Brassersplein 2
2612 CT Delft
Postbus 5050
2600 GB Delft

www.tno.nl

T +31 88 866 70 00
F +31 88 866 70 57

TNO-rapport

TNO 2014 R10864

Technologieradar Veiligheid 2014
Relevante technologische ontwikkelingen als input voor (kennis- en) innovatieagenda's

Datum	19 september 2014
Auteur(s)	ir. P.J. van Vliet, C.J.C. Smit-Rietveld, MSc, ir. H.F.B.F. Gelevert, Drs. M.P. Hasberg, ir. A.C. Kernkamp
Exemplaarnummer	
Oplage	
Aantal pagina's	56 (incl. bijlagen)
Aantal bijlagen	2
Opdrachtgever	NCTV en Nationale Politie
Projectnaam	Technologieradar Veiligheid
Projectnummer	060.06536

Alle rechten voorbehouden.
Niets uit deze uitgave mag worden vermenigvuldigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook, zonder voorafgaande toestemming van TNO.

Indien dit rapport in opdracht werd uitgebracht, wordt voor de rechten en verplichtingen van opdrachtgever en opdrachtnemer verwezen naar de Algemene Voorwaarden voor opdrachten aan TNO, dan wel de betreffende terzake tussen de partijen gesloten overeenkomst.
Het ter inzage geven van het TNO-rapport aan direct belanghebbenden is toegestaan.

© 2014 TNO

Samenvatting

Het verbeteren van de veiligheid in Nederland is het hoofddoel van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), de Nationale Politie en hun partners binnen het veiligheidsdomein. Innovatie vormt een essentieel element in het verwezenlijken van deze missie en draagt bij aan het continu verbeteren van de efficiëntie en effectiviteit van de afzonderlijke veiligheidsorganisaties en hun onderlinge samenwerking. Technologische ontwikkelingen en vernieuwingen zijn daarbij van cruciaal belang en vormen het onderwerp van het project Technologieradar Veiligheid, dat door TNO in opdracht van de NCTV en de Nationale Politie is uitgevoerd.

Dit rapport, dat de conclusies van TNO bevat, is één van de resultaten van het project. Het verschaft de lezer een overzicht van de technologische ontwikkelingen die voor de periode 2015 - 2019 als meest relevant zijn beoordeeld voor het verbeteren van de veiligheid in Nederland, in de vorm van een technologieradar. Het beschrijft – op hoofdlijnen – de relevantie en de mogelijke impact van deze technologieën voor het veiligheidsdomein en het stelt een aantal vervolgstappen voor. Het rapport dient daarmee als inspiratie- en voedingsbron voor de strategische innovatieagenda's en onderzoeksprogramma's van het ministerie van Veiligheid en Justitie (VenJ) en de Nationale Politie.

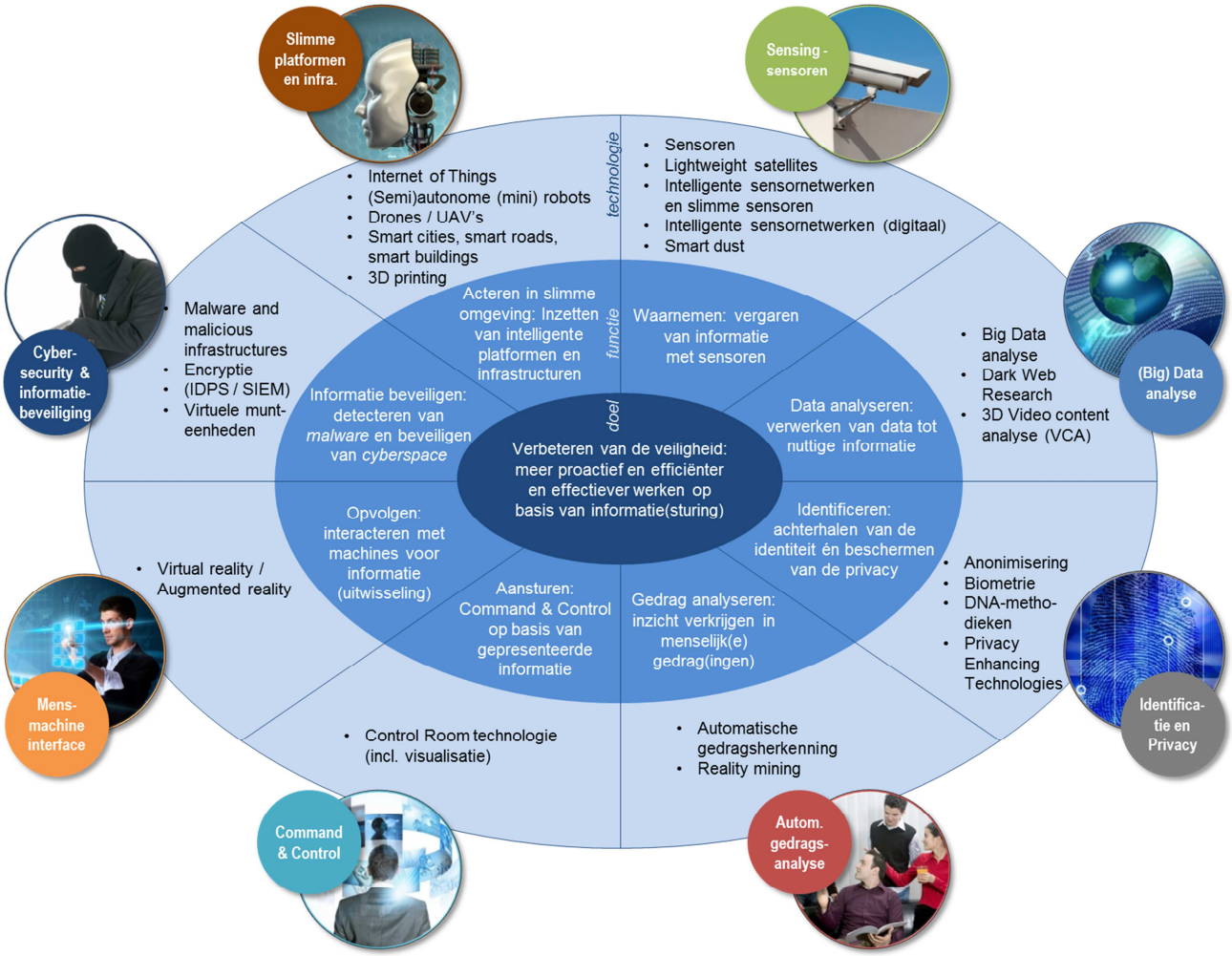
Naast de Technologieradar Veiligheid zoals gepresenteerd in dit rapport, heeft het project vier themaradars opgeleverd, die specifiek ten behoeve van de Nationale Politie zijn opgesteld voor vier door de politie gekozen thema's (*high impact crime*, ondermijning, *cybercrime* en dienstverlening). Deze themaradars gaan dieper in op de consequenties voor de operationele praktijk van de politie en zijn vastgelegd in vier afzonderlijke rapportages. Ook is in het project een adviesnota opgesteld over het actueel houden van de technologieradars en het via een gegevensbestand toegankelijk maken van de onderliggende informatie.

Genoemde resultaten zijn tot stand gekomen in nauwe samenwerking met de NCTV en de Nationale Politie. Het project is begonnen met een brede technologieverkenning, waarin op basis van een groot aantal bronnen een lange lijst van technologieën is opgesteld. Deze *longlist* beschrijft circa tweehonderd technologieën en is apart opgeleverd. Door middel van verschillende *workshops* met vertegenwoordigers van de NCTV en de Nationale Politie is hieruit door TNO een selectie gemaakt van de meest relevante technologieën voor de komende vijf jaar, en is in kaart gebracht welke impact de geselecteerde technologieën kunnen hebben voor de veiligheid in Nederland.

De in dit rapport opgenomen selectie van technologieën, de indicatie van hun relevantie en impact, en de per technologie voorgestelde vervolgstappen heeft TNO gebaseerd op een analyse van de tijdens het project verkregen informatie. Onder andere uit de *workshops* met veiligheidspartners bleek dat de komende jaren de nadruk binnen het veiligheidsdomein naar verwachting zal liggen op het meer proactief, efficiënter en effectiever werken op basis van informatie(sturing). De zesentwintig technologieën die een plek hebben gekregen op de Technologieradar Veiligheid zoals opgenomen in dit rapport, zijn dan ook voor een groot deel gerelateerd aan het verzamelen, toepassen, verwerken en presenteren van

informatie. De technologieën zijn gegroepeerd naar functionaliteit, waarbij is getracht zo nauw mogelijk aan te sluiten op functies zoals die door veiligheidsorganisaties worden verricht. Dit heeft geresulteerd in acht groepen van technologieën.

Onderstaande figuur vat de resultaten samen. Centraal in deze illustratie staat het doel van veiligheidspartners, namelijk het verbeteren van de veiligheid in Nederland, samen met de hierboven beschreven rode draad in de invulling daarvan voor de komende periode: efficiënter en effectiever kunnen werken op basis van informatie(sturing). De tweede ring bevat de acht functies die binnen het project zijn onderscheiden, en in de derde ring zijn de afzonderlijke technologieën opgenomen. De daadwerkelijke technologieradar, waarin de technologieën door TNO zijn gerangschikt naar relevantie en tijdshorizon, is in de hoofdtekst van dit rapport opgenomen.



Figuur 1 Overzicht van de in dit project onderscheiden relevante technologieën voor de komende vijf jaar, geordend naar functies in het veiligheidsdomein.

Inhoudsopgave

1 Inleiding

Het verbeteren van de veiligheid in Nederland is het hoofddoel van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), de Nationale Politie en hun partners binnen het veiligheidsdomein. Innovatie vormt een essentieel element in het verwezenlijken van deze missie en draagt bij aan het continu verbeteren van de efficiëntie en effectiviteit van de afzonderlijke veiligheidsorganisaties en hun onderlinge samenwerking. Innovatie is meer dan een korte termijn doel dat direct operationeel resultaat moet opleveren: het is ook een strategische keuze. Technologische vernieuwing speelt hierbij een belangrijke rol.

In het project 'Technologieradar Veiligheid', dat TNO gedurende het eerste halfjaar van 2014 heeft uitgevoerd in opdracht van en in nauwe samenwerking met de NCTV en de Nationale Politie, is een groot aantal voor het veiligheidsdomein belangrijke technologische ontwikkelingen in kaart gebracht en beoordeeld. Dat is zowel gedaan in de breedte als in de diepte, waarbij is gekeken naar de periode 2015 - 2019. De resultaten van het project zijn daarmee bedoeld als inspiratie- en voedingsbron voor de strategische innovatieagenda's en onderzoeksprogramma's van het ministerie van Veiligheid en Justitie en van de Nationale Politie.

Dit rapport is één van die resultaten en beoogt de lezer een overzicht te geven van de technologieën die in de komende vijf jaar naar verwachting het belangrijkst zullen zijn voor het veiligheidsdomein. Deze zesentwintig technologieën zijn op basis van de door TNO uitgevoerde analyse van de resultaten uit *desk research* en *workshops* geselecteerd uit een tijdens het project opgestelde *longlist*, die een kleine tweehonderd technologieën bevat, en in dit rapport weergegeven in de vorm van een technologieradar. De technologieën zijn daarbij gegroepeerd naar functionaliteit, waarbij is getracht zo nauw mogelijk aan te sluiten op functies zoals die door veiligheidsorganisaties worden verricht. Het rapport beschrijft – op hoofdlijnen – de relevantie en de mogelijke impact van deze technologieën voor het veiligheidsdomein en het bevat mogelijke vervolgstappen ten behoeve van de eerder genoemde innovatieagenda's en -programma's.

De opbouw van dit document is als volgt: in hoofdstuk 2 worden het project en de als onderdeel van het project opgeleverde rapporten toegelicht, evenals de aanpak die is gevolgd om tot deze resultaten te komen. Hoofdstuk 3 bevat een toelichting op de uit de analyse van TNO naar voren gekomen rode draad voor de komende vijf jaar en een vooruitblik op mogelijke langere termijn ontwikkelingen. Ook de gehanteerde structuur voor het clusteren van de technologieën naar functie wordt in hoofdstuk 3 toegelicht. Hoofdstuk 4 beschrijft de in de technologieradar opgenomen technologieën per functie en bevat onder andere voorbeelden van de (mogelijke) toepassing van de technologieën. In hoofdstuk 5 zijn de conclusies en aanbevelingen volgend uit de technologieradar opgenomen.

2 Het project ‘Technologieradar Veiligheid’

2.1 Doelstellingen en resultaten van het project

Technologie draagt in de operationele praktijk van de NCTV en de Nationale Politie bij aan een effectieve en efficiënte bedrijfsvoering en samenwerking met de andere veiligheidspartners. Technologie is dan ook een belangrijke aanjager voor vernieuwing en verbetering van de werkwijze van deze organisaties. Nieuwe technologieën leiden tegelijkertijd echter ook tot nieuwe kwetsbaarheden en bedreigingen van de veiligheid, bijvoorbeeld doordat ze door kwaadwillende personen kunnen worden ingezet voor criminele doeleinden. Het hebben van een goed en actueel inzicht in de technologische ontwikkelingen is om beide redenen van groot belang voor de NCTV en de politie.

Het project ‘Technologieradar Veiligheid’ had tot doel om de NCTV en de Nationale Politie te voorzien van dit inzicht, in de vorm van een overzicht van de belangrijkste technologieën die op ons afkomen, inclusief een beoordeling van de relevantie en impact van deze ontwikkelingen voor het veiligheidsdomein. In het project is daartoe een overzicht gemaakt van technologische ontwikkelingen en hun relevantie voor de veiligheid in Nederland. De door TNO tijdens het project als meest relevant beoordeelde technologieën voor de komende vijf jaar hebben een plaats gekregen op de ‘Technologieradar Veiligheid’, die het onderwerp van dit rapport vormt. De in het project gemaakte *longlist*, waaruit de technologieën op de technologieradar zijn geselecteerd, is apart opgeleverd.

Daarnaast zijn in het project vier themaradars opgesteld, waarbij voor elk van de thema’s een verdieping is aangebracht ten behoeve van de operationele praktijk van de politie. De politie heeft gekozen voor de thema’s *high impact crime*, ondermijning, *cybercrime* en dienstverlening. De vier themaradars zijn als op zichzelf staande rapportages opgeleverd, waarvan in de bijlagen van dit rapport een beknopt overzicht is opgenomen. Naast de Technologieradar Veiligheid en de vier themaradars heeft het project geresulteerd in een adviesnota over het actueel houden van de technologieradars en het via een gegevensbestand toegankelijk maken van de onderliggende informatie.

De resultaten van het project moeten de NCTV en de politie in staat stellen om onderbouwde keuzes te maken met betrekking tot de inzet van nieuwe technologieën en het volgen van technologische ontwikkelingen. Gezamenlijk dienen ze dan ook als bron voor de strategische innovatieagenda’s van VenJ en politie, en als inspiratie voor mogelijke onderzoeksprojecten.

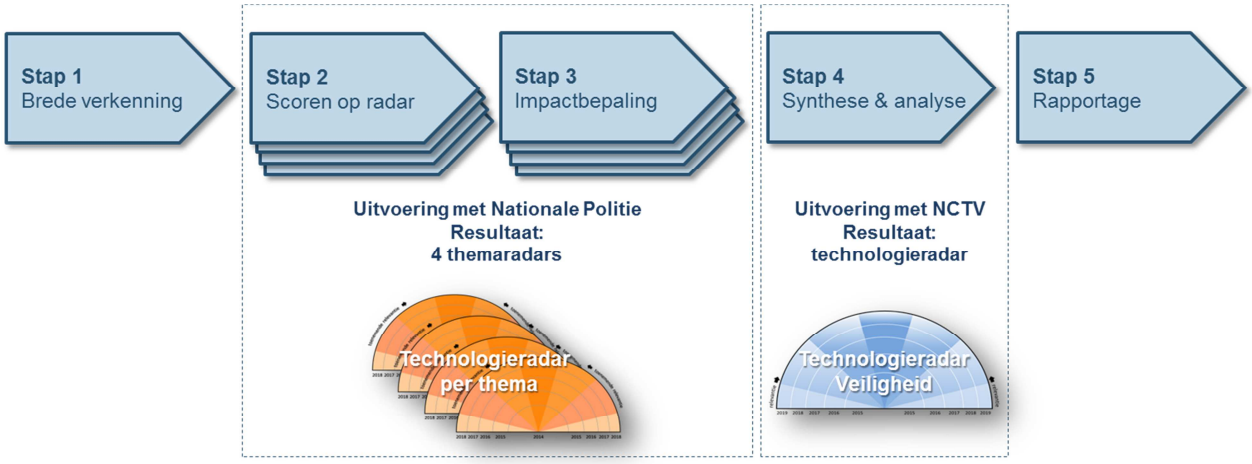
2.2 *Scope* van het project

De in het project opgeleverde technologieradars bestrijken de periode 2015 - 2019 en zijn gericht op het veiligheidsdomein, in lijn met de missie van de NCTV: ‘*De NCTV draagt bij aan een veilig en stabiel Nederland door dreigingen te onderkennen en de weerbaarheid en bescherming van vitale belangen te versterken. Doel is het voorkomen en beperken van maatschappelijke ontwrichting.’*

Onderwerpen als *cyber security*, contraterrorisme en crisisbeheersing vallen binnen deze *scope*. Ook maatschappelijke veiligheid in bredere zin is meegenomen in de beschouwingen: het als maatschappij bestand zijn tegen criminaliteit, radicalisering, terrorisme, brand, rampen en crises (zoals milieurampen, overstromingen, vliegrampen).

2.3 Binnen het project gevolgde methodiek

In het project is de in Figuur 2 aangegeven methodiek gevolgd.



Figuur 2 De in het project gevolgde methodiek.

In de eerste stap, de 'brede verkenning', is een brede inventarisatie gemaakt van technologische ontwikkelingen, die uiteenlopen van meer omvattende technologische trends tot specifieke technologische ontwikkelingen. Hiertoe is gebruik gemaakt van een groot aantal bronnen, zoals eerder door TNO opgestelde technologieradars en –verkenningen[1], internationale technologieverkenningen, studies en trendrapporten van onder andere Frost & Sullivan, Gartner, STT, HCSS, Rathenau en het UK Government Office for Science, projecten op het gebied van Key Enabling Technologies en (EU-) onderzoeksprogramma's, zoals het ETCETERA-project en het FESTOS-project. Dit heeft geresulteerd in de al eerder genoemde *longlist* met circa tweehonderd technologieën.

Op grond van een analyse van de geïdentificeerde ontwikkelingen heeft TNO in deze stap tevens een eerste clustering van technologieën naar functionaliteit aangebracht. In een eerste *workshop* met vertegenwoordigers van de NCTV is deze clustering aangescherpt en zijn de belangrijkste clusters bepaald (zie bijlage B). Later zijn deze clusters vertaald naar functies, waarbij is getracht zo nauw mogelijk aan te sluiten op functies zoals die door veiligheidsorganisaties worden verricht.

Vervolgens zijn in de stappen 2 en 3 de vier themaradars voor de Nationale Politie opgesteld. Voor stap 2 ('scoren op de radar') heeft de politie de vier al genoemde thema's gekozen, namelijk *high impact crime*, ondermijning, *cybercrime* en

[1] Onder andere het rapport *'Technologieverkenning Nationale Veiligheid'*, TNO, Analistennetwerk Nationale Veiligheid, 2013.

dienstverlening. In deze stap zijn ook de criteria voor het beoordelen van de relevantie van de verschillende technologieën vastgesteld. De volgende criteria zijn gekozen: de bijdrage van de technologie aan de beleidsdoelen; de mate waarin de technologie past binnen de organisatie; de kosten en baten; de maatschappelijke impact en het jaar waarin de technologie actueel is voor de organisatie. Met behulp van deze criteria zijn vervolgens de meest relevante technologieën voor de komende vijf jaar bepaald. Dat is per thema gedaan, in een *workshop* met bij dat thema betrokken vertegenwoordigers van de politie. Deze mensen waren zowel afkomstig vanuit de operationele praktijk als vanuit het innovatienetwerk en het management.

