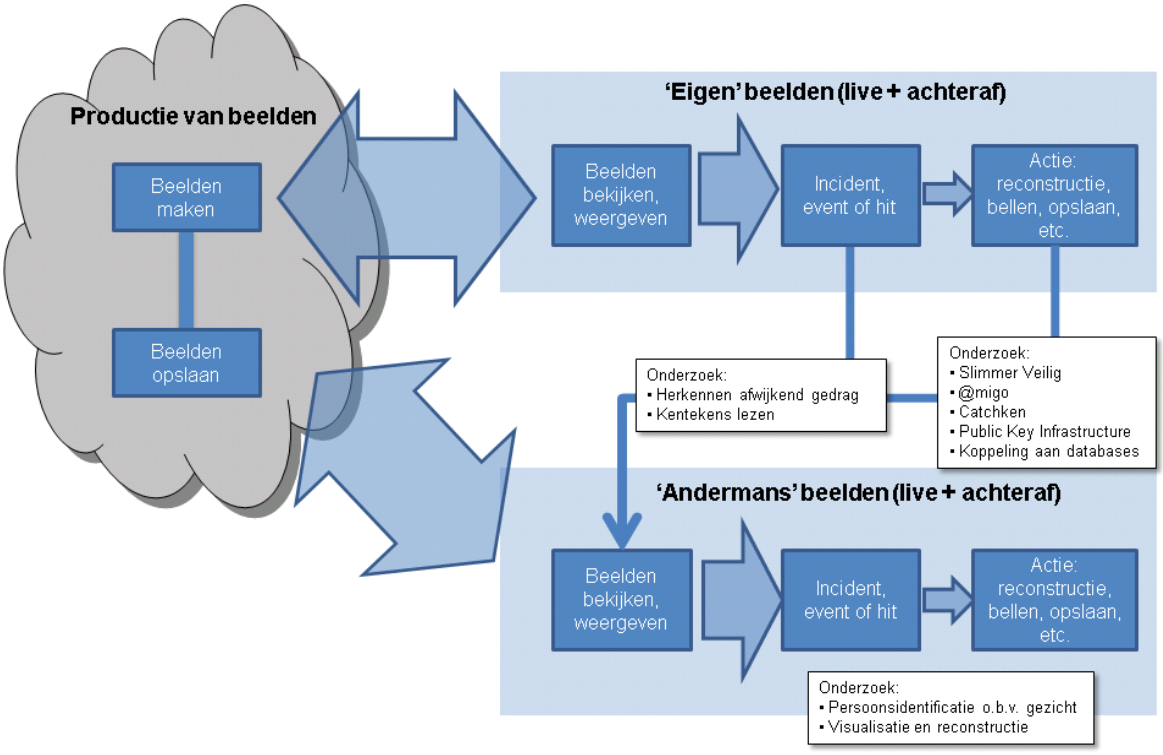
Actie
Als een ´hit´ is geconstateerd, wordt in een deel van de gevallen besloten in actie te komen. Daaronder wordt verstaan het op pad sturen van een eenheid voor noodhulp, het starten van een opsporingsonderzoek, het inschakelen van een toezichthouder op straat of het reconstrueren van een gebeurtenis.

Nogmaals: dit is maar één manier om de beeldenketen weer te geven. Voor deze roadmap bleek deze weergave goed te werken, omdat het een kader bood waar alle behoeften van de verschillende partijen in het veiligheidsdomein in pasten.

Onderzoeksvoorstellen gehonoreerd

Als alle tot nu toe gehonoreerde onderzoeksvoorstellen een plek krijgen in de beeldenketen, blijkt dat verreweg de meeste onderzoeksvoorstellen zich richtten op beter gebruik van andermans beelden achteraf of koppeling van beelden aan andere databases. Dat is een interessante constatering, omdat

op puur logische gronden verwacht mag worden dat op elke plek in de beeldenketen innovaties wenselijk zijn. Kennelijk was de focus tot nu toe sterk gericht op het eind van de keten en niet op de bron.



De belangrijkste behoeften van het veiligheidsdomein zijn gelokaliseerd aan het eind van de beeldenketen. Wat dat betreft zijn de onderzoeksvoorstellen dus terecht daar gehonoreerd. Maar er zijn ook behoeften die juist gaan over de productie van beelden, zoals de behoefte aan betere kwaliteit van beeldsensoren, het toevoegen van metadata aan de bron, een betere plaatsing camera's, een standaard beeldformat en dergelijke.

Op basis van de belangrijkste behoeften aan het eind van de keten, moet worden teruggeredeneerd naar innovaties die nodig zijn aan het begin van de keten. Het is echter niet zinvol alleen vanuit de behoeften aan het eind van de keten te redeneren. Dat zou er namelijk toe kunnen leiden dat interessante (technologische) ontwikkelingen bij de productie van beelden (die de rest van de keten grondig kunnen veranderen) geen kans krijgen.

Wel moet van elke innovator die aan het begin van de keten werkt, worden gevraagd vooraf aan te geven wat de opbrengsten zijn van de innovatie voor de eindgebruikers die moeten observeren en handelen of de efficiëntie in de hele keten.