Defensie & Veiligheid
Oude Waalsdorperweg 63
2597 AK Den Haag
Postbus 96864
2509 JG Den Haag

www.tno.nl

T +31 88 866 10 00

TNO-rapport

TNO 2021 R10809

Verkenning Federatieve Beveiliging – een beveiligingsconcept voor de veilige uitwisseling van informatie tussen publieke en private partijen

Datum	Maart 2021
Auteur(s)	Drs. J.H.C. van Rest J. Nahumury MSc Ir. P.P. Meiler Ing. G.P. van Voorthuijsen Drs. B.W.A. Govers M.H. Wessels MSc
Aantal pagina's	66 (incl. bijlagen)
Aantal bijlagen	4
Vraagsturing	NCTV
Projectnaam	Verkenning van een data- en informatiegedreven beveiligingsconcept
Projectnummer	060.43638

Samenvatting

Deze verkenning betreft een nieuw, informatiegedreven concept om de veiligheid rondom objecten en gebieden efficiënter en effectiever in te richten: federatieve beveiliging. In traditionele beveiligingsconcepten zijn beveiligingsringen hoofdzakelijk bedoeld voor het object dat beveiligd dient te worden. In veel gevallen is echter sprake van overlappende beveiligingsringen door de complexiteit van stedelijke gebieden of openbaarvervoerslocaties. Daarnaast groeit het aantal te beschermen objecten en neemt de complexiteit van het bewaken en beveiligen in stedelijk gebied toe. In samenhang met de toename van ondersteunende ICT-systemen van beveiligingsringen, leidt dit tot de vraag naar een informatiegedreven beveiligingsconcept voor objecten. In dit rapport worden de kansen verkend die een dergelijk concept biedt, en de barrières die daartoe overwonnen moeten worden.

In het concept federatieve beveiliging delen beveiligers hun informatiebehoefte met hun fysieke buren en geven ze inzicht in hun eigen aanbod aan sensordata. De daadwerkelijke informatieverwerking bestaat uit het toetsen van sensordata (zoals gezichten, kentekens, of beschrijvingen van gedrag) tegen volglijsten[1] en profielen – zonder dat deze informatie met een andere partij wordt gedeeld. Hiermee wordt tegemoet gekomen aan privacy regels en wetten.

De doelgroep voor deze verkenning bestaat uit de belanghebbenden bij publiek-private samenwerkingen rond de beveiliging van objecten, personen, gebieden en locaties. Beoogde eindgebruikers van het concept federatieve beveiliging zijn beveiligingsmanagers op tactisch niveau van te beveiligen objecten en evenementen.

In de verkenning staat de volgende vraag centraal: wat zijn de voornaamste technologische en procesmatige kansen van, en barrières voor, het gebruik van federatieve beveiliging bij het beveiligen van objecten en personen? De volgende deelvragen worden hierbij onderscheiden en beantwoord: wat wordt bedoeld met federatieve beveiliging? Welke voorbeelden van overlappende beveiligingsringen zijn te identificeren en wat zijn de voornaamste kansen en barrières (juridisch, technologisch, procesmatig) voor de totstandkoming van een federatieve beveiliging?

Deze verkenning is een eerste stap in een zogeheten *Concept Development & Experimentation* (CD&E) proces. De functie van CD&E is om de risico's die inherent zijn aan innoveren zo goed mogelijk te beheersen. Dit wordt gedaan door vooraf informatie over waarschijnlijkheid van slagen en meerwaarde af te leiden uit beschikbare bronnen, zoals vergelijkbare projecten en ontwikkelingen. Deze studie kent daarom vier onderdelen: a) een verkenning van relevante documenten rondom beveiligingsringen en organisatorische vermogens ('*capabilities*'), b) een verkenning naar initiatieven en (inter)nationale projecten waar TNO bij betrokken is (geweest), c) brainstormsessies met het projectteam om het concept steeds verder te kunnen

[1] Een volglijst ('*watchlist*') is een lijst van dingen of personen die nadere surveillance vereisen, bijvoorbeeld omdat ze gezocht worden.

verfijnen en tot slot d) een interview met een stakeholder waarbij aan de hand van stellingen het concept is verkend en getoetst.

De antwoorden op de deelvragen luiden als volgt. Federatieve beveiliging (FB) is een organisatievorm, een manier van werken en bijbehorende technologie voor organisaties met beveiligde objecten waarvan de observatiegebieden elkaar fysiek raken of overlappen. Dat noemen we overlappende beveiligingsringen.

In federatieve beveiliging delen beveiligers hun informatiebehoefte met hun fysieke buren, waarop zij kunnen intekenen met een aanbod aan sensordata. De daadwerkelijke informatieverwerking bestaat uit het toetsen van sensordata (zoals gezichten, kentekens, of beschrijvingen van gedrag) tegen volglijsten en profielen – zonder dat deze informatie met een andere partij wordt gedeeld. Om te borgen dat de kwaliteit van de sensordata voldoende goed is en blijft, wordt deze aan de verzendende kant gemonitord en gemanaged met behulp van geautomatiseerde analyses. Om verwachtingen te maken voor toekomstige informatiebehoeftes van beveiligers, worden simulaties uitgevoerd van de omgeving van te beveiligen objecten.

Overlappende beveiligingsringen zijn op heel veel plekken te vinden. Overal waar organisaties objecten hebben die grenzen aan de openbare ruimte en die dicht bij elkaar staan, zal sprake zijn van overlappende beveiligingsringen. Het is door toenemende verstedelijking en industrialisatie te verwachten dat het aantal situaties dat zich leent voor federatieve beveiliging zal toenemen.

Er komen drie wettelijke grondslagen in aanmerking als mogelijke juridische basis voor federatieve beveiliging. Wellicht leidt dit ook tot drie soorten federatieve beveiliging:

- Als het een wettelijke taak is van een overheidsorganisatie: in deze context is dat typisch de WPG (Wet Politiegegevens).
- Als het gebeurt door een private partij in opdracht van een overheidsorganisatie: dan is dat AVG (Algemene verordening gegevensbescherming), artikel 6, lid e.
- Als het gebeurt door een private partij vanwege een gerechtvaardigd belang: dat gaat over AVG, artikel 6, lid f.