In stap 3 (‘impactbepaling’) is door middel van een tweede reeks *workshops* de impact van de geselecteerde technologieën voor de politie bepaald. Daarbij is onder andere gekeken naar de kansen en bedreigingen die de technologieën opleveren voor de operationele praktijk, en naar mogelijke vervolgstappen om deze technologieën daadwerkelijk toe te kunnen passen binnen de politie. Dit heeft geresulteerd in de vier themaradars, die zijn beschreven in aparte rapportages (zie bijlage A voor een samenvatting van de resultaten).

In stap 4 (‘synthese en analyse’) heeft TNO de resultaten uit de verschillende *workshops* met de politie samengebracht en gecombineerd met de inzichten zoals verkregen uit *desk research* en een tweede *workshop* met vertegenwoordigers van de NCTV. De bevindingen zijn vertaald in de technologieradar die in dit rapport is opgenomen. De selectie van technologieën, de indicatie van hun relevantie en impact en de voorgestelde vervolgstappen zijn dus gebaseerd op de in deze stap door TNO opgedane inzichten. Met andere woorden: de technologieradar bevat de technologieën die volgens TNO in de komende vijf jaar het meest relevant zullen zijn voor het veiligheidsdomein.

In stap 5 (‘rapportage’) zijn de resultaten van dit project vastgelegd in de verschillende rapporten en opgeleverd.

3 De Technologieradar Veiligheid

3.1 Rode draad voor de komende vijf jaar

Uit een analyse van de vier themaradars voor de politie en de uitkomsten van de *workshops* met vertegenwoordigers van de NCTV en de Nationale Politie, heeft TNO geconcludeerd dat veel van de technologische ontwikkelingen die de komende vijf jaar relevant zijn voor het verhogen van de veiligheid in Nederland gerelateerd zijn aan het verzamelen, toepassen, verwerken en presenteren van informatie. Het gaat dan specifiek om technologieën op het gebied van data-analyse, *Command & Control*, sensoren, *cyber security* en informatiebeveiliging, identificatie, slimme platformen en infrastructuur, mens-machine-interface en automatische gedragsanalyse. Rode draad in deze technologieradar is dan ook het meer proactief, efficiënter en effectiever werken op basis van informatie(sturing).

Genoemde onderwerpen hangen samen met het begrip ‘informatiemaatschappij’, waarin slimmer, sneller, effectiever en efficiënter werken met behulp van informatie- en communicatietechnologie centraal staat. Dit is een brede trend. Onze maatschappij bevindt zich nu en de komende tijd middenin de zogenoemde ‘*Information Age*’. Dit komt onder andere tot uiting in het altijd en overal online (willen) zijn van mensen, de ontwikkeling van autonome voertuigen, het gebruik van informatie in logistieke ketens, de ontwikkeling van *smart grids* in de energiesector, de proefnemingen met slimme dijken en wegen en de trend naar ‘*Intelligence Led Policing*’. Hieraan gerelateerde technologieën zullen de komende jaren volop worden doorontwikkeld en krijgen in deze technologieradar daarom veel aandacht.

Figuur 3 We bevinden ons middenin de ‘*Information Age*’.

3.2 Ontwikkelingen op de langere termijn

De vraag is wat er na de *Information Age* komt. Nanotechnologie, biotechnologie, informatietechnologie en neurowetenschappen (*cognitive science*) raken steeds verder met elkaar verweven in wat wel de NBIC-convergentie is gaan heten. Convergentie van technologieën leidt tot nieuwe toepassingen, zoals brein-machine-interactie en moleculaire geneeskunde. Misschien volgt op de *Information Age* daarom wel een *Brain Age*, waarin een verregaande integratie van informatietechnologie en neurotechnologie centraal staat.

Neurotechnologie is gericht op het beter begrijpen van de werking van de hersenen[2]. Wanneer hierover meer bekend is, wordt het mogelijk gedrag beter te begrijpen en wellicht zelfs te beïnvloeden. Het aanbrengen van technologische middelen in of aan het brein om hersenactiviteit 'af te tappen' of te sturen behoort dan misschien tot de mogelijkheden. Iets vergelijkbaars gebeurt bijvoorbeeld al in bepaalde medische toepassingen, waarbij kunstledematen direct door het brein worden aangestuurd. Ook het onlangs door het Amerikaanse DARPA-instituut[3] aangekondigde onderzoek naar de ontwikkeling van chips die in de hersenen kunnen worden aangebracht om posttraumatische stress, angst en depressies te kunnen detecteren, voorspellen en mogelijk zelfs te behandelen past in dit beeld.

Ook op andere terreinen spelen interessante ontwikkelingen, bijvoorbeeld op het gebied van de gen-, nano-, materiaal-, en energietechnologie[2,4]. Onder gentechnologie worden methoden en technieken verstaan waarbij organismen genetisch worden gemodificeerd om bepaalde producten te maken of te verbeteren. In de 'synthetische biologie' wordt hiervan gebruik gemaakt en kan met behulp van standaard stukjes DNA zelfs 'nieuw' DNA worden ontworpen. Bij genetische modificatie wordt het genoom van een organisme kunstmatig veranderd, op een manier die door voortplanting of natuurlijke recombinatie niet mogelijk is. Meestal worden één of enkele genen in het genoom van het ontvangende organisme ingebracht. Deze genen kunnen afkomstig zijn van eenzelfde soort organisme, maar er kunnen ook genen van andere soorten gebruikt worden. Gentechnologie kent vele toepassingsgebieden, zoals de landbouw, de gezondheidszorg, de levensmiddelentechnologie en de industrie. De mogelijke risico's van genetische modificatie worden al geruime tijd uitgebreid onderzocht, maar lang niet alle risico's zijn al duidelijk en er is veel discussie over de mogelijke lange termijneffecten.

Nanotechnologie is gericht op ontwikkeling van materialen en componenten die het formaat hebben van individuele atomen en moleculen. Ontwikkelingen in de nanotechnologie maken het dan ook mogelijk om doelgericht en gecontroleerd nieuwe, kleine structuren (met afmetingen kleiner dan 100 nanometer) op te bouwen uit atomaire of moleculaire bouwstenen[5]. Bijzonder van nanomaterialen is dat materialen op nanoschaal andere eigenschappen hebben dan op grotere schaal. Door op nano-formaat objecten te bestuderen en te manipuleren kunnen daardoor nieuwe materialen en systemen ontwikkeld worden, met unieke eigenschappen en functies. Denk bijvoorbeeld aan vuilafstotende of antimicrobiële oppervlakken, aan extreem resistente materialen of aan *coatings* die reageren op veranderende omgevingssituaties. Er zijn ondertussen al honderden toepassingen van de nanotechnologie bekend. Sommige daarvan zijn al commercieel verkrijgbaar, terwijl andere pas in de toekomst beschikbaar zullen komen.

Materiaaltechnologie bouwt onder andere voort op ontwikkelingen in de bio- en nanotechnologie en richt zich bijvoorbeeld op *high performance* materialen, functionele *coatings*, geavanceerde industriële materialen, elektronische en optische materialen, slimme materialen, biomaterialen en energie-materialen. Inzichten uit de nanotechnologie en materiaaltechnologie dragen bijvoorbeeld bij aan de ontwikkeling van slimme verpakkingen, die voedingsmiddelen beter

---

[2] *'Technologieverkenning Nationale Veiligheid'*, TNO, Analistennetwerk Nationale Veiligheid, 2013.
[3] Defense Advanced Research Projects Agency.
[4] '*Oog voor Innovatie - Een omgevingsanalyse voor de verzekeringssector'*, TNO, 2013.
[5] TNO, Dossier Nanotechnologie.

beschermen en conserveren en zo de voedselkwaliteit en -veiligheid helpen garanderen[6]. Ook maakt materiaaltechnologie het mogelijk bouwmaterialen te ontwikkelen die bijzondere eigenschappen hebben, zoals het vermogen om zichzelf te herstellen bij eventuele schade, of het vermogen om zichzelf te reinigen.

Ontwikkelingen in de energietechnologie zijn onder meer gericht op duurzame energiebronnen. Daarnaast wordt gekeken naar een herwaardering van bestaande technologieën, zoals verdere winning van fossiele brandstoffen (onder andere schaliegaswinning) en nucleaire energie (onder andere kernfusie). Onder de noemer van energietechnologie kunnen ook ontwikkelingen op het gebied van batterij-technologie worden geschaard. Zo wordt er gezocht naar alternatieven voor traditionele lood-zuur batterijen en worden batterijen steeds geavanceerder, onder andere ten aanzien van capaciteit, omvang, gewicht en levensduur. Ook wordt er gewerkt aan de ontwikkeling van zogenaamde '*biodegradable*' batterijen, die na verloop van tijd smelten of oplossen in het (menselijk) lichaam en daarom gebruikt zouden kunnen worden om slimme, invasieve medische instrumenten of apparaten van stroom te voorzien.

Veel van de ontwikkelingen die in deze paragraaf worden beschreven zal de lezer niet expliciet terugvinden in de in dit project gemaakte technologieradar. De reden daarvoor is tweeledig. Enerzijds wordt een grootschalige, operationele toepassing van veel van de onderliggende technologieën niet binnen de tijdshorizon van vijf jaar van de in dit project gemaakte technologieradar verwacht; de praktische toepassing door veiligheidsorganisaties ligt waarschijnlijk zelfs nog verder in de toekomst. Anderzijds geldt voor andere ontwikkelingen (waaronder die ten aanzien van *high performance* materialen, die al wel op grotere schaal worden toegepast), dat ze buiten de kern van de *Information Age* vallen, terwijl TNO concludeert dat juist deze rode draad de komende vijf jaar van groot belang zal zijn voor het veiligheidsdomein (zie paragraaf 3.1). Desondanks zijn enkele technologieën die zijn gerelateerd aan de ontwikkelingen in deze paragraaf toch terug te vinden in de technologieradar, omdat ze in verband met het voorbereiden van beleid al van belang (kunnen) zijn.

3.3 Clustering van technologieën naar functies

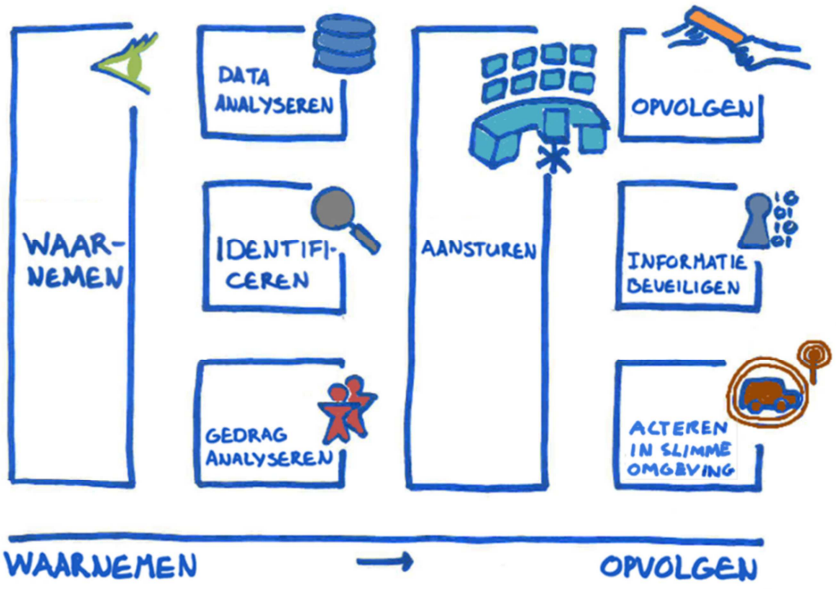
De technologieën op de technologieradar zijn gegroepeerd naar functionaliteit. Daarbij is getracht zo nauw mogelijk aan te sluiten op functies zoals die door veiligheidsorganisaties worden verricht.

De volgende acht functies zijn aldus gedefinieerd:

- *Waarnemen*: vergaren van informatie met sensoren;
- *Data analyseren*: verwerken van data tot nuttige informatie;
- *Identificeren*: achterhalen van de identiteit én beschermen van de privacy;
- *Gedrag analyseren*: inzicht verkrijgen in menselijk(e) gedrag(ingen);
- *Aansturen*: *Command & Control* op basis van de gepresenteerde informatie;
- *Opvolgen*: interacteren met machines voor informatie(uitwisseling);
- *Informatie beveiligen*: detecteren van *malware* en beveiligen van *cyberspace*;
- *Acteren in slimme omgeving*: inzetten van intelligente platformen en infrastructuren.

[6] '*Sectoral Innovation Foresight, Food and Drinks, Foresight study for Europe INNOVA Sectoral Innovation Watch',* Leis et al, 2010.

Figuur 4 geeft de samenhang tussen deze functies schematisch weer.



Figuur 4 Samenhang tussen de ten behoeve van de technologieradar onderscheiden functies.

Om meer proactief, efficiënter en effectiever te kunnen werken op basis van informatie, is het allereerst van belang te beschikken over data, ofwel om waar te nemen. Waarnemen betreft in dit verband dan ook het vergaren van data in zowel de fysieke als de virtuele wereld.

Het analyseren van de verkregen data is vervolgens nodig om te komen tot informatie die relevant is voor het vergroten van de veiligheid, bijvoorbeeld voor het verhogen van de *situational awareness* bij crisisbeheersing of voor het in kaart brengen van criminele netwerken bij de bestrijding van cybercriminaliteit. In het veiligheidsdomein zijn daarbij specifieke functionaliteiten van belang, namelijk het identificeren van mensen en het analyseren van (hun) gedrag.

De informatie wordt gebruikt om op strategisch, tactisch en operationeel niveau processen aan te sturen en om beslissingen te kunnen nemen, met andere woorden, voor *Command & Control*. Hieraan wordt – via de uitwisseling van informatie – opvolging gegeven in de vorm van maatregelen of operaties door de ketenpartners in het veiligheidsdomein. Acteren vindt plaats in een steeds ‘slimmer’ wordende omgeving, waarin intelligente platformen en infrastructuren kunnen worden ingezet. Het beveiligen van informatie speelt daarbij een belangrijke rol.

Het volgende hoofdstuk bevat een beknopte beschrijving van technologieën per functie. Daarin is per technologie aangegeven wat deze inhoudt en wat eventuele toepassingsmogelijkheden zijn voor het verbeteren van de veiligheid, ondersteund door voorbeelden van (mogelijke) toepassingen. Globaal worden bovendien vervolgstappen voorgesteld, per technologie. De beschreven technologieën verschillen soms enigszins in aggregatieniveau: afhankelijk van de betreffende ontwikkeling zijn sommige technologieën meer omvattend van aard terwijl andere specifieker gedefinieerd zijn.

4 Beschrijving van de technologieën per functie

4.1 Waarnemen

Vergaren van informatie met sensoren

Beschrijving van het cluster

Sensoren zetten omgevingsvariabelen om in een (elektrisch) signaal. Technologische ontwikkelingen zorgen ervoor dat er meer typen en kleinere sensoren beschikbaar komen. Koppelen van informatie van sensoren (‘sensorfusie’) levert extra informatie. Ontwikkelingen op het gebied van nanotechnologie en micro- en nano-elektromechanische systemen maken kleine sensoren die complexe analyses kunnen uitvoeren mogelijk, zoals een *lab-on-a-chip* waarin meet- en analysefuncties zijn geïntegreerd op één chip. Verdere ontwikkelingen gaan in de richting van sensoren op nanoschaal: moleculaire nanosensoren.

Slimme sensoren verzamelen en verzenden niet alleen gegevens, maar kunnen ook leren, zich aanpassen en configureren, en gegevens valideren, interpreteren en combineren. In sensornetwerken zijn sensoren onderling gekoppeld in een netwerk dat de informatie van de sensoren doorgeeft naar een ontvanger. *Smart dust* is een vorm van een draadloos sensornetwerk. Elke sensor bevat intelligentie (een *processor*) en is hierdoor in staat om eigen waarnemingen te verwerken en al dan niet door te sturen. De sensoren in een draadloos sensornetwerk worden daarom ook wel *sensor nodes* (sensorknooppunten) genoemd.

Miniaturisering leidt ook tot de ontwikkeling van kleine, goedkopere satellieten: *lightweight satellites*. Deze kunnen (naast voor communicatie) voor observatietaken worden ingezet en daarmee een platform vormen voor observatie vanuit de ruimte.

Naast sensoren voor omgevingsvariabelen in de fysieke wereld zijn ‘digitale sensoren’ van belang voor *sensing* van dataverkeer (relatie met de functie ‘Informatie beveiligen’). Sensorfusie op basis van een combinatie van sensoren in de fysieke en de virtuele wereld is mogelijk (relatie met de functie ‘Data analyseren’).

Toepassing

Met sensoren kan continu worden waargenomen op plaatsen waar mensen niet kunnen komen en kan informatie worden verzameld om een omgevingsbeeld te verkrijgen. Sensoren kunnen worden toegepast voor het observeren op afstand of voor het detecteren en identificeren van bepaalde (gevaarlijke) stoffen, zoals explosieven.

Impact

Toepassing van sensoren kan leiden tot verhoging van het (relevante) waarnemingsvermogen en een versterking van de informatiepositie. Sensoren bieden de gebruiker de mogelijkheid om te beschikken over *real-time* informatie,

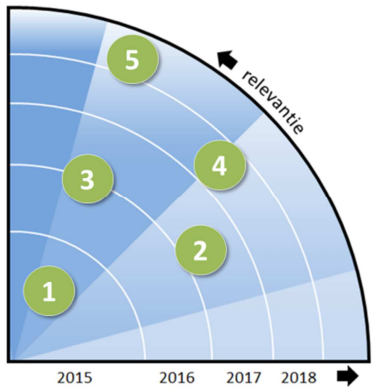
bijvoorbeeld ten behoeve van *real-time* detectie van (afwijkend) gedrag. Op basis van de door middel van sensoren verzamelde informatie kan meer vroegtijdig en gericht worden geacteerd. De effectiviteit en de efficiëntie van (gerichte) inzet kan daarmee worden verhoogd.

Voor specifieke scenario's en processen (strategie, tactiek) kan worden bepaald welke type(n) sensoren een meerwaarde bieden en kunnen worden ingezet. Op basis daarvan kan tevens worden bepaald hoe sensoren het best met elkaar samen kunnen werken.

De samenhang met het verwerken van de informatie en het gebruiken daarvan in het opvolgingsproces is van belang (relatie met de functies 'Data analyseren' en 'Aansturen'). *Privacy issues* spelen hier een rol (relatie met de functie 'Identificeren') en verdienen aandacht bij opvolging van de voorgestelde vervolgstappen.

Relevante technologieën en hun positie op de technologieradar

1. Sensoren
2. *Lightweight satellites*
3. Intelligente sensornetwerken en slimme sensoren
4. Intelligente sensornetwerken (digitaal)
5. *Smart dust*



Toelichting per technologie

Sensoren

- *Beschrijving en status:* Sensoren zetten omgevingsvariabelen om in een (elektrisch) signaal. Dit betreft veelal bestaande technologie, waarbij technologische ontwikkelingen ervoor zorgen dat er goedkopere en/of kleinere sensoren beschikbaar komen, die tijdens gebruik minder energie vereisen. Ook worden er nieuwe typen sensoren ontworpen, die weer andere fysieke aspecten van de werkelijkheid kunnen registreren.
- *Toepassing:* Het continu kunnen waarnemen en verzamelen van informatie om een omgevingsbeeld te maken is vooral van belang voor crisisbeheersing, handhaving en opsporing.
- *Voorbeeld van een toepassing:* Door het aanbrengen van sensoren in de nabijheid van kritische infrastructuren kan de waarschuwingstermijn voor het optreden van een crisis worden vergroot, zodat de verantwoordelijke partijen meer tijd hebben om te anticiperen. Een voorbeeld is de inzet van sensoren voor het waarnemen van langzame, ondergrondse veranderingen, die invloed kunnen hebben op het nationale gasdistributie-netwerk (zie http://www.ijknet.nl). Op basis van de meetgegevens kan met behulp van rekenmodellen worden voorspeld wanneer leidingen mogelijk gaan falen. Naast *in-situ* sensoren wordt tegenwoordig ook *remote sensing* met satellieten ingezet (maaiveldzakking, bijvoorbeeld als gevolg van ontwatering).
- *Voorgestelde vervolgstappen:* Nu beschikbare sensoren kunnen – vanuit een gedefinieerde informatiebehoefte – worden ingezet om de informatiepositie te versterken. Voor het kunnen toepassen van nieuwe (typen) sensoren (zuiniger, goedkoper, slimmer) is het belangrijk de verdere ontwikkelingen in de technologie volgen en waar nodig te stimuleren.

