# DE TOEKOMST VAN SENSING VOOR VEILIGHEID

TNO innovation for life

Hoe ontwikkel je een visie op sensing voor jouw domein?

# COLOFON

AUTEURS
Jeroen van Rest
Ingrid Weima

REVIEWERS
Ido Nap (Nationale Politie)
Arie van Tol (TNO)
Henri Bouma (TNO)
Mark van den Brink (TNO)
Krishna Taneja (TNO)
Jimmy Troost (Voorzitter roadmap Security topsector High-tech Systems and Materials)

TEKSTADVIES EN VORMGEVING
Koen Donker van Heel
Jennifer Keek

DRUK


## DE VRAAG IS:

**HOE ONTWIKKEL JE EEN VISIE OP SENSING VOOR JOUW DOMEIN?**

**TNO Wegwijzer:**
**088 866 08 66**

Dit boekje staat ook online op:
www.tno.nl/sensing



# VOORWOORD

Nog geen 20 jaar geleden voer ik voor het eerst zelf met mijn 30 voet zeiljacht naar Engeland. Om de dreiging van de grote zee een beetje weg te nemen had ik mezelf een luxe veroorloofd: een hand gps.

Het apparaat gaf alleen de coördinaten, die we dan zelf op de papieren kaart moesten intekenen, waarna we konden bepalen waar we waren. Geen gedoe meer met sextanten, Loran-peilingen etc.  Toen we ‘s nachts voor Harwich waren en ik met slecht zicht, harde wind en stroom een verkeerde inschatting maakte over de te volgen koers om de zandbanken, kwam vanuit de kajuit – op basis van de GPS- de duidelijke instructie dat we echt een andere route moesten varen. Vertrouw je dan op jezelf of op je elektronica?

Het vertrouwen in dat kleine apparaat werd beloond en ondertussen hebben we allemaal geleerd dat sensoren en de bijbehorende technologie ons leven gemakkelijker en veiliger maken. Een auto zonder achteruit-rij-sensor is toch maar behelpen, je telefoon zit er vol mee, bewegingssensoren schakelen je verlichting aan of uit en ouderen kunnen langer zelfstandig wonen doordat sensoren hun omgeving waarschuwen als er iets aan de hand is.

De sensor geeft alleen maar een signaal. Het gaat erom wat er met dat signaal gebeurt. De navigator die het signaal intekent op de kaart en aan de hand daarvan de koers plot, of de slimme software die het signaal van een val-sensor oppikt en een bericht naar de hulpverlener stuurt.
Sensing is niet alleen waarnemen, maar ook interpreteren en opvolgen. Een sensingtoepassing is zo goed als degene die de interpretatie uitvoert en heeft geen enkele toegevoegde waarde als er geen actie volgt of bewust wordt gekozen om geen actie te ondernemen. Hoe groot is de kans dat de interpretatie niet correct is? Wat zijn de kosten van een actie of het uitblijven van een actie op basis van een verkeerde interpretatie? Wie vertrouwt u toe om die interpretatie te maken?

De andere kant van deze ontwikkelingen is ook veel in het nieuws. Sensingtoepassingen geven mij niet alleen extra informatie over mijn omgeving, ze geven mijn omgeving ook veel informatie over mij.
Onze samenleving heeft het gemak van sensoren en sensingtoepassingen in het dagelijks leven omarmd. De politie gaat in die ontwikkeling vanzelfsprekend mee. Uitwassen rond technische ontwikkelingen tonen evenwel het belang aan daarmee uiterst zorgvuldig om te gaan. De waargenomen trend van Do iT Yourself Policing geeft bovendien aan dat zowel politie, overheid als samenleving nog veel te leren hebben over de aard van sensingtoepassingen en de consequenties van het gebruik. Het vraagt ook om herbezinning op het sociaal construct waarbinnen we in goed vertrouwen met sensingtoepassingen willen werken.

De uitdaging is om sensingtoepassingen de juiste plek in ons leven te geven. Wat is dan ‘juist’ in deze context? Dat is iets wat we als samenleving moeten bepalen. Dit boek is daarvoor een basis. Het geeft u inzicht in sensingtoepassingen rond veiligheids- en leefbaarheidsvraagstukken. Ik hoop dat het u uitnodigt om deel te nemen in de dialoog rond dit onderwerp!

IDO NAP
Programmamanager Sensing – Politie

# INLEIDING

In dit boek nemen we je op reis door de wereld van sensoren en veiligheid. Onderweg zullen we je wijzen op de meest interessante perspectieven en doorkijkjes. Voor we vertrekken, reflecteren we eerst samen op het doel van de reis.

De Nederlandse samenleving is een open en vrije samenleving, en die waarden willen we continu beschermen tegen criminaliteit en terrorisme. Die vrijheid komt deels tot uiting in onze privacy. Daardoor is veiligheid in beginsel ondergeschikt aan privacy.

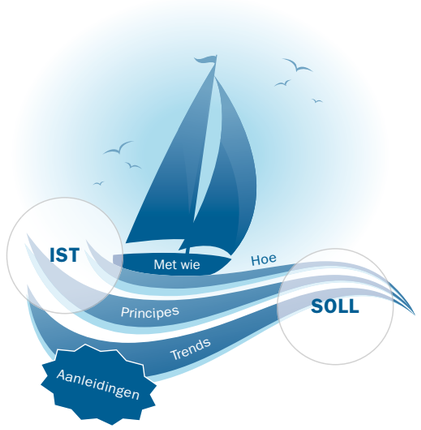
Dat vraagt dus om proportioneel veiligheidsbeleid. Relaxed als het kan, maar er staan als het moet. Beleid dat – zonder naïef te worden – waar mogelijk ruimte laat om in concrete situaties de menselijke maat te vinden. Hiervoor is betrouwbare, accurate, actuele en tijdige informatie nodig waarmee die proportionaliteit in concrete situaties bepaald kan worden. Daar zijn toekomstvaste en proportionele werkvormen gebaseerd op sensoren voor nodig.

Een eenzijdige focus op meer data en informatie over burgers en bedrijven is niet de oplossing. Dat leidt alleen maar tot minder privacy en dus minder vrijheid. Uitvoerende veiligheidsorganisaties moeten meer dan ooit kunnen bepalen welke informatie ze wel én welke ze niet nodig hebben.

De context waarin deze organisaties aan die uitdaging moeten werken is fors aan het veranderen. Juist in dergelijke veranderlijke tijden is het van belang om zelf een toekomstvisie te ontwikkelen. Zo'n visie kan helpen om regie te krijgen en te behouden in een complex speelveld van overheid, industrie en diverse veiligheids- en informatie partners. Het begrijpen van de redenen waarom en waardoor die context verandert, helpt om een robuuste visie op sensing te ontwikkelen.

FIGUUR 1

De verandervragen helpen om de visie op sensing gestalte te geven en duidelijk te krijgen hoe ze kan worden gerealiseerd.








Met dit boekje plaatsen we sensing voor veiligheid in een maatschappelijke context. We geven inzicht in wat er nodig is om zelf een visie op sensing te kunnen ontwikkelen ter ondersteuning van de uitvoering van operationele taken, gestoeld op expliciet beschreven principes die de relatie tussen maatschappij, uitvoerende veiligheidsorganisatie en technologie duiden. We laten tevens zien hoe uitvoerende veiligheidsorganisaties zelf tot een visie op dit zeer actuele onderwerp kunnen komen, zonder dat men vervalt in een welles-nietesdiscussie over kraaltjes en spiegeltjes.

Waar nodig maken we gebruik van metaforen uit de reiswereld. Een architectuurprincipe is te vergelijken met een kompas: het geeft richting aan, maar laat de bestemming over aan degene die het kompas hanteert. De visie die we schetsen is een ansichtkaart uit een mogelijke bestemming. Het is aan jou om te kiezen op welk perron je op welke trein stapt, en wie je uitnodigt om deze reis met jou te maken. Sta je ons toe je daarbij te gidsen?

DE STRUCTUUR VAN HET VERHAAL VOLGT DIE VAN DE VERANDERVRAGEN (Bennebroek Gravenhorst, 2015).

WAT
is sensing nu eigenlijk?

WAAROM
is het nodig om (door) te ontwikkelen op sensing?


WAARHEEN
moet deze ontwikkeling dan toe leiden?

HOE
realiseren we onze visie op sensing?

WIE
zijn daar dan bij nodig?

**"UITVOERENDE VEILIGHEIDS-ORGANISATIES MOETEN MEER DAN OOIT KUNNEN BEPALEN WELKE INFORMATIE ZE WEL, ÉN OOK WELKE ZE NIET NODIG HEBBEN."**

# INHOUDSOPGAVE

# WAT IS SENSING?

Sensing is het vermogen van een organisatie om relevante informatie te verzamelen met behulp van sensoren, met de intentie tot opvolging. Bij uitvoerende veiligheids-organisaties ondersteunt het taken zoals het meldproces, opsporing, heimelijke observatie, bewaking en beveiliging en grensbeheer. Moderne veiligheidsorganisaties staan voor de taak om sensing duurzaam (door) te ontwikkelen. Dit betekent dat ze in staat moeten zijn om volwassen verandervragen op een volwassen manier te beantwoorden.





Bij de strandrellen in Hoek van Holland gaf de video uit een bodycam een uniek beeld van de dreiging naar hulpverleners. De politie staat op het punt om bodycams in te voeren. Hoe zien de processen eruit waarmee de regionale eenheden zelf de invoering van bodycams kunnen aansturen, monitoren en bijsturen?

Satellieten helpen om illegale stort van drugsafval in natuurgebieden te signaleren. Is het ook mogelijk om de daders zelf live in beeld te krijgen? Hoe identificeren uitvoerende veiligheidsorganisaties nieuwe potentiële informatiepartners, en hoe wordt daarbij rekening gehouden met juridische en maatschappelijke vraagstukken?

Als er veilig met drones kan worden gevlogen, kunnen ze dan beter alarmen verifiëren dan met mensen ter plekke? Hoe blijven uitvoerende veiligheidsorganisaties relevant ten overstaan van potentieel disruptieve nieuwe technologieën en businessmodellen?


Bij een overval delen winkeliers met hulp van beveiligingsbedrijven hun camerabeelden met de politie. Hoe bouwen ze voort op dergelijke innovatieve samenwerkingsconcepten, en welke vorm van governance past daarbij?

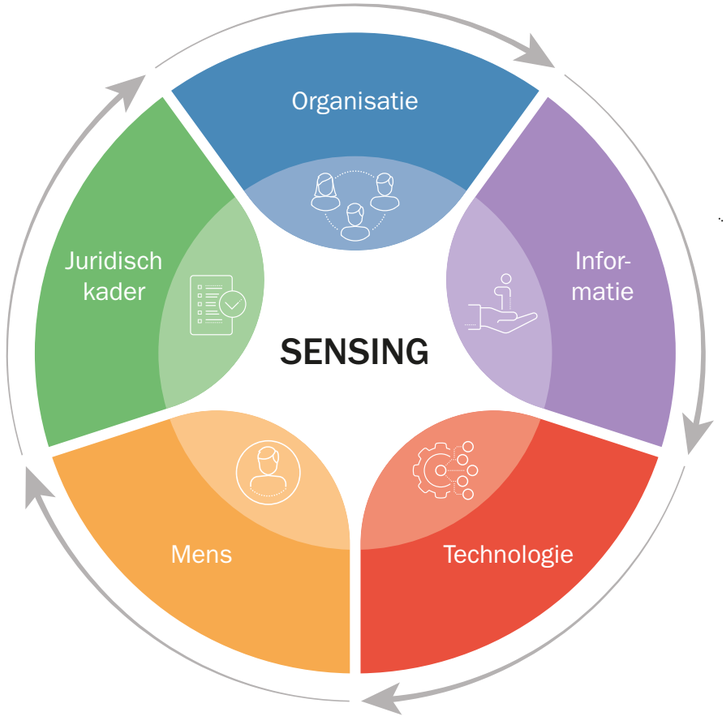
Burgers in onveilige wijken vragen om cameratoezicht tegen overlast en criminaliteit. Helpen die camera's alleen symptomen te bestrijden, of helpen ze ook de oorzaak weg te nemen? Hoe wordt ervoor gezorgd dat evaluaties van innovatieve sensingstrategieën met voldoende kennis van zaken worden gedaan?

Kentekenherkenning helpt om georganiseerde criminaliteit aan banden te leggen door verdachte voertuigen te identificeren, en ook andere nieuwe soorten intelligente sensoren dienen zich aan. Hoe wordt regie gehouden op de introductie van nieuwe sensortechnologie zodat kansen niet gemist worden, en de taak van de organisatie centraal blijft staan?

De tolerantie voor knalvuurwerk in de samenleving daalt. Met behulp van microfoons kunnen knallen worden gedetecteerd. Burgers kunnen valideren of het echt om vuurwerk ging, zelf reageren en de politie informeren. Er zijn ook andere vormen van geluidsoverlast waar andere instanties mee bezig zijn. Is het wenselijk om tot een *smart city* infrastructuur te komen waar verschillende dataleveranciers en -gebruikers op aangesloten zijn?

Om de risico's van en rond mensenmassa's te beheersen is het belangrijk om de grootte te kunnen bepalen. Een groot deel van het publiek heeft een mobiele telefoon bij zich die op afstand te detecteren is en daarmee gebruikt kan worden om de grootte van een mensenmassa te schatten. Welke andere factoren van een mensenmassa zijn essentieel om te kennen, en hoe kunnen die accuraat en op proportionele wijze bepaald worden?

# SENSING VRAAGT EEN INTEGRALE BLIK VANUIT DE PERSPECTIEVEN ORGANISATIE, INFORMATIE, TECHNOLOGIE, MENS EN JURIDISCHE KADER




## ORGANISATIE

**sensing is een verzameling van capabilities**

Sensing is in feite een verzameling van capabilities*: het kunnen plaatsen van sensoren, het verkrijgen van toegang tot sensoren, het in stand houden van sensoren en het kunnen koppelen van sensoren aan informatievoorzieningen en het presenteren van informatie aan eindgebruikers zodat zij tot opvolging kunnen komen.

> Onder de noemer *predictive policing* experimenteert de politie met systemen die op basis van big data en patroonherkenning een verwachting bepalen van misdaad in een bepaald gebied. De volgende stap is om daarbij ook een handelingsperspectief mee te geven: *prescriptive policing*. Welke werkvorm wordt toegepast, bepaalt welke sensing er nodig is.

* Een capability is iets wat een organisatie functioneel gezien kan. De capaciteit is de hoeveelheid middelen die daarvoor beschikbaar is.