De belangrijkste grondslag lijkt AVG artikel 6 lid f te zijn. Die wordt door de Autoriteit Persoonsgegevens expliciet als mogelijke grondslag voor de verwerking van persoonsgegevens voor beveiliging geopperd. Daar worden wel voorwaarden aan gesteld. De wet schrijft immers voor dat voor een verwerking, inclusief informatiedeling, op basis van dit artikel, er sprake moet zijn van een echte, reële dreiging. Voor de verzendende partij kan het echter moeilijk zijn om te bepalen of iets een dreiging vormt op de ontvangende partij. Voor de ontvangende partij kan het zonder de betreffende informatie moeilijk zijn om te bepalen of de dreiging echt is. Dat levert dus mogelijk een barrière op om informatie over echte dreigingen te delen.

Een andere barrière is dat er geen grondslag lijkt te zijn voor informatiedeling tussen meerdere partijen tegelijkertijd (1:N of N:N). Daardoor zijn alleen bilaterale relaties mogelijk in één richting per relatie. Bij situaties waar meerdere organisaties

samen willen werken, leidt deze beperking tot een complexere organisatie en hogere eisen aan de ondersteunende techniek.

Om de barrières voor federatieve beveiliging te beslechten moet een centraal loket worden opgezet dat de juridische, organisatorische en technische complexiteit helpt beheersen. Daarnaast zijn een aantal specifieke extra stappen nodig in het reguliere beveiligingsproces. Voor federatieve beveiliging zullen objectbeveiligers bij het bepalen van de dreiging explicieter moeten maken waar deze dreiging – of vroege signalen daarvan – zich fysiek zou kunnen manifesteren. Daarmee kunnen ze inschatten op welke andere plekken ze sensoren nodig zouden hebben. Ook kunnen ze zelf sensoren aanbieden voor anderen om gebruik van te maken. Een centraal loket kan hierbij ondersteunen.

Bij het ontwerpen van het concept voor federatieve beveiliging is gebruik gemaakt van deelconcepten en technologieën uit eerdere projecten die zijn ontwikkeld conform de principes van waardenbewust ontwerpen (‘*value sensitive design’*). In relatie tot federatieve beveiliging zijn vier soorten innovatieve technologie geopperd. Het gaat om profileren, *secure multi-party computation*, *digital twin*, en *managed analytics*. Profileren is het scheiden van series van casussen op basis van een inschatting van een kenmerk, met als doel om opvolging beter (meer proportioneel, eerder) te kunnen plegen. Om te voorkomen dat partijen informatie krijgen die ze strikt gezien niet nodig hebben, is profileren in dit concept gekoppeld aan *secure multi-party computation*. Dit is een vorm van versleuteling waarbij meerdere partijen op een veilige manier een technische verwerking kunnen doen, zonder de invoer voor die verwerking met elkaar te hoeven delen. Een *digital twin* is een digitaal model van een fysieke omgeving waarmee verwachtingen kunnen worden berekend. *Managed analytics* is een klasse van analyse van sensordata, waarmee de kwaliteit van de sensordata (semi-)automatisch kan worden beheerst. Hiermee kunnen mogelijk onnodige foutieve matches zo veel als mogelijk worden voorkomen. Deze technologieën kunnen helpen om de effectiviteit, efficiëntie, en conformiteit met de wet te vergroten.

Het federatieve beveiligingsconcept lijkt recht te doen aan de lessen die geleerd zijn uit eerdere projecten , en lijkt nuttig op basis van een interview met een externe domeinexpert. De gebruikte technologieën zijn in vergelijkbare doch andere contexten in andere projecten deels ontwikkeld op Technology Readiness Level 3 tot 6. Federatieve beveiliging lijkt op basis van deze stappen haalbaar, maar eerst moet het praktische nut op kleine schaal gedemonstreerd worden, om het vervolgens eventueel op te schalen.

Zowel *secure multi-party computation* als profileren zijn nu maatwerk. Daar is wel “confectiewerk” van te maken. Dat vereist aanvullend onderzoek. Een *digital twin* met de functionaliteit zoals beschreven in deze verkenning lijkt nog niet te bestaan voor beveiliging. *Managed analytics* bestaat in de beschreven vorm alleen nog op papier. Goede praktische voorbeelden in een coherent verband bestaan nog niet. Dit leidt tot de barrière “onbekend maakt onbemind”. Vervolgonderzoek en demonstraties in een praktische omgeving zouden deze barrières kunnen beslechten.

Het wordt aanbevolen aan de NCTV om samen met gemeenten, het OM, politie, KMar, en met nader te selecteren sectoren uit de vitale infrastructuur en overige

welwillende (particuliere) uitvoerende beveiligingsorganisaties de wenselijkheid en haalbaarheid verder te verkennen. Het concept kan binnen de CD&E-benadering worden doorontwikkeld en geoperationaliseerd, om het vervolgens in een aantal stappen te testen. Een eerste volgende stap is het organiseren van workshops om het nieuwe beveiligingsconcept in een spelvorm toe te passen op een variëteit aan omgevingen en situaties. Met de opgedane informatie kan vervolgens een eerste basale werkbare variant van het concept worden gedefinieerd. Naar verwachting kan dit grotendeels aan de hand van reeds bestaande technologie. In een latere stap kunnen nieuw te ontwikkelen of te configureren technologieën samen met de industrie worden gerealiseerd. Hierop volgend kunnen praktijkproeven worden uitgevoerd, in eerste instantie in een (deels) gesimuleerde omgeving, vervolgens in een afgebakende fysieke omgeving met een beperkt aantal partijen en tenslotte in een operationele fysieke omgeving met alle relevante partijen.

Inhoudsopgave

1 Inleiding

In dit rapport wordt een nieuw beveiligingsconcept voorgesteld voor samenwerkende (publiek/private) organisaties in het (semi-) openbare domein. Dit is gedaan vanuit een modern perspectief op beveiligen, dat is onderbouwd vanuit een verzameling trends die in eerdere studies als relevant zijn aangemerkt voor het beveiligingsdomein.