Lightweight satellites

- *Beschrijving en status:* Miniaturisering heeft kleine, goedkope *lightweight satellites* mogelijk gemaakt. Het een bestaande en verder in ontwikkeling zijnde technologie. De mogelijkheden om dergelijke satellieten te lanceren komen breder beschikbaar en de kosten daarvan worden lager.
- *Toepassing: Lightweight satellites* zijn geschikt voor communicatie- en observatiedoeleinden, bijvoorbeeld bij rampen, en zijn daarmee vooral interessant voor crisisbeheersing.
- *Voorbeeld van een toepassing:* De Canadian Space Agency heeft onlangs contracten toegekend voor vijf haalbaarheidsstudies naar microsatelliet-missies[7]. De voorgestelde missies zijn gericht op Canada en bestrijken het gebied van veiligheid, gezondheid, brand- en watersurveillance en het monitoren van waterkwaliteit. Eén van de projecten, QEYSSat, is gericht op het ontwikkelen van een platform voor quantumcryptografie en beoogt de veilige distributie van cryptografische sleutels over lange afstanden. Op basis daarvan is zeer veilige communicatie mogelijk, omdat met quantumcryptografie herkend kan worden wanneer een sleutel wordt onderschept.
- *Voorgestelde vervolgstappen:* De ontwikkelingen volgen en de kansen (bijvoorbeeld voor aardobservatie ten behoeve van crisisbeheersing) en mogelijke dreigingen inventariseren.

Intelligente sensornetwerken en slimme sensoren

- *Beschrijving en status:* Slimme sensoren kunnen zich aanpassen en gegevens slim verwerken. Ze kunnen onderling gekoppeld zijn in een netwerk. Deze technologie is in ontwikkeling: er worden steeds intelligentere en slimmere sensoren ontwikkeld en ook de onderlinge communicatietechnologie wordt nog constant verbeterd.
- *Toepassing:* Intelligente sensornetwerken kunnen worden gebruikt voor detectie, identificatie en controle en zijn daarmee vooral van belang voor handhaving, opsporing en crisisbeheersing.
- *Voorbeeld van een toepassing:* sensornetwerken die ontworpen zijn volgens de zogenaamde Zigbee radio standaard (http://www.zigbee.org) zijn minder gevoelig voor het uitvallen van een specifieke communicatielijn dan bedrade netwerken. Een zogenaamde ‘Zigbee’ *node* − met daarop één of meerdere sensoren – kan onderdeel worden van een wolk van *nodes*, waarbij communicatie met partijen buiten het netwerk plaatsvindt via een zogenaamde *gateway node*. De meetgegevens worden van *node* naar *node* doorgestuurd, totdat de *gateway* is bereikt. Als de *gateway* uitvalt, dan voorziet de Zigbee standaard in een mechanisme waardoor automatisch een nieuw pad van een zender naar een alternatieve *gateway* kan worden opgezet. Deze standaard vormt een voorbeeld van zogenaamde *self-organizing networks*, die robuuster zijn dan netwerken van sensoren die eenmalig vooraf geconfigureerd worden. Zo kan bijvoorbeeld een mobiel netwerk op een colonne van voertuigen met sensoren worden gerealiseerd, zonder dat de voertuigen aan een bepaalde volgorde en positie zijn verbonden.
- *Voorgestelde vervolgstappen:* Als bij sensoren: de verdere ontwikkelingen in de technologie volgen en waar nodig stimuleren. De meerwaarde van intelligente sensornetwerken en slimme sensoren voor operationele toepassing nagaan in een proeftuin of testomgeving.

Intelligente sensornetwerken (digitaal)

- *Beschrijving en status:* Deze sensoren halen informatie uit datacommunicatienetwerken of IT-systemen, ook wel de ‘virtuele wereld’ genoemd. Ook in digitale sensornetwerken zijn sensoren onderling gekoppeld in een netwerk. Door het steeds verder verweven raken van de virtuele en fysieke wereld zullen netwerken steeds vaker een combinatie van sensoren in beide werelden omvatten.
- *Toepassing:* Intelligente sensornetwerken (digitaal) kunnen worden gebruikt voor het detecteren en monitoren van activiteiten in *cyberspace*, bijvoorbeeld ten behoeve van het opsporen of tegengaan van *cybercrime*. De technologie is daarmee vooral interessant voor *cyber security*.

[7] http://www.asc-csa.gc.ca/eng/media/news_releases/2014/0429.asp

- *Voorbeeld van een toepassing:* Door de opkomst van technieken op het gebied van *'artificial intelligence'* worden sensornetwerken steeds vaker ingezet in combinatie met '*anomaly detection'*. Het intelligente sensornetwerk leert eerst wat het 'standaard' patroon van meetwaarden is, door een tijd lang te monitoren. Als er op een bepaalde manier verandering ontstaat in het patroon van gemeten waarden, dan is er sprake van een 'anomalie'. Er is geen precies begrip van de onderliggende mechanismes nodig: er wordt 'slechts' op basis van bepaalde variabelen gedetecteerd dat het systeem zich anders gedraagt dan normaal. Een voorbeeld betreft de analyse van informatie over de positie van mensen in een gebouwencomplex. Wanneer er een verandering optreedt in de manier waarop mensen zich voortbewegen in het gebouw dan kan dat, in combinatie met informatie over de functie van bepaalde kamers in dat gebouw, aanleiding zijn voor nader onderzoek. Zijn mensen verdachte activiteiten aan het ontplooien?
- *Voorgestelde vervolgstappen:* Dit is een langere termijn ontwikkeling: het is van belang bij te houden welke kant deze ontwikkeling opgaat.

Smart dust

- *Beschrijving en status: Smart dust* is een ontwikkeling in het verlengde van intelligente sensornetwerken. Het betreft vooral een verdergaande miniaturisering en een potentieel zeer groot aantal sensor *nodes*. Operationele toepassing wordt op langere termijn verwacht.
- *Toepassing:* Zie 'Intelligente sensornetwerken en slimme sensoren'.
- *Voorbeeld van een toepassing:* In een project dat TNO uitvoert met Q-Park wordt een *smart lighting*-systeem ontwikkeld voor een parkeergarage. Op basis van de beweging van personen of voertuigen moeten automatisch de juiste lichtinstellingen worden toegepast. Dergelijke technologie zou je ook op andere plekken in de stad kunnen toepassen, om bijvoorbeeld de bewegingsintensiteit van personen en voertuigen in een stad te meten. In de publieke ruimte lijken lantaarnpalen de meest geschikte objecten om uit te rusten met dergelijke (kleine) sensoren, omdat ze beschikken over een elektriciteitsaansluiting en hoog zijn. Daarbij kan een combinatie gemaakt worden met (miniatuur-)radartoepassingen, zodat ook de snelheid van objecten gemeten kan worden.
- *Voorgestelde vervolgstappen:* Dit als vervolg op 'Intelligente sensornetwerken en slimme sensoren' oppakken.

4.2 Data analyseren

Verwerken van data tot nuttige informatie

Beschrijving van het cluster

Vanuit sensoren, internet en andere bronnen is een toenemende hoeveelheid gegevens beschikbaar. Data-analyse is het verwerken van deze data tot voor de gebruiker nuttige informatie. Data-analyse loopt uiteen van het verwerken van relatief eenvoudige sets van data tot grote hoeveelheden, soms snel veranderende data uit diverse typen bronnen: *Big Data*-analyse. In aanvulling hierop kunnen visualisatietechnieken worden gebruikt om de informatie aan de gebruiker te presenteren en complexe verbanden inzichtelijk te maken.

Technieken voor automatische analyse van video *content* zijn bijvoorbeeld gericht op gezichtsherkenning, voertuigherkenning, detectie van afwijkend gedrag of het herkennen van sentimenten (relatie met de functie ‘Gedrag analyseren’). Extra diepte-informatie uit 3D-beelden maakt het analyseren van gedrag- en bewegingspatronen eenvoudiger. Dit betreft bestaande technologieën die verder worden ontwikkeld. Hoewel 3D-video *content* analyse technisch al mogelijk is en bestaat, is de cameradichtheid in de praktijk vaak zo laag dat er geen overlappende beelden beschikbaar komen. Ook is de eigenaar van de camera-infrastructuur vaak niet de gebruiker, en dan kan het lastig worden om de business case voor het gebruik van de beelden rond te krijgen.

Een specifieke vorm van data-analyse is *Dark Web Research*: het vanuit een data-centrische aanpak onderzoeken van internationale fenomenen, zoals terrorisme, op ‘verborgen’ delen van het internet. Het betreft een combinatie van verschillende data-, tekst- en web-*mining* technieken om relatie-, inhouds-, sentiment- en auteurschap-analyses uit te voeren. Nu speelt dit nog vooral in de wetenschappelijke wereld en op beperkte schaal ook al in testomgevingen.

Voor het verwerken van grote hoeveelheden data zijn rekenkracht en slimme analysemethodieken nodig. Technologische ontwikkelingen op het gebied van *new computing techniques*, *advanced artificial intelligence* en *agent based modelling* dragen daar aan bij.

Toepassing

(Big) Data-analyse levert inzicht in relaties, patronen, trends en anomalieën en geeft inzicht in de situatie ten behoeve van (*real-time*) *situational awareness*. (3D) Video *content* analyse kan worden toegepast voor herkenning van bijvoorbeeld personen, voertuigen en afwijkend gedrag.

Impact

(Big) Data-analyse is de basis om meer informatie-gestuurd te kunnen werken: niet alleen achteraf analyseren van data, maar ook *real-time*. Koppelen van data uit verschillende bronnen kan leiden tot extra informatie (bijvoorbeeld voor

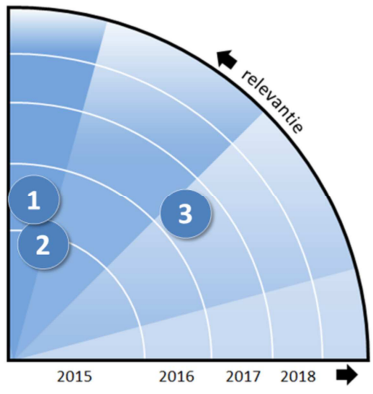
anomaliedetectie) en een basis zijn voor voorspellende modellen. De verkregen informatie kan worden gebruikt voor een optimale opvolging. Dit leidt tot een verhoging van de efficiëntie en effectiviteit van de inzet van de capaciteit: weten waar en op welke manier mensen moeten worden ingezet en proactief kunnen aansturen van deze inzet.

Bij *Big Data*-analyse gaat het om het verwerken én het delen van informatie. Informatiedeling kan binnen de organisatie zelf plaatsvinden, of met ketenpartners en andere externe partners. Daarbij dient te worden gekeken naar informatiebeveiliging en ook bij deze technologie spelen *privacy*-aspecten een belangrijke rol (relatie met de functies 'Informatie beveiligen' en 'Identificeren').

Nieuwe technieken voor *(Big) Data*-analyse kunnen worden ingepast in de organisatie en processen. Belangrijk is het om de opvolging in het proces te organiseren. Verschillende databronnen kunnen worden gekoppeld door koppelvlakken voor datafusie te definiëren en te zorgen voor een goede, schaalbare ICT-infrastructuur met koppelingen naar alle relevante bronnen.

Relevante technologieën en hun positie op de technologieradar

1. *Big Data*-analyse
2. *Dark Web Research*
3. 3D-Video *content* analyse (VCA)



Toelichting per technologie

***Big Data*-analyse**

- *Beschrijving en status: Big Data* kenmerkt zich door grote hoeveelheden, gevarieerde en soms ook snel wijzigende data. Koppelen van data (uit verschillende bronnen) kan leiden tot extra informatie (bijvoorbeeld ten behoeve van anomaliedetectie, zoals ook in de vorige paragraaf genoemd) en mogelijk zelfs worden gebruikt voor voorspellende modellen. Analysetechnieken, bijvoorbeeld op basis van tekst- en *media mining*, geavanceerde patroonherkenning of *semantic web*-technologie, kunnen hierbij worden gebruikt. *Big Data* op zich is vooral een 'containerbegrip' en nog een *hype*. Met een koppeling van data en een combinatie van analysetechnieken kunnen de eerste stappen worden gezet.
- *Toepassing: Big Data*-analyse is interessant voor de meeste onderdelen van het veiligheidsveld, omdat inzicht kan worden verkregen in trends, het (*real-time*) *situational awareness* mogelijk maakt en inzicht in toekomstige ontwikkelingen kan opleveren (voorspellend vermogen).
- *Voorbeeld van een toepassing:* In de praktijk wordt *'predictive policing'* steeds vaker toegepast. Zo wordt in Los Angeles gebruik gemaakt van de software 'PredPol', die oude misdaadstatistieken analyseert en op een kaart plot. In combinatie met andere gegevens (zoals weerberichten) worden voorspellingen gemaakt over bijvoorbeeld het aantal

inbraken dat men op een bepaald moment verwacht[8]. Ook Nederland kent een dergelijk systeem: het zogenaamde Criminaliteits Anticipatie Systeem, dat gebruikt wordt door wijkteams en flexteams in Amsterdam en dat in samenwerking met TNO wordt geoptimaliseerd[9]. In de nabije toekomst zal het aantal databronnen dat in dergelijke systemen wordt ontsloten en gecombineerd naar verwachting blijven stijgen – zal het uiteindelijk leiden tot een scenario zoals in de film 'Minority Report' wordt neergezet? *Privacy* issues spelen in ieder geval een belangrijke rol.

- *Voorgestelde vervolgstappen:* De ontwikkelingen volgen en beschikbare analysetechnieken inzetten, bijvoorbeeld in *testbeds* voor *real-time* intelligence. Van daaruit met (keten)partners verder uitbreiden naar gebruik van meerdere databronnen en meer geavanceerde visualisatie, afgestemd op de operationele gebruiker. Bepalen hoe *Big Data*-analyse is in te passen in de processen waarin opvolging wordt gegeven op basis van de verkregen informatie. Koppeling van databronnen mogelijk maken, rekening houdend met *privacy*-aspecten.

Dark Web Research

- *Beschrijving en status:* Een specifieke vorm van internet-onderzoek, gericht op online criminaliteit, extremisme en terrorisme. Deze activiteiten vinden vaak plaats in anonieme netwerken zoals TOR of I2P. Met een data-centrische aanpak in combinatie met data-, tekst- en web-*mining* technieken wordt inzichtelijk gemaakt welke activiteiten ontplooid worden − denk aan activiteiten op het gebied van drugs- of wapenhandel, vals geld, *cybercrime-as-a-service*, huurmoorden en kinderporno.
- *Toepassing:* Met behulp van *Dark Web Research* worden op strategisch, tactisch en operationeel niveau inzicht én handvatten ontwikkeld om maatregelen te treffen en interventiestrategieën te ontwikkelen. Het succes van *Dark Web Research* is afhankelijk van het vermogen om de benodigde gegevens (fora, *blogs*, enz.) te verzamelen.
- *Voorbeeld van een toepassing:* In 2011 heeft de politie in samenwerking met Fox-IT enkele weken gejaagd op kinderporno in het *Dark Web*. Deze operatie staat bekend als operatie Descartes. Gegeven de maatschappelijke impact van online kindermisbruik wordt momenteel in samenwerking met partners in de veiligheidsketen een totaalbeeld van de problematiek ontwikkeld. Het betreft onder andere een toepassing die 24/7 geautomatiseerd moet gaan 'jagen' op plekken waar dit type materiaal gedeeld wordt. Zodra er compromitterend materiaal gevonden wordt, kan dit worden voorgelegd aan een bevoegd persoon. Daarbij kan gedacht worden aan de politie, aan het openbaar ministerie of aan 'ethische *hackers'*. Deze toepassing vereist hoogwaardige *real-time* technologie, in combinatie met internationale samenwerking.
- *Voorgestelde vervolgstappen:* De techniek testen en inzetten voor onderzoeken naar communicatie. Internationaal netwerk opzetten met partijen om een gezamenlijk beeld te ontwikkelen. Internationale samenwerking is cruciaal omdat de genoemde fenomenen zich internationaal manifesteren en oplossingen niet door één partij te leveren zijn. Data over criminele netwerken door onderzoekers laten analyseren, zodat meer bekend wordt over de structuren, logistiek en infrastructuren van deze netwerken.

3D-video *content* analyse (VCA)

- *Beschrijving en status:* Analyse van gedrag- en bewegingspatronen op basis van 3D-beelden. 3D-beelden kunnen worden gemaakt met meerdere camera's of met een bewegende camera (monoculair) met bekende posities. Producten voor 3D-reconstructie bestaan. Voor sport en industriële toepassingen zijn er 3D VCA-producten. Het toepassen van 3D VCA op beelden van een bewegende mensenmassa is momenteel nog lastig.
- *Toepassing:* Met VCA op basis van 3D-beelden kunnen gedrags- en bewegingspatronen worden geanalyseerd, bijvoorbeeld verdacht gedrag in massa's mensen op luchthavens of rondom huizen.
- *Voorbeeld van een toepassing:* Voor indringerdetectie en voor de detectie van weggenomen of achtergelaten spullen is deze technologie al op de markt. De bedrijven CameraManager en VicarVision gebruiken 3D VCA om in de *retail* en bij consumenten

[8] http://socialmediadna.nl/predictive_policing/
[9] http://socialmediadna.nl/data-detective/

misdaad te signaleren[10]. TNO beschikt over deze technologie in een vorm waarmee 'huftergedrag' in het verkeer kan worden gedetecteerd op de snelweg en werkt eraan om deze technologie vanaf mobiele platformen te laten werken zoals vanaf *bodycams*, *wearables*, UAV's en rijdende voertuigen.

- *Voorgestelde vervolgstappen:* De verdere ontwikkelingen volgen en stimuleren en vanuit proefprojecten de meerwaarde voor specifieke toepassingen nagaan, rekening houdend met *privacy*-aspecten.

[10] https://www.cameramanager.com/website/nl/press/panasonic-brengt-video-analytics-naar-de-cloud

4.3 Identificeren

Achterhalen van de identiteit én beschermen van de privacy

Beschrijving van het cluster

Technologische ontwikkelingen maken het aan de ene kant eenvoudiger om anoniem te blijven en bieden aan de andere kant juist mogelijkheden voor de identificatie van personen. Daarnaast bieden technologieën de mogelijkheid de *privacy* te beschermen.

Huidige mogelijkheden om anoniem gebruik te maken van internetdiensten zijn onder andere technieken als *onion routing*, *anonymous proxies* en *VPN-tunnels*. Nieuwe ontwikkelingen zoals '*spy-proof*' en beveiligde *smartphones* met gecodeerde communicatiemogelijkheden en andere *gadgets* en apps maken versleutelde communicatie eenvoudig mogelijk. Allerlei nieuwe apps helpen berichten te coderen, 'onbreekbare' wachtwoorden te construeren, etc.

Geautomatiseerde methoden voor het herkennen van een persoon op basis van anatomische, fysieke of gedragskenmerken (zoals irisherkenning, tredherkenning en gelaatsherkenning) ontwikkelen zich verder. Met biometrie kan steeds meer: herkenning over grotere afstanden, sneller en met nauwkeuriger technologie. Herkenningsalgoritmes vormen een belangrijke ontwikkeling (relatie met de functie 'Data analyseren').