> Grote internationale luchthavens zijn onderdeel van de vitale infrastructuur, en vereisen daarom een extra goede beveiliging. Het kunnen vinden, volgen en lokaliseren van personen die betrokken zijn bij verdachte situaties te midden van enorme mensenstromen is een essentiële capability voor de organisaties die daar een gezamenlijke verantwoordelijkheid hebben voor de veiligheid. TNO beschreef in een roadmap welke stappen er nodig zijn – ook organisatorisch – om personen sneller en met minder middelen te kunnen vinden, volgen en lokaliseren (Bouma, van Rest, van Buul-Besseling, de Jong, & Havekes, 2016).

Het gebruik van sensingtechnologie en bijbehorende informatievoorzieningen (onder architectuur) vereist dus ook een uitwerking in werkprocessen en beheer, en gekwalificeerd personeel. Effectief gebruik vraagt overigens om meer competenties en technologieën. Veiligheidsorganisaties moeten het vermogen hebben om betekenisvolle stukjes informatie om te zetten in veiligheidseffecten, zoals toezicht en handhaving, en bewaking en beveiliging. Bijkomende factoren in de keten zijn interne processen, zoals intelligenceprocessen, de screening van personeel of de bescherming van medewerkers tegen dreigingen.

## INFORMATIE

**sensing is onderdeel van het besluitvormings- en intelligenceproces**

Sensing is een onderdeel van het besluitvormingsproces (zoals op operationeel niveau de OODA loop (Boyd, 1996)) en moet dus altijd beschouwd worden in relatie met de omgeving (waarin de sensor zich in bevindt en die wordt waargenomen), deoriëntatiefase (die de informatie gebruikt om tot een situationeel beeld te komen) en de acteerfase (de opvolging waartoe de informatie is verzameld).

Het intelligenceproces is een cyclisch proces van informatieverzameling en -analyse dat typisch op een hoger aansturingsniveau speelt. Sensing speelt een belangrijke rol in de informatieverwerving. In sommige situaties is een sensor de enige informatiebron. In andere situaties is sensing essentieel om andere informatiebronnen te valideren om daarmee tot een voldoende betrouwbaar beeld te komen.

Er zijn verschillende soorten intelligence. Sensing valt onder MASINT en IMINT. Soms wordt een bredere scope gehanteerd waartoe ook OSINT, SIGINT, COMINT en HUMINT worden gerekend.

Er zijn verschillende typen intelligence gedefinieerd – soms met wat overlap. Ieder type heeft eigen kenmerken wat betreft bijvoorbeeld traceerbaarheid, subjectiviteit en tijdigheid. Bij de selectie van die bronnen en de analyse van die informatie moeten we die kenmerken meewegen.

- Open Source intelligence (OSINT) – open bronnen, zoals kranten en nieuwswebsites.
- Human intelligence (HUMINT) – menselijke bronnen, zoals informanten en spionnen, en ook regulier eigen personeel dat surveilleert.
- Measurement and signature intelligence (MASINT) – het detecteren, volgen, identificeren of beschrijven van de onderscheidende karakteristieken van vaste of bewegende doelen.
- Imagery intelligence (IMINT) – intelligence uit luchtwaarneming.
- Geospatial intelligence (GEOINT) – intelligence met een ruimtelijk aspect, zoals uit kaarten en geografische informatiesystemen (GIS).
- Signal intelligence (SIGINT) – het onderscheppen van elektronische signalen, zoals wifi sniffing.
- Technical intelligence (TECHINT) – intelligence uit de analyse van technische capabilities van tegenstanders, bijvoorbeeld uit technische documentatie.
- Travel intelligence (TRAVINT) – intelligence uit reisgegevens.
- Communications intelligence (COMINT) – (een vorm van SIGINT) het onderscheppen van elektronische communicatie tussen mensen, zoals telefonie en online berichtendiensten.

**HET IS VERSTANDIG OM OOK EEN VISIE TE GAAN ONTWIKKELEN OP BIG DATA EN KUNST-MATIGE INTELLIGENTIE – IN SAMENHANG MET EEN VISIE OP SENSING.**





## TECHNOLOGIE

**sensing is sensoren en ICT**

De technologie van sensing gaat over sensoren die grootheden omzetten naar elektronische signalen: data, die tegenwoordig overwegend digitaal zijn. Sensing kan verschillende soorten sensoren omvatten. Veelgebruikte soorten sensoren zijn:

- Transducer: een sensor die een fysieke grootheid, zoals licht, geluid, gewicht, omzet naar elektrische signalen (intelligence: MASINT en IMINT);
- Virtuele sensor: een stuk software (vandaar virtueel) dat digitale data monitort, zoals open bronnen op internet (intelligence: OSINT/SIGINT/COMINT);
- De mens als sensor: het verkrijgen van informatie via mensen, waaronder ook via eigen personeel (intelligence: HUMINT).

In dit boekje ligt de nadruk op de eerste soort sensoren: de transducer. Maar in de praktijk vermengen deze verschillende soorten sensing snel.

Sensoren genereren enorme data-stromen. Daarom zijn er tegenwoordig ook platforms voor het transport, de opslag en de verwerking van deze data. Er zijn slimme algoritmes beschikbaar die gebruikmaken van voorkennis om die digitale datastromen real-time of achteraf om te zetten in betekenisvolle stukjes informatie: een biometrische beschrijving van een gezicht, een kenteken of een transcriptie van gesproken tekst. Uitvoerende veiligheidsorganisaties zijn nog maar recent begonnen om die mogelijkheden te verkennen. Het is dus verstandig om ook een visie te gaan ontwikkelen op big data en kunstmatige intelligentie – in samenhang met een visie op sensing.

## MENS

**sensing is eindgebruikers en ondersteunend personeel**

Sensing gaat ook over eindgebruikers en ondersteunend personeel. Dat zijn de medewerkers die direct met sensingtechnologie werken. Dat kunnen camera-observanten zijn, analisten die profielen maken om ANPR-gegevens te verwerken, meldkamercentralisten die geautomatiseerde meldingen binnenkrijgen of sensing gebruiken om reguliere meldingen te duiden, of surveillanten met een bodycam. Tegenwoordig is dus bijna iedere uitvoerende medewerker van een veiligheidsdienst ook eindgebruiker van tenminste één sensingvariant. Daarnaast zijn er medewerkers die het gebruik van sensingtechnologie mogelijk maken door sensoren te plaatsen (soms stiekem) en te onderhouden. Ten slotte zijn er de gebruikers van de uitkomsten van sensing, zoals analisten, bewakers en beveiligers, rechercheurs en wijkagenten.

## JURIDISCH KADER
**voor sensing**

Sensing voor veiligheid gaat – direct of indirect – over het waarnemen van mensen. Er moet dus aandacht zijn voor de privacy. Met de opkomst van ICT in de jaren tachtig en negentig gebeurde dat ook. De EC voerde in 1995 een privacyrichtlijn in, waarin zes mogelijke grondslagen voor het verwerken van persoonsgegevens werden beschreven (EC, 1995). De bekendste is toestemming (Eng. consent), dat wil zeggen het expliciet of impliciet (door je gedrag) toestemming geven, bijvoorbeeld voor het plaatsen van cookies door websites. Maar consent is zelden een effectieve grondslag om criminelen waar te mogen nemen – zij zullen immers weigeren.

Bij sensing voor veiligheid kan een grondslag bijvoorbeeld zijn: het kunnen uitvoeren van een taak van algemeen belang, zoals handhaving van de openbare orde. Of de behartiging van gerechtvaardigde belangen van een organisatie, zoals de bescherming van haar gebouwen, personeel en bedrijfsprocessen.

Deze grondslagen moeten we afwegen tegen andere rechten, zoals die in de Verklaring van de Rechten van Mens zijn vastgelegd (Raad van Europa, 1950). Vanaf 25 mei 2018 geldt de (geactualiseerde en aangescherpte) Algemene Verordening Gegevensbescherming (AVG). De grondslagen zijn hetzelfde gebleven (Council Regulation (EC), 2012).

In Nederland hebben we – gebaseerd op de internationale regelgeving en verdragen – specifieke wetten en wetsartikelen voor cameratoezicht, kentekenherkenning, bewaking en beveiliging, de inzet van bijzondere opsporingsmiddelen, het vorderen van sensordata door veiligheidsorganisaties bij andere organisaties, en natuurlijk ook voor bepaalde organisaties (zoals de Wet politiegegevens). Deze zullen allemaal in lijn moeten worden gebracht met de nieuwe richtlijn en verordening.

Ook het domein waarin sensing wordt toegepast is van belang. Dit heeft te maken met de verwachting van privacy die mensen mogen hebben, en die is anders in het publieke domein dan op of zelfs in het menselijk lichaam. In oplopende volgorde van verwachting van privacy zijn er het (semi)publieke domein (zoals de openbare weg, of een treinstation), het private domein (zoals binnen een bedrijf), het privédomein (bij iemand thuis) en het lichamelijk domein (direct op of in je lichaam).

Over het algemeen is het wettelijk kader– ook het nieuwe – specifieker over het *verkrijgen* van sensordata dan over het delen ervan (WRR, 2016). Voor eindgebruikers betekent dit dat het minder duidelijk is of en hoe ze data mogen hergebruiken voor andere doelen, zeker wanneer men vaker gebruikmaakt van sensoren van anderen, die met een ander doel zijn geplaatst. Bijvoorbeeld, mogen camera's langs de snelweg – die daar ooit zijn geplaatst om de verkeersdoorstroming te monitoren – ook gebruikt worden om gevaarlijk verkeersgedrag te signaleren? Tegenstanders voeren aan dat dit een vorm van mission creep is: het onbeheerst uitbreiden van de doelen van een systeem. Echter, als dit weloverwogen en op beheerste wijze gebeurt, dan is het een manier om bestaande middelen te hergebruiken: een verstandig economisch principe. Het juridische kader moet dan de basis vormen voor een raamwerk van vertrouwen tussen de verschillende samenwerkende partijen (zoals in dit voorbeeld politie en Rijkswaterstaat) en de burger.

Organisaties kunnen overigens ook zelf besluiten om sensordata of afgeleide intelligence (eventueel anoniem) te delen met uitvoerende veiligheidsorganisaties. Voor particuliere alarmcentrales is in de wet vastgelegd dat zij assistentie aan hulpdiensten kunnen vragen naar aanleiding van een (geautomatiseerde) melding van een incident.





In het kader van een visie op sensing is ook van belang welke ruimte er juridisch gezien is om te experimenteren met nieuwe werkvormen. Zowel de kamerbrief over waarnemen met technische middelen van 2015 (Van der Steur, 2015), als de kabinetsreactie op het WRR-rapport over big data (Van der Steur, 2016) benoemen dat expliciet en creëren daar ruimte voor.

SENSING VOOR VEILIGHEID GAAT (DIRECT OF INDIRECT) OVER HET WAARNEMEN VAN MENSEN. ER MOET DUS AANDACHT ZIJN VOOR DE PRIVACY.

# WAAROM ONTWIKKELEN OP SENSING?

Uitvoerende veiligheidsorganisaties kunnen allerlei redenen hebben om zich te ontwikkelen op het gebied van sensing. Die redenen vinden hun oorsprong typisch in de grote maatschappelijke trends.

De volgende vier trends zijn relevant voor de toekomst van sensing. Ze zijn met name gebaseerd op een selectie van voor sensing relevante trends (HCSS, 2017). Deze trends zijn krachtig en ingrijpend. De consequenties ervan zijn onmogelijk volledig te overzien. Reden genoeg om ze regelmatig te herijken.

De redenen die uitvoerende organisaties aanvoeren om met sensing aan de slag te gaan, vormen de basis voor de volgende verandervragen.



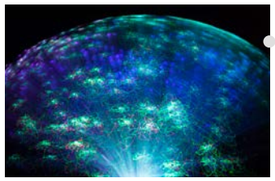


## TREND 1
## DIGITALISERING, INFORMATISERING EN OPKOMST NIEUWE TECHNOLOGIE

Technische sensoren kunnen steeds meer meten, met een grotere nauwkeurigheid en bereik en tegen lagere kosten. Ook digitale communicatie en opslag zullen navenant sterk in prijs dalen. Sensoren zijn op steeds meer plaatsen te vinden, en er komt dus steeds meer digitale informatie beschikbaar.

Uitvoerende veiligheidsorganisaties hebben daarmee in potentie de beschikking over grote hoeveelheden data. Dit biedt enorme kansen in de hele veiligheidsketen. Moderne uitvoerende veiligheidsorganisaties begrijpen daarom heel goed het belang van sensing, zeker in combinatie met verrijking met – weliswaar subjectieve – door mensen ingevoerde interpretaties (bijvoorbeeld via sociale media). Het beheergemak, de flexibiliteit en de mogelijkheden van digitale sensoren, communicatie, verwerking en opslag zijn zo groot dat de gehele maatschappij (en dus ook veiligheidsorganisaties) digitaal afhankelijk zijn. Het belang van informatiebeveiliging is dus ook toegenomen.

Digitalisering biedt de mogelijkheid om data automatisch te verwerken. Diverse vormen van patroonherkenning zijn al operationeel, zoals nummerplaatherkenning en biometrie, maar ook de automatische detectie en analyse van bepaalde soorten



Data-explosie

Snellere en slimmere systemen


Smart City

Verzamelen van data

gedrag. Dit laatste maakt het mogelijk om gedrag te analyseren op indicatoren die tijdens of zelfs voor een incident opduiken. Voor uitvoerende veiligheids-organisaties is het dan wel belangrijk dat men kan uitleggen waarom hun systemen op bepaalde resultaten zijn uitgekomen. Dit stelt eisen aan het ontwerp en het ontwerpproces van deze systemen. Het moet mogelijk blijven om in de systemen in te grijpen als ze ongewenste uitkom-sten geven (zoals discriminatie).

Digitalisering is overal in de samenleving. Veiligheidsorganisaties worstelen daarom met de vraag hoe om te gaan met technische databronnen van derden. Immers, vanuit het besef dat veiligheid een gezamenlijk goed is, worden traditionele stovepipes vervangen door sensor-, data- en informatiekoppelvlakken. Big data die van belang kunnen zijn voor de veiligheid. Uitvoerende veiligheidsorganisaties spiegelen zich daartoe aan de big data-bedrijven zoals Uber, AirBnb, en Google, niet alleen de ultieme uitbaters van digitale informatie, maar ook partijen die hebben geleerd hoe ze middelen van een ander ook voor eigen doelen kunnen inzetten. Voor hen gaat het wat betreft sensing dus ook om het vermogen om te kunnen waarnemen via de sensoren van anderen.