Voor het adequaat beveiligen van objecten is allerlei soorten informatie nodig. Bijvoorbeeld informatie over de locatie van die objecten (zoals personen of voertuigen), dreigingen (zoals of er bekende tegenstanders in de buurt zijn, of mensen die gedrag vertonen dat lijkt op een bekende modus operandi), of de toestand van beveiligingsmaatregelen (zoals hun integriteit en beschikbaarheid en ook eventuele kwetsbaarheden daarin). Ook contextuele informatie is van belang, zoals of er ongewone situaties in de omgeving plaatsvinden, wat het algemene dreigingsniveau is in relatie tot specifieke soorten dreigingen, het sentiment van bepaalde bevolkingsgroepen ten opzichte van de eigen organisatie, tot en met informatie over het weer en verkeer.

Er staan allerlei databronnen ter beschikking van beveiligingsmanagers en hun partners om aan deze informatie te komen. De potentie van één soort bron lijkt echter nog maar matig ontsloten te worden: de informatiesystemen van partners in de fysieke omgeving.

Klassieke beveiligingstheorie schrijft voor dat te beveiligen zaken moeten worden omringd door beveiligingsringen. In druk bebouwde omgevingen zullen de buitenste beveiligingsringen overlappen met de beveiligingsringen van fysieke buren. Deze overlappende beveiligingsringen zijn de context voor deze verkenning.

1.1 Probleemstelling

Beveiligingsorganisaties van naburige objecten lijken in toenemende mate nut te hebben bij het onderling delen van data, maar er lijken ook barrières te zijn om dit nut te realiseren. Zowel het nut als de barrières, evenals de werking en meerwaarde van mogelijke oplossingsrichtingen zijn nog onvoldoende duidelijk beschreven.

Een voorbeeld van een barrière kan in de interpretatie en toepassing van de wet zitten. Bijvoorbeeld, er zijn juridische kaders om informatie te delen tussen beveiligingspartijen. In de wet is het proportionaliteitsbeginsel van belang. Die gaat over het afwegen van de mate waarin het risico wordt beheerst, versus de negatieve (maatschappelijke) effecten daarvan. Echter, een dreiging kan zich op andere objecten richten, of er kan plotseling een kwetsbaarheid optreden in de beveiliging. Maatregelen mogen dan dus vanuit dit proportionaliteitsbeginsel gezien “mee ademen”. Werkprocessen en mensen kunnen deze flexibiliteit vaak wel bieden, maar de technologie waarvan zij gebruik maken is daar niet altijd op voorbereid. Het gevolg is dat “om” de technologie heen moet worden gewerkt om toch op tijd benodigde informatie te leveren. Bijvoorbeeld door het kenteken van een bezoeker snel via WhatsApp te delen met het hoofd beveiliging van het naburige object. Dit is typisch niet conform informatiebeveiligingseisen. De

afgelopen jaren zijn ook beveiligde alternatieven verkend om informatie te delen. Soms zijn daarbij lokale convenanten, zoals voor beveiligingsterreinen, gesloten waarbinnen informatie “wel gedeeld mocht worden”. De rechtsgeldigheid hiervan is echter niet duidelijk. Het enkele feit dat partijen een convenant hebben gesloten ontslaat hen niet van de plichten die de wet (AVG, WPG) aan hen stelt. Hooguit kan een convenant meer duidelijkheid verschaffen.

Er is ook een ander probleem met het ontsluiten van dit soort (persoons)gegevens met anderen. Vaak is niet zozeer de data zelf nodig, maar alleen informatie over het resultaat van een verwerking daarmee. Bijvoorbeeld, of een kenteken of een gezicht op een volglijst (‘*watchlist*’) staat. Of de mate waarin gedrag wordt vertoond door passanten dat past bij een bekende modus operandi. Door technische beperkingen is het noodzakelijk om de ruwe gegevens zelf te delen, waarmee de ontvangende partij zelf die verwerking kan doen. Echter, de ontvangende partij kan er ook andere dingen mee doen die niet passen bij het oorspronkelijk doel van de verwerking.

Een ander voorbeeld zit in de technische vorm van maatregelen. Bijvoorbeeld, beveiligingscamera’s kunnen geselecteerd, geplaatst en ingesteld worden voor de detectie van indringers aan de buitenkant van een hekwerk op de grens van het beveiligd gebied. Hiermee kunnen vroege signalen van indringing tijdig worden gedetecteerd. Deze camera’s pakken onvermijdelijk ook een deel van de openbare ruimte mee. Na een overval in de buurt kan het nuttig en toegestaan zijn om de overvaller te zoeken in dergelijke beveiligingscamera’s in de buurt. Maar alleen op camera’s waarop dat een kans van slagen heeft, en bij voorkeur nog gedurende de heterdaadsfase. Echter, bij het selecteren, plaatsen en instellen van die beveiligingscamera’s is geen rekening gehouden met deze functie. Of ze daar dus ook geschikt voor zijn, blijkt typisch pas op het moment zelf – juist wanneer de cameraobservant het al druk heeft met het zoeken naar de dader.

1.2 Oplossingsrichting

Een mogelijke oplossingsrichting is om naast de ringenbeveiliging van individuele objecten ook een structuur te bieden voor samenwerking tussen de verschillende beheerders/beveiligers van objecten binnen een bepaald (semi) publiek gebied of locatie. Een dergelijke intensievere samenwerking tussen publieke en private stakeholders zonder centrale aansturing, en met bijbehorende ondersteunende technologie wordt binnen deze verkenning *federatieve beveiliging* (FB)[2] genoemd. Mogelijk biedt dit meer effectiviteit en efficiëntie, meer proportionele inzet van maatregelen en in drukke gebieden ook een minder “invasieve omgeving” die daarmee voor het publiek aantrekkelijker is.

Meer effectiviteit kan worden bereikt door:

- Betere preventieve werking doordat tegenstanders een lagere slaagkans inschatten.
- Betere voorbereiding waardoor tijdens incidenten minder capaciteit nodig is voor het voorbereiden van data en informatie.