Technologische ontwikkelingen hebben het mogelijk gemaakt om met minder en andersoortig materiaal, steeds sneller en goedkoper, een completer DNA-profiel te vergaren. Efficiëntere DNA-methodieken bieden mogelijkheden snellere voor identificatie van personen.

Met behulp van zogenaamde *Privacy Enhancing Technologies* (PET) kan persoonlijke informatie worden beschermd. Zonder alle persoonlijke gegevens bekend te maken kunnen met behulp van deze technologieën bepaalde gegevens worden gecheckt, bijvoorbeeld of iemand een bepaalde leeftijd heeft.

Toepassing

Anonimisering kan enerzijds worden toegepast door veiligheidspartners in de opsporing en Intel en anderzijds door kwaadwillenden. Biometrie kan worden toegepast voor het snel en waar nodig op afstand identificeren van mensen. Met DNA-methodieken is het – in combinatie met andere sporen – mogelijk direct te linken naar personen.

Impact

Anonimiteit is een *issue* bij het bestrijden van *cyber security* en contraterrorisme. Wat dit betreft is er sprake van een spanningsveld tussen identiteit en *privacy*. Aan de ene kant is het gewenst iemands identiteit te weten en zaken en informatie aan personen te kunnen koppelen. Aan de andere kant is het gewenst de *privacy* van personen te beschermen.

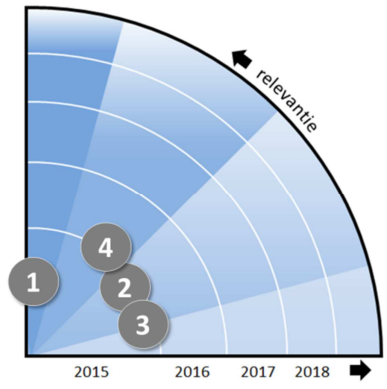
Privacy Enhancing Technologies kunnen onderdeel uitmaken van *privacy by design*, ofwel het ontwerpen van systemen waarbij al vanaf de eerste idee- en ontwerpfase rekening wordt gehouden met *privacy*-aspecten. Dit kan een belangrijk ontwerpprincipe zijn voor nieuwe informatie(verwerkings)systemen.

Door de technologische ontwikkelingen die anonimisering vereenvoudigen is het nodig om bij opsporing niet alle energie op het ontcijferen van encryptie te richten, maar om te zoeken naar alternatieve oplossingen om informatie te vergaren en meer traditionele manieren van opsporing toe te passen.

Bij nieuwe technieken voor identificatie, zoals nieuwe DNA-technieken, is het van belang dat deze tijdig een goede juridische basis krijgen zodat deze technieken operationeel toegepast kunnen en mogen worden.

Relevante technologieën en hun positie op de technologieradar

1. Anonimisering
2. Biometrie
3. DNA-methodieken
4. *Privacy Enhancing Technologies*



Toelichting per technologie

Anonimisering

- *Beschrijving en status:* Technische mogelijkheden om anoniem gebruik te maken van internetdiensten via technieken als *onion routing*, *anonymous proxies* en *VPN-tunnels*. Daarnaast ook *Blackphone* en andere gadgets en apps die versleutelde communicatie mogelijk maken: '*spy-proof*' en beveiligde *smartphones* en allerlei nieuwe apps die mensen helpen berichten te coderen en 'onbreekbare' wachtwoorden te construeren en versleutelde USB-drives die zichzelf kunnen wissen. Dit betreft bestaande technologie, waarop nieuwe ontwikkelingen zullen volgen.
- *Toepassing:* Anonimisering kan worden toegepast door kwaadwillenden en is dus in die zin een bedreiging. Kan ook voor eigen gebruik worden toegepast.
- *Voorbeeld van een toepassing:* Het aantal downloads van zogenaamde *TOR-browsers* lijkt een hoge vlucht te nemen[11]. Het betreft dan geen specialistische '*hackers software'*, maar eenvoudig verkrijgbare *browsers*. Met behulp van hiervan wordt het voor de massa mogelijk om eenvoudig berichten te versturen zonder je IP-adres kenbaar te maken, waardoor het achterhalen van de identiteit van de afzender nagenoeg onmogelijk is. Naar verwachting zal dit in de toekomst steeds meer gebeuren. Ook een grappig bedoeld bericht, zoals de aankondiging van de 14-jarige Sarah die in april 2014 via een *tweet* aankondigde een vliegtuig van American Airlines op te blazen[12] of een nieuw 'Project X', kan dan leiden tot aanzienlijke onrust en schade – veel meer nog dan nu al het geval is.
- *Voorgestelde vervolgstappen:* Volgen van de ontwikkelingen. Kennis opbouwen.

[11] https://blog.torproject.org/blog/how-to-handle-millions-new-tor-clients
[12] http://www.ondertussen.nl/074-nieuws/grap-over-opgeblazen-vliegtuig-bereikt-fbi

Biometrie

- *Beschrijving en status:* Geautomatiseerde methoden voor het herkennen van een persoon op basis van anatomische, fysieke of gedragskenmerken: gezicht, vingerafdrukken, geometrie van de hand, handschrift, iris, netvlies, bloedvaten en stem. Het betreft bestaande technieken die verder worden ontwikkeld. Herkenningsalgoritmen vormen een belangrijke ontwikkeling. Herkenning over grotere afstanden zal sneller en nauwkeuriger worden. Sommige technologieën zijn op kortere termijn toepasbaar dan andere.
- *Toepassing:* Herkennen van mensen, bijvoorbeeld bij handhaving, opsporing en bewaken en beveiligen.
- *Voorbeeld van een toepassing:* Biometrische kenmerken worden in toenemend tempo ook gebruikt voor de identificatie van mensen op het internet. FIDO Alliance, een samenwerkingsverband waarbij organisaties als Google, Visa, Apple en PayPal zijn aangesloten, houdt zich bezig met de ontwikkeling van een authenticatiestandaard die onder meer biometrische identificatiemiddelen ondersteunt[13]. Zo wil men het traditionele wachtwoord vervangen door nieuwe authenticatiemethoden op basis van onder andere vingerafdruk- of stemherkenning. De verwachting luidt dat er eind 2015 al twee- tot driehonderd miljoen apparaten zullen voldoen aan de bijbehorende standaarden.
- *Voorgestelde vervolgstappen:* De ontwikkelingen volgen en stimuleren. Onderzoek starten gericht op ontwikkeling en implementatie. Algoritmen verbeteren. Technologieën uittesten voor specifieke toepassingen en borgen in operaties en routines.

DNA-methodieken

- *Beschrijving en status:* Met nieuwe DNA-methodieken kan met minder en andersoortig materiaal steeds sneller en goedkoper een completer DNA-profiel worden vergaard. Efficiëntere DNA-methodieken bieden mogelijkheden voor de identificatie van personen.
- *Toepassing:* Identificatie van personen met behulp van DNA-profiel is in eerste instantie interessant voor opsporing. Met snellere technieken wordt identificatie op termijn ook interessant voor andere toepassingen binnen het veiligheidsveld.
- *Voorbeeld van een toepassing:* Een voorbeeld is de ontwikkeling van *handheld* DNA *sequencers*. Onderzoekers van de Universiteit van Otago in Nieuw-Zeeland ontwikkelden recent de Freedom4[14], een prototype van een dergelijke DNA *sequencer* ter grootte van een baksteen. Met een dergelijk mobiel apparaat kunnen binnen een uur verdachte virussen en bacteriën en de mate van besmetting van personen worden gedetecteerd – direct in het veld. Ze kunnen ook worden gebruikt voor de identificatie van mensen, bijvoorbeeld bij grenscontroles of forensisch onderzoek. De Freedom4 kan draadloos worden verbonden met een *laptop* of *smartphone*[15].
- *Voorgestelde vervolgstappen:* De ontwikkelingen volgen en toepassen. Daarbij nieuwe technieken een goede juridische basis geven.

Privacy Enhancing Technologies (PET)

- *Beschrijving en status: Privacy Enhancing Technologies* zijn technische middelen die zorgen voor de bescherming van de *privacy* van persoonlijke informatie.
- *Toepassing: Big Data*-ontwikkelingen en de trend van informatie(sturing) zorgen ervoor dat meer data, waaronder persoonlijke informatie, wordt verwerkt door partners in het veiligheidsveld. Hierbij zal moeten worden voldaan aan wetgeving, o.a. rondom *privacy*. PET kan het beste worden meegenomen in de ontwerpfase: *privacy by design* als basisvoorwaarde voor systemen die informatie verwerken en opslaan.
- *Voorbeeld van een toepassing:* Homomorfe encryptie (zie ook paragraaf 4.7) maakt het mogelijk om te rekenen in vercijferde data. Hierdoor hoeven persoonlijke gegevens niet meer ontcijferd te worden om er iets mee te doen, kan persoonlijke data in de cloud ook vercijferd worden opgeslagen en kan de controle over het ontcijferen bij de persoon zelf blijven. Dit kan bijvoorbeeld gebruikt worden om als overheid twee datasets te vergelijken op gezochte personen, of om commerciële aanbevelingen te doen voor patiënten zonder te

[13] http://nu.nl/internet/3876530/achtergrond-einde-van-wachtwoord.html
[14] http://www.otago.ac.nz/news/news/otago077848.html
[15] Technisch Weekblad; 5 september 2014

weten wie de patiënten zijn. Deze techniek staat op het punt om zijn intrede te maken in de dagelijkse praktijk, hoewel nog niet alle soorten berekeningen met vercijferde data efficiënt kunnen worden uitgevoerd.

- *Voorgestelde vervolgstappen:* Specifieke technologieën verkennen. Investeren in *Privacy Enhancing Technologies* en in het ontwerp van eigen systemen *privacy by design* toepassen.

4.4 Gedrag analyseren

Inzicht verkrijgen in menselijk(e) gedrag(ingen)

Beschrijving van het cluster

Het automatisch analyseren van gedrag is mogelijk dankzij technologische ontwikkelingen die gebruik maken van visuele informatie en van data uit diverse bronnen.

Intelligente camera's interpreteren beelden op basis van beeldverwerking, -verbetering en -analyse, visuele patroonherkenning en kunstmatige intelligentie. De ontwikkelingen gaan in de richting van een verdere verfijning van beeldinterpretatie. Technieken voor automatische interpretatie van beelden voor detectie van afwijkend gedrag en het herkennen van sentimenten maken gebruik van een gegevensbestand met daarin gedragingen die opvallend zijn. Beelden worden automatisch geanalyseerd en geïnterpreteerd en kenmerken van gedrag worden gerapporteerd in natuurlijke taal.

Reality mining is het analyseren van via sensoren verkregen data met betrekking tot menselijk sociaal gedrag met als doel voorspelbare patronen van gedrag te identificeren. Menselijke interacties worden geanalyseerd op basis van bijvoorbeeld gebruik van mobiele telefoons, locatiegegevens en sensordata. Met behulp van *data-mining* algoritmen kan dit inzicht geven in individuele gedragspatronen en zelfs in het welzijn van gemeenschappen (relatie met de functie 'Data analyseren').

Een langere termijn-ontwikkeling voor het verkrijgen van inzicht in menselijk gedrag komt vanuit de neurowetenschappen. Kennis van het functioneren van de hersenen verschaft inzicht in menselijk gedrag en maakt het (wellicht) mogelijk om determinanten te identificeren waardoor mensen die meer kans maken op afwijkend gedrag technisch gesproken kunnen worden geïdentificeerd – juridische implicaties daargelaten.

Een gerelateerde ontwikkeling is *Persuasieve Technologie* (PT), een technologie om attitudes, intenties en gedrag van mensen te beïnvloeden. Voorbeelden zijn apps die mensen helpen stoppen met roken en energiedisplays om zuiniger met energie om te gaan.

Toepassing

Technologieën voor automatische gedragsanalyse of -herkenning, onder meer gebaseerd op beeldinformatie en data uit verschillende bronnen, maken het mogelijk om (afwijkende) gedragingen (soms zelfs *real-time*) te herkennen. Een andere mogelijke toepassing wordt gevormd door nieuwe leugendetectors die zich baseren op micro-analyse van het gelaat.

Impact

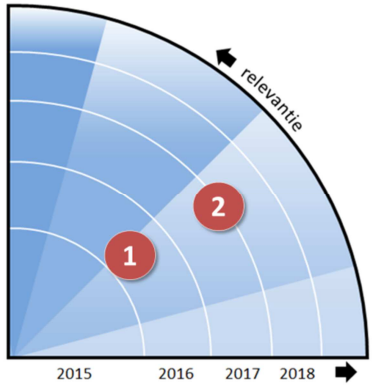
Automatische gedragsanalyse of -herkenning vergroot het identificerend vermogen. Naast toepassing voor analyse achteraf zijn er mogelijkheden om te beschikken over *real-time* informatie. Wanneer snelle voorspelmodellen kunnen worden gemaakt, zou *reality mining* zelfs mogelijkheden voor voorspellende scenario's

kunnen leveren. Dit kan bijdragen aan een verschuiving van reactief naar (meer) proactief opereren.

Technieken voor *reality mining* kunnen in samenhang met technieken voor *(Big) Data*-analyse worden ingepast in de organisatie en processen. Daarbij dient te worden onderzocht welke informatiebronnen gebruikt kunnen worden. Bij persoonlijke sensordata dient daarbij uiteraard zorgvuldig te worden omgegaan met de *privacy* (relatie met de functie 'Identificeren').

Persuasieve Technologie (PT) kan een middel zijn voor bewustwording rond veiligheid bij de burger en verhoging van preventie. Vooralsnog is het toepassingsgebied veiligheid niet sterk vertegenwoordigd in dit relatief jonge wetenschapsveld.

Relevante technologieën en hun positie op de technologieradar

1. Automatische gedragsherkenning 2. *Reality mining*	

Toelichting per technologie

Automatische gedragsherkenning

- *Beschrijving en status:* Technieken voor automatische interpretatie van beelden, zoals de detectie van afwijkend gedrag en het herkennen van sentimenten, die zijn gebaseerd op een database met gedragingen die opvallend zijn. Met 'visuele intelligentie', kan (visuele) informatie worden geïnterpreteerd en omgezet in metadata. Ook andere dan 'visuele' sensoren kunnen worden ingezet. De analysecapaciteit van deze technieken wordt verder ontwikkeld, waardoor interpretatie van beelden en daarmee gedragsherkenning continu beter wordt.
- *Toepassing:* Tijdig signaleren van afwijkend gedrag. Dit is vooral relevant voor handhaving en opsporing.
- *Voorbeeld van een toepassing:* Het bedrijf QVI maakt technologie om automatisch afwijkend gedrag te herkennen op Schiphol: mensen die onwel worden, zakkenrollerij en achtergelaten bagage[16]. Er is ook al technologie ontwikkeld voor het automatisch detecteren van samenwerkende zakkenrollers in een winkelcentrum[17], en voor de detectie van overvallers op parkeerplaatsen langs snelwegen[18]. In de toekomst kan deze technologie gebruikt worden om een zogenaamd normaalbeeld te maken van een

[16] http://www.nrc.nl/nieuws/2014/09/11/slimme-camera-spot-afwijkend-gedrag-van-reizigers-op-schiphol/
[17] Automatic detection of suspicious behavior of pickpockets with track-based features in a shopping mall, Proc. SPIE, vol. 9253, Bouma, H. et al, 2014, accepted for submission.
[18] ARENA Consortium, website, http://www.arena-fp7.eu/

stedelijke omgeving, waarmee vervolgens bij een terroristische dreiging relevant afwijkend gedrag automatisch kan worden gedetecteerd[19].

- *Voorgestelde vervolgstappen:* Experimenteren met systemen en nagaan hoe deze technologie kan bijdragen aan de doelen van een specifiek thema binnen het veiligheidsveld.

Reality mining

- *Beschrijving en status:* Met *reality mining* worden via sensoren verkregen gegevens over menselijk sociaal gedrag geanalyseerd om voorspelbare patronen van gedrag te identificeren. Deze technologie is in ontwikkeling en is gerelateerd aan *Big Data*-analyse. Persoonlijke sensordata zullen naar verwachting de komende decennia meer worden gebruikt voor onder andere toepassingen in de gezondheidszorg.
- *Toepassing:* Identificeren van voorspelbare patronen van gedrag is vooral interessant voor contraterrorisme en opsporing.
- *Voorbeeld van een toepassing:* In paragraaf 4.2 is *Big Data*-analyse behandeld en wordt als voorbeeld 'PredPol' genoemd. Aan de universiteit van Virginia gebruikt men als bron voor het voorspellen van misdaad *geotweets* (*tweets* met *geolocatie*). Dat leidt tot interessante resultaten, zo kan bijvoorbeeld een aantal *tweets* over 'dronken worden' uit een bepaalde geografische locatie een aanwijzing vormen dat op die plek de kans op misdaad toeneemt[20].
- *Voorgestelde vervolgstappen: Reality mining* in samenhang met *Big Data*-analyse verder ontwikkelen, uittesten en toepassen om de ambitie van 'terug-rechercheren' naar 'real-time-rechercheren' mogelijk te maken – rekening houdend met aspecten op het gebied van *privacy*.

[19] TACTICS Consortium, D3.1 Conceptual Solution Description, 2013, http://www.fp7-tactics.eu/
[20] http://socialmediadna.nl/misdaad-voorspellen-met-twitter/

4.5 Aansturen

Command & Control op basis van gepresenteerde informatie

Beschrijving van het cluster

Technologische ontwikkelingen op het gebied van *Command & Control*-systemen zijn gericht op het effectiever en efficiënter aansturen van operaties en operationele processen. *Command & Control*-technologie biedt informatie ter ondersteuning van het maken van beslissingen. Het betreft systemen voor in een meld- of controlekamer of andere centrale tactische of operationele ruimtes, maar ook systemen voor het via communicatiesystemen uitwisselen van informatie met mensen van veiligheidsorganisaties in het veld.

Met behulp van *Command & Control*-technologie kan in een controlekamer een beter beeld van een situatie worden weergegeven. Informatie (onder andere van sensoren) wordt inzichtelijk gepresenteerd samen met het operationele beeld. Deze *situational awareness* is van belang om op tactisch en/of strategisch niveau ondersteuning van de operatiën te kunnen bieden en om de operatiën waar gewenst beter te kunnen aansturen. Dit beeld kan worden aangevuld met *Threat Intelligence*. Door informatie uit meerdere externe bronnen (*open source intelligence*, *honeypots* / *honeynets*[21], externe controlekamers) te combineren kan een beter beeld gevormd worden van wat er zich afspeelt buiten de organisatie.

Nieuwe ontwikkelingen betreffen het presenteren en visualiseren van informatie aan gebruikers, bijvoorbeeld met behulp van 3D-visualisatie en interactieve gebruikers*interfaces* (relatie met de functie ‘Opvolgen’). Ook samenwerking op afstand (*telepresence*) wordt hiermee beter ondersteund. *Command & Control*-systemen krijgen een meer gedistribueerd karakter: *smart devices* van gebruikers in het veld worden geïntegreerd in een netwerk.

Naast het monitoren van de (huidige) situatie vindt er een verschuiving plaats naar het voorspelen van ontwikkelingen. Dit biedt ondersteuning bij het opstellen en evalueren van scenario’s. Technologische ontwikkelingen op het gebied van de informatie- en communicatietechnologie dragen onder andere met sneller wordende datacommunicatie en informatieverwerking bij aan hierboven beschreven ontwikkelingen.

Toepassing

Command & Control-technologieën kunnen worden toegepast ter ondersteuning van de besluitvorming en het aansturen van operaties en operationele processen. Dit gebeurt door *real-time* informatieoverdracht (*pull* en *push*, dus over en weer*)* met veiligheidsmensen en partners. Daarnaast kunnen ze ook worden ingezet ten behoeve van betere werkvoorbereiding en briefing, dankzij de mogelijkheden tot

[21] Een *honeypot* is in de informatica een computersysteem dat zich bewust kwetsbaar opstelt voor (worm)virussen en andere aanvallen, met als doel het verzamelen van informatie over virussen en aanvallen. Een *honeynet* bestaat uit een verzameling gebruikers die samenwerken om op deze wijze informatie over internetbedreigingen te verzamelen.(bron: Wikipedia)

interactie en het gebruik van informatie uit alle relevante bronnen die deze technologieën bieden.