Ontwikkelingen in kunstmatige intelligentie, energieopwekking en -opslag en robotica kunnen zorgen voor proportionaliteit in de verzameling van sensordata. Op afstand bestuurde en gedeeltelijk autonome mobiele platforms maken het mogelijk sensoren dynamisch aan te sturen. Misschien zien we straks dronezwermen die bij een acute dreiging of incident direct ter plekke vliegen en zelf de beste gezichtspunten kiezen voor een actueel situationeel overzicht. Drones kunnen echter ook een dreiging vormen, en het zal niet lang meer duren voordat andere autonome platforms dat ook zijn. Inbraak via de brievenbus door een kleine robot? Niet onmogelijk.

Zakkenrollerij is een veelvoorkomend type criminaliteit waarvan de daad-werkelijke handeling zelfs voor getrainde toezichthouders lastig is te signaleren. Om zakkenrollerij te signaleren moet dus ook heel goed naar het gedrag rond de handeling worden gekeken.

Om te illustreren dat dit inzicht het ook voor automatische systemen makkelijker maakt om zakkenrollerij waar te nemen, hebben in 2014 acteurs in de rol van zowel dader als slachtoffer in een winkelcentrum meer dan twintig zakkenrolincidenten nagespeeld. Dit gebeurde te midden van gewoon winkelend publiek. De videodata die dit heeft opgeleverd zijn gebruikt om een expertsysteem mee te ontwikkelen en evalueren dat automatisch zakkenrolincidenten kon onderscheiden van andere situaties. Er is gekozen om de kennisregels expliciet te maken en niet om een ondoorzichtige patroon-herkenner (bijv. een neuraal netwerk zoals een deep-learning-netwerk) te trainen, om zodoende gedurende de ontwikkeling en evaluatie te kunnen blijven begrijpen waarom bepaalde onderdelen juist wel, of juist niet werkten.

Zo leerden we bijvoorbeeld dat het signaleren op basis van een lage snelheid van het kandidaat-slachtoffer en een plotselinge verandering van oriëntatie van de zakkenroller redelijk werkte. Wellicht maakte die lage snelheid het makkelijk om te stelen, en wellicht wilde de zakkenroller zo snel mogelijk afstand creëren tussen hem en het slachtoffer (Bouma et al., 2014).





**UITVOERENDE VEILIGHEIDS-ORGANISATIES SPIEGELEN ZICH AAN BIG DATA-BEDRIJVEN, NIET ALLEEN DE ULTIEME UITBATERS VAN DIGITALE INFORMATIE, MAAR OOK PARTIJEN DIE HEBBEN GELEERD HOE ZE MIDDELEN VAN EEN ANDER OOK VOOR EIGEN DOELEN KUNNEN INZETTEN.**


## TREND 2
## NIEUWE ECONOMISCHE MODELLEN

Innovatie is niet meer alleen van een aparte afdeling, of beperkt tot de brainstorm tijdens de heisessie, maar gebeurt tegen-woordig continu en overal. Dit betekent dat medewerkers zelf met nieuwe snufjes de organisatie binnenwandelen, maar ook dat bestaande middelen snel zijn achterhaald. Moet een uitvoerende veiligheids-organisatie investeren in body-cams, of wachten we tot onze smartphones die functie kunnen overnemen? En hoe zit het met de persoonlijke drone?

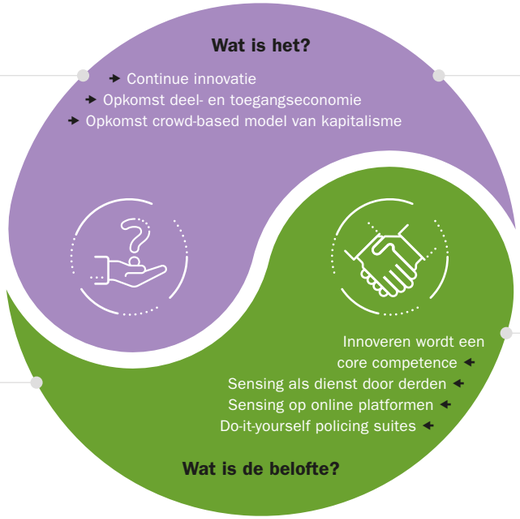
De opkomst van de deel- of toegangs-economie betekent dat organisaties en burgers online toegang krijgen tot allerlei producten en diensten. Criminelen zitten natuurlijk ook online. Er is daarom een behoefte aan online sensing op bijvoorbeeld sociale media om online gedrag in verband te kunnen brengen met gedrag in de fysieke omgeving.

Een tweede gevolg van de nieuwe economie is dat sensingcapabilities voor iedereen te koop zijn. Crowdfunding kan er op termijn toe leiden dat significante capabilities in de handen komen van relatieve leken.

Er zijn diverse concepten in ontwikkeling waarbij de burger wordt ondersteund in het zelf uitvoeren van veiligheidstaken, zoals het melden van incidenten en het oplossen van (kleine) misdrijven. Niet alleen de technologie en proceskant zijn onderwerp van onderzoek, maar ook hoe overheidsdiensten zich überhaupt tot dergelijke initiatieven kunnen en moeten verhouden. Het is bijvoorbeeld denkbaar dat er een crowd-funded do-it-yourself opsporingssuite wordt ontwikkeld door vrijwilligers die burgers in staat stelt op grote schaal zelf misdaad op te lossen.

Continue innovatie

Nieuwe economische modellen





Deeleconomie


Innoveren



## TREND 3
## STIJGEND BELANG VAN VERTROUWEN IN PUBLIEKE INSTITUTIES

De burger is kritischer dan vroeger en stelt hogere eisen aan het sociale contract met de overheid. Ze kan dat contract door de alomtegenwoordige (sociale) media ook beter dan voorheen handhaven.

Voor uitvoerende veiligheidsorganisaties is dit een afbreukrisico. Sensing kan hier negatief aan bijdragen als data buiten context worden gebruikt, maar ook positief als ondersteuning en illustratie van een compleet beeld, zoals in Nederland met de bodycam voor het eerst gebeurde bij de strandrellen in Hoek van Holland.

Een gebrek aan vertrouwen kan makkelijk leiden tot een negatieve spiraal. Voor de veiligheid van reizigers en voor de nationale veiligheid is het bijvoorbeeld essentieel dat grensbewakers zoals de Koninklijke Marechaussee en douane accurate informatie hebben over reizigers en hun bagage (J. H. C. van Rest & Weima, 2017). Een gebrek aan vertrouwen in deze instanties bij reizigers kan tot minder medewerking leiden bij grensposten, en op termijn ook tot een gebrek aan steun bij bestuur en politiek. Het Europese grensbeleid veronderstelt meerdere vertrouwensrelaties tussen het publiek, overheden, private vervoerders en reizigers: een raamwerk van vertrouwen. Als dit raamwerk faalt, of op enige wijze onvoldoende robuust is, dan kan het nodig zijn dat grensbewakers terug moeten vallen op andere juridische gronden om aan de benodigde informatie te komen, desnoods zonder de medewerking van de andere betrokken partijen. Daar zouden meer invasieve vormen van surveillance toe kunnen behoren, die de vertrouwensrelatie verder zouden schaden.

Hogere eisen aan contract



Interactie met burgers

# TREND 4
## MEER AANDACHT VOOR DUURZAAM GEZOND PRESTEREN

Uitvoerende veiligheidsorganisaties hebben de plicht om hun personeel te beschermen tegen werkgerelateerde risico's. Te hoge werkdruk kan leiden tot stress: een van meest voorkomende beroepsziekten. Een overvloed aan ruwe sensordata kan leiden tot te lage of te hoge werkdruk.

De analyse van de data van situaties waarin weinig relevants gebeurt is voor toezichthouders en analisten ontzettend saai. Gebeuren er juist veel relevante dingen, maar is het door de overvloed aan data lastig om hoofd- van bijzaken te onderscheiden, dan kan dat ook tot stress leiden. Er zal een groeiende behoefte zijn aan sensingconcepten waarin de werkdruk voor de mens optimaal is. Een voorbeeld: de toezichthouder krijgt data (zoals een surveillancevideo) aangeboden van een situatie waarop hij normaal geen toezicht hoeft te houden, en waarmee hij dus nog niet vertrouwd is (zoals het geval kan zijn bij Live View).

Data overload


Quantified self


Verharde samenleving leidt tot geweld

Schade op daders verhalen





Personeel van uitvoerende veiligheidsorganisaties is geselecteerd, getraind en uitgerust om bestand te zijn tegen een zeker geweldsniveau. Objectief gezien blijft het geweld tegen publieke handhavers constant. Maar in de samenleving bestaat het beeld dat de samenleving verhardt, waardoor medewerkers met een publieke taak meer kans zouden lopen op een confrontatie met (zwaar) geweld.

Op straat, maar ook binnen de muren van de veiligheidsorganisatie. Er is daardoor behoefte gekomen – zowel bij de samenleving als bij personeel van veiligheidsorganisaties – aan sensoren (bijvoorbeeld bodycams of voertuigsensoren) om objectieve data vast te leggen over de interactie tussen veiligheidspersoneel en burgers. Het is nog maar de vraag tot welke effecten dit gaat leiden.

Met Live View kan de meldkamer van de politie rechtstreeks meekijken met de camerabeelden van een winkelier of horecaondernemer. Zo is die direct op de hoogte als er een inbraak of overval (of ander gewelddadig delict) wordt gepleegd.

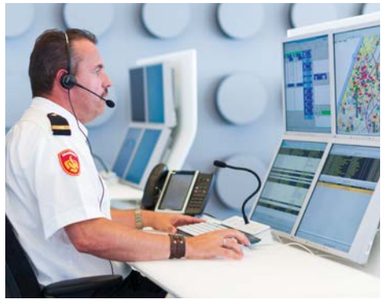
Als winkels of bedrijven hun bewakingscamera hebben aangesloten bij een particuliere alarmcentrale krijgt deze bij onraad via een (alarm)sensor een melding. Een beveiligingsmedewerker van de alarmcentrale kan de beelden dan ook zien en alle gegevens en de livebeelden snel doorschakelen naar de politiemeldkamer. Politiemedewerkers kunnen meteen de situatie inschatten.

Bij Live View ligt het initiatief voor het openen van de verbinding bij de eigenaar van de sensor, niet bij de politie (Politie, 2018).

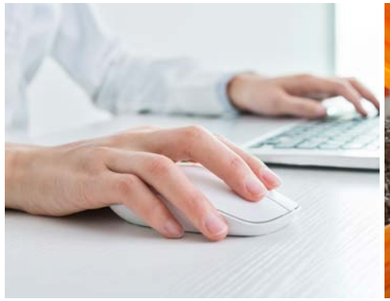
Bij veel organisaties gaan beleid en cultuur richting zelfsturing wat betreft de gezondheid en ontwikkeling van medewerkers. Bij uitvoerende veiligheidsorganisaties vallen hieronder ook gedetineerden en terbeschikkinggestelden. Onder de noemer quantified self wordt breed geëxperimenteerd met het monitoren van prestaties en gezondheid, zowel tijdens evaluaties en trainingssituaties als tijdens het reguliere werk en leven. Sensoren (zoals fitness trackers) kunnen hierbij helpen. Deze leggen allerlei fysiologische parameters vast in relatie tot de situationele context. Dit kan helpen om aandoeningen zoals PTSS vroeger te signaleren en te behandelen of om gedetineerden met een zorgindicatie te ondersteunen bij hun terugkeer in de maatschappij.

# WAAR ONTWIKKELT SENSING NAARTOE
# EEN KOMPAS

Het oude plateau: **hoe gaat sensing NU?**



Het oude plateau bestaat onder andere uit toezichtruimtes en meldkamers en gespecialiseerde toezichthouders. Zij kunnen zowel reactief als proactief uitkijken, en assisteren of sturen medewerkers buiten aan. Ze verifiëren geautomatiseerde meldingen handmatig.



Als medewerkers op surveillanceronde zijn geweest dan zijn ze daarna net zo veel tijd kwijt aan de rapportage.

Plaatsing en activering van sensoren gebeuren handmatig. Daardoor duurt het uren, soms dagen voordat sensorcapaciteit kan worden opgeschaald of aangepast. Bij evenementen die van te voren bekend zijn is dat geen probleem, maar bij ad-hocdreigingen gaan daardoor kostbare uren en soms dagen verloren.





Sensing voor veiligheid is in ontwikkeling naar een nieuw plateau van functionaliteit. In dit hoofdstuk wordt een beeld geschetst van hoe nu invulling wordt gegeven aan sensing, op welke manieren sensing verder ontwikkeld kan worden, en hoe sensing er dan in de toekomst uit kan zien.

Is die capaciteit eenmaal georganiseerd, dan creëert dit direct informatie-*overload* verderop in het intelligenceproces. Deels is dit doordat niet duidelijk is welke informatie echt nodig is, en welke overbodig.

Opsporing is een apart proces. Als er voor opsporing sensordata nodig zijn dan moeten die handmatig bij de bron worden gevorderd en vaak zelfs fysiek worden opgehaald.

**ARCHITECTUUR-PRINCIPES HELPEN OM EEN VOORGESTELDE OPLOSSING AAN DE VISIE TE TOETSEN.**

Van dit huidige plateau is redelijk goed bekend wat de effectiviteit kan zijn, hoe we de betreffende organisaties het beste kunnen inrichten en welke componenten er nodig zijn.

## Een volgend plateau: **een TOEKOMST van sensing**

Sensing levert relevante, betrouwbare informatie voor een accuraat situationeel beeld. De veiligheidsorganisatie weet wat ze weet, hoe betrouwbaar dat is, wat de bronnen zijn, waar de witte vlekken zitten, en hoe die tijdig op te lossen. Daar worden sensoren op proportionele wijze voor gebruikt, bijvoorbeeld alleen voor de periode dat ze nodig zijn. De sensoren die daarvoor nodig zijn worden waar mogelijk betrokken bij partners. Dat kunnen eigenaren zijn van vitale infrastructuur, collega-veiligheidspartners, private beveiligers en niet in de laatste plaats ook gewone burgers. Sensing blijft op beheerste wijze in ontwikkeling in reactie op zich ontwikkelende kansen en bedreigingen. Van nieuwe werkvormen gebaseerd op sensing wordt de verwachte kosteneffectiviteit voor, tijdens en na de ontwikkeling integraal geëvalueerd.

Van dit plateau is op dit moment hooguit de werkzaamheid van onderdelen bekend. Gerichte experimenten onder regie van de uitvoerende veiligheidsorganisaties kunnen deze toekomst dichterbij brengen.


Meldingen, al dan niet geautomatiseerd, komen binnen op een communicatie-platform. Daarop concurreren burgers, dronedienstverleners en bedrijven die personeel buiten hebben lopen (zoals postbedrijven) met elkaar om de melding te mogen verifiëren. Dat doen ze op prijs, maar ook op snelheid en betrouwbaarheid.