[2] In het projectvoorstel is de term “Federatie van Beveiligingsringen” gebruikt. Die term semantisch onjuist omdat een federatie een samenwerking zonder centrale leiding is van een verzameling organisaties, en een beveiligingsring is geen organisatie.

- Betere informatiepositie tijdens en na incidenten waardoor de stopkracht, heterdaadkracht en opsporingspercentage vergroot worden.

Meer efficiëntie kan worden bereikt doordat sensoren voor verschillende functies worden ingezet, en er dus minder van nodig zijn. Meer proportionele inzet van sensordata doordat de werking van de maatregelen verandert naar gelang het risico verandert. Meer conformiteit met de wet en met beveiligingsnormen doordat legitieme functies (zoals delen van informatie in bepaalde omstandigheden) beter in techniek zijn voorzien.

Ten slotte kan een meer aantrekkelijke omgeving worden gerealiseerd door een betere veiligheid (zie effectiviteit) en daarnaast door een vermindering van het *chilling effect* doordat maatregelen meer conform de wet worden ingezet (zie conformiteit) en er minder maatregelen in het straatbeeld te zien zijn (zie efficiëntie).

1.3 Doel, afbakening en beoogd publiek

Het doel van dit onderzoek is te verkennen welke kansen en barrières er zijn wanneer een individuele ringenbeveiliging wordt uitgebreid met een samenwerking tussen verschillende partijen binnen een (semi) publiek gebied of locatie. Met de informatie die dat oplevert kunnen belanghebbenden zich een oordeel vormen ten aanzien van het nut, de haalbaarheid en de wenselijkheid van het concept.

Deze verkenning spitst zich toe op publiek-private samenwerking binnen het domein bewaken en beveiligen van objecten in de openbare ruimte. De verkenning richt zich op de kansen die dergelijke federatieve beveiliging biedt en hoe technologie kan bijdragen om op een goede manier informatie te kunnen delen, zodat met deze verbeterde informatiepositie beter kan worden bewaakt en beveiligd. Daarbij is gekeken naar een gebied waar over het algemeen verschillende soorten partijen fysiek dicht bij elkaar zitten. Deze studie focust (dan ook) op de fysieke beveiliging, en dan met name op aspecten die te maken hebben met het waarnemen met behulp van technische sensoren (hierna: *sensing*)[3] en informatiedeling. Hierbij wordt ook gekeken naar de mogelijke barrières rondom een dergelijk concept voor wat betreft de (inzet van) moderne technologie. Juridische kaders worden meegenomen voor zover ze relevant zijn, maar dit is niet het hoofddoel van deze verkenning.

De beoogde doelgroep voor dit nieuwe informatie-gedreven beveiligingsconcept is de verzameling belanghebbenden bij publiek-private samenwerkingen ten behoeve van de beveiliging van objecten, gebieden en locaties. Specifiek kan daarbij gedacht worden aan gemeenten, hoofden beveiliging van zowel publieke als private (risicovolle) objecten, tactisch leidinggevenden bij de politie en beleidsmakers bij de NCTV en het Ministerie van Justitie en Veiligheid.

1.4 Onderzoeksvragen

De centrale vraag luidt: wat zijn de voornaamste technologische en procesmatige kansen van, en barrières voor, federatieve beveiliging om objecten te beveiligen?

[3] *Sensing* is het waarnemen met behulp van technische sensoren met de bedoeling een opvolging mogelijk te maken (Van der Steur, 2015).

De volgende deelvragen worden hierbij onderscheiden:

1 Welke voorbeelden/casuïstiek van beveiliging zijn te identificeren (in de literatuur en in de praktijk), waarbij sprake is van overlappende beveiligingsringen?
2 Wat wordt bedoeld met federatieve beveiliging? Is daar een typering in aan te brengen?
3 Wat zijn de voornaamste kansen en barrières (juridisch, technologisch, procesmatig) voor de totstandkoming van een federatieve beveiliging?
   a. Wat zijn de belangrijkste juridische kaders? Welke gronden voor het delen van informatie zitten daar in, en welke barrières?
   b. Wat zijn de belangrijkste procesmatige veranderingen voor de totstandkoming van federatieve beveiliging?
   c. Welke kansen biedt innovatieve technologie?
   d. Wat zijn eventuele barrières om die in te zetten en hoe kunnen die worden overwonnen?
   e. Hoe kunnen digitale modellen van fysieke objecten (‘*digital twinning*’) helpen bij federatieve beveiliging?

1.5 Aanpak en resultaat

De aanpak van deze verkenning bestaat uit de eerste stap van een *concept development & experimentation* (CD&E)[4] aanpak op CML niveau één[5] (Van der Wiel, Hasberg, Weima, & W. Huiskamp, 2010). Dat betekent dat het eerste idee van federatieve beveiliging is uitgewerkt en de kansen in abstracte termen worden geduid. De methodiek van CD&E is gekozen omdat het hier om een meer complexe vernieuwing gaat die meerdere partijen raakt[6].

In deze verkenning zijn daartoe inzichten uit recente en lopende onderzoeken, documentstudie en een interview gewogen, gecombineerd en verwerkt om te komen tot een concept dat aansluit bij het doel en de scope van dit onderzoek.

De CD&E aanpak is ingevuld middels concrete onderzoeksactiviteiten (zie tabel 1). De functie van de **verkenning van relevante documenten** is om de context en het relevante juridische kader duidelijk te krijgen. De functie van de **verkenning naar initiatieven en (inter)nationale projecten** waar TNO bij betrokken is geweest, is om binnen het projectteam een gedeeld beeld te krijgen van de casuïstiek en van de oplossingsrichtingen. Met dit aldus ontstane beeld zijn diverse **brainstormsessies** georganiseerd waarin het concept is ontwikkeld en verfijnd. Het resultaat daarvan is vervolgens getoetst middels een serie opeenvolgende hypotheses en middels een **interview**. Een terugkerende barrière bleek de beschikbaarheid van uitvoerende organisaties te zijn. De methodiek was daar bestand tegen, maar de kwaliteit van het resultaat kan er onder geleden hebben.

---

[4] Bijlage A bevat een overzicht van de gebruikte afkortingen.