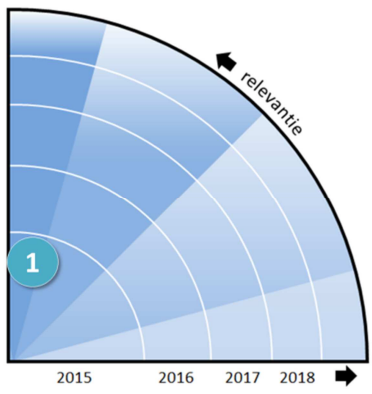
Impact

Command & Control-technologie maakt een verschuiving mogelijk van reactief via *real-time* naar proactief optreden, waarbij de technologie ook de opvolging faciliteert. Dankzij *Command & Control*-technologie wordt het mogelijk om bij brede (integrale) interventies overzicht en controle (sturing) te behouden. De verschuiving van reactief naar proactief handelen heeft impact op de manier van opereren van veiligheidsorganisaties en daarmee op hun operationele processen en cultuur.

Het is van belang duidelijk onderscheid te blijven maken tussen de informatiefunctie en sturing en coördinatie. Meer informatie staat niet gelijk aan meer beheersing. *Command & Control*-systemen kunnen een ondersteunende functie vervullen, zodat op basis van informatie de juiste beslissingen voor aansturing kunnen worden genomen. Het kan echter ook verder gaan dan alleen het ondersteunen van beslissingen: *Command & Control*-systemen kunnen beslissingen zelfs (deels) uit handen nemen (autonome systemen).

Vernieuwingen in de toepassing van *Command & Control*-technologie hangen nauw samen met die op het gebied van de informatieverwerking en -vergaring (relatie met de functies ‘Waarnemen’ en ‘Data analyseren’). Bij het implementeren van innovaties zullen deze functies dus in nauwe onderlinge samenhang moeten worden beschouwd.

Relevante technologieën en hun positie op de technologieradar

1. *Control Room*-technologie (inclusief visualisatie)	

Toelichting per technologie

***Control Room*-technologie (incl. visualisatie)**

- *Beschrijving en status: Control Room-technologie* is erop gericht in een controlekamer een beter beeld van een situatie weer te gegeven. Informatie (onder andere van sensoren) wordt inzichtelijk gemaakt, bijvoorbeeld ten aanzien van waar de eenheden zich bevinden. Visualisatie is hierbij een belangrijk element. De gepresenteerde informatie dient ter ondersteuning van besluitvorming.
- *Toepassing: Situational awareness* is van belang om op operationeel/tactisch/strategisch niveau ondersteuning van de operatiën te bieden en deze te kunnen aansturen. Dit is vooral van belang bij crisisbeheersing en operationeel optreden (politie, brandweer).
- *Voorbeeld van een toepassing:* Een goed voorbeeld van de ambitie om proactief te handelen is de inrichting van een weerbureau in het Operationeel Controle Centrum Rail

(OCCR). Op het OCCR worden online weergegevens uit diverse bronnen gecombineerd en geanalyseerd om een meerdaags weerbericht op te stellen dat is toegespitst op de spoorbranche. Als kritische grenzen overschreden dreigen te worden, kan vroeg worden geanticipeerd op mogelijke risico's zodat indien nodig de treindienst kan worden aangepast. *Real-time* kan gebruik worden gemaakt van de *social weather map*; berichten op de sociale media over het lokale weer kunnen op een landkaart worden gevolgd en bij bijvoorbeeld storm of zware sneeuwval worden gebruikt voor vroegtijdige aansturing van het onderhoudspersoneel.

- *Voorgestelde vervolgstappen:* Vanuit bestaande aansturing de functies op het gebeid van *Command & Control* uitbreiden. Bepalen welke informatie relevant is voor besluitvorming en op welke manier deze wordt opgevolgd. Zorgen voor aanpassing van de cultuur van reactief naar proactief. Duidelijk onderscheid blijven maken tussen de informatiefunctie en sturing en coördinatie. Voor de langere termijn: bepalen waar de grens ligt tussen informatie en besluitvorming. *Command & Control*-systemen kunnen verder gaan dan alleen het ondersteunen van beslissingen: ze kunnen beslissingen (deels) uit handen nemen (autonome systemen).

4.6 Opvolgen

Interacteren met machines voor informatie(uitwisseling)

Beschrijving van het cluster

Diverse technologische ontwikkelingen maken nieuwe manieren van interactie tussen mensen en apparaten mogelijk: visualisatietechnieken bieden meer mogelijkheden, spraaktechnologie wordt krachtiger, *multi-touch interfaces* worden uitgebreid met besturing op basis van bewegingen of gebaren (*gestures*). Zogenaamde haptische interfaces (bijvoorbeeld een trilvest) bestaan al enige tijd en bieden mogelijkheden voor nieuwe toepassingen. Een langere termijn ontwikkeling is het met gedachten aansturen van apparaten (Brein-Machine-Interface), waarvoor al eerste systemen zijn ontwikkeld.

Op het gebied van *virtual reality* vinden verdere ontwikkelingen plaats en *augmented reality* wordt meer toepasbaar. *Virtual reality* is het simuleren en visualiseren van de werkelijkheid op basis van (3D-)modellen in een computer. *Augmented reality* betreft vermenging van de werkelijke wereld met een virtuele wereld. Informatie wordt toegevoegd aan de werkelijke wereld (*mixed reality*) en aan de gebruiker getoond via *smart glasses* of een *head-up display* (en op langere termijn mogelijk via *contact lens displays* en op de nog langere termijn misschien zelfs wel via een Brein-Machine-Interface.

Portables & Wearables, zoals *smartphones*, *smart glasses*, *smart watches* en *smart clothing* zijn technologieën die mens-machine-interfaces ondersteunen. Technologische ontwikkelingen op dit gebied worden ook sterk vanuit de *gaming*-industrie gedreven.

Toepassing

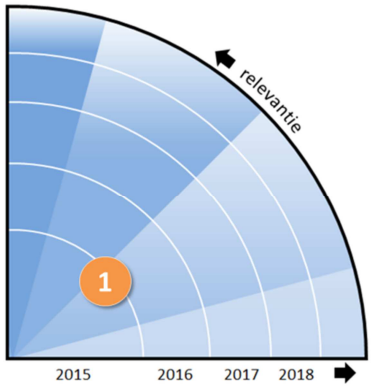
Met nieuwe mens-machine-interfaces kunnen apparaten op een andere manier worden aangestuurd dan met de huidige mogelijkheden. Tegelijkertijd kan informatie op een andere manier worden aangeboden aan de gebruiker. Uiteindelijk is het doel de interactie tussen mensen en apparaten hiermee te vereenvoudigen en ‘natuurlijker’ te maken.

Met behulp van *augmented reality* kan informatie op een overzichtelijke manier worden aangeboden.

Impact

Nieuwe mens-machine-interfaces kunnen het opereren van mensen in het veld vergemakkelijken. Een voorbeeld is het gebruik van *augmented reality* door de politie, voor het verkrijgen van informatie over personen of voertuigen. Door herkenning van locaties en objecten kan informatie op een specifieke locatie of behorend bij een specifiek object worden weergegeven. Door gebruik te maken van *virtual reality* kunnen situaties en scenario’s van tevoren worden geanalyseerd en geoefend in een *serious game*.

Relevante technologieën en hun positie op de technologieradar

1. *Virtual reality / Augmented reality*	

Toelichting per technologie

Virtual reality / Augmented reality

- *Beschrijving en status: Virtual reality* gaat over het simuleren van de werkelijkheid op basis van (3D-) modellen in een computer. *Augmented reality* betreft vermenging van de werkelijke wereld met een virtuele wereld en het toevoegen van informatie aan de werkelijke wereld (*mixed reality*). Deze extra informatie kan aan de gebruiker worden getoond via een *smartphone*, *tablet*, *smart glasses* of *head-up display*.
- *Toepassing:* Nieuwe mens-machine-interfaces kunnen het opereren van mensen in het veld vergemakkelijken.
- *Voorbeeld van een toepassing:* Tijdens het plannen van een belangrijk evenement kunnen de vliegbanen op een vliegveld tijdelijk aangepast worden. Meestal worden deze vliegbanen ingetekend op een platte kaart, maar veel beslissers zijn het niet gewend om hiermee te werken. Hetzelfde geldt voor andere beslissingen, zoals het inzetten van mensen in een gebied. Het verrijken van een 2D-situatie op een kaart met een 3D-beeld dat zichtbaar is via een *tablet* kan dan helpen om de effecten van een keuze beter in te schatten. Twee voorbeelden op YouTube zijn de moeite van het kijken waard: het eerste voorbeeld betreft *real-time* vluchten in 3D[22], het tweede gaat over de Arena in Amsterdam[23]. In beide voorbeelden kijkt de gebruiker via een *tablet* naar een kaart op een *touch*-tafel, waarbij de *tablet* de markers en locaties op de kaart herkent.
- *Voorgestelde vervolgstappen:* Aanbevolen wordt om de ontwikkelingen op het gebied van mens-machine-interfaces bij te houden en producten te testen en selecteren om te komen tot toepassing van de juiste techniek en middelen. Daarbij moet worden gekeken naar een goede inpassing in de processen en de organisatie.

[22] https://www.youtube.com/watch?v=bsiHB8AxpqQ&feature=youtu.be
[23] https://www.youtube.com/watch?v=zhnKipiUCJQ&feature=youtu.be

4.7 Informatie beveiligen

Detecteren van *malware* en beveiligen van *cyberspace*

Beschrijving

Malware (*malicious software*) omvat alle vormen van vijandige, opdringerige of vervelende *software*. Het vormt een essentieel ingrediënt van vele soorten *cyber*-aanvallen en is een conditio sine qua non voor het genereren van maatschappelijke en economische impact voor aanvallers. *Botnets*, aan elkaar gekoppelde geïnfecteerde computers, zijn een veel gebruikt hulpmiddel voor *cybercrime*. *(Distributed) denial-of-service* ((D)DoS)-aanvallen zijn pogingen om een computer, computernetwerk of dienst onbruikbaar te maken door met een of meerdere computers tegelijk een aanval uitvoeren. *Ransomware* is *software* die een systeem en/of een bestand 'gijzelt' en vervolgens geld vraagt om het te 'bevrijden'. *Cryptoware*, vergelijkbaar met *ransomware*, is in opkomst: bij *cryptoware* wordt de harde schijf vercijferd en vervolgens wordt om ‘losgeld’ gevraagd.

Encryptie biedt de mogelijkheid informatie te beveiligen en de authenticiteit van het uitwisselen van gegevens te waarborgen. Vercijfering van data wordt in toenemende mate standaard ingebouwd in applicaties en wordt bovendien sterker. In dit opzicht is een geheel nieuwe methode noemenswaardig: homomorfe encryptie. Dit is een recente ontwikkeling (2009) in de cryptografie, die kan worden beschouwd als disruptieve technologie. Dataverwerking in de traditionele encryptietechniek is gebaseerd op het principe dat 'leesbare' data worden versleuteld, bijvoorbeeld voor veilig transport of opslag, maar dat uiteindelijk altijd ontsleuteling moet plaatsvinden om weer 'leesbare' data te verkrijgen. De versleutelde data zijn immers onleesbaar en daarmee niet waardevol. Het veiligheidsniveau hangt af van bijvoorbeeld de sleutellengte en de beveiliging van de sleuteldistributie. Homomorfe encryptie maakt het mogelijk om versleutelde data met elkaar te vergelijken, zonder dat ontsleuteling plaatsvindt. Doordat de vergelijking in het versleutelde domein plaatsvindt en alleen het resultaat van de vergelijking weer ontsleuteld wordt, blijven de vergeleken grootheden geheim. Populair gesteld maakt homomorfe encryptie het rekenen aan versleutelde data mogelijk, zonder de noodzaak om de data eerst te ontsleutelen. Homomorfe encryptie maakt het technisch dus mogelijk om de grenzen die (juridisch) zijn gesteld aan data-opslag en dataverwerking op te rekken door 'verstrekking' van data te vervangen door 'validatie', bijvoorbeeld op basis van een *'hit/no hit*'-systeem.

Intrusion Detection Prevention Systems (IDPS) zijn systemen voor het detecteren en waar mogelijk voorkomen van kwaadaardige activiteiten in netwerken. De trend gaat van signatuur-gebaseerde detectie (virussen, etc.) naar anomalie-gebaseerde detectie (afwijkingen van een ‘normaal’ patroon). *Security Information and Event Management* (SIEM) *software* en producten maken *real-time* analyse van beveiligingswaarschuwingen mogelijk.

Virtuele munteenheden, zoals Bitcoins, vormen alternatieven voor bestaande munteenheden en bieden criminelen de mogelijkheid gemakkelijker anoniem geld uit te wisselen en wit te wassen.

Toepassing

Malware, *botnets*, (D)DoS en *ransomware* / *cryptoware* worden toegepast door *cyber* criminelen. Virtuele munteenheden kunnen hun activiteiten ondersteunen.

IDPS en SIEM zijn technologieën ten behoeve van preventie en detectie van *cybercrime*. Dit naast de al eerder genoemde technologieën zoals *Dark Web Research* (relatie met de functie 'Data analyseren').

Impact

Botnets vormen een belangrijke basis voor veel *cyber*criminaliteit en zijn daarom belangrijk om terug te dringen. Ter bestrijding van *malware* kunnen ontwikkelingen op het gebied van *reverse engineering*, de-verduistering (*de-obfuscation*), *botnet tracking*, analyse van criminele infrastructuren en classificatie en clustering van *malware* worden ingezet. Deze worden aangevuld met methoden om het aantal geïnfecteerde machines en de doeltreffendheid van tegenmaatregelen te schatten en met het in kaart brengen van de *cybercrime*-markt.

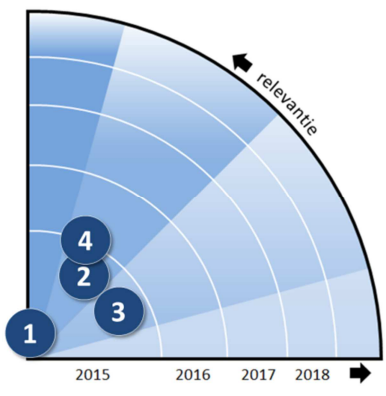
(Big) Data-analyse technieken kunnen hierbij ondersteunen en het identificerend vermogen vergroten: ze kunnen helpen in het herkennen en verkrijgen van een beter inzicht in welke activiteiten plaatsvinden. Detectie- en preventietechnieken als IDPS en SIEM kunnen kwaadaardige activiteiten onderkennen en helpen voorkomen. Zo kan een actueel beeld van *cybercrime* worden gevormd, waardoor de heterdaadkracht kan worden vergroot.

Informatiebeveiliging en encryptie zijn van belang voor contra-strategieën en voor het beveiligen van de eigen data en communicatie. De kwaliteit van de vercijfering wordt steeds beter, waardoor het moeilijker wordt om deze te breken. Voor contra-strategieën betekent dit dat ook alternatieven voor encryptie moeten worden gezocht, zoals de meer traditionele observatietechnieken.

Kennis van en inzicht in virtuele munteenheden tot slot, is van belang omdat geldstromen veel informatie en aanknopingspunten opleveren voor het opsporen van criminele activiteiten.

Relevante technologieën en hun positie op de technologieradar

1. *Malware and malicious infrastructures*
2. Encryptie
3. *Intrusion Detection Preventions Systems* / *Security Information and Event Management* (IDPS / SIEM)
4. Virtuele munteenheden



Toelichting per technologie

Malware and malicious infrastructures

- *Beschrijving en status: Malware* betreft vijandige, opdringerige of vervelende software. Met *botnets* kan *malware* verder worden verspreid en kunnen (*distributed*) *denial-of-service* ((D)DoS aanvallen worden uitgevoerd. *Ransomware* 'gijzelt' een systeem of een bestand. Bij *cryptoware* wordt de harde schijf vercijferd en vervolgens wordt om 'losgeld' gevraagd.
- *Toepassing: Malware*, *botnets*, (D)DoS en *ransomware / cryptoware* worden toegepast door *cyber*-criminelen. Dit vormt een dreiging ten aanzien van *cyber security*. Daarnaast zijn *malware* en *malicious infrastructures* ook van belang voor contraterrorisme.
- *Voorbeeld van een toepassing:* Het is zorgelijk dat feitelijk nauwelijks gedetecteerd kan worden wat de werking van verschillende soorten *malware* precies is. Als het doel van de aanvaller het vergaren van waardevolle informatie is, dan kan *malware* hem hierbij helpen, maar een complexe combinatie van bijvoorbeeld *social engineering*, *malware* en *phishing* kan veel effectiever zijn. Er wordt hierbij vaak gebruik gemaakt van ogenschijnlijk onverdachte handelingen, zoals inloggen met ontvreemde toegangscodes, etc. Men spreekt hierbij van *Advanced Persistant Threats* (APT's).
- *Voorgestelde vervolgstappen:* De ontwikkelingen van (ver)nieuwe(de) typen van *malware* en *malicious infrastructures* bijhouden en contrastrategieën en technieken bepalen. Om in te spelen op *malware* kunnen nieuwe ontwikkelingen ten aanzien van *reverse engineering*, de-verduistering (*de-obfuscation*), *botnet tracking*, analyse van criminele infrastructuren en classificatie en clustering van *malware* worden ingezet. Dit kan worden aangevuld met betrouwbare methoden om het aantal geïnfecteerde machines en de doeltreffendheid van tegenmaatregelen te schatten en om de *cybercrime*-markt in kaart te brengen.

Encryptie

- *Beschrijving en status:* Binnen de cryptografie staat encryptie voor het coderen (versleutelen) van gegevens op basis van een bepaald algoritme. Deze versleutelde gegevens kunnen nadien weer ontcijferd of gedecodeerd worden, zodat men de originele informatie weer terugkrijgt. Dit proces wordt decryptie genoemd. Encryptie wordt in toenemende mate standaard ingebouwd in applicaties. De kwaliteit van de vercijfering wordt steeds beter, waardoor het moeilijker wordt om deze te breken.
- *Toepassing:* Van belang voor contra-strategieën en voor het beveiligen van de eigen data en communicatie. Dit onderwerp is gerelateerd aan *cyber security*.
- *Voorbeeld van een toepassing:* Homomorfe encryptie is een relatief nieuwe technologie die een groot aantal potentiële toepassingen kent. Voorbeelden zijn: *privacy*-bescherming (geen verstrekking maar een vergelijking van persoonsgegevens, zoals toegepast in *TrustTester* technologie), werkelijk veilige data-opslag van gevoelige gegevens (bijvoorbeeld *matchings*-gegevens zoals vingerafdrukken, gelaatsafdrukken, stemfragmenten, autokentekens, etc.), valoriseren van bestaande gesloten *databases* en het delen van validatie-informatie tussen partijen die elkaar niet helemaal vertrouwen (denk aan intersectorale of internationale samenwerking of aan publiek-private samenwerking).
- *Voorgestelde vervolgstappen:* Voor contrastrategieën betekent dit dat ook alternatieven voor encryptie moeten worden gezocht, zoals de meer traditionele observatietechnieken.