Voor bijzondere gevallen zijn er nog steeds private alarmcentrales. Zij mogen extra en bijzondere sensingwerkvormen aanwenden zoals drones, maar moeten daar in bepaalde gevallen wel toestemming voor vragen. En zorgen dat het situationele beeld compleet, tijdig en accuraat is. Daarbij maken ze gebruik van informatie van eerdere incidenten, ook van conculega's. In geval van nood roepen ze tijdig de assistentie van hulpdiensten in. Daarbij wordt het hele relevante deel van het situationele beeld gedeeld.





# HET COMBINEREN VAN SENSING-PRINCIPES IS SOMS EENVOUDIG EN VANZELFSPREKEND

Personeel van de hulpdiensten kan zelfstandig beschikken over het situationele beeld. Voor grotere incidenten ligt de regie over de incidentafhandeling nog steeds centraal, waarbij hypotheses aangereikt worden over wat de situatie zou kunnen zijn, aangevuld met handelingsopties om de betrouwbaarheid van het situationeel beeld te verbeteren. Dat kunnen suggesties zijn om bepaalde omstanders te interviewen of door een mens of sensor simpelweg een ander gezichtspunt in te laten nemen.

Opsporing gebeurt in eerste instantie door het slachtoffer en zijn sociale netwerk zelf. Op basis van de eigen sensoren in en rond de woning (en zijn auto) en de sensordata uit zijn sociale netwerk is zijn informatiepositie rond het incident van hoog niveau. Burgers en bedrijven gebruiken daarvoor software die door vrijwilligers wordt onderhouden en uitgebreid (open source), en die continu toegankelijk is voor de overheid (open standaarden). Zij kan daardoor toezicht houden op de legitimiteit, zoals proportionaliteit van de ingezette middelen. Ook kan ze direct bijspringen of overnemen als nieuwe informatie daar aanleiding toe geeft.

Opsporingstaken zijn geïntegreerd met zowel het meld- als het surveillanceproces. Bijvoorbeeld, voor ieder type melding en iedere soort aangifte voert men direct semi-automatisch een vordering van mogelijk relevante sensordata uit.

## SENSINGARCHITECTUURPRINCIPES

Architectuurprincipes helpen om een voorgestelde oplossing aan de visie te toetsen. Het zijn algemene ontwerppatronen die als good practice zijn aangemerkt en die leidend zijn in het ontwerp van concrete oplossingen. Ze vormen de toekomstvaste schakel tussen behoeften en specifieke (deel)oplossingen. Hier volgt een aantal voorbeelden van families van sensingprincipes die als vertrekpunt voor een discussie over sensing kunnen dienen*.

Voordat men over een concept voor een (sensing)oplossing spreekt, is het verstandig om de sensingprincipes te kiezen waaraan men zich bij het werken aan die oplossing wil houden. Men hoeft dus niet alle principes altijd toe te passen. Het combineren van sensingprincipes is soms eenvoudig en vanzelfsprekend, zoals dynamische sensing door het tijdelijk koppelen aan sensoren van derden. In andere gevallen leiden ze weer tot uitdagingen. Bijvoorbeeld, hoe kan je filteren bij de bron als je niet de eigenaar bent van de sensor?

### TOEKOMSTIG SCENARIO

De politie kan op basis van een 112-melding, een aangifte of een melding via Live View direct bij de online private camera's, inclusief de opgeslagen beelden van relevante momenten. Als onderdeel van het onderliggende protocol wordt er aan de eigenaar van de beelden toestemming gevraagd via een telefoontje of een push-bericht op de politieapp.

Hierdoor kan na een winkeldiefstal, overval (of erger) direct online aangifte worden gedaan met opgaaf van camerabeelden, waarna de gemeentelijke toezichtruimte door de politie wordt gevraagd om in de buurt naar de verdachte uit te kijken. Dit hele proces speelt zich binnen enkele minuten af, dus nog in de heterdaadfase van het betreffende incident.

Met het actuele beeld van het uiterlijk van een verdachte is het ook beter mogelijk om intelligente camera's naar hem te laten uitkijken. Immers, ook de kleding van de verdachte kan gebruikt worden om iemand te herkennen of juist uit te sluiten. De gemeentelijke toezichtruimte kan dus een observatiecirkel trekken rond het incident en alle mensen die daar nu binnen zijn, of in het afgelopen uur zijn geweest, vergelijken met dit beeld. Dat levert een duidelijk plaatje op van waar de verdachte vandaan kwam en waar hij naartoe ging.

Boeven worden hierdoor ook nog afgeschrikt, omdat ze weten dat er actief wordt gezocht en ze niet alleen de locatie van het incident moeten ontvluchten, maar het hele gebied waar camera's hangen. Dat is een stuk lastiger.

Een prettige bijkomstigheid van het gebruiken van architectuurprincipes is dat ze anderen in staat stellen mee te denken. Het wordt minder belangrijk om sturing op de ontwikkeling van sensingcapabilities hard af te dwingen of er continu bovenop te blijven zitten, omdat collega's de principes ook zelf kunnen toepassen.

Een ander effect van het gebruik van architectuurprincipes is dat het makkelijker wordt om als organisatie te leren uit de ervaringen met verschillende capabilities die gebaseerd zijn op dezelfde architectuurprincipes. Bijvoorbeeld, waarom lukt het soms wel om middels geautomatiseerde patroonherkenning afwijkend gedrag te herkennen, maar in een ander geval niet (J. H. C. van Rest, Roelofs, & van Nunen, 2014)?

* Sommige sensingarchitectuurprincipes zijn geïnspireerd op principes uit value-sensitive design.





# PRINCIPE 1
## PRIVACY-BY-DESIGN EN SECURITY-BY-DESIGN VOOR SENSING

De potentie voor stelselmatigheid (altijd), pervasiviteit (overal) en geautomatiseerde verwerking van sensing en bijbehorende informatiesystemen roept ook ethische vragen op, bijvoorbeeld over de privacy. Uitvoerende veiligheidsorganisaties zullen zich wat betreft (het gebruik van) de informatievoorzieningen, inclusief sensingcapabilities, moeten conformeren aan meer actuele wetgeving (zoals de Wet bescherming persoonsgegevens en de nieuwe Wet op de inlichtingen- en veiligheidsdiensten).

Het maatschappelijk draagvlak voor sensing hangt sterk af van de legitimiteit, al zullen incidenten en persoonlijke ervaringen hier veel invloed op hebben. Na een datalek roept men om minder sensing, na een terroristische aanslag om meer. Sensing moet uiteindelijk berusten op value-sensitive design (waaronder privacy-by-design en security-by-design). Zo kunnen we garanderen dat informatiebeveiliging en menselijke waarden een intrinsiek onderdeel van sensing zijn, al moet er nog veel gebeuren om (her)gebruik van data te reguleren.

### VARIATIE 1

Ondanks de privacyrichtlijn (EC, 1995) zag men privacy voorheen in grootschalige ICT-projecten vooral nog als een add-on die men in de latere ontwerpfases nog moest inregelen. Grote desinvesteringen, ook in het veiligheidsdomein, ondermijnden bovendien het vertrouwen van burgers in de overheid. Had deze het wel goed met ons voor en was ze eigenlijk wel in staat om ICT-systemen te bouwen die rekening zouden houden met menselijke waarden?

> Bij de introductie van het biometrische paspoort in Nederland is pas laat in de ontwikkeling rekening gehouden met privacy. De overheid wilde vingerafdrukken ook centraal opslaan, maar na commotie zag men daar vanaf, en moest de overheid aantonen dat de centrale database was vernietigd.

### VARIATIE 2

Daarom ging men vanaf het einde van jaren negentig meer onderzoek doen naar manieren om menselijke waarden eerder in het ontwerpproces mee te nemen. In Nederland begon bijvoorbeeld de registratiekamer (een voorloper van de Autoriteit Persoonsgegevens) in 1995 met TNO aan het ontwikkelen van privacy-enhancing technologies, en aan privacy-by-design. Ook de industrie stapte in door technologie en zelfs patenten te ontwikkelen voor sensingtechnologie die persoonsgegevens direct bij het opnemen al uit de datastroom filterde.

> KPN ontwikkelde eind jaren negentig de PrivaCam-technologie. Een voorbeeld van deze technologie is het detecteren van persoonsgegevens in een videostroom, zoals gezichten of kentekens, om deze apart en extra beveiligd op te slaan. Daardoor kon een toezichthouder nog wel zien wat er gebeurde, maar niet welke specifieke personen of voertuigen daar dan bij betrokken waren. Pas bij een verhoogde dreiging werden de persoonsgegevens vrijgegeven.

VARIATIE 3

*Privacy-by-design* ontwikkelde zich verder in de richting van ontwerpprincipes zoals *visibility and transparency – keep it open*, maar het bleef allemaal nogal abstract. Als reactie kwam er – opnieuw uit Nederland – een aantal voorstellen om privacy-by-design meer concreet te maken.

Tegelijkertijd kwamen er ook andere vormen van *value-sensitive design* op, zoals *security-by-design* en *ethics-by-design*. In de nieuwe Europese richtlijn en verordening zijn ook verschillende vormen van value-sensitive design en onderliggende principes opgenomen (Council Regulation (EC), 2012).

Het principe van privacy-by-design betekent dat privacy en gegevensbescherming ingebed zijn in de gehele levenscyclus van technieken, vanaf de eerste ontwerpfase tot aan het uitrollen, gebruik en uiteindelijke uitfasering. Als PbD gehanteerd wordt, moet een ontwerpmethode gekozen worden die al die fases omvat. Privacy en gegevensbescherming zouden ingebed moeten worden door het hanteren van ontwerppatronen die goed begrepen zijn en die gelden als 'best practice' voor hun doel en gebruiksdomein. Het resulterende ontwerppatroon en systeem moeten alle privacy schendende activiteiten omvatten en hun consequenties beperken volgens de 7 principes van privacy-by-design (Rest van, Boonstra, Everts, Rijn van, & Paassen van, 2014).

De gemeente Den Haag liet een sensor- en informatiedelingsplatform voor het beveiligen van de Internationale Zone ontwerpen en beproeven in de praktijk. TNO voerde een privacy impact assessment uit om de impact op de privacy van zowel burgers als medewerkers van internationale organisaties te bepalen, en om de risico's op dat gebied te helpen minimaliseren (J. H. C. van Rest, Weima, Stolk, & Herder, 2017).

## KIES EERST EXPLICIET DE SENSINGPRINCIPES, EN ZOEK DAARNA DE OPLOSSING IN DIE RICHTING





## PRINCIPE 2
## METADATEREN EN FILTEREN BIJ DE BRON

Sensing is de eerste plek waar informatie de informatiehuishouding van de uitvoerende veiligheidsorganisatie binnenkomt. Door deze informatie bij iedere transactie direct op de juiste wijze te behandelen en van metadata te voorzien wordt het mogelijk om informatie te beheersen en een overdaad aan informatie verderop in de verwerkingsketen te voorkomen.

Metadata vormen samen de informatie die data beschrijft, zoals bijvoorbeeld de locatie en tijd van een video-opname, of een transcriptie van een audiofragment. Metadata kunnen enorm helpen om data te interpreteren. Ze spelen dus een belangrijke rol bij het koppelen van systemen en bij het beoordelen van de prestaties van analytics-systemen. In 2013 onderzochten we de geschiktheid van verschillende metadatatalen voor moderne sensingtoepassingen (J. van Rest et al., 2014).

VARIATIE 1

In een eerste variant van dit principe worden data uit sensoren niet opgeslagen, maar alleen live uitgekeken. De functionaris die uitkijkt kan beslissen om data veilig te stellen en voegt daar vervolgens de benodigde metadata aan toe. Dit is de gangbare praktijk voor het merendeel van de sensoren in het bezit van uitvoerende veiligheidsorganisaties.

VARIATIE 2

In een tweede variant worden voor specifieke taken de data ten behoeve van een specifieke toepassing verwerkt en van metadata voorzien. Een nadeel van deze variant is dat het stovepipes in de hand werkt.

VARIATIE 3

In een meer geavanceerde variant worden alle relevante kernobjecten (zoals 'persoon', 'auto', enz.) direct (dus zo veel mogelijk automatisch) gedetecteerd en indien mogelijk van karakteristieken voorzien (zoals biometrische template, enz.), zodat ze direct beschermd kunnen worden en beschikbaar zijn voor verdere verwerking. De operator kan daar indien nodig extra metadata aan toevoegen.

Voor het voorkomen, stoppen en oplossen van vermissingen, zware criminaliteit en terrorisme kan het nodig zijn om in bepaalde gevallen (grote groepen) mensen of voertuigen gedurende korte of lange tijd te volgen. Gezichtsherkenning en ANPR zijn volwassen technieken waarmee mensen en voertuigen onder geconditioneerde omstandigheden kunnen worden herkend, maar dit is niet schaalbaar. TNO ontwikkelt complementaire technologie (suspect search) en bedenkt inzetconcepten waarmee de verschillende deeltechnologieën samen de gewenste schaalbare sensing-capability kunnen leveren. Met privacy-by-design wordt de menselijke waarde vanaf het begin meegenomen (JRC, 2018).

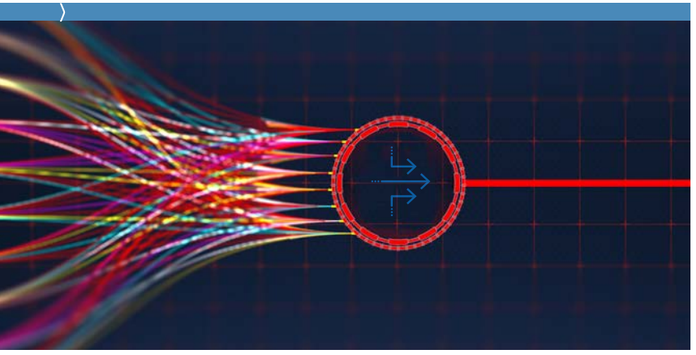
**DOOR INFORMATIE BIJ IEDERE TRANSACTIE DIRECT OP DE JUISTE WIJZE TE BEHANDELEN EN VAN META-DATA TE VOORZIEN WORDT HET MOGELIJK OM INFORMATIE TE BEHEERSEN**

## PRINCIPE 3
## SENSORDATA VAN VOLDOENDE KWALITEIT

De kwaliteit van sensing en van sensordata is bepalend voor het nut ervan, zeker als deze (tevens) als bewijsmateriaal moeten dienen. Kwaliteit betekent niet alleen betrouwbaar en tijdig, maar omvat ook niet-functionele aspecten, zoals beheerbaarheid en gebruikersvriendelijkheid.