[5] Er bestaan verschillende schalen om de volwassenheid van een nieuw idee te duiden. Voor technologie wordt typisch Technology Readiness Level (TRL) gebruikt. Voor ideeën die meer integraal zijn, dus ook werkprocessen, een nieuwe organisatievorm etc. omvatten, is het Concept Maturity Level (CML) geschikt.

[6] CD&E is een ontwikkelmethodiek die in het militaire domein is ontstaan. De functie van CD&E is om de risico’s die inherent zijn innoveren zo goed mogelijk te beheersen. Dit wordt gedaan door vooraf informatie over waarschijnlijkheid van slagen en meerwaarde af te leiden uit beschikbare bronnen, zoals vergelijkbare projecten en ontwikkelingen.

Per activiteit is in onderstaande tabel beschreven welke onderzoeksvragen daarmee beantwoord konden worden.

Tabel 1 De activiteiten waarmee de onderzoeksvragen beantwoord zijn.

	1	2	3a	3b	3c	3d	3e
Een **verkenning van relevante documenten** rondom beveiligingsringen en organisatorische vermogens (‘*capabilities’)*.		x	x	x			
Een **verkenning naar initiatieven en (inter)nationale projecten** waar TNO bij betrokken is (geweest), zodat een actueel beeld is verkregen rondom object- en gebiedsbeveiliging, en in het bijzonder de onderlinge informatie-uitwisseling tussen actoren.	x	x	x		x	x	
Brainstormsessies met het projectteam waarbij nieuwe inzichten worden gewogen om het concept steeds verder te ontwikkelen en te verfijnen**.**		x		x	x	x	x
Een **interview** met een stakeholder (Bureau Nationale Taken (BNT), Landelijke Eenheid, Nationale Politie), waarbij aan de hand van stellingen het concept van een federatie voor beveiligingsringen is verkend en getoetst.	x				x	x	

Deze rapportage geeft een eerste integrale beschrijving van het concept. De functie en de kansen van het concept zijn vooral uit te drukken in het *informatieperspectief* met behulp van eerder gedefinieerde organisatorische vermogens (hierna: *capabilities*). In het *organisatorische perspectief* gaat het om de processen en rollen die nodig zijn om het concept uit te kunnen voeren. Op basis hiervan is kansrijke *technologie* geïdentificeerd waarmee dit concept kan worden gerealiseerd, inclusief eventuele barrières voor de inzet van die technologie.

1.6 Leeswijzer

Hoofdstuk 2 geeft generieke achtergrondinformatie over beveiligen. Dat gaat onder andere over de juridische achtergronden en basiskennis over het ringenmodel. Ook worden relevante maatschappelijke trends geïntroduceerd en wordt kort gereflecteerd op een selectie van eerder geïdentificeerde sleuteltechnologieën. Deze voorkennis is nodig om in de volgende hoofdstukken de werking en toegevoegde waarde van federatieve beveiliging te duiden. Hoofdstuk 2 bevat ook een korte beschouwing op waardenbewust ontwerpen (hierna ‘*value-sensitive design*’) voor bewaken en beveiligen. Hoofdstuk 2 sluit af met een korte beschrijving van projecten waaruit inspiratie en casuïstiek is gehaald. In bijlage B worden deze projecten uitgebreider beschreven. Dat vormt het antwoord op de eerste onderzoeksvraag.

De eerste twee secties van hoofdstuk 3 beschrijven het concept en de werking van federatieve beveiliging en vormen daarmee het antwoord op de tweede onderzoeksvraag.

Secties 3.3 en 3.4 beschrijven de technologieën waarop de werking is gebaseerd. Ook wordt toegelicht welke richtinggevende principes de motivatie vormden voor het concept van federatieve beveiliging.

Hoofdstuk 4 geeft een aantal *use cases* die de werking illustreren van ieder technologisch onderdeel van federatieve beveiliging. In bijlage D staan de stellingen beschreven die in een interview zijn gebruikt waarin een eerste externe toets van het concept is gedaan. Dit vormt gezamenlijk het antwoord op de derde onderzoeksvraag.

Hoofdstuk 5 geeft de beantwoording van de onderzoeksvragen, de conclusies en de aanbevelingen. Veiligheidsorganisaties met specifieke taakstellingen kunnen bijlage C gebruiken om snel een beeld te vormen van het mogelijke nut van federatieve beveiliging voor hun specifieke taak.

Dit rapport gebruikt zo veel mogelijk de Nederlandse taal. Termen waarvoor geen goede equivalente Nederlandse termen bestaan, en die al eerder in formele overheidsdocumenten in het Engels worden gebruikt, zijn in dit rapport ook in het Engels. Voorbeelden hiervan zijn *sensing*, *digital twin*, *capability*, en *value sensitive design*.

2 Achtergrond

De functie van dit hoofdstuk is om benodigde inhoudelijke achtergrondkennis te geven, waarmee de waarde en werking van federatieve beveiliging kan worden uitgedrukt.

Allereerst worden enkele basistermen uit de beveiliging geïntroduceerd, waaronder de betekenis en werking van een beveiligingsring. Daarbij wordt ook nader ingegaan op het begrip ‘capability’ en het *capability-model*. Vervolgens wordt een selectie van globale trends beschreven die relevant zijn voor fysieke beveiliging en voor informatiedeling in het bijzonder. Dit is nodig om de meerwaarde van het concept specifiek te kunnen duiden. Daarna worden enkele sleuteltechnologieën geïntroduceerd, waarmee later de keuze voor bepaalde van die technologieën om het concept mee te concretiseren, gemotiveerd kan worden. Dit hoofdstuk sluit af met een overzicht van recente en lopende onderzoeksinitiatieven rondom informatiedeling.

2.1 Beveiliging

Om objecten tegen dreigingen te beschermen worden veiligheidsmaatregelen getroffen.

2.1.1 Juridische gronden voor beveiliging

In deze sectie worden twee soorten juridische gronden voor beveiliging beschreven. Eén voor overheidsorganisaties wanneer zij een wettelijke taak uitoefenen op het gebied van bewaken en beveiligen, en één voor andere situaties en organisaties[7].