IDPS / SIEM

- *Beschrijving en status: Intrusion Detection Prevention Systems* (IDPS) zijn *network security*- toepassingen die netwerk- en / of systeemactiviteiten monitoren op kwaadaardige activiteiten. *Security Information en Event Management* (SIEM) is een term voor diensten en producten die *Security Information Management* (SIM) en een *Security Event Manager* (SEM) combineren. SIEM-technologie maakt *real-time* analyse mogelijk van beveiligingswaarschuwingen die worden gegenereerd door netwerk-*hardware* en applicaties. De *state-of-the-art* in bestaande IDS/IPS systemen is vrijwel uitsluitend gebaseerd op het detecteren van 'harde' *signatures* van bestaande *malware*. De reden hiervoor is dat *signatures* relatief eenvoudig zijn te detecteren in het netwerkverkeer, door *'probes'* of firewalls het verkeer te laten analyseren. Verschillende commerciële partijen

bieden hiervoor (relatief *stand-alone*) systemen aan. Dit werkt op zichzelf vrij redelijk, maar alleen bekende *signatures* worden gedetecteerd (de *zero-days*[24] blijven ongedetecteerd).

- *Toepassing:* IDPS en SIEM zijn technologieën ten behoeve van preventie en detectie van *cybercrime* en dus voor *cyber security* relevant, naast al eerder genoemde technologieën als *Dark Web Research*. Met deze technologieën kan het identificerend vermogen worden vergroot, met als resultaat beter inzicht in welke activiteiten wanneer en waar plaatsvinden.
- Voorbeeld van een toepassing: *Advanced Persistant Threats* (APT's), zoals genoemd onder *malware* and *malicious infrastructures*, worden door IDS/IPS-systemen niet of nauwelijks gedetecteerd. Er wordt gewerkt aan *'policies'* die verdachte combinaties van handelingen detecteren, de zogenaamde *'situational awareness'*, maar dit staat nog in de kinderschoenen. De component *'Intelligence'* over geavanceerde aanvalsmethodieken en hoe deze te detecteren zijn is nog volop in ontwikkeling. Bovendien ontbreekt het organisaties simpelweg aan mankracht en expertise om mogelijke *Indicators of Compromise* (IOC's) allemaal af te handelen. Ook de geautomatiseerde uitwisseling van deze IOC's staat nog in de kinderschoenen. De benodigde technische protocollen, zoals STIX en TAXII, bevinden zich nog in het stadium van standaardisatie. In het buitenland (bijvoorbeeld het BKA in Duitsland) gebruikt men inmiddels wel een (industrie-)standaard. Kortom: traditionele IDS/IPS-systemen zijn slechts beperkt effectief en een nieuwe generatie detectietools is nog niet commercieel beschikbaar.
- *Voorgestelde vervolgstappen:* Detectie en *logging*-technologieën met gebruikers inzetten voor monitoring van de actuele situatie. Nieuwe technieken voor detectie, monitoring en opsporing inpassen in de organisatie.

Virtuele munteenheden

- *Beschrijving en status:* Ontwikkeling van door technologie ondersteunde alternatieven voor bestaande munteenheden of geld, zoals Bitcoins. Een term die hiervoor ook wel wordt gebruikt is *'crypto currency'*.
- *Toepassing:* Geldstromen leveren veel informatie en aanknopingspunten op voor wat betreft illegale en criminele activiteiten. Met virtuele munteenheden zijn er voor criminelen mogelijkheden om gemakkelijker anoniem geld uit te wisselen en wit te wassen. Kennis van deze technologieën is relevant voor *cyber security* en contraterrorisme.
- *Voorbeeld van een toepassing:* Doordat geld anoniem, snel, en onherroepelijk kan worden overgemaakt heeft de online handel in illegale goederen de afgelopen jaren een grote vlucht genomen. Het bekendste voorbeeld daarvan is Silk Road Online, een handelswebsite verborgen in het zogenaamde *Dark Web*. Tussen februari 2011 en juli 2013 bedroeg de totale omzet 1,2 miljard dollar, grotendeels gerelateerd aan *'business to business'* drugshandel. Hoewel de FBI deze *website* inmiddels heeft ontmanteld zijn er tal van alternatieven en deze *Dark Net Markets* blijven een rol spelen in het verhandelen van illegale goederen en diensten. Een kwetsbaar punt in de keten van anonieme handel is de conversie tussen anonieme digitale valuta en normale valuta: deze wordt momenteel vooral gemaakt met behulp van directe transacties tussen consumenten, gefaciliteerd door websites als 'localbitcoins.com'.
- *Voorgestelde vervolgstappen:* Kennis van nieuwe ontwikkelingen op gebied van virtuele munteenheden opbouwen en actualiseren. Digitale geldstromen van virtuele munteenheden koppelen aan de reële wereld (de huidige, reële financiële stromen).

[24] Een *zero-day* aanval is een aanval die gebruik maakt van een nog onbekend lek in een computerapplicatie, dat door de ontwikkelaars nog niet is ontdekt c.q. verholpen. (Bron: Wikipedia)

4.8 Acteren in slimme omgeving

Inzetten van intelligente platformen en infrastructuren

Beschrijving van het cluster

Technologische ontwikkelingen op het gebied van informatietechnologie leiden ertoe dat niet alleen mensen maar ook steeds meer ‘dingen’ – zoals apparaten, infrastructuur en voertuigen – via het internet worden verbonden en gegevens met elkaar kunnen uitwisselen. Daarmee wordt *ambient intelligence*, alom aanwezige intelligentie, realiteit. De eerste voorbeelden van het *Internet of Things* zijn al voorhanden, bijvoorbeeld thermostaten en verlichting die via internet kunnen worden bediend.

Als gevolg van technologische ontwikkelingen wordt er steeds meer ‘intelligentie’ ingebracht in ‘platformen’, zoals voertuigen, robots en *drones*. Auto’s worden in toenemende mate *Smart Cars* die zelf functies uitvoeren. Slimme platformen worden verder ontwikkeld in de richting van kleinere, slimmere, en meer autonome systemen. Bij robots en *drones* is er sprake van een langere termijn ontwikkeling gericht op samenwerking tussen verschillende platformen, tot ‘zwermen’ (robot / *drone swarms*).

Naast (mobiele) platformen worden ook infrastructuren steeds ‘slimmer’, doordat er intelligentie aan wordt toegevoegd, in de vorm van sensoren en technologieën voor informatieverwerking en communicatie. Voorbeelden hiervan zijn *Smart Cities*, *Smart Roads* en *Smart Buildings*. Het interpreteren van data van sensoren en het automatisch slim aansturen van systemen op basis van die data, maakt van steden in toenemende mate *Smart Cities*. Intelligente wegen kunnen zichzelf een beeld vormen van de omstandigheden (gladheid, drukte, mist) en het verkeer daar via informatievoorziening op laten reageren. Slimme gebouwen kunnen zelf hun klimaatbeheersingssystemen aanpassen op de voorkeuren van de medewerkers.

Additive manufacturing of *3D-printing* maakt het mogelijk driedimensionale producten op nieuwe manieren te produceren met behulp van een 3D-printer, de juiste grondstoffen (vergelijk de *toner* in een *laserjetprinter*) en een databestand met de ‘bouwtekening’.

Toepassing

Slimme platformen, zoals robots en *drones*, kunnen worden ingezet voor het verrichten van inspecties en surveillances in voor de mens ontoegankelijke of gevaarlijke omgevingen. Gegevens uit slimme infrastructuur, slimme platformen en het *Internet of Things* kunnen worden gebruikt voor het verkrijgen van een beter inzicht in de omgeving en daarop reageren, bijvoorbeeld door het gericht sturen van verkeersstromen bij een ramp.

Impact

Deze technologieën kunnen als bron (*input*) worden gebruikt voor *real-time* informatie, die kan bijdragen aan een versterking van de informatiepositie en

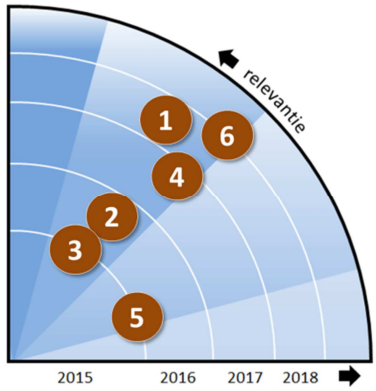
daarmee aan een verschuiving naar een meer proactief opereren (relatie met de functie ‘Data analyseren’).

Een potentieel (nieuw) risico is het *hacken* van de ‘*Connected World*’. Slimme infrastructuur kan een bedreiging vormen wanneer (*cyber-)*aanvallen zich richten op *Smart Cities / Roads / Buildings*, bijvoorbeeld op ondermijning van een logistiek systeem in een haven (relatie met de functie ‘Informatie beveiligen’).

Nieuwe technologie op het gebied van ‘slimme platformen en infrastructuur’ past binnen de al langer lopende ontwikkelingen in de *ambient intelligence*-trend. Het is van belang om inzicht te hebben en behouden in de mogelijkheden om deze technologie toe te passen voor het verhogen van de veiligheid, en in de mogelijkheden van potentieel misbruik. Dit kan in samenwerking met de partners in het veiligheidsnetwerk worden gedaan.

Relevante technologieën en hun positie op de technologieradar

1. *Internet of Things*
2. (Semi-)autonome (mini)robots
3. *Drones / UAV’s*
4. *Smart cities, smart roads, smart buildings*
5. *3D-printing*
6. *Swarm robots*



Toelichting per technologie

Internet of Things

- *Beschrijving en status:* Steeds meer ‘dingen’ – zoals apparaten, infrastructuur en voertuigen – worden via het internet verbonden en kunnen gegevens met elkaar uitwisselen (*machine-to-machine*, kortweg M2M).
- *Toepassing:* Informatie uit het *Internet of Things* maakt het mogelijk op grote schaal gebeurtenissen te meten met behulp van bestaande of zelf geplaatste informatiebronnen in apparaten, infrastructuur, voertuigen, etc. In de toekomst zullen steeds meer apparaten verbonden zijn met internet, misschien zelfs zonder dat we dat weten. Toepassing van het *Internet of Things* is vooral relevant voor crisisbeheersing en maatschappelijke veiligheid. *Machine-to-machine*-communicatie wordt al toegepast. Het *Internet of Things* omvat de trend naar de verdere koppeling van ‘dingen’ en zal naar verwachting in de toekomst steeds prominenter aanwezig zijn.
- *Voorbeeld van een toepassing:* Een idee is *crowd management* om de veiligheid te verbeteren, gebruikmakend van de verschillende typen sensoren die zich in *smartphones* bevinden (*Sensing-as-a-Service*)[25].
- *Voorgestelde vervolgstappen:* De verdere ontwikkelingen volgen. Voor specifieke toepassingen de impact bepalen: welke meerwaarde levert het *Internet of Things* op als bron van informatie of als middel toegepast voor operationeel gebruik (koppeling van eigen apparaten).

[25] Kantarci, Burak, and Hussein T. Mouftah; *Trustworthy Sensing for Public Safety in Cloud-Centric Internet of Things*; IEEE Internet of Things Journal, Vol. 1, No. 4, pp. 360-368; August 2014.

(Semi-)autonome (mini)robots

- *Beschrijving en status:* Intelligente en slimme robots worden verder ontwikkeld en op termijn zullen robots autonomer worden. Daarnaast vindt er een ontwikkeling plaats op het gebied van miniaturisering van robots.
- *Toepassing: (*Semi-)autonome (mini)robots kunnen worden ingezet voor het verrichten van inspecties in voor de mens gevaarlijke omgevingen of voor het uitvoeren van surveillances. Dit is vooral relevant voor crisisbeheersing en observatiedoeleinden.
- *Voorbeeld van een toepassing:* Het bedrijf Knightscope ontwikkelt autonome robots voor surveillance van bekende terreinen in rustige periodes. Eén van de producten van het bedrijf is de Knightscope K5. Deze rijdende 'robocop' werd in april 2014 gepresenteerd aan het Amerikaanse publiek, en kan onder andere kentekenplaten lezen, de luchtkwaliteit meten, beelden maken van de omgeving (ook infrarood) en geluid opnemen. Hij registreert niet alleen, maar kan ook analyses maken van de data, op basis waarvan hij voorspellingen kan doen (*predictive policing*). Op termijn kan hij wellicht ook gezichten of stemmen herkennen[26,27]. Autonome minirobots kunnen door interventieteams gebruikt worden om hen een beter omgevingsbeeld te verschaffen van het gebied waarin ze zich bewegen[28]. Ze worden ook ontwikkeld voor heimelijke observatie, bijvoorbeeld om een persoon op afstand te volgen. Als de kosten dalen en de vliegveiligheid van de robots verder verbetert, zijn ze wellicht ook geschikt om verkeersovertredingen te signaleren.
- *Voorgestelde vervolgstappen:* De verdere ontwikkelingen volgen. Experimenteren om de meerwaarde van robots te bepalen in specifieke toepassingen.

Drones / UAV's

- *Beschrijving en status:* Een *Unmanned Aerial Vehicle* (UAV) of *drone* is een onbemand luchtvaartuig dat op afstand wordt bestuurd of autonoom kan vliegen. Ontwikkeling vindt plaats op het gebied van kleinere en slimmere systemen, bijvoorbeeld *Micro Remotely Piloted Vehicles* en ook meer autonome *UAV's*. Er bestaan al allerlei soorten en maten *UAV's*, maar de wetgeving staat ze nog niet (altijd) toe. De technologie is klaar voor toepassing en geschikte *use cases* zijn talrijk.
- *Toepassing: Drones* worden ingezet voor observatietaken, maar ook voor offensieve missies. Deze toepassingen zijn vooral relevant voor crisisbeheersing en operationeel gebruik (observatiedoeleinden).
- *Voorbeeld van een toepassing:* Het bedrijf MicroDrones verkoopt *drones* voor surveillance van rustige, uitgestrekte gebieden, zoals bij landsgrenzen, pijpleidingen, transportmiddelen en andere soorten vitale infrastructuur[29]. Ook zijn *drones* geschikt om bij crisissituaties snel een actueel overzichtsbeeld te geven, zowel op kleine schaal, bij een verkeersongeluk, als op grote schaal, bij een overstroming of terroristische aanslag. In de toekomst zullen *drones* ook hulpgoederen afleveren in rampgebieden[30].
- *Voorgestelde vervolgstappen:* De ontwikkelingen bijhouden. Experimenteren uitvoeren om de meerwaarde van *drones* te bepalen vanuit een specifieke vraagstelling.

Smart cities, smart roads, smart buildings

- *Beschrijving en status:* Het interpreteren van data van sensoren en het inzetten van deze data voor geautomatiseerde, slimme sturing van systemen maakt van steden in toenemende mate *smart cities*. Het gaat ook om de connecties tussen mensen, gebouwen en producten. Intelligente wegen kunnen een beeld vormen van de omstandigheden (gladheid, drukte, mist) en via informatie het verkeer daarop laten reageren. Slimme gebouwen kunnen hun klimaatbeheersingssystemen aanpassen aan de voorkeuren van de mensen in het gebouw. Dit betreft lange termijn-ontwikkelingen, maar de eerste stappen in de richting van de toekomstvisie worden al gezet (bijvoorbeeld bij experimenten met sensoren in wegen).

---

[26] http://knightscope.com/
[27] http://socialmediadna.nl/knightscope-k5/
[28] http://www.policeone.com/drones/articles/7455866-Why-your-newest-SWAT-team-member-is-a-drone/
[29] http://www.microdrones.com
[30] http://matternet.us/

- *Toepassing: Smart cities, smart roads, smart buildings* zijn te gebruiken als bron van informatie, maar ook als communicatiemiddel. Dit zal vooral relevant worden voor crisisbeheersing en operationele toepassingen.
- *Voorbeeld van een toepassing:* In *Smart Cities* worden gegevens over stedelijke infrastructuren, zoals het vervoersnetwerk, het energienet en de openbare verlichting gecombineerd met gegevens over het gedrag en de wensen van burgers, om tot slimmere keuzes te komen rondom de inzet en het gebruik van die infrastructuren. Hier wordt onder andere aan gewerkt in het Europese onderzoeksproject Accus (www.projectaccus.eu). Een mogelijke *use case* in dat project gaat over incidentmanagement: bij (grote) incidenten zou een stadsbestuur op een eenvoudige manier zowel de verkeerstromen moeten kunnen leiden (besturen van de verkeersregelinstallaties) alsook de straatverlichting zó moeten kunnen schakelen dat hulp- en ordediensten maximale toegang tot de locatie van het incident krijgen, en dat verkeer en personen die daar niets te zoeken hebben er juist van weggeleid worden.
- *Voorgestelde vervolgstappen:* De ontwikkelingen volgen en de (toekomstige) toepassingsmogelijkheden verkennen. Voor wat betreft het mogelijk *hacken* van de *'Connected World'*, de risico's in kaart brengen (*cyber security*).

3D-printing

- *Beschrijving en status: 3D-printing* maakt het mogelijk driedimensionale producten, zoals gebruiksvoorwerpen, te produceren. Daarvoor zijn alleen een 3D-printer, grondstoffen en een digitale 'bouwtekening' benodigd. Verdere ontwikkelingen vinden onder andere plaats op het gebied van de nauwkeurigheid en de snelheid van het printen. Ook wordt er gewerkt aan de toepassing van meerdere materialen (*multi-material*) en aan het printen van structuren op micro- en zelfs nanoschaal.
- *Toepassing: Tailor made*-producten en systemen kunnen worden gemaakt voor toepassing door veiligheidsorganisaties. Productie, bijvoorbeeld van reserveonderdelen, kan op locatie en ad hoc gebeuren. Bedreigingen zijn dat 'iedereen' wapens kan produceren (lange termijn) en dat er producten met minder kwaliteit op de markt komen (korte termijn).
- *Voorbeeld van een toepassing:* Het bedrijf Clear Flight Solutions werkt aan de ontwikkeling van een levensechte roofvogel, die wordt gemaakt door middel van *3D-printing* en die met behulp van sensor- en robottechnologie zelfstandig moet kunnen vliegen om ganzen rondom Schiphol te verjagen[31]. Een tot de verbeelding sprekende ontwikkeling die op langere termijn veel impact kan hebben, is de integratie van elektronica in menselijk weefsel, ook wel bionica genoemd. *3D-tissue printing* maakt dit in principe mogelijk. Zo heeft Princeton University in de VS recent een 'echt' menselijk oor geprint dat radiosignalen kan detecteren en uitzenden[32].
- *Voorgestelde vervolgstappen:* De ontwikkelingen van *3D-printing* bevinden zich nog in de hype-fase, vooral waar het consumententoepassingen betreft. Op basis van verdere ontwikkelingen en toepassingen kan worden bepaald wat de feitelijke kansen zijn om de veiligheid te vergroten met behulp van *3D-printing* en welke bedreigingen de technologie oplevert.

Swarm robots

- *Beschrijving en status:* Naast een ontwikkeling van autonome platformen, zoals robots en *drones*, wordt gewerkt aan platformen die samen kunnen werken in een 'zwerm'. Dit is een langere termijn-ontwikkeling, die nu nog vooral bij universiteiten plaatsvindt.
- *Toepassing:* Net als robots en *drones* zijn *swarm robots* interessant voor het verrichten van inspecties en surveillances in voor de mens ontoegankelijke of gevaarlijke omgevingen.
- *Voorbeeld van een toepassing:* Een *robot swarm* kan een lokaal communicatienetwerk verzorgen bij rampen. Ook kan een *robot swarm*[33] autonoom op zoek gaan naar vermiste personen, en ze kunnen nuttig blijken bij het vinden van zieke mensen in een menigte, door fysiologische kenmerken als temperatuur, transpiratie en hartslag op afstand te meten. Later zal een *robot swarm* bij uitstek geschikt zijn als interventiemiddel tegen een mobiele,

[31] http://www.nu.nl/gadgets/3862301/nederlandse-robotroofvogel-eind-jaar-beschikbaar.html
[32] http://www.technologyreview.com/demo/517991/cyborg-parts/
[33] http://www.cnas.org/sites/default/files/pdf/CNAS_ConferenceTranscript2014_Robotics.pdf

niet-meewerkende tegenstander, zoals een overvaller of een onbekende, dreigende UAV. De grootste *robot swarm* is nu duizend 'platformen' groot[34].

- *Voorgestelde vervolgstappen:* De ontwikkelingen bijhouden en op termijn de mogelijkheden voor toepassing verder onderzoeken, in het verlengde van onderzoek naar de toepassing van robots en *drones*.

[34] Rubenstein, Michael, Alejandro Cornejo, and Radhika Nagpal. "Programmable self-assembly in a thousand-robot swarm." Science 345.6198, 2014: 795-799.

5 Conclusies en aanbevelingen

5.1 Conclusies

Dit rapport biedt inzicht in de technologische ontwikkelingen die de komende vijf jaar relevant zullen zijn voor het verbeteren van de veiligheid in Nederland. Uit de in het kader van dit project uitgevoerde *workshops* met de Nationale Politie en de NCTV, en uit de daarop volgende analyse, trekt TNO de conclusie dat het veiligheidsdomein zich wat technologie betreft de komende jaren zal (moeten) richten op het meer proactief, efficiënter en effectiever werken op basis van informatie(sturing). De zesentwintig technologieën die uit een *longlist* met een kleine tweehonderd technologieën zijn geselecteerd voor dit rapport, zijn dan ook voor een groot deel gerelateerd aan het verzamelen, toepassen, verwerken en presenteren van informatie. Ontwikkelingen op het gebied van de 'informatiemaatschappij' zijn daarmee (ook) voor het veiligheidsdomein bestempeld als zeer relevante technologische ontwikkelingen in de komende jaren.

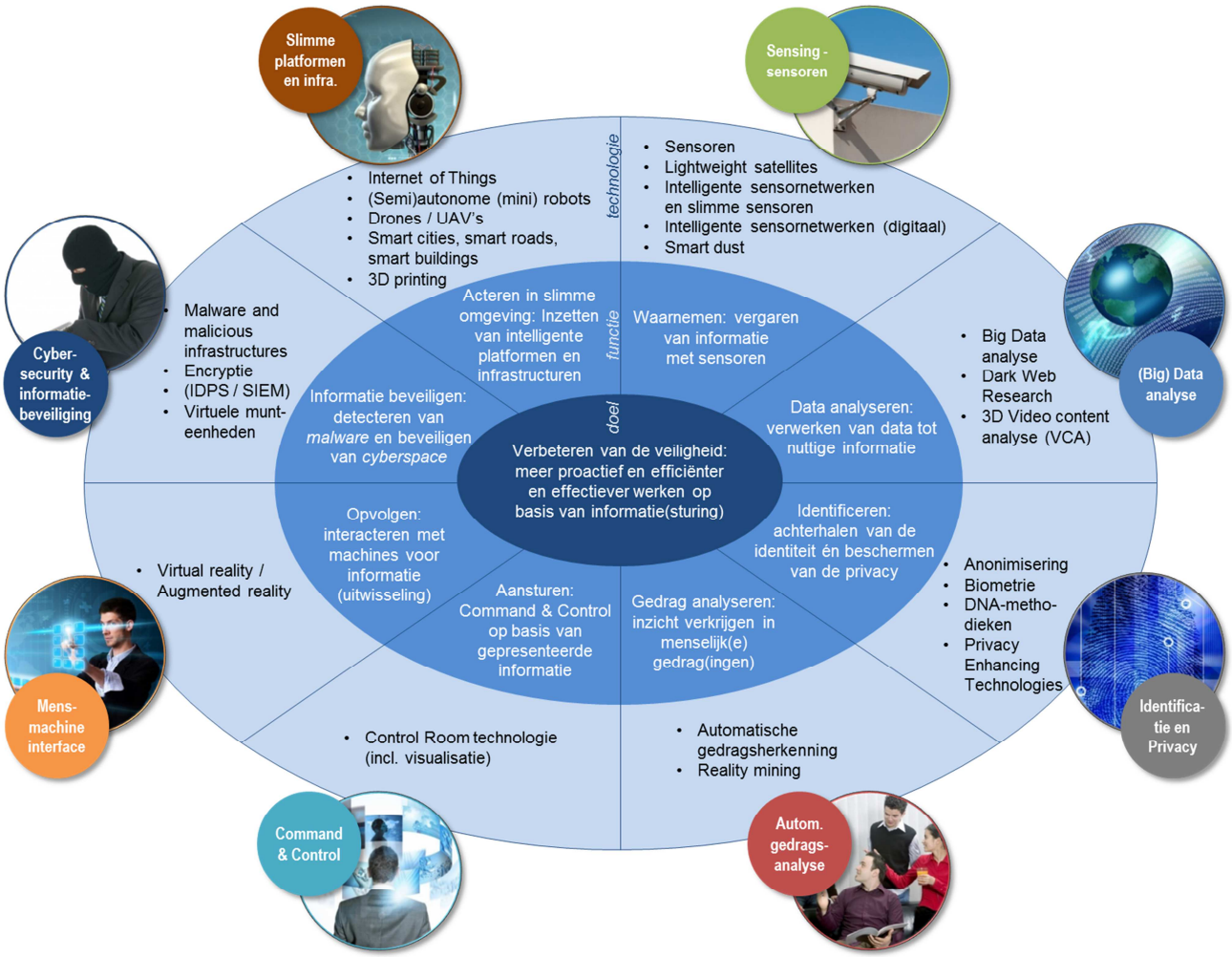
Figuur 5 op de volgende pagina bevat een overzicht van de zesentwintig geselecteerde technologieën. Centraal in deze illustratie staat het doel van veiligheidspartners, namelijk het verbeteren van de veiligheid in Nederland. De tweede ring bevat functies die daarvoor nodig zijn; deze zijn gebruikt als kapstok voor de clustering van de afzonderlijke technologieën, die in de derde ring zijn opgenomen. Opgemerkt zij dat sommige van de beschreven technologieën technisch gesproken al beschikbaar zijn, maar pas hun toegevoegde waarde kunnen leveren als ook aan andere voorwaarden is voldaan. Zo kan wetgeving de toepassing van een aantal in dit rapport genoemde technologieën in de weg staan, zoals bij *drones* het geval is. Verder is het maatschappelijke bewustzijn ten aanzien van veiligheid en *privacy* aan verandering onderhevig, bijvoorbeeld onder invloed van nieuwe dreigingen. Ook dit kan invloed hebben op de acceptatie van nieuwe en reeds bestaande technologieën en verdient daarom aandacht bij veel van de in dit rapport voorgestelde vervolgstappen.

In de Technologieradar Veiligheid heeft TNO de in dit rapport beschreven ontwikkelingen geordend en geprioriteerd op basis van in het project uitgevoerde synthese en analyse. Figuur 6 op pagina 46 schetst deze technologieradar, met per technologie een indicatie van de relevantie en de 'actualiteit' van de ontwikkeling, zoals verwacht op basis van de bevindingen in dit project. De relevantie van een technologie neemt toe naar het midden van de radarplot (er is geen verschil in relevantie tussen de linker- en de rechterhelft) en de afstand vanaf het centrum van de radar geeft de termijn aan waarop organisaties in het veiligheidsdomein zouden moeten zijn voorbereid op de betreffende technologie. De technologieradar vormt aldus een basis voor het maken van (beter) onderbouwde keuzes met betrekking tot het innoveren met technologie, en is bedoeld als inspiratiebron voor strategische kennis- en innovatieagenda's.

5.2 Aanbevelingen

Aanbevolen wordt om de Technologieradar Veiligheid te gebruiken als *input* voor het opstellen van de strategische innovatieagenda's van VenJ, de NCTV en de Nationale Politie. Dat kan door de maatschappelijke opgaven (uitdagingen) te

definiëren vanuit het onderwerp ‘veiligheid’ en van daaruit te bepalen welke kennis en innovaties gewenst zijn om deze op te lossen. De Technologieradar Veiligheid geeft daarbij inzicht in de relevante technologische ontwikkelingen.



Figuur 5 Overzicht van de in dit project onderscheiden relevante technologieën voor de komende vijf jaar, geordend naar functies in het veiligheidsdomein.

Voor borging en betrokkenheid binnen het veiligheidsdomein is het gewenst dit rapport en mogelijk ook de andere rapportages van dit project te delen binnen de eigen organisatie en binnen het netwerk van veiligheidspartners. Aanbevolen wordt om daarbij aan te geven wat er met resultaten wordt gedaan, en om de partners bij dat vervolg te betrekken.

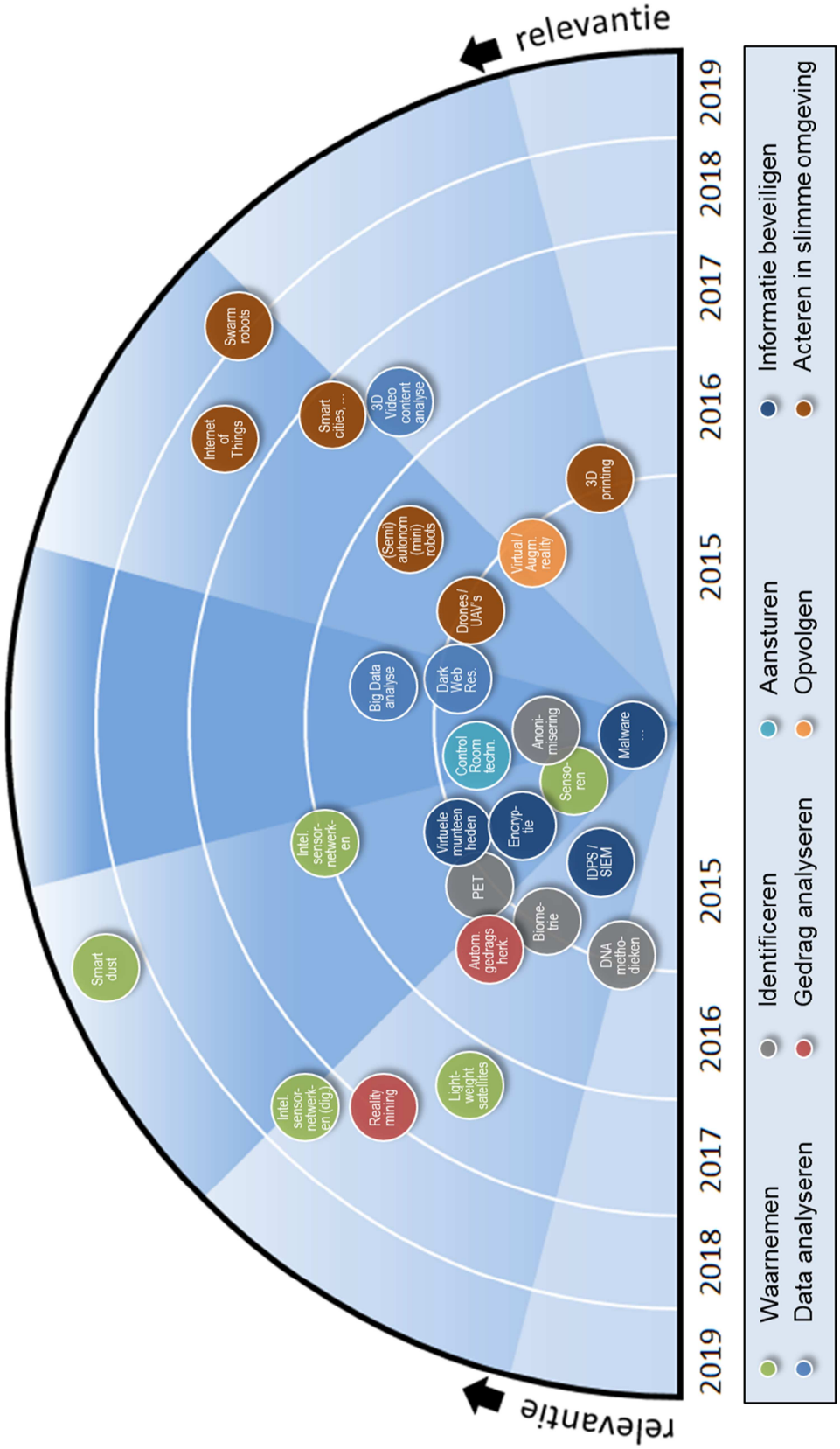
Per technologie worden in dit rapport vervolgstappen voorgesteld. Voor sommige technologieën bestaan de vervolgstappen uit het volgen van de beschreven ontwikkeling, terwijl in andere gevallen wordt gesuggereerd om een proces te starten dat zich richt op een daadwerkelijke toepassing van de betreffende technologie binnen de organisatie. De voorgestelde vervolgstappen kunnen worden

gebruikt bij het opstellen van de eerder genoemde innovatieagenda's en kennisprogramma's.

De ervaring met technologieradars leert dat het voor verdere verdieping en bewustwording van de beschreven ontwikkelingen inspirerend werkt (en leuk is) om periodieke discussiebijeenkomsten te organiseren voor medewerkers die zijn betrokken bij innovatie, waarbij bijvoorbeeld telkens een thema of technologie centraal wordt gesteld en wordt toegelicht door (bij voorkeur) een expert van buiten de eigen organisatie.

Deze Technologieradar Veiligheid kijkt vijf jaar vooruit (2015 - 2019). Aanbevolen wordt om het proces van de technologieradar periodiek te herhalen en om de inhoud telkens te actualiseren, als onderdeel van het (eventueel nog in te richten) innovatieproces binnen de organisatie.

Naast de technologieradar kan – voor innovatiemanagement in het algemeen en voor het opstellen van innovatieagenda's in het bijzonder – het maken van een 'trendradar' met trends op gebied van maatschappij en veiligheid van nut zijn. Met een dergelijke trendradar worden de relevante trends – voor één bepaald thema of in de breedte, voor veiligheid – in kaart gebracht, zodat een goed beeld ontstaat van de maatschappelijke uitdagingen op gebied van veiligheid.



Figuur 6 Technologieradar Veiligheid.

A Technologieradars politiethema's

Deze bijlage bevat een samenvatting van de vier themaradars die voor en met de Nationale Politie zijn gemaakt, afzonderlijk opgeleverd als:

[1] Technologieradar Veiligheid – thema High Impact Crime; TNO; 2014.
[2] Technologieradar Veiligheid – thema Ondermijning; TNO; 2014.
[3] Technologieradar Veiligheid – thema Cybercrime; TNO; 2014.
[4] Technologieradar Veiligheid – thema Dienstverlening; TNO; 2014

A.1 Thema: High Impact Crime

A.1.1 Afbakening en uitdagingen

Onder High Impact Crime (HIC) vallen overvallen/straatroof, woninginbraken (met en zonder braak of geweld, inclusief babbeltrucs), mobiel banditisme en criminele jeugdgroepen. Het betreft 'delicten met een grote impact op het slachtoffer, diens directe omgeving en het veiligheidsgevoel in de maatschappij'. Woninginbraak is momenteel het grootste probleem. Voor 2015-2019 komen er nieuwe prioriteiten. Het Artikel 19 overleg beslist hierover (Burgemeesters en Minister).

Doelstelling is te komen tot minder delicten en meer boeven te vangen: voorkomen van slachtofferschap en verminderen van recidivisme. Voor woninginbraak is het doel te investeren op heterdaadkracht. Burgerparticipatie (bijvoorbeeld: Burgeralert *real-time*: BART) is daarbij een middel. De wens is om verder op te schuiven naar proactief informatie-gestuurd politiewerk (*predictive policing*). Een uitdaging is het orde krijgen van de 'intelligence': informatiesystemen, data.

A.1.2 Strategische vervolgstappen

Het is gewenst de introductie van toepassing van nieuwe technologieën vanuit een samenhangende visie (met combinatie van cultuur, technologie en organisatie) op te pakken. Ontwikkeling in samenhang kan worden gestimuleerd door proeftuinen op te zetten.

- *Sensoren*: Aansluiten bij de visie op Sensing en sensorontwikkeling en -beheer politie-breed organiseren. Bepalen welke informatie relevant is en hoe de informatiepositie kan worden versterkt. De opvolgorganisatie regelen om op basis van sensorinformatie te kunnen acteren. Afspraken maken over hoe verschillende systemen aan elkaar te koppelen.

- *Informatieverwerking*: Technologieën selecteren die kunnen helpen bij het voorspellen. De toegankelijkheid van systemen binnen de nationale politie en extern met partners verzorgen. Informatie(bronnen) koppelen en informatieverwerking integreren in het proces.

- *Command, Control, Communicatie en Informatie*: Eerste fase, gericht op communicatie en afstemming: implementatiegericht de basis leggen voor

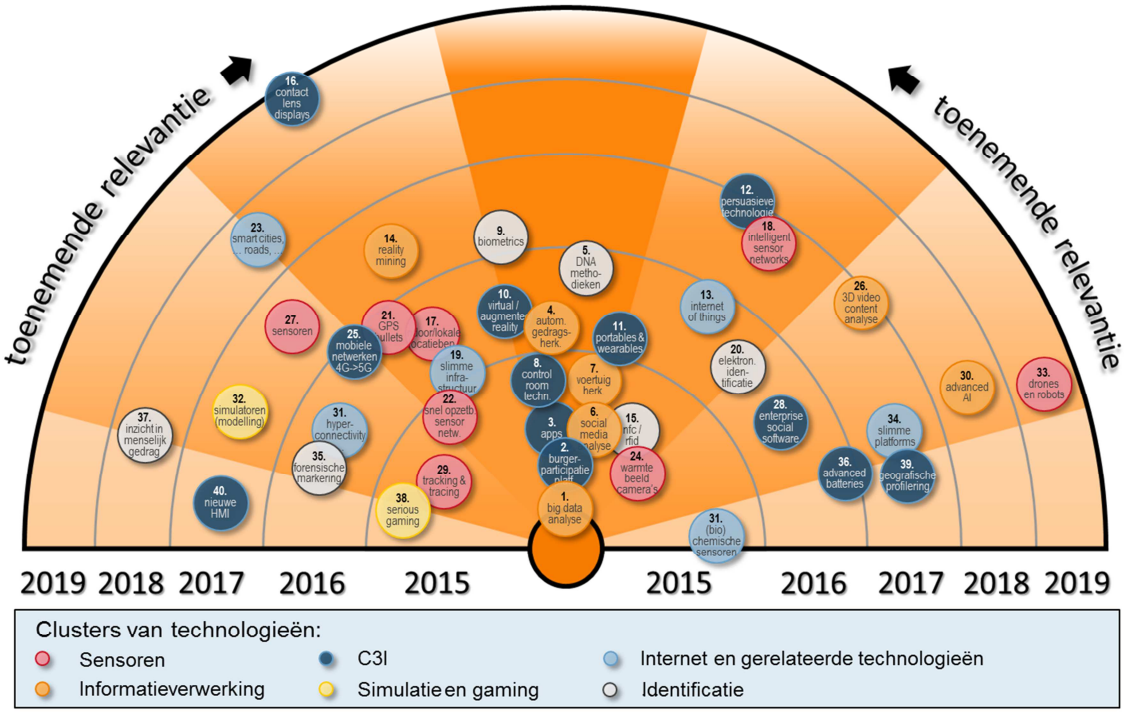
communicatie, meebewegen met de externe ontwikkelingen en daarop koppelpunten definiëren. Tweede fase, gericht op het vergroten van het waarnemend vermogen: experimenteeromgeving opzetten.

- *Simulatie en gaming*: Ervaringen vanuit bestaande simulatie en *gaming* overgedragen tussen de eenheden. Zorgen voor een technisch en functioneel platform dat simulatie en *gaming* ondersteunt.

- *Internet en gerelateerde technologieën*: Selecteren welke informatie de politie wil gebruiken en technisch invullen.

- *Identificatie*: De juridische aspecten in een vroeg stadium verkennen.

A.1.3 Themaradar High Impact Crime



A.2 Thema: Ondermijning

A.2.1 Afbakening en uitdagingen

Een definitie van ondermijning is: ‘Het verzwakken of misbruiken van de structuur van onze maatschappij, leidend tot aantasting van haar fundamenten en/of van de legitimiteit van het stelsel dat haar beschermt.’ Het is een breed onderwerp dat gaat over misbruik van legale structuren waarbij onder- en bovenwereld zijn verweven. Ondermijning is een sluipend proces. Het loopt uiteen van asociale families tot criminele organisaties en kan al dan niet een strafrechtelijke component hebben. Prioriteiten worden gesteld op twee niveaus: gemeentelijk door burgemeesters en landelijk door de Minister. Thema’s zijn momenteel: mensenhandel, drugs, zware milieucriminaliteit, witwassen, motorclubs.

Om ondermijnend gedrag en criminaliteit aan te pakken is het noodzakelijk tijdig signalen op te vangen en gezamenlijk effectief actie te ondernemen. Hierdoor kan het veiligheidsprobleem worden voorkomen, kan een barrière geplaatst of een interventie gepleegd worden. Belangrijk doel is het (vroegtijdig) zichtbaar maken van het onzichtbare en samen met partners (OM, gemeenten, Belastingdienst, banken, …) een interventie vast te stellen en uit te voeren. De ingreep wordt bepaald op basis van het gezamenlijk bepaalde gewenste effect. Het is ook gewenst de effecten van interventies te kunnen meten. Het vroegtijdig signaleren en het delen van informatie vragen om een nieuwe cultuur binnen de betrokken organisaties.

A.2.2 Strategische vervolgstappen

Het is gewenst keten-brede oplossingen te vinden en toepassing van technologieën samen met ketenpartners op te pakken.

Zet een proeftuin op voor één geselecteerd fenomeen. Begin een dergelijke proeftuin klein, in samenwerking met ketenpartners en met koppeling naar lopende projecten. Pas het sturingsregime aan, regel opvolging en ondersteun het proces, onder andere voor het koppelen, verwerken en analyseren van data en het bepalen van interventies.

- *Sensoren*: Op basis van het fenomeen bepalen wat de processen zijn en welke sensoren kunnen worden ingezet. Bepalen hoe sensoren met elkaar samen kunnen werken (sensorfusie). Samenhang aanbrengen tussen Sensoren en *Big Data*-analyse. De stap maken van terug-rechercheren naar real-time rechercheren.

- *Informatieverwerking*: Inzicht verkrijgen in welke informatiebronnen er zijn en signalementen definiëren. Resources (techniek, basisvoorziening, mensen) arrangeren dan wel uitbreiden. Vanuit de proeftuin voor één casus stapsgewijze uitbreiden.

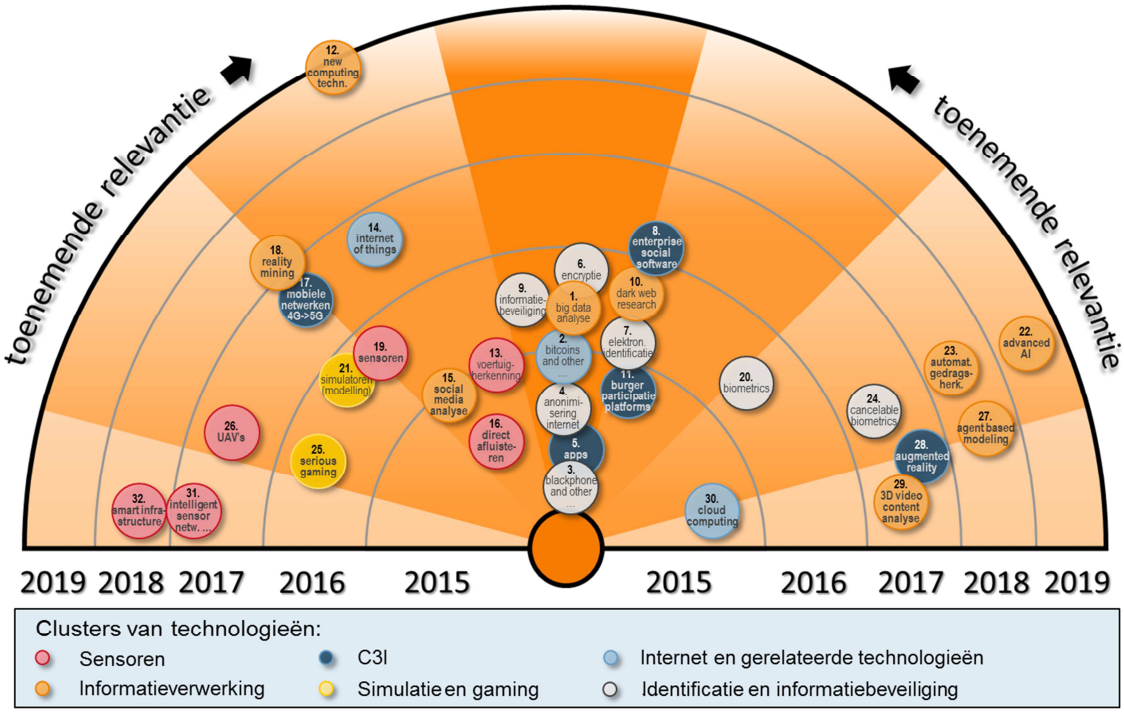
- *Command, Control, Communicatie en Informatie*: De driehoek intelligence, operatie en expertise in samenhang nemen als een elkaar versterkend systeem dat in staat moet zijn om fenomenen te duiden. Van Big Data (real-time) brengen en halen van informatie stappen zetten naar delen van informatie.

- *Simulatie en gaming*: Toepassen om interventie- en barrièremodellen en samenwerken te toetsen op basis van casussen en een nieuwe manier van aansturing te stimuleren.

- *Internet en gerelateerde technologieën*: Uitgaande van fenomenen bepalen hoe de technologieën zijn toe te passen.

- *Identificatie en informatiebeveiliging*: Meegaan met de ontwikkelingen en kennis en technieken inrichten. Alternatieven voor encryptie zoeken: heimelijk observeren.

A.2.3 Themaradar Ondermijning



A.3 Thema: Cybercrime

A.3.1 Afbakening en uitdagingen

Cybercrime betreft misdrijven tegen ICT-systemen met gebruikmaking van ICT. Voor de Technologieradar Veiligheid wordt *cybercrime* afgebakend tot het hi-tech gedeelte er van, dat wordt gekenmerkt door criminaliteit als basis, complexe onderzoeken, innovativiteit, ondermijnende effecten, en/of politieke speerpunten.

Doelstelling is boeven te pakken, de veiligheid te verhogen en Nederland onaantrekkelijk te maken voor cybercriminelen. Uitdagingen zijn de complexiteit van het netwerk, het kunnen herkennen en identificeren van wie achter de cybercriminaliteit zit, het gebruik van sterkere encryptie en mobiele toepassingen, de *cloud*-ontwikkelingen en de jurisdictie (m.b.t. het buitenland). Daarnaast zijn uitdagingen het bepalen van het startpunt van een onderzoek (waar de informatie vandaan te halen) en de forensische integriteit van informatie om zaken te kunnen bewijzen.

A.3.2 Strategische vervolgstappen

Met de technologieën in het cluster '*Detectie, monitoring en opsporing*' kan proactief worden gezorgd voor de eigen mogelijkheden voor preventie, detectie en repressie. Technologische ontwikkelingen in de clusters '*Cybercrime instrumenten*', '*(Cyber)crime ondersteunend*', '*Nieuwe potentiele doelen*' en '*Computing*' zijn externe ontwikkelingen waarvoor is gewenst te weten wat de mogelijkheden zijn er iets mee / tegen te doen.

- *Cybercrime instrumenten*: Informatiepositie versterken: actueel en met een link naar herkennen en identificeren. De *cybercrime* markt (*facilitators*) in kaart brengen. Reverse engineering / software-sporenonderzoek toepassen. Leren omgaan met de financiële componenten; de geldstromen rond *cybercrime*.

- *(Cyber)crime ondersteunend*: Ontwikkelingen signaleren en identificeren.

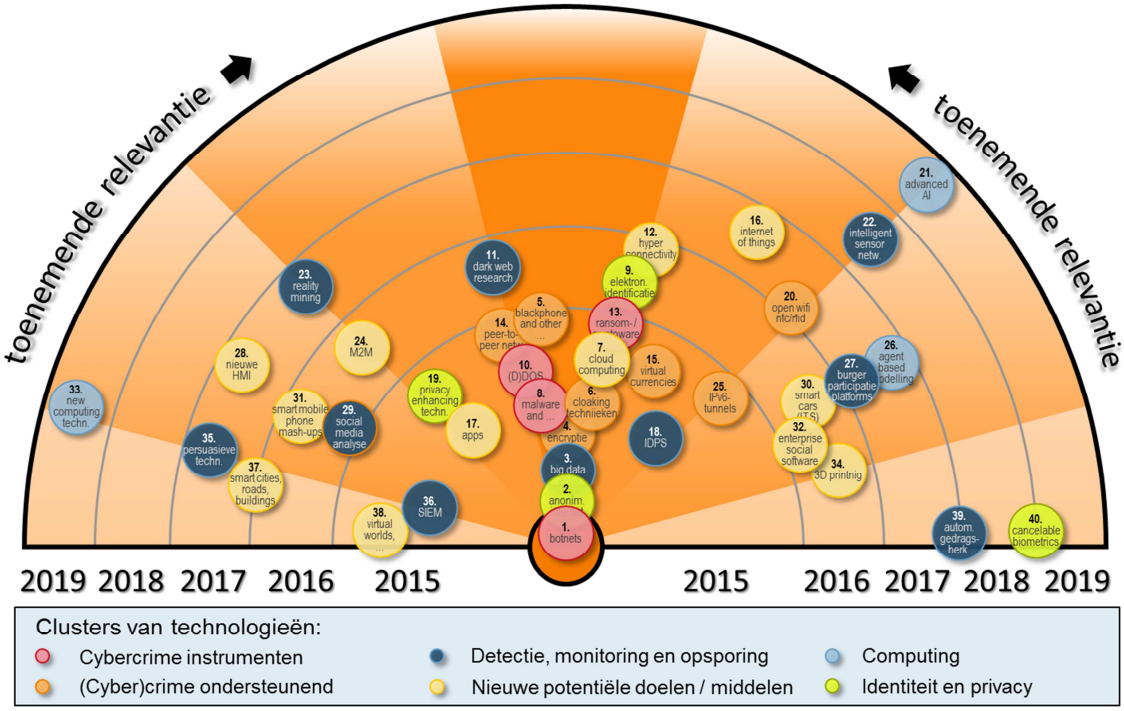
- *Detectie, monitoring en opsporing*: Vergroten van de heterdaadkracht met behulp van detectie en *logging*-technologieën. Binding met de maatschappij versterken: Secure Cyber Community opzetten. Vergroten van het identificerend vermogen met behulp van *(Big) Data*-analyse en slimme sensoren.

- *Nieuwe potentiële doelen / middelen*: Technologische ontwikkelingen en trends volgen. Op basis van potentiële *cybercrime* issues concrete stappen bepalen.

- *Computing*: Lopende projecten (*Web voyager*, *Predictive policing*, *Big data*, etc.) voortzetten in samenwerking in de gouden driehoek.

- *Identiteit en privacy*: Transparant worden naar de burger en in eigen systemen *privacy by design* meenemen

A.3.3 Themaradar Cybercrime



A.4 Thema: Dienstverlening

A.4.1 Afbakening en uitdagingen

Dienstverlening betreft de dienstverlening aan de burger: alle contacten die de politie heeft met burgers. Het gaat daarbij om verschillende processen, zoals: intake en opsporing. Voor dienstverlening wordt uitgegaan van een multikanaal-benadering: telefonie, balie, internet (o.a. www.politie.nl), 3D-aangifte en als verbreding daarvan aangifte op locatie. Naast bovengenoemde kanalen gaat dienstverlening ook om de contacten die wijkagenten en rechercheurs met burgers hebben.

Doel is goede dienstverlening leveren die bijdraagt aan vertrouwen en legitimiteit. Uitdagingen en knelpunten zijn: standaardisatie, de eigen mensen tussen de oren te krijgen het goed te doen en in het gehele proces de burger goed te kunnen volgen (“beleving van de ‘klant’”). Uitdaging is te komen tot landelijke eenduidige dienstverlening met dezelfde kwaliteit en kwaliteitsnormen: opvolging en afhandeling, bereikbaarheid en beschikbaarheid. Gewenst is terugkoppeling te kunnen geven op een melding of aangifte. Voor aangifte is er een vervolgproces (van aangifte tot en met opsporing) met dienstverlening bij verschillende stappen in dat proces. Verder is een uitdaging het (objectief) kunnen meten wat burgers van de dienstverlening vinden.

A.4.2 Strategische vervolgstappen

Voor Dienstverlening ligt de prioriteit bij het realiseren van de kanalen (multikanaal-benadering). De eerste stap daarin is de internetaangifte. Op basis daarvan kunnen andere nieuwe kanalen worden toegevoegd.

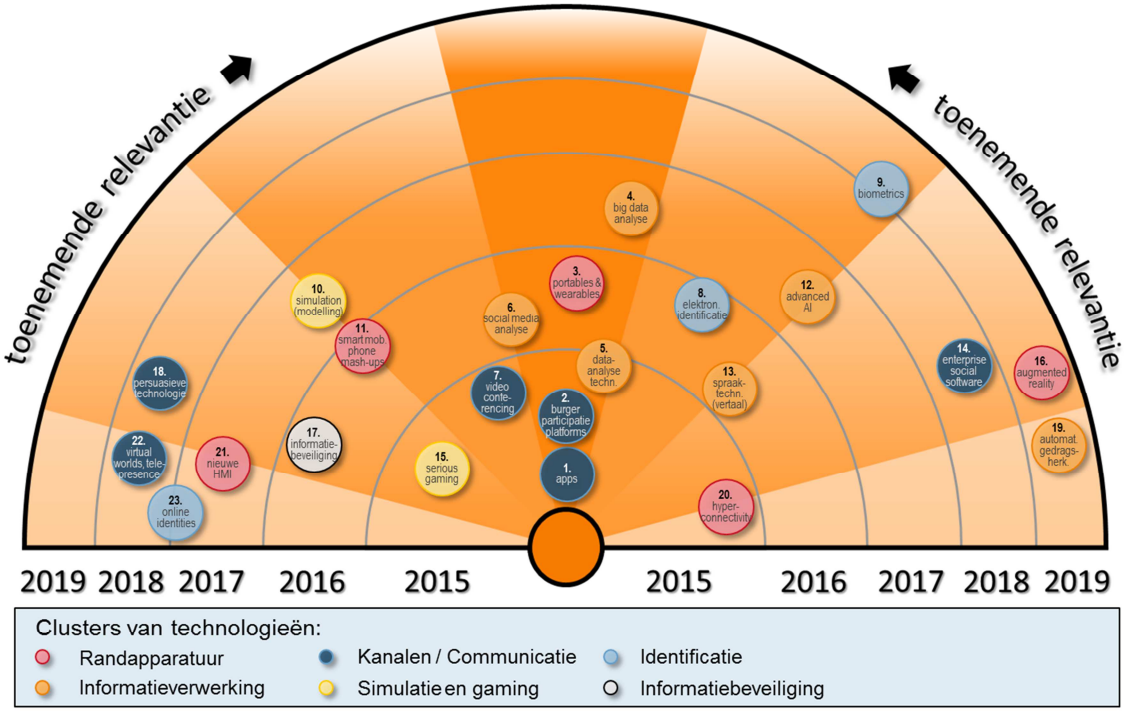
De belangrijkste clusters van technologieën zijn: Kanalen / Communicatie, Informatieverwerking en Randapparatuur.

- *Kanalen / Communicatie*: Robuuste basissystemen ontwikkelen. Internetaangifte ontwikkelen en afstemmen op doelgroepen. Vanuit internetaangifte als basis, apps en andere kanalen ontwikkelen.

- *Informatieverwerking*: Eisen en wensen opstellen voor het inrichten van de techniek en het proces. Informatieanalyse verbeteren als onderdeel van internetaangifte. Het proces voor diverse manieren van meldingen inrichten. Zorgen voor opvolging en koppeling leggen met het systeem voor afhandeling en procesaansturing. Het delen van informatie aanjagen en verbeteren.

Randapparatuur: Bijblijven bij de lopende ontwikkelingen en selectief daarop inspelen. Gebruik maken van verjonging van de dienstverlening of aansluiten bij afdelingen elders binnen de politie die de ontwikkelingen op het gebied van randapparatuur bijhouden.

A.4.3 Themaradar Dienstverlening



B Indicatie van de relevantie van clusters van technologische ontwikkelingen

Technologische ontwikkelingen zijn op vele manieren in te delen; bijvoorbeeld naar (basis)technologie (nano-, bio-/gen-, neuro-, materiaal-, informatie- en communicatie-, energietechnologie, etc.) of naar product of systeem (voertuig, computer, wapensysteem, …). Voor de praktische toepasbaarheid als input voor innovatieagenda's zijn de technologieën in het project Technologieradar Veiligheid zo veel mogelijk gegroepeerd naar functionaliteit.

De onderstaande tabel geeft echter een overzicht van clusters van technologische ontwikkelingen, zoals op basis van de *longlist* van technologieën opgesteld tijdens de eerste *workshop* met de NCTV, bij aanvang van het project. Daarbij is een eerste orde waardering aangegeven van de relevantie voor het verbeteren van de veiligheid in Nederland.

Cluster	Indicatie van de relevantie[35]	
Applicaties (apps, software)	●	Wel kansen, maar al lopende innovatie; geen *game changer*.
Command & Control, Computing en Simulatie	●●●	Vooral Command & Control; *real-time intelligence and action*; veel winst te behalen. Bij Simulatie en Gaming ook: Predictive Intelligence en Artificial Intelligence.
Communicatie	●	Is een middel.
Cyber en Informatiebeveiliging	●●●	Ontwikkelingen gaan snel; gewenst is aan de voorkant te komen.
Data-analyse en -opslag	●●●	Vooral data-analyse: sneller en efficiënter kunnen handelen -> analyse. Data-opslag is een onderliggende technologie.
Energievoorziening	●●	Dit is een ander soort categorie dan de andere technologische ontwikkelingen: meer een onderwerp / brede trendontwikkeling.
Fysieke bescherming en camouflage	●	Gebeurt veel, maar meer voor Defensie.
Gedragsanalyse en -beïnvloeding	●●●	Veel behoefte; heeft een relatie met data-analyse.
Identificatie	●●●	Vooral m.b.t. biometrie, herkenning en DNA. Technologische ontwikkelingen gaan door en worden door zowel veiligheidsorganisaties als maatschappij ingezet (risico en kans; maatschappelijke vraagstukken).
Internet en sociale media	●	Er gebeurt al veel. Wel interessant zijn de Internet of Things-ontwikkelingen. Heeft een relatie met data-analyse.
Mens-machine-interface	●●	Kansen liggen in de verdere toekomst. Is breed toepasbaar door alle partners in het operationele veld.
Mensverbetering: biomedisch en fysiek	●	De ontwikkelingen worden naar verwachting pas op langere termijn relevant. Wel ethische vragen en maatschappelijke impact.

(Wordt vervolgd op de volgende pagina.)

[35] ●: minder relevant; ●●: relevant; ●●●: zeer relevant.

Cluster	Indicatie van de relevantie	
Navigatie en plaatsbepaling	•	Wel belangrijk voor politie en brandweer. Link met social media. Defensie loopt voor.
Platformen en infrastructuur	••	Vooral platformen: UAV als sensorplatform. Industrie doet daar veel effort.
Portables & Wearables	•	Is een middel: gebruiken.
Productie	••	3D printing is risico en kans: is al snel op de radar. De maakindustrie verandert.
Robotica	••	Snelle ontwikkelingen: interessant te weten wat kan (kansen en risico's). Heeft een relatie met platformen (UAV's).
Sensoren	••	Belangrijk voor *situational awareness*: weten wat er gebeurt.
Wapens	•	Meer voor Defensie. *Non-lethal weapons* meer voor de politie zelf.
_Overige	••	De volgende ontwikkelingen zijn relevant: - Convergerende technologieën; - Neurotechnologie: o.a. leugendetectie; - Nanotechnologie: materialen, nanobiologie.

Concept