Er is geen eenduidige ondergrens aan de kwaliteit van sensing en sensordata te stellen waaronder sensordata hun nut verliezen. Voor sommige toepassingen in het veiligheidsdomein is ieder spoor, ongeacht de kwaliteit, van belang. Bijvoorbeeld om te bepalen waar men de capaciteit van een onderzoeksteam inzet, of hoe en in welke richting een ondervraging verder moet gaan. Maar, ‘garbage in is garbage out’; met andere woorden: als je onzin in een proces stopt, dan komt er ook onzin uit.

Aan de bovenkant van het kwaliteits-spectrum zit eveneens geen harde grens. Als de (sensor)data van uitstekende kwaliteit zijn, dan kan dit tot gevolg hebben dat een verdachte eieren voor zijn geld kiest, en bereid is om meer waarheidsgetrouw te verklaren dan bij minder hard bewijs. Echter, perfect is de vijand van goed. Streeft men in bepaalde gevallen naar te hoge kwaliteit, dan gaat dit ten koste van een voldoende goede kwaliteit in het algemeen.







VARIATIE 1

De eerste variant van dit principe stelt dat bekend is wat men bedoelt met betrouwbaarheid van sensing en sensordata, en wat mogelijke bronnen van onbetrouwbaarheid zijn (biases bijvoorbeeld). Deze kennis is bestemd voor de eigen organisatie en eventuele ketenpartners. Neem de borgregeling tussen particuliere alarmcentrales en hulpverleners. Daarin wordt wederzijds erkend dat meldingen uit geautomatiseerde alarmsystemen vaak loos zijn, en er zijn verschillende studies beschikbaar die beschrijven hoe dit komt (van der Lee, Peters, & van Rest, 2014).

De gemeente is vergunningverlener voor evenementen. Eén van de criteria voor die vergunning – en de daaraan gekoppelde beveiligingsmaatregelen en inzet van hulpdiensten – is het (verwachte) aantal mensen. Vanuit het oogpunt van risicomanagement en beveiliging (i.e. crowd management en crowd control) gaat het dan specifiek om het aantal mensen dat tegelijkertijd aanwezig is.

Het is uitdagend om het aantal mensen in een menigte betrouwbaar vast te stellen. Het telproces kan tijd kosten en mensen kunnen ondertussen arriveren of juist weggaan. Afhankelijk van de manier van tellen en de daarbij gebruikte instrumenten kunnen mensen ook onzichtbaar zijn door bijvoorbeeld occlusie van andere mensen, van paraplus, van luifels, enz. Telmethoden die gebruikmaken van het dragen van mobiele telefoons kunnen beïnvloed worden door de demografie van de menigte, of het geografische bereik van zendmasten (te groot of juist te klein).

Voor een betrouwbare vaststelling van het aantal mensen is de methode van tellen het belangrijkst. Als die methode nauwkeurig is, en het resultaat is ook door anderen zelf te controleren, dan maakt het niet veel meer uit wie er telt.

Er zijn verschillende manieren van tellen. Sommigen maken gebruik van (lucht)fotografie, anderen van (getrainde) observanten ter plekke of via cameratoezicht. Weer andere manieren tellen afgeleide parameters zoals het aantal mobiele telefoons, het aantal keren dat een toilet is doorgetrokken of dat een bierfust is vervangen. Sommige van deze manieren zijn deels geautomatiseerd en/of commercieel verkrijgbaar. TNO helpt gemeenten overzicht te krijgen over de verschillende manieren van tellen, hun betrouw-baarheid en om bij een concreet evenement ook te bepalen welke manier van tellen het meest geschikt is.

**VARIATIE 2**

In een tweede variant van dit principe is ook bekend hoe betrouwbaar sensordata moeten zijn voor een bepaalde toepassing en hoe betrouwbaar een bepaalde sensingopstelling in de praktijk is. Een voorbeeld van een kwaliteitsondergrens is het aantal pixels tussen de ogen in een opname van een gezicht van een persoon, waarbij nog gezichtsherkenning mogelijk is. Met een rotakinpop of automatische kalibratie kan men in de praktijk bepalen of dergelijke kwaliteitsmaten ook daadwerkelijk worden behaald. Bij deze variant weet de uitvoerende veiligheidsorganisatie ook wat ze niet hoeft te weten en kan ze onderbouwen dat ze voldoende (nauwkeurige) (sensor) data heeft.

Er zijn verschillende concepten in ontwikkeling – zoals ComproNet – waarbij uitvoerende veiligheidsorganisaties gebruikmakend van moderne (sociale) media meldingen krijgen van burgers. De kwaliteit van de melding – waaronder de betrouwbaarheid van de bron – maakt veel uit voor de duiding en daarna de opvolging. Een expliciet model van de betrouwbaarheid van verschillende soorten van burgermeldingen – zoals het verschil tussen een melding via Twitter en een melding via een Whatsapp buurtapp – kan helpen om de kwaliteit van het meldproces te verbeteren.

**VARIATIE 3**

In een derde variant van dit principe is – ten slotte – ook bekend welke handelingsopties er zijn voor, tijdens en na een incident, om de betrouwbaarheid van (sensor-)data te verbeteren. Men kan bijvoorbeeld extra (typen) sensoren plaatsen op een locatie zodat er meerdere onafhankelijke databronnen ontstaan. Of men kan geavanceerde signaalverwerking toepassen om temporele resolutie in te leveren voor spatiale resolutie (i.e. superresolutie).

Zowel ten behoeve van grensmanagement als ten behoeve van opsporing is het onderscheid kunnen maken tussen leugens en oprechte verklaringen een basisvaardigheid. TNO signaleerde dat er op dat gebied de laatste tien jaar in de wetenschap en bij industrie grote stappen zijn gezet. TNO agendeerde deze ontwikkelingen op eigen initiatief bij eindgebruikers door het zelfstandig uitvoeren en aanbieden van een verkenning naar moderne leugendetectietechnologie (van der Zee, Kleij, van Rest, & Bouma, 2016).





# PRINCIPE 4
## SENSING SLECHTS ALS HET NODIG IS

Sensing met geautomatiseerde middelen kan snel persistent en invasief worden. De inzet moet dus proportioneel zijn. Dynamische situaties vragen om dynamische sensing: sensing als het nodig is.

*Remote sensing* met behulp van satellieten kan helpen om illegale dump van afvalstoffen in natuurgebieden te detecteren. Maar satellieten draaien vaste rondjes om de aarde waardoor ze niet continu kunnen observeren. Door hun hoogte kunnen ze ook niet onder wolken kijken. Is het mogelijk om dit informatiegestuurd – dus alleen als daar aanwijzingen voor zijn – aan te vullen met (onbemande) vliegende platformen die ook de daders in beeld kunnen krijgen?

**VARIATIE 1**

In een eerste variant van dit principe worden sensoren geplaatst of weggehaald, naargelang de lokale behoefte aan sensingcapaciteit. Een voorbeeld is mobiel cameratoezicht.

**VARIATIE 2**

In een tweede variant zijn sensoren continu aanwezig, maar worden ze alleen aangekoppeld als daar aanleiding toe is. Een voorbeeld is Live View.


**VARIATIE 3**

In een derde variant worden de sensoren via autonome platformen (bijv. via drones) ter plekke gestuurd als daar noodzaak toe is. Ze gaan weer weg als die noodzaak voorbij is.

# PRINCIPE 5
## GEBRUIKMAKEN VAN ANDERMANS SENSOREN

Uitvoerende veiligheidsorganisaties maken gebruik van sensoren van anderen en dit zal toenemen. Ze doen dat echter met andere doelen dan de sensoreigenaar dat doet. In deze familie van sensingprincipes gaan de principes in oplopende mate van samenwerking. Daarbij geldt: hoe intensiever de samenwerking, hoe verfijnder de cyberveiligheid moet zijn.

Ook moet de juridische basis voor de samenwerking kloppen. Het minimum is een een juridische basis voor het vrijwillig delen van (sensor)data met de veiligheidsorganisatie. Vanuit het perspectief van de eigenaar van de (sensor)data kunnen dergelijke samenwerkingsvormen echter knagen aan de vertrouwensband die zij met hun klanten hebben. Als samenwerking op basis van vrijwilligheid niet voldoende veiligheidseffect sorteert, dan kan het nodig zijn om ‘eenzijdig’ beslag te mogen leggen op (sensor)data.

### VARIATIE 1

In de eerste variant inventariseert de uitvoerende veiligheidsorganisatie welke sensoren er zijn op bepaalde locaties en wie de eigenaar is. Als er een incident is (geweest) op die locatie dan weet de uitvoerende veiligheidsorganisatie of daar mogelijk data zijn opgenomen, en bij wie ze terecht kan om die data te verkrijgen. Een voorbeeld is Camera in Beeld.

> Een organisatie in het openbaar vervoer wenst een update van het camerahandboek waarmee ze haar leveranciers op gebied van beveiliging aanstuurt. Ze wenst daarbij meer dan voorheen rekening te houden met de belangen van partners op haar locaties. Als onderdeel van het opstellen van deze nieuwe visie kan een gezamenlijke herijking van het dreigingsbeeld nuttig zijn.

### VARIATIE 2

In een geavanceerdere variant worden sensordata op verzoek van de eigenaar van de sensor bij een incident direct digitaal doorgestuurd naar de uitvoerende veiligheidsorganisatie. Om te voorkomen dat men te vaak moet reageren op loze alarmen stelt bijvoorbeeld de politie kwaliteitseisen aan (het gebruik van) sensoren alvorens ze de koppeling accepteert. Het is in ieders belang om de veiligheidsorganisatie invloed te geven op het verwerven en beheren van sensoren van anderen. Een voorbeeld is Live View voor camera’s.

> Den Haag herbergt honderden internationale organisaties in de binnenstad, waaronder een aantal dat onder het Stelsel Bewaken en Beveiligen valt. De binnenstad van Den Haag is daarmee het woon-, werk- en leefgebied van honderdduizenden burgers, maar vanuit objectbeveiliging ook het observatiegebied van vele beveiligingsafdelingen en het International Frontoffice van de politie. De beschrijving van een gezamenlijk dreigingsbeeld maakte het mogelijk om een modern sensing- en informatiedeelconcept te ontwikkelen waarmee politie en beveiligingsafdelingen van hoogrisicoobjecten op proportionele wijze (sensor)informatie kunnen delen (J. H. C. van Rest et al., 2017).

### VARIATIE 3

In een nog geavanceerdere variant wordt de sensor op basis van prioriteit bediend en gebruikt op basis van afspraken. Meerdere partijen, waaronder de politie, kunnen direct bij de sensor, en afhankelijk van het doel van het gebruik krijgt een bepaalde partij prioriteit. Een voorbeeld is de Gemeenschappelijke Meldkamer Infrastructuur van Schiphol. Mogelijk gaan smart-city-concepten deze rol vervullen voor uitvoerende veiligheidsorganisaties.

> In het Europese project TACTICS is verkend hoe de bestaande (veiligheids)infrastructuur van een stad kan worden ingezet en uitgebreid om een terreurdreiging het hoofd te bieden. Binnen het project zijn juridische, ethisch, organisatorische en technische aspecten verkend van deze uitdaging (TACTICS Consortium, 2013). Dit soort moderne sensingconcepten zullen gebaseerd moeten zijn op een robuust *trust framework* tussen overheid, informatieproducenten en -consumenten en datasubjecten.

**MODERNE SENSINGCONCEPTEN ZULLEN GEBASEERD MOETEN ZIJN OP EEN ROBUUST *TRUST FRAMEWORK* TUSSEN OVERHEID, INFORMATIEPRODUCENTEN EN -CONSUMENTEN EN DATA SUBJECTEN**

# PRINCIPE 6
## NIEUW SENSINGCONCEPT ONTWIKKELEN

Innoveren is het succesvol toepassen van een vernieuwing in de praktijk. Daar zijn inherent risico's aan verbonden, en de bedoeling van innovatiemanagement is om dergelijke risico's te beheersen. Aangezien iedere vernieuwing uniek is, is innoveren dus per definitie maatwerk.

Naarmate de gewenste innovatie meer ketenpartners (meer) raakt, of meer specialisatie vereist, moet met meer partijen worden samengewerkt. Voor een belangrijk deel gaat dat maatwerk dus om de manier waarop de omgeving bij het innoveren wordt betrokken. Voor de meer geavanceerdere vormen van innovatie is dan ook een meer genuanceerd beeld van het sensingecosysteem nodig (zie hoofdstuk 5).

**VARIATIE 1**

De meest eenvoudige variant betreft een (typisch kortcyclische) innovatie die geheel zelfstandig binnen de uitvoerende veiligheidsorganisaties met bestaande middelen te realiseren is. Men gebruikt geen andere sensoren dan die al beschikbaar zijn.

Voor sommige uitdagingen op het gebied van sensing zijn kortetermijnoplossingen mogelijk met een kortcyclisch veredeld verwervingsproces en/of binnen één uitvoerende dienst. Echter, vaak vereist de oplossing structurele afstemming en samenwerking op de (middel)lange termijn met andere organisaties, soms onder regie, waarbij de nieuwe sensing-capability ontstaat uit de samenwerking van die betrokken organisaties. Beide uitersten vallen onder innovatie: het realiseren van een nuttige vernieuwing in de praktijk. Het is verstandig om dit te doen vanuit een richtinggevend kader, een coherent stelsel van principes op het gebied van sensing en informatiemanagement (bijvoorbeeld 'need to know' versus 'need to share'), ethiek en privacy, waarbinnen good practices alle ruimte krijgen en stovepipes worden vermeden.

**HET ONTWIKKELEN VAN SENSING CAPABILITIES KAN ONDERSTEUND WORDEN DOOR HET TER BESCHIKKING STELLEN VAN – VOOR HET PROBLEEM REPRESENTATIEVE – TESTDATASETS**





**VARIATIE 2**

Een volgende variant betreft het ontwikkelen van een nieuw sensingconcept op basis van voor de organisatie nieuwe, maar reeds bestaande producten en diensten (Eng. *off-the-shelf*). De innovatie vereist een verwervings- en implementatieproces.

Moderne sensing en big data systemen maken intensief gebruik van patroonherkenning en andere vormen van kunstmatige intelligentie (zoals deep learning). Dergelijke systemen moeten getraind en geëvalueerd worden met hoogwaardige data. Het ontwikkelen van sensing capabilities kan ondersteund worden door het ter beschikking stellen van – voor het probleem representatieve – testdatasets. Een voorbeeld is I-Lids van UK Home Office (UK Home Office CAST, 2015). Die datasets verouderen naarmate technologie zich verder ontwikkelt, en de behoeften veranderen. TNO nam in 2017 het initiatief voor een toekomstvast internationaal platform waarmee eigenaren van dergelijke datasets ze op een veilige wijze kunnen ontsluiten.