2.1.1.1 Het stelsel Bewaken en beveiligen

Het geheel aan wet- en regelgeving en werkafspraken met betrekking tot het bewaken en beveiligen van personen, objecten en diensten vormt het stelsel bewaken en beveiligen (hierna: stelsel). Een van de uitgangspunten van het stelsel is dat in beginsel de veiligheidszorg voor alle personen, objecten en diensten onder verantwoordelijkheid van het decentrale gezag plaatsvindt. Een uitzondering hierop is de bijzondere verantwoordelijkheid van het centrale gezag (de rijksoverheid) voor bepaalde (groepen) personen, objecten en diensten die een nationaal belang vertegenwoordigen.

In het stelsel wordt op verschillende aspecten van informatiedeling ingegaan. Hierbij gaat het om informatieverstrekking aan de te beveiligen persoon, en het informeren van het gezag. Ook wordt beschreven welke informatieproducten er worden gemaakt om tot (aanpassingen in de) beveiliging te komen.

De overheid heeft de bevoegdheid om in het openbare domein beveiligingsmaatregelen te treffen. Het is op basis van de tekst echter niet duidelijk of die maatregelen gebruik mogen maken van de middelen voor maatregelen van andere (private) partijen.

[7] De informatie in deze sectie is niet door juristen gevalideerd.

2.1.1.2 De Algemene Verordening Gegevensbescherming (AVG)

De AVG geeft in artikel 6 zes grondslagen voor de verwerking van persoonsgegevens.

Lid e van artikel 6 is voor partijen relevant die in opdracht van overheidsorganisaties verwerkingen uitvoeren. Bijvoorbeeld een private beveiligingsorganisatie die ten behoeve van een overheidstaak, en in expliciete opdracht van die overheid, bepaalde beveiligingstaken uitvoert:

> *"de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen."*

Lid f van artikel 6 van de AVG is relevant voor overige situaties en organisaties die persoonsgegevens willen verwerken voor hun eigen veiligheid:

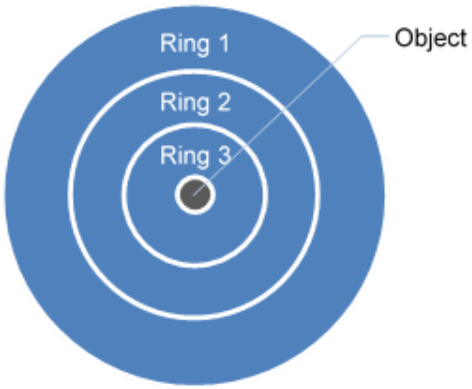
> *"de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is."*

De AP heeft over dit lid een "Normuitleg grondslag 'gerechtvaardigd belang" gepubliceerd (Autoriteit Persoonsgegevens, 2019). In dat document worden o.a. drie cumulatieve voorwaarden gesteld om deze grondslag te mogen hanteren. Onder de voorwaarde "Gerechtvaardigd" wordt o.a. als voorbeeld gegeven "*een veilig en gezond leven te hebben of eigendommen te beschermen in een dreigende ('real and hazardous', stelt de EDPB-guideline) situatie*."

Dit betekent dat zowel de echtheid als de dreiging daarvan duidelijk moet zijn. Echter, als de informatieverwerking gaat over het delen van informatie, dan is het voor de verzendende partij moeilijk om te weten of het om een dreiging gaat op de ontvangende partij, en voor de ontvangende partij is het zonder de informatie te kennen, moeilijk om te weten of het om een echte dreiging gaat. Dit lijkt op de paradox van *need-to-know* versus *need-to-share*, en kan een barrière zijn voor het delen van informatie.

2.1.2 Het ringenmodel

Een objecteigenaar is verantwoordelijk voor, en beveiligt, zijn object. Het basisprincipe wat hij daarvoor toepast heet *security in depth,* ook wel bekend als *layered security* (Nunes-Vaz, Lord, & Ciuk, 2011). *Security-in-depth* wordt gedefinieerd als "*het ontwerp en de gecoördineerde implementatie van meerdere beveiligingsmaatregelen tot beveiligingsringen, om ervoor te zorgen dat een aanval van elke soort niet kan slagen (of een incident geen doorgang kan vinden) zonder dat alle beveiligingsringen zijn uitgeschakeld*." (Nunes-Vaz, Lord, & Ciuk, 2011).



Figuur 1 Traditionele ringenbeveiliging t.b.v. objectbeveiliging.

Dit principe wordt voor een specifiek object dus uitgedrukt in een ringenmodel, zowel in de digitale, als in de fysieke omgeving[8]. Voor een specifiek te beveiligen object wordt dus een stelsel van ringen bepaald, dat er op is gericht om het individuele object te beschermen tegen dreigingen.

Zo kan een beveiligingsring bijvoorbeeld worden ingevuld met vertragings- en detectiemiddelen waardoor de interventietijd voor beveiligers korter is dan de tijd die nodig is voor kwaadwillenden om het te beveiligen object of persoon te bereiken, of, als dat niet kan, potentiële slachtoffers de tijd te geven om te vluchten (Garcia, 2008). Denk hierbij aan het beveiligen van een gebouw waar een hek omheen staat, toegangscontrole is, maar waar ook aparte ruimtes zijn waar alleen geautoriseerde medewerkers mogen komen. Deze ringen hebben hierbij elk hun eigen beveiligingsfuncties en de ingestelde maatregelen dragen daar aan bij. Een ringenmodel is dus een bijzondere vorm van compartimentering, namelijk één waar de compartimenten elkaar omringen, en de compartimenten specifieke functies hebben (Coole, Corkill, & Woodward, 2012).

De ringen hebben typisch één of meerdere specifieke beveiligingsfuncties. Van binnen naar buiten zijn er:

- Het vitale gebied: als de kwaadwillende hier komt dan manifesteert het risico zich. Alles is er op gericht dit te voorkomen.
- Het beveiligde gebied: dit is de ruimte waar detecterende, vertragende en stoppende maatregelen worden toegepast. Dit gebied fungeert als een soort buffer rondom het vitale gebied.
- Het observatiegebied: dit is de ruimte waar het relevante deel van de omgeving wordt geobserveerd.