**VARIATIE 3**

Een derde variant betreft het laten ontwikkelen van nieuwe producten en diensten. Deze innovatie vereist naast een verwervings- en implementatieproces ook een vraagarticulatieproces, in nauw overleg met de industrie en dienstverleners. Er zijn in Nederland verschillende organisaties en samenwerkingsverbanden die dat – ook specifiek voor sensing – ondersteunen. Een voorbeeld is de stichting *Dutch Institute for Technology, Safety & Security* (DITSS).

### VOLWASSENHEID VAN SENSING

Een sensingconcept of -technologie is meer volwassen naarmate het aantal kinderziektes afneemt. Om de volwassenheid van een technologie uit te drukken zijn er verschillende schalen. De *Technology Readiness Level* (TRL) is een negenpuntsschaal, en is ook het bekendst, maar alleen geschikt om technologie in isolatie te beoordelen (Wikipedia, 2017).

In de jaren tachtig is het *capability maturity model* ontwikkeld in de ICT-wereld (Humphrey, 1988). Dat model beschrijft de kenmerken van een organisatie(onderdeel) in een vijftal stappen van maturiteit. Het begint bij ad hoc en reactief, en eindigt bij een proces dat zichzelf op beheerste wijze steeds verder verbetert.

Moderne sensing- en big data-systemen vragen echter om een meer integraal perspectief dan alleen technologie of organisatie. Daarom heeft men ook andere schalen bedacht, zoals het *Concept Maturity Level* (CML) een zespuntsschaal die in *Concept Development & Experimentation* (CD&E) wordt gebruikt. CD&E is een in NAVO-verband ontwikkeld innovatiemanagementproces. Het is buiten Defensie ook in gebruik om complexe innovatieprocessen in het veiligheidsdomein te helpen beheersen, bijvoorbeeld bij meerdere stakeholders (Weima, Huiskamp, Hasberg, & van der Wiel, 2010).

## PRINCIPE 7
# SENSING WAARDEREN OP EFFECTEN

Bij een investeringsbeslissing in sensing hoort ook een onderbouwde waardering van de effecten. Dezelfde camera als onderdeel van cameratoezicht kan, mits goed geïmplementeerd in een integraal veiligheidsbeleid, bijdragen aan zowel preventie, repressie als herstel van incidenten. Dat onderbouwen kan op verschillende manieren, waarbij het veel uitmaakt welke potentiële effecten men in de beschouwing opneemt. Immers, als de maatschappelijke business case niet compleet is, dan worden investeringen in sensing dus niet op waarde geschat en/of zullen kosten bij de verkeerde partijen worden belegd. Sensinginnovaties komen dan niet van de grond of gaan wanneer de subsidie opdroogt alsnog ten onder.

**VARIATIE 1**

In een eerste variant kijkt men puur naar de interne effecten op de bedrijfsvoering. Een investering in sensing meet men dan bijvoorbeeld af aan de mate waarin dit bestaande werkprocessen efficiënter maakt.

**VARIATIE 2**

In een tweede variant weegt men mee dat de uitvoerende veiligheidsorganisatie een extern doel heeft, namelijk veiligheid ‘produceren’. Vervolgens worden de effecten van de investering op de kans en impact van incidenten meegewogen, belangrijke onderdelen van de effectiviteit van veiligheidsmaatregelen.

**VARIATIE 3**

In de meest genuanceerde variant neemt men ook indirecte en neveneffecten van risicobeheersing mee, zoals (de beleving van) hinder veroorzaakt door veiligheidsmaatregelen, het effect op de risicoperceptie van burgers (of klanten) en de mogelijkheid om als gevolg van de investering de schade op anderen te verhalen (zoals de dader).





### MAATSCHAPPELIJKE BUSINESS CASE VAN SENSING

Sensing kan op allerlei manieren bijdragen aan een maatschappelijke business case, vast te stellen middels een kosteneffectiviteitsanalyse. Maar wat zijn dan de (potentiële) positieve en negatieve effecten van sensing? Sommige voorbeelden hieronder zijn hypothetisch.

- Minder incidenten, bijvoorbeeld minder overvallen doordat overvallers zich laten afschrikken door sensoren. De keerzijde is het chilling-effect, goedbedoelende burgers die zich in hun vrijheid ingeperkt voelen.
- Minder impact van incidenten: minder heftige agressie tegen medewerkers uitgerust met bodycams.
- Meer zakelijke transacties: meer reizigers kiezen voor een efficiënt werkende security check met intelligente sensoren die vroegtijdig de laagrisicoreizigers signaleren.
- Meer zakelijke transacties: reizigers kiezen voor wat zij zien als een goed werkende security check met geavanceerde sensoren.
- Minder restschade: sensordata maakten het mogelijk om een andere partij aansprakelijk te stellen.
- Efficiëntere beveiliging door minder directe kosten: minder mensen nodig om een automatische melding te verifiëren.
- Efficiëntere beveiliging door minder indirecte kosten: intelligente sensoren nemen het stressvolle deel van het werk over.

Het doel van een sensinginnovatie kan elk van deze effecten zijn, maar dat neemt de andere effecten niet weg. De effecten moeten dus als het ware worden ‘geclaimd’ door het juiste innovatietraject.

**DEZELFDE CAMERA ALS ONDERDEEL VAN CAMERA-TOEZICHT KAN BIJDRAGEN AAN ZOWEL PREVENTIE, REPRESSIE ALS HERSTEL VAN INCIDENTEN**

# HOE INNOVEER JE OP HET GEBIED VAN SENSING?

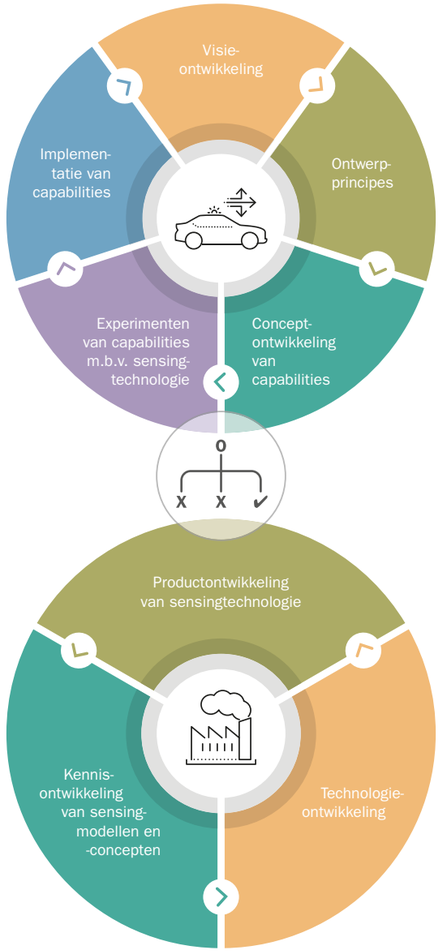
Hoe start je een verandering op het gebied van sensing? In dit hoofdstuk geven we daar drie handvatten voor op het gebied van het proces, de proefomgeving en de regie.





## HET PROCES

Het proces moet in ieder geval bestand zijn tegen een valse start, een verkeerde afslag of een te lange pauze. Een manier om dit te ondervangen is om het innovatie-proces cyclisch te laten zijn. Innoveren is dus geen lineair proces, en op het gebied van sensing al helemaal niet. Er zijn namelijk altijd tegelijkertijd meerdere actoren bezig om hun visie te realiseren: industrie, informatiepartners, het ministerie en ook andere (uitvoerende) veiligheidsorganisaties. Het kan helpen om rond een concreet innovatieproces drie verschillende clusters te onderscheiden: de innoverende partij (i.e. de uitvoerende veiligheidsorganisatie zelf), de aanbieder van innovaties (industrie of interne leveranciers) en de neutrale derde. Ieder van deze clusters speelt een unieke en essentiële rol in het realiseren van de innovatie, en dus ook in het realiseren van een visie op sensing. Waar deze partijen samenkomen, kan geëxperimenteerd worden. Bijvoorbeeld in een proefomgeving.




FIGUUR 2

De ontwikkeling en implementatie van nieuwe sensingcapabilities verloopt in meerdere niet-lineaire processen

# PROEFOMGEVING

## EEN SUCCESVOLLE PROEFTUIN WORDT AFGEROND ZODRA DE VERANDER-DOELEN ZIJN BEHAALD

Een proeftuin is een praktijkomgeving waarin verschillende experimenten plaatsvinden, en waarbinnen de risico's die inherent zijn aan innovatie expliciet worden beheerst. Een proeftuin kan instrumenteel zijn om sensinginnovaties te waarderen, om te kunnen bepalen welke voortgang er wordt gemaakt, om samen met innovatiepartners te leren van de uitdagingen die voorbijkomen en om tijdig successen te claimen.

Daarbij dient te worden voorkomen dat de proefomgeving leidend gaat worden. Het is slechts een tijdelijk middel om bepaalde veranderdoelen te behalen. De governance, het businessmodel (hoe stroomt het geld) en de wijze van evalueren van experimenten zijn daarbij essentieel. Als de governance en wijze van evalueren goed zijn, dan is het goed mogelijk om selectief innovaties al vroeg op te pakken en daarmee als organisatie meer wendbaar te worden.

Het organisatieonderdeel dat die veranderdoelen heeft, en waar die veranderingen en innovaties moeten gaan landen, moet ook eigenaar zijn van de proeftuin. Die veranderdoelen moeten dus niet door een veranderprogramma (aan de proeftuin) worden gesteld – zij is immers slechts uitvoerder.

In 2004 stelden ADO Den Haag en de gemeente Den Haag vast dat het wenselijk was om de bouw van een nieuw stadion te overwegen. Voor een betere beheersing van de objectieve en subjectieve veiligheid moest een nieuw crowd management-concept worden ontwikkeld. Zowel in het oude stadion in het Zuiderpark (op TRL 6), als in het nieuwe stadion bij het Prins Clausplein (op TRL 7-9) werden diverse experimenten uitgevoerd door ADO, de industrie, politie en TNO. Doordat ADO en de gemeente zich als eigenaren van deze ontwikkeling opstelden werd het mogelijk om dit concept bij de overgang naar het nieuwe stadion geleidelijk in de praktijk te implementeren.





Vanaf 2007 tot 2014 bood het Utrechtse Centrum voor Innovatie en Veiligheid (CIV) de mogelijkheid om in de regio Utrecht experimenten te doen. Bijvoorbeeld op het gebied van sensing in het winkelcentrum Kanaleneiland, met medewerking van de cameratoezichtruimte aldaar. TNO voerde hier samen met de industrie, Koninklijke Marechaussee en politie experimenten uit op TRL 5 en 6, onder meer met geluidssensoren en intelligente camera's.

In de governance van een proeftuin moeten innovaties integraal worden beschouwd: niet alleen de veranderingen op technologisch gebied, maar ook die in de informatiestromen, de organisatie, het personeel en het juridisch kader. Om dat te ondersteunen kunnen de experimenten gegroepeerd worden in functionele bouwstenen, die de integraliteit van deeloplossingen bewaken.

Een proeftuin is representatief voor alle omgevingen waar de verandering daarna moet gaan landen. In elk geval moet duidelijk zijn op welke manier de proeftuin daarin anders is, en wat dus mogelijk nog voor onzekerheid gaat zorgen.

Om mogelijke barrières zo vroeg mogelijk te identificeren maakt de proeftuin waar mogelijk gebruik van de bestaande middelen en infrastructuur van de uitvoerende veiligheidsorganisatie. Daarbij wordt ook rekening gehouden met de verwervingsstrategie die tussen de proeftuin(fase) en de implementatie in zit.

Een succesvolle proeftuin wordt afgerond zodra de veranderdoelen zijn behaald. Dit voorkomt ook mission creep en zorgt er voor dat de verwervingsstrategie normaal kan verlopen.

Vanaf 2012 tot 2015 voerden de Koninklijke Marechaussee, de politie en TNO het programma Experimenteeromgeving Bewaken en Beveiligen uit. Op een afgeschermde locatie van Defensie voerde men experimenten uit op het gebied van objectbeveiliging van hoogrisico-objecten, zoals bedoeld onder het centrale deel van het stelsel Bewaken en Beveiligen. Op basis van *off-the-shelf*-technologie werden in totaal twaalf innovatieve concepten, waaronder vijf sensingconcepten, uitgeprobeerd op TRL 6 en 7. De implementatie van de resultaten werd overgelaten aan respectievelijk de Koninklijke Marechaussee en de politie.

## REGIE
## OPEN INNOVATIE EN VRAAGSTURING

**VRAAGT SENSING EEN APARTE ORGANISATIE-STRUCTUUR BINNEN EEN UITVOERENDE VEILIGHEIDS-ORGANISATIE?**

Open innovatie is het combineren van interne en externe bronnen (zoals een proefomgeving) voor zowel de ontwikkeling als het vermarkten van nieuwe technologieën en producten. Organisaties kunnen hiertoe overgaan om:

- ervoor te zorgen dat men minder afhankelijk wordt van de kwaliteit van de eigen onderzoeksafdeling
- via partners (extra) te profiteren van resultaten van de eigen afdeling (die men zelf niet nodig heeft)
- te profiteren van de onderzoeksresultaten van anderen

Belangrijke blokkades voor open innovatie zijn onduidelijke afspraken over intellectueel eigendom, over eerlijke concurrentie en – in het veiligheidsdomein – regels met betrekking tot rubricering. Paradoxaal genoeg vereist open innovatie dus vaak juist een gesloten ecosysteem waarbinnen duidelijke regels gelden, en de uitsluiting van partijen die mogelijk een oneerlijk concurrentievoordeel kunnen verkrijgen.

Met zo veel partijen die vanuit zo veel verschillende soorten rollen actief zijn in sensing dreigt het gevaar dat goede vraagarticulatie en vraagsturing in de knel komen. Immers, er zijn veel partijen die op basis van deskundigheid mee zouden kunnen praten. Het vergt modern en inspirerend leiderschap van uitvoerende veiligheidsorganisaties om daar effectief mee om te kunnen gaan. Hopelijk helpt deze publicatie daarbij.

Een belangrijk thema daarin is wat er nu eigenlijk leidend moet zijn: het technologisch aanbod of de behoeftestelling van de uitvoerende veiligheidsorganisatie? Daar zou echter geen twijfel over mogen bestaan. Een goed geïnformeerde en capabele behoeftesteller moet op de hoogte zijn van de (on)mogelijkheden van zowel de eigen organisatie als van de technologie. Hij weet welke belangen en krachten er van invloed zijn op de partijen waarmee hij samen zal moeten werken om zijn doelen te realiseren.





Een andere vraag is of sensing en bijbehorende capabilities om een aparte organisatiestructuur (een afdeling, project of programma) vragen binnen een uitvoerende veiligheidsorganisatie, hoe deze is ingericht, en wat diens opdracht en mandaat is. Sensing is een zich snel ontwikkelende specialisatie die als enige objectieve informatie kan verzorgen. Dat is voor sommige uitvoerende veiligheidsorgansiaties voldoende reden om er een apart ontwikkelprogramma op te zetten.

Vanuit het idee dat sensing slechts een ondersteunende capability is, is een infrastructurele benadering te verkiezen, in tegenstelling tot een stovepipe-benadering. Sensing wordt dan als onderdeel van de informatievoorzieningen gezien, en omvat praktisch alle sensingvarianten binnen de organisatie. Maar er kunnen ook andere overwegingen zijn, bijvoorbeeld vanuit de wens om bepaalde complexiteit of aanlooprisico's te vermijden of om op korte termijn duidelijk zichtbare resultaten te behalen.

De middenweg is om eerst vanuit een breder sensingperspectief een aantal sensingprincipes te identificeren, zodat er een basis ligt voor alle betrokkenen, om vervolgens zelf bepaalde sensingcapabilities te prioriteren, zodat men daarmee de ontwikkeling van innovatieve capabilities kan initiëren die voor meerdere veiligheidsvraagstukken nuttig zijn. Deze benadering is toekomstbestendig doordat zowel rekening wordt gehouden met de grote trends als met de kortetermijnaanleidingen.

**DEZE BENADERING IS TOEKOMST-BESTENDIG DOORDAT ZOWEL REKENING WORDT GEHOUDEN MET DE GROTE TRENDS ALS MET DE KORTETERMIJN-AANLEIDINGEN.**

# MET WIE SAMENWERKEN?

De laatste vraag uit de veranderredenering is: ‘(met) wie veranderen?’. Om de ontwikkeling van sensing richting te geven (zie hoofdstuk 3) en om uiteindelijk relevante innovaties te ontwikkelen (zie hoofdstuk 4) is samenwerking onontbeerlijk. We identificeren in dit hoofdstuk de typen partijen die daarvoor nodig zijn.

Deze samenwerking is zowel binnen de uitvoerende veiligheidsorganisatie relevant als met partners van andere organisaties en partijen (de ketenpartners). Interne partners zijn bijvoorbeeld leidinggevenden en vertegenwoordigers van uitvoerend personeel, of van een bepaalde (technische) afdeling of dienst. Maar ook de collega’s op de werkvloer die bijvoorbeeld mogelijk via hun privéleven of samenwerking met andere organisaties al vroeg in aanraking komen met nieuwe technische middelen.

Externe partners zijn echter net zo belangrijk. Bijvoorbeeld, voor het opbouwen en in stand houden van een sensing-capability bij uitvoerende veiligheidsorganisaties is het nodig dat de daartoe benodigde producten en diensten ergens beschikbaar zijn of gaan komen. Ook helpt het als er partners meedoen die met enige afstand en abstractievermogen naar het veranderproces kunnen kijken. Vanuit de uitvoerende veiligheidsorganisatie bezien zijn er vier belangrijke soorten relaties die ze kan hebben met haar omgeving.





## PARTNERS BINNEN DE PRODUCTIEKETEN

Ten eerste is er de productieketen van organisaties die halffabricaten, producten, systemen en diensten leveren voor sensoren en hun systemen. Bij uitvoerende veiligheidsorganisaties is de vraagzijde vaak belegd bij het organisatieonderdeel dat over de informatievoorzieningen gaat, ondersteund door een afdeling inkoop. Gaat het om publieke organisaties, dan gelden vanaf een bepaald bedrag aanbestedingsregels.

## PARTNERS BINNEN EEN INFORMATIENETWERK

Ten tweede is er het informatienetwerk tussen burgers, private dienstverleners (zoals een beveiligingsbedrijf of een bedrijf in sociale media), overige overheidsdiensten (zoals de belastingdienst), de uitvoerende veiligheidsorganisatie (zoals de politie) en haar zuster(veiligheids)organisaties (in het geval van de politie bijvoorbeeld het OM). Ieder van deze partijen kan een technische sensor in beheer hebben, die voor de uitvoerende veiligheidsorganisatie relevante informatie kan genereren. Afspraken tussen partijen over het delen en gebruiken van die informatie kunnen op allerlei manieren vastgelegd zijn, in contracten, in Service Level Agreements (SLA), of soms helemaal niet, zoals tussen burgers die via sociale media relevante (veiligheids)informatie met elkaar delen.

## PARTNERS VANUIT TOEZICHTS- EN REGIEROLLEN

Naast deze twee ketens zijn er ook partijen die zich bezighouden met de invulling en bewaking van de randvoorwaarden. Dit zijn regulerende en regievoerende partijen (bijvoorbeeld ministeries) en toezichtorganen (zoals de Autoriteit Persoonsgegevens). Ook zijn er aparte organisaties gespecialiseerd in standaardisering en certificering.

## PARTNERS VANUIT KENNIS- EN INNOVATIENETWERKEN

Ten slotte zijn er ook diverse kennisinstellingen en consultancybedrijven die kennisproducten leveren om de beleidscyclus te ondersteunen. Zij zorgen dat alle partijen in de keten kunnen innoveren, in kortcyclische innovatieprocessen of meerjarige onderzoeksprogramma’s. Dit gebeurt altijd vanuit een van de drie rollen die nodig zijn voor een geslaagde innovatie. In de rol van governmental innovator worden (uitvoerende) veiligheidsorganisaties geholpen om (ondersteunende) sensingcapabilities te implementeren. Bijvoorbeeld door het schrijven van een aanbesteding voor een sensingdienst of -product. In de rol van innovation catalyst neemt men een neutrale positie in om (onderdelen van) het ecosysteem beter te helpen functioneren. Bijvoorbeeld door het schrijven van een visie of het opzetten van een nieuwe vorm van certificering van intelligente sensoren. In de rol van innovation factory bedenkt en ontwikkelt men sensingtechnologie. Dit gebeurt typisch op (indirect) verzoek van uitvoerende veiligheidsorganisaties, met als derde partner de industrie. Bepalend in deze laatste vorm van samenwerking zijn voorschriften over vertrouwelijkheid en de internationale regels voor eerlijke concurrentie (zoals aanbesteding).

# VAN START

In de waaromvraag ligt de noodzaak besloten waarom uitvoerende veiligheidsorganisaties zich überhaupt op sensing willen ontwikkelen (zie hoofdstuk 2). Maar daarnaast is er de aanleiding om concreet in beweging te komen. Beide zijn nodig. Blindstaren op de grote trends geeft te weinig perspectief op concrete acties. Daarom geven we in dit hoofdstuk typische aanleidingen om van start te gaan. Zo'n lijstje helpt om alert te zijn op kansen om vooruitgang te boeken.

Maar let op: als alleen op basis van aanleidingen wordt gestuurd, dan zullen de oplossingen niet toekomstbestendig zijn. Wat bijvoorbeeld als er een nieuwe aanleiding opduikt voordat de oplossing voor een vorige is gerealiseerd?

ALS ALLEEN OP BASIS VAN AANLEIDINGEN WORDT GESTUURD, DAN ZULLEN DE OPLOSSINGEN NIET TOEKOMST-BESTENDIG ZIJN

## AANLEIDINGEN OM VAN START TE GAAN

Het zetje om in beweging te komen ligt typisch meer in één van de volgende aanleidingen:

1. Verandering in het dreigingsbeeld: dit is de meest voor de hand liggende aanleiding om te innoveren, omdat dit het bestaansrecht van uitvoerende veiligheidsorganisaties direct raakt. De veranderende terroristische dreiging vraagt om andere vormen van sensing dan high-impact criminaliteit.
   Deze aanleiding wordt ook wel eens cynisch omschreven als *'never waste a good crisis'*.
2. Veroudering van kapitaalintensieve middelen: is ook een aanleiding voor innovatie. Bijvoorbeeld vervanging van defensiematerieel (bijvoorbeeld de F16) is dan de aanleiding om tegelijkertijd een vernieuwing van de capabilities voor luchtdominantie door te voeren. Gaat een veiligheidsorganisatie van analoge netwerken en sensoren naar digitaal, dan innoveren de opslag en verwerking van data en metadata mee.

Voorbeeld van risicogestuurd optreden: een grensbewakingsorganisatie wil de stroom van reizigers en goederen zo weinig mogelijk verstoren, maar moet wel bepaalde controles uitvoeren. Binnen de grenzen van de wet maakt zij op basis van o.a. actuele sensordata een situationele inschatting van de dreiging die van bepaalde reizigers uitgaat. Op basis van die inschatting kunnen bepaalde reizigers sneller door de controles heen, terwijl het restrisico over de hele stroom reizigers hetzelfde blijft. Die dreigingsinschatting moet accuraat, uitvoerbaar en doeltreffend zijn.

3. Een verandering in het takenpakket: als de uitvoerende veiligheidsorganisatie een ander takenpakket krijgt, dan zijn daar logischerwijs ook andere middelen voor nodig. Dit kan aanleiding zijn om de huidige capabilities en middelen te herzien. Dit kan gebeuren als taken verschuiven tussen organisaties, of als de samenleving zodanig verandert dat bepaalde taken compleet verdwijnen of er juist bij komen. Dit zou bijvoorbeeld kunnen gebeuren naar aanleiding van de introductie van zelfrijdende auto's.
4. Het vermoeden dat bepaalde innovaties, zoals het gebruik van nieuwe technologie, een verbetering zijn. Een symptoom: medewerkers die hun werk doen met privé aangeschafte sensingmiddelen, zoals een privésmartphone of GoPro.
5. Ontwikkelingen in de professie zelf: zoals de groeiende aandacht voor risicogestuurd optreden: er staan als het moet, relaxed als het kan. Dit vraagt om bredere inzet van sensingmiddelen voor een actueel beeld van de situatie, naast dynamische inzet om recht te doen aan de belofte van proportionaliteit: als het niet nodig is, dan ook geen gebruik van invasieve sensingmiddelen. De opkomst van exponentiële organisaties gebaseerd op moderne ICT, gestandaardiseerde koppelvlakken en big data heeft ook gevolgen voor veiligheidsorganisaties. Deze zien zich uitgedaagd om de lijnen van Uber, AirBNB en Google te volgen.

## BLINDSTAREN OP DE GROTE TRENDS GEEFT TE WEINIG PERSPECTIEF OP CONCRETE ACTIES. EEN LIJSTJE MET AANLEIDINGEN HELPT OM ALERT TE ZIJN OP KANSEN OM VOORUITGANG TE BOEKEN

In sensing voor veiligheid was de introductie van IP-technologie disruptief voor de installatiebranche die zorgde voor de surveillancesystemen. Digitale onderdelen zoals sensoren en ICT vinden was nog gemakkelijk. De uitdaging werd groter toen ze hun producten niet meer in stovepipes moesten opleveren maar als onderdeel van een groter geheel (een system-of-systems), soms zelfs verbonden aan het internet. Bijvoorbeeld, waar ze voorheen Closed-Circuit Television (CCTV) konden leveren, moest dat nu een Video Surveillance System (VSS) zijn dat als onderdeel van een Physical Security Information Management-systeem (PSIM) moest kunnen draaien. Omdat digitale systemen kwetsbaarder bleken voor cyberaanvallen, moesten ze hier ook in hun dienstverlening rekening mee gaan houden. Dit betekende vaak andersoortig personeel en aanvullende diensten, zoals een informatiebeveiligingsaudit.





Eén van de primaire functies van private beveiligingsbedrijven is de verificatie van alarmen uit geautomatiseerde detectiesystemen, zoals inbraak- en brandmeldsystemen. Dit model is gebaseerd op de aanname van de alarmeigenaar dat die verificatie binnen korte tijd gebeurt, en met een bepaalde kwaliteit. Het is goed denkbaar dat iemand een vraag- en aanbodplatform ontwikkelt waarop alarmeigenaren *per alarm* een verificatievraag kunnen neerleggen. Partijen die kunnen verifiëren, kunnen vervolgens bieden op de vraag. De beste aanbieder krijgt het recht om te verifiëren en wordt daarvoor betaald. Dat kan een omwonende zijn of iemand die toevallig in de buurt is. Dit is disruptief voor het traditionele businessmodel van private beveiligers.

In ditzelfde scenario is het eveneens denkbaar dat het legaal wordt om autonome voertuigen de weg op te sturen voor het afhandelen van meldingen. Een bedrijf dat autonome voertuigen verhuurt kan deze dus ook op rustige momenten inzetten om automatische meldingen te verifiëren op bedrijventerreinen en in woonwijken. Opnieuw een disruptief vooruitzicht voor het businessmodel van private beveiligers.

Het is ook mogelijk dat de invulling van sommige functies van uitvoerende veiligheidsorganisaties fundamenteel verandert. Het fenomeen *do-it-yourself policing* betekent bijvoorbeeld dat burgers zelf activiteiten gaan ondernemen die traditioneel voorbehouden zijn aan de politie. Burgerwachten die gebruikmaken van berichtendiensten zoals WhatsApp. Burgers die opsporingsdossiers aanmaken met soms verrassend degelijke en uitvoerige analyses. Hoe lang zal het nog duren voordat er een *open source, crowd-funded* softwarepakket op de markt komt waarmee burgers zelf opsporingsdossiers kunnen samenstellen die voldoen aan de kwaliteitseisen van het OM?

### HET LAATSTE ZETJE

Naast de eerder beschreven redenen om te innoveren is er nog een laatste cruciaal motief: de uitvoerende veiligheidsorganisaties moeten relevant blijven in een samenleving waarin de ontwikkelingen in sensor- en informatietechnologie steeds sneller gaan. Die relevantie moet dus niet alleen blijken uit een juridisch kader ('ze zijn de enigen die dit mogen'), maar ook uit de feitelijke effectiviteit ('ze boeken de nodige resultaten').

Sensingontwikkelingen kunnen immers disruptief zijn. Een disruptieve innovatie voorziet nog steeds in dezelfde behoefte, maar doet dat op een fundamenteel andere manier, waardoor er een compleet nieuw type veiligheidsorganisatie nodig is. De steeds snellere ontwikkelingen in de technologie vergroten de kans dat een organisatie – dus ook uitvoerende veiligheidsorganisaties, hun partners en hun leveranciers – te maken krijgen met disruptie.

# PERSPECTIEF

JIMMY TROOST Trekker Bedrijfsleven Roadmap Security HTSM Topsectoren

De ontwikkelingen in sensing technologie gaan razendsnel en maken toepassingen mogelijk waar we nog maar enkele jaren geleden slechts van konden dromen. De toenemende connectiviteit draagt daar mede aan bij. Op afstand kunnen veel verschillende dingen waargenomen worden en door deze waarnemingen op een slimme manier bij elkaar te brengen komen scenario's binnen handbereik die we vroeger alleen kenden uit science fiction films.

Die nieuwe scenarios leiden ook tot meer complexiteit. Niet alleen technisch, maar ook organisatorisch. Neem het gebruik van lokatiegebonden camerabeelden voor toegangscontrole en bewakingsdoeleinden, die door een menselijke gebruiker worden geïnterpreteerd. Camera's en onderliggende technologie worden al decennia gebruikt. We weten ook dat als het aantal camera's in en rond een object te groot wordt, de grenzen bereikt worden van wat menselijke waarnemers binnen een bepaald tijdsbestek kunnen verwerken.

Het omzetten van beelddata in bruikbare informatie komt daarmee onder druk te staan, immers een menselijke waarnemer is nodig om deze vertaalslag te maken. Tegenwoordig hangen hele steden en ons wegennet vol met camera's voor allerlei doeleinden. Het aantal instanties dat afnemer is van beelddata neemt toe, evenals de gebruikers die hiervan informatie maken binnen de specifieke gebruiksdoelstellingen. Deze informatie wordt binnen instanties afgehandeld, er worden beslissingen genomen en vervolgacties uitgezet die de onderliggende bedrijfsprocessen beïnvloeden. Het innoveren op het gebied van sensing is dus niet zozeer een exclusieve kwestie van sensortechnologie, maar heeft verstrekkender gevolgen in de bedrijfsvoering van instanties. Het betrekken van kennis over het menselijk functioneren en van algemene en specifieke bedrijfsprocessen is daarom essentieel voor het slagen van initiatieven.

Dit geldt zonder meer ook voor het veiligheidsdomein, dat onder invloed van de veranderende geopolitieke situatie waaronder terrorisme, meer zal moeten innoveren. Op Europees niveau kennen we het "Secure Societies" H2020 onderzoeksprogramma en in Nederland de maatschappelijk uitdaging "Veilige Samenleving" en binnen de topsector "High Tech Systems en Materialen" de Security roadmap. Dit zijn dynamische netwerken - met zowel vraag- als aanbodzijde aan boord - die een voedingsbodem vormen voor allerlei interessante innovaties binnen het veiligheidsdomein. Deelname aan deze netwerken levert kansen en toegevoegde waarde aan betrokkenen en belanghebbenden in het veiligheidsdomein, van welke signatuur dan ook. Maar hoe komen deze innovaties tot stand en wat komt erbij kijken? En wat bedoelen we eigenlijk met innovatie? Over wat innovatie is, zijn boeken volgeschreven en een paar opdrachten in een zoekmachine levert een grote variëteit aan aansprekende voorbeelden.

In deze publicatie is een andere invalshoek gekozen. Het geeft aan de hand van voorbeelden uit de praktijk weer hoe in een ecosysteem met verschillende spelers en belangen in de veiligheidsketen, aansprekende resultaten bereikt worden. De camera die de receptioniste gebruikt voor toegang tot het pand, is technologisch niet zo verschillend van de camera's die binnen het veiligheidsdomein gebruikt worden om steden en het wegennet te monitoren. De connectiviteit introduceert een organisatorische complexiteit die innovatie echt mensenwerk maakt – en dus ook betrokkenheid van de menswetenschappen vraagt.

Hopelijk heeft u deze publicatie met plezier gelezen. Wie gaat u er mee inspireren?

Delft, Mei 2018



**DEZELFDE CAMERA ALS ONDERDEEL VAN CAMERA-TOEZICHT KAN BIJDRAGEN AAN ZOWEL PREVENTIE, REPRESSIE ALS HERSTEL VAN INCIDENTEN**

# NAWOORD

KRISHNA TANEJA Directeur Nationale Veiligheid, TNO

De exponentiële groei van de in de samenleving aanwezige data gaat gepaard met een snelle ontwikkeling van sensoren die onder andere gebuikt worden voor waarneming, spraak- en geurherkenning, en detectie. Voor uitvoerende veiligheidsorganisaties zoals de politie biedt dit een enorme kans om de relatie met burgers, het informatieproces en de effectiviteit van de opsporing te versterken. Denk maar aan een toekomst waarin je als bestuurder van een auto met een camera wordt waargenomen en thuis een e-mail ontvangt dat de APK is verlopen of de verzekering niet is betaald. Denk aan heldere camerabeelden van een misdrijf die automatisch onderdeel uitmaken van het strafrechtdossier, of denk aan sensoren die mogelijke wapens en explosieven kunnen detecteren bij de organisatie van een evenement.

Tegelijkertijd vraagt deze kans ook dat de uitvoerende veiligheidsorganisatie waar kan maken waar zij voor staat, namelijk het naleven van de waarden van de rechtsstaat. Mensen verwachten dat aspecten als privacy en betrouwbaarheid bij de grote hoeveelheid data die straks worden verwerkt en opgeslagen worden gewaarborgd en dat het herkenbaar is wanneer zij als voorbeeld wel of niet door de overheid worden opgenomen met een camera. Uitvoerende veiligheidsorganisaties zoals de politie moeten hiervoor de komende jaren talloze vragen beantwoorden, zoals over de hoeveelheid data die de organisatie kan verwerken, over hoe men zorgt voor een herkenbaar profiel van de wijze waarop met sensoren wordt gewerkt, op welke wijze sensing kan worden gekoppeld aan dienstverlening en hoe de wetgever tijdig wordt gevraagd om aanpassingen in de wet aan te brengen?

Sensing is daarmee een grote kans voor de toekomst van uitvoerende veiligheidsorganisaties, maar tegelijkertijd vormt het op onderdelen een risico voor de waarden waar zij voor staan. Een landelijke aanpak, waarbij projectmatig wordt gewerkt aan de ontwikkelingen, is daarbij een belangrijke eerste stap voor de verdere ontwikkeling. Daarbij is het goed te blijven benadrukken dat de snelle technologische ontwikkelingen niet alleen iets vragen van het adaptief vermogen van de organisatie, maar ook vele kansen bieden. Data van sensoren die in een gesloten systeem werden gehouden, worden nu bijvoorbeeld steeds meer op basis van geprogrammeerde en transparante algoritmen ontsloten. Dat maakt het mogelijk om als uitvoerende veiligheidsorganisatie veel effectiever en met minder inzet van mensen en middelen te werken.

Het opstellen van deze visie is een belangrijke eerste stap op de lange weg die te gaan is. Ik wens uitvoerende veiligheidsorganisaties zoals de politie, de Koninklijke Marechaussee en operators van vitale infrastructuur daarbij toe dat verschillende gezichtspunten en kennis van zowel binnen als buiten de organisatie daarbij een plek krijgen. Als TNO leveren we hier, in nauwe samenwerking met universiteiten en bedrijven, graag een bijdrage aan.




**SENSING IS EEN GROTE KANS VOOR DE TOEKOMST VAN UITVOERENDE VEILIGHEIDSORGANISATIES, MAAR TEGELIJKERTIJD VORMT HET OP ONDERDELEN EEN RISICO VOOR DE WAARDEN WAAR ZIJ VOOR STAAN**

## VERANTWOORDING

De kennis in dit boekje is gebaseerd op tientallen jaren onderzoek op het gebied van sensing en aanverwante vakgebieden, in het bijzonder de projecten die onder het topsectorenbeleid zijn uitgevoerd (roadmap *security* van de topsector *high-tech systems and materials*).

Het opstellen van een visie (op sensing) is geen harde wetenschap, maar daarmee niet minder moeilijk. Die complexiteit wordt bepaald door het aantal variabelen (relevante trends, architectuurprincipes) en de breedte waarin een uitvoerende veiligheidsorganisatie haar omgeving wenst te beschouwen. Het is goed mogelijk om daar in te ver door te schieten, waardoor de visie vertekend raakt, of veel te gedetailleerd wordt.

Dit boekje bevat daarom slechts de belangrijkste ingrediënten die aan de hand van de vijf verandervragen zijn geïdentificeerd. In het bijbehorende TNO-rapport (J. van Rest, 2018) worden meer achtergrond en meer voorbeelden gegeven.

# REFERENTIES


Bennebroek Gravenhorst, K. (2015). De veranderversneller Academic Service.

Bouma, H., Baan, J., Burghouts, G. J., Eendebak, P. T., van Huis, J. R., Dijk, J., & van Rest, J. H. (2014). (2014). Automatic detection of suspicious behavior of pickpockets with track-based features in a shopping mall. Paper presented at the Optics and Photonics for Counterterrorism, Crime Fighting, and Defence X; and Optical Materials and Biomaterials in Security and Defence Systems Technology XI, , 9253 92530F.

Bouma, H., van Rest, J., van Buul-Besseling, K., de Jong, J., & Havekes, A. (2016). Integrated roadmap for the rapid finding and tracking of people at large airports. International Journal of Critical Infrastructure Protection, 12, 61-74.

Boyd, J. R. (1996). The essence of winning and losing. Unpublished Lecture Notes, 12(23), 123-125.

Council Regulation (EC). (2012). COM(2012) 11 final proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation). (). Brussels: EC.

Directive 95/46/EC of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive U.S.C. (1995).
Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

HCSS. (2017). Grote bewegingen, grote impact. eerste verkennende studie naar belangrijke trends en maatschappelijke vraagstukken voor de politie. ().HCSS.
Retrieved from https://hcss.nl/report/grote-bewegingen-grote-impact-eerste-verkennende-studie-naar-belangrijke-trends-en

Humphrey, W. S. (1988). Characterizing the software process: A maturity framework. IEEE Software, 5(2), 73-79.

JRC. (2018). ERNCIP thematic group on extended virtual fencing.
Retrieved from https://erncip-project.jrc.ec.europa.eu/networks/tgs/fencing

Politie. (2018). Live view.
Retrieved from https://www.politie.nl/themas/live-view.html

Europees verdrag voor de rechten van de mens, (1950).

Rest van, J. H. C., Boonstra, D., Everts, M., Rijn van, M., & Paassen van, R. (2014). Designing privacy-by-design. Privacy Technologies and Policy.Springer Berlin Heidelberg, , 55-72.

TACTICS Consortium. (2013). D3.1 TACTICS conceptual solution description. (). The Hague: TACTICS Consortium.
Retrieved from https://repository.tudelft.nl/view/tno/uuid:3f009a91-3888-41ba-8f0d-9522681419bc/

UK Home Office CAST. (2015). Image library for intelligent detection systems.
Retrieved from https://www.gov.uk/guidance/imagery-library-for-intelligent-detection-systems

van der Lee, M., Peters, C., & van Rest, J. (2014). Terugdringen nodeloze alarmen: Een literatuurstudie. ( No. TNO 2014 R11590).TNO.
Retrieved from https://repository.tudelft.nl/view/tno/uuid:19224231-a9e9-423e-82cc-0fd1ba4992b8/

Van der Steur, G. A. (2015). In Voorzitter van de Tweede Kamer (Ed.), Waarnemen met technische middelen. Den Haag: Ministerie van Veiligheid en Justitie.
Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2015/11/24/tk-waarnemen-met-technische-hulpmiddelen

Van der Steur, G. A. (2016). Kamerbrief met kabinetsstandpunt over WRR rapport. ( No. 2012877). Den Haag: Ministerie van Veiligheid en Justitie.
Retrieved from https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2016/11/11/tk-kabinetsstandpunt-over-wrr-rapport-big-data-in-een-vrije-en-veilige-samenleving/tk-kabinetsstandpunt-over-wrr-rapport-big-data-in-een-vrije-en-veilige-samenleving.pdf

van der Zee, S., Kleij, R., van Rest, J., & Bouma, H. (2016). Actuele ontwikkelingen in leugendetectie. Security Management, Maart, 2,

van Rest, J., Grootjen, F., Grootjen, M., Wijn, R., Aarts, O., Roelofs, M., . . . Kraaij, W. (2014). Requirements for multimedia metadata schemes in surveillance applications for security. Multimedia Tools and Applications, 70(1), 573-598.

van Rest, J. (2018). Sensing voor veiligheid. ().TNO.

Van Rest, J. H. C., Roelofs, M., & Van Nunen, A. (2014). Afwijkend gedrag: Maatschappelijk verantwoord waarnemen van gedrag in context van veiligheid– tweede herziene druk. no. TNO 2014 R10987. ().TNO.

Van Rest, J. H. C., & Weima, I. (2017). Sturen op risico's - een verkenning in het veiligheidsdomein. Den Haag: TNO.
Retrieved from https://www.tno.nl/media/9205/sturen_op_risicos_tno.pdf

Van Rest, J. H. C., Weima, I., Stolk, D., & Herder, A. (2017, Gezamenlijke bewaking en beveiliging in de (semi-)openbare ruimte. Magazine Nationale Veiligheid En Crisisbeheersing, 4
Retrieved from https://www.nctv.nl/onderwerpen_a_z/mnvc/index.aspx

Weima, I., Huiskamp, W., Hasberg, M., & van der Wiel, W. (2010). Concept maturity levels bringing structure to the CD&E process.

Wikipedia. (2017). Lemma technology readiness level.
Retrieved from https://en.wikipedia.org/wiki/Technology_readiness_level

Sensing is het vermogen van een organisatie om relevante informatie te verzamelen met behulp van sensoren, met de intentie tot opvolging. Met dit boekje plaatsen we sensing voor veiligheid in een maatschappelijke context. Een eenzijdige focus op meer data en informatie over burgers en bedrijven is niet de oplossing. Dat leidt alleen maar tot minder privacy en dus minder vrijheid. Uitvoerende veiligheidsorganisaties moeten meer dan ooit kunnen bepalen welke informatie ze wel én welke ze niet nodig hebben. We geven inzicht in wat er nodig is om zelf een visie op sensing te kunnen ontwikkelen ter ondersteuning van de uitvoering van operationele taken, gestoeld op expliciet beschreven principes die de relatie tussen maatschappij, uitvoerende veiligheidsorganisatie en technologie duiden. We laten tevens zien hoe uitvoerende veiligheidsorganisaties zelf tot een visie op dit zeer actuele onderwerp kunnen komen, zonder dat men vervalt in een welles-nietesdiscussie over kraaltjes en spiegeltjes. Sta je ons toe je daarbij te gidsen?

TNO innovation for life

**WWW.TNO.NL/SENSING**