Deze drie gebieden worden meer specifiek ingevuld met zones met barrières (hekken, muren en grachten) en zones met in- en uitgangen. Dit is een basaal model dat in de praktijk met allerlei variaties kan worden ingevuld.

Het observatiegebied kan in eigendom zijn bij de eigenaar van het betreffende object. Dan kan het fungeren als semi-openbaar gebied waar bezoekers of passanten kunnen zijn. Denk bijvoorbeeld aan de campus gedachte die bij

[8] Beveiliging is typisch georganiseerd langs drie “poorten”. De fysieke poort (gebruikt door een die fysieke indringer), de logische / digitale poort (gebruikt door een hacker) en de menselijke poort (gebruikt om medewerkers te misleiden of anderszins te beïnvloeden).

sommige grote organisaties in gebruik is, zoals bij de Philips High Tech Campus. Het kan ook privaat gebied zijn van een andere organisatie: beveiligd of semi-openbaar. Dat kan gebeuren als beveiligde objecten direct naast elkaar staan.

Het observatiegebied kan ook openbaar gebied zijn, zoals bij bedrijventerreinen of in een binnenstad, zoals bij de Internationale Zone in Den Haag, of bij de Digitale Perimeter in Amsterdam. In dit observatiegebied zullen andere partijen ook een (veiligheids)belang hebben, zoals de openbare orde, en het beveiligen van andere objecten die aan het betreffende openbare gebied grenzen. Dit soort observatiegebied en aanpalende zones (zoals toegangen tot beveiligde objecten) zijn daarom het focusgebied voor deze studie.

Dan zijn er ook de privé situaties van mensen thuis. De AVG is niet bedoeld voor het reguleren van informatieverwerking voor privé gebruik. Maar uiteraard hebben mensen (juist) ook in woonwijken recht op bescherming van hun persoonsgegevens. Dit valt buiten de afbakening van deze verkenning.

2.1.3 Operationele toestand van beveiligingsorganisatie

Het kan nuttig zijn om de operationele toestand van een beveiligingsorganisatie expliciet te maken. Daarmee is het voor eigen medewerkers en ook voor partners duidelijk hoe de beveiligingsorganisatie zal handelen. Het kan daarmee ook een informatiebehoefte aangeven.

In het Internationale Zone project waren de volgende operationele toestanden geopperd door de betreffende deelnemende partijen:

- **Normaal:** Niets bijzonders aan de hand. Er kunnen wel kleine incidentjes zijn die door de lokale beveiligingsmedewerkers kunnen worden opgelost.
  - Er is geen extra informatiebehoefte.
- **Pre-alert:** Er zijn duidelijke (vroege) signalen opgevangen dat de situatie snel tot een incident kan leiden. Medewerkers zijn extra alert.
  - Er is een extra informatiebehoefte gerelateerd aan de vroege signalen.
- **Surprise:** Er zijn signalen dat er zich onverwacht mogelijk een incident voordoet of heeft gedaan. Medewerkers zijn extra alert.
  - Er is een extra informatiebehoefte gerelateerd aan de signalen en aan het type incident.
- **Incident:** Er doet zich met zekerheid een incident voor. Medewerkers die bij het incident betrokken zijn, zijn alert.
  - Er is een extra informatiebehoefte gerelateerd aan het incident.
- **Recovery:** De organisatie is zich aan het herstellen na een incident. De alertheid neemt af.
  - De informatiebehoefte neemt af.
- **High alert:** De organisatie is in opperste staat van paraatheid. Alertheid is hoog.
  - De informatiebehoefte is hoog, maar kan zeer specifiek gericht zijn.

Met dit soort informatie over de operationele toestand van een beveiligingsorganisatie kunnen partners zelf beter inschatten of, en zo ja welke soort informatie mogelijk aangeboden moet en mag worden.

2.1.4 De toegevoegde waarde van beveiliging voor organisatorische capabilities

Om de functie van beveiliging en om de meerwaarde van innovaties daarin beter te begrijpen is het nuttig om gebruik te maken van het begrip ‘capability’. Een ‘capability’ is gedefinieerd als “het vermogen van een organisatie om in en gedurende een bepaalde periode met de haar beschikbare personele en/of materiële middelen de betreffende taak of functie adequaat uit te voeren. Een capability kan worden beschreven vanuit het perspectief van een organisatie, proces, informatie, technologie en mens (Schwedersky, Weima, Stolk, & van Rest, 2020).

In bijlage C zijn allerlei veiligheidscapabilities beschreven zoals die in het project “Voorkomen Aanslagen” voor de NCTV zijn gedefinieerd (zie bijlage A, sectie B.1 voor een samenvatting van de resultaten van dat project). Eén van de capabilities heet “beschermen”. Daar valt het bewaken en beveiligen onder. Deze capability maakt gebruik van voorbereidende en ondersteunende capabilities op gebied van intelligence en vroegsignalering.

2.2 Trends in beveiliging

Verschillende maatschappelijke en technologische ontwikkelingen geven aanleiding om het traditionele beveiligingsconcept te herzien. Deze ontwikkelingen staan hieronder beschreven.

2.2.1 Verstedelijking

Veel te beveiligen objecten staan (steeds vaker) dicht op elkaar in stedelijke omgevingen. De beveiligingsringen van verschillende beveiligde objecten overlappen elkaar daardoor geografisch, zodat er feitelijk sprake is van een “beveiligd gebied”, in plaats van een aantal afzonderlijke beveiligde objecten. Denk bijvoorbeeld aan de Internationale Zone in Den Haag, waar zich diverse internationale instellingen in een relatief klein gebied bevinden, een druk stationsgebied zoals Utrecht Centraal Station en Hoog Catharijne, of een omgeving waar diverse vormen van ontspanning en vermaak geconcentreerd zijn zoals het gebied van de Bijlmer Arena. In dergelijke gebieden hebben vele organisaties een eigen beveiligingstaak met bijbehorende sensoren en informatiebehoeften, zoals de beheerder van het OV-object, de vervoerders, de uitbaters van verhuurde retail ruimtes, de politie en soms ook de KMar. De nabijheid en overlap van beveiliging in dergelijke gebieden biedt mogelijkheden voor gebiedsbeveiliging. De verwachting is dat de verstedelijking zich doorzet (HCSS, 2017).

2.2.2 Aanslagen op soft targets

De laatste jaren zien we dat plaatsen in de (semi) openbare ruimte waar veel mensen samenkomen, een aantrekkelijk doelwit vormen voor aanslagen. Voorbeelden hiervan zijn buitenlocaties die vrij toegankelijk zijn, zoals pleinen en winkelstraten, of vrij toegankelijke gebouwen, zoals cafés, restaurants, winkelcentra en stationshallen. Het gaat hier om *soft targets* waarmee wordt bedoeld dat het publiek het doelwit is. Deze locaties worden gekozen omdat de aanslag relatief makkelijk is en zich richt op het maken van (veel) willekeurige slachtoffers. Dit zorgt mede voor een symbolisch karakter van dergelijke aanslagen, vaak getypeerd als een aanval op de Westerse samenleving en heersende normen en waarden. Een derde van de aanslagen die plaatsvonden in het Westen sinds 2013 was gericht op (semi) openbare locaties (AIVD, 2019). Alhoewel het meest recente Dreigingsbeeld

Terrorisme Nederland laat zien dat de grootschaligheid en complexiteit van aanslagen sinds 2017 is afgenomen, blijven meer provisorische en kleinschalige aanslagen een aannemelijk scenario (NCTV, 2020). Voor (semi) openbare locaties betekent dit een blijvende beveiligingsuitdaging voor de diverse partijen die een rol spelen in de beveiliging van objecten binnen deze locaties of het gebied zelf. Daarnaast zorgt de toegankelijke aard van dergelijke locaties voor complexiteit van de beveiligingsuitdaging om deze locaties te beveiligen tegen aanslagen zonder dat diezelfde toegankelijkheid al te veel in het geding komt.

2.2.3 Voortschrijdende technologie

De ontwikkelingen op gebied van technologie gaan razendsnel (HCSS, 2017). Dat maakt het lastig om betrouwbare en stabiele verwachtingen te maken. Het is mogelijk om de ontwikkeling en met name de *toepassing* van technologie in een patroon, in golven te beschouwen. Dat helpt om actuele ontwikkelingen van elkaar te onderscheiden, en ook om verwachtingen over de toekomst te structureren. Op het hoogste aggregatieniveau van dat patroon zien we de industriële revoluties[9]. We bevinden ons nu in de vierde industriële revolutie, die gaat over de transitie van het gebruik van ICT voor de productie van economische waarde, naar het gebruik van cyber-fysieke systemen (World Economic Forum, 2016).

Als we nauwkeuriger kijken dan zien we binnen die vierde industriële revolutie verschillende soorten nieuwe technologie. In het veiligheidsdomein hebben verschillende partijen in de afgelopen jaren een aantal “sleuteltechnologieën” gedefinieerd. Dit zijn technologieën die:

- Van strategisch belang zijn, i.e. die helpen om grote uitdagingen op te lossen.
- Van strategisch belang zijn voor meerdere taken van de (betreffende) overheid.

De sleuteltechnologieën zijn:

- Big data and data analytics;
- Kunstmatige intelligentie;
- Quantum computing (lijkt vooral relevant voor de logische poort);
- Sensing & Robotica;
- Identificatietechnieken.

En ook zijn *cyberphysical/embedded* systems genoemd (Weima, Schwedersky, van Vliet, & van Rest, 2019).

Dit is nog een wat ongestructureerd lijstje waarvan de inhoudelijke relatie met fysieke beveiliging niet direct duidelijk is. In sectie 2.4 wordt daarom een selectie uit deze technologieën gemaakt, wordt meer structuur aangebracht, en wordt per technologie een relatie (zowel kans als bedreiging) gelegd met fysieke beveiliging.

Als reactie op de opkomst van ICT zijn de afgelopen jaren diverse wetten ingevoerd die het gebruik van persoonsgegevens in verschillende domeinen moeten helpen reguleren.

2.2.4 Coproductie van veiligheid

Veiligheid wordt steeds meer een proces van co-creatie van verschillende stakeholders. Zowel publieke als commerciële bedrijven krijgen steeds meer een

[9] De eerste industriële revolutie werd gevoed door de introductie van de stoommachine, de tweede door de verbrandingsmotor, en de derde door de introductie van ICT.

actieve rol in het veiligheidsdomein. Hierdoor ontstaan in toenemende mate publiek-private samenwerkingen (HCSS, 2017), waarop ook in het kader van bewaken en beveiligen verder op voortgebouwd kan worden.

Kortom, de maatschappelijke en technologische trends bieden kansen en mogelijkheden om een beveiligingsconcept te ontwikkelen dat samenwerking, interactie en informatiedeling tussen verscheidene beveiligingspartijen stimuleert en mogelijk maakt. Technische, functionele, juridische en politiek-bestuurlijke barrières die samenwerking en informatiedeling in de weg staan moeten daarbij worden overwonnen.

2.3 Sleuteltechnologieën voor beveiliging

Eerder, in sectie 2.2.3, is het gebruik van nieuwe technologie, en met name de vierde industriële revolutie als belangrijke trend benoemd. Bij nadere beschouwing binnen die vierde industriële revolutie zijn verschillende golven van nieuwe technologie te ontwaren. Op die golven gaat deze sectie in meer detail in.

Het gebruik van nieuwe technologie maakt het typisch mogelijk om daar boven op weer andere technologie te gebruiken. ICT heeft bijvoorbeeld platformtechnologie mogelijk gemaakt. Een ontwikkeling kan ook een latente behoefte ontsluiten en daardoor een zelfversterkende kracht worden voor de vorige golf. Denk bijv. aan mensen die een *smartphone* (een vorm van ICT) kochten om op *social media* (een bepaalde soort platformtechnologie), te kunnen interacteren. De golven interacteren dus met elkaar. Deze algemene patronen zijn niet vanzelfsprekend op iedereen van toepassing. Niet iedere (soort) gebruiker kan en wil gebruik maken van nieuwe technologie. Bijvoorbeeld als er kwetsbaarheden of dreigingen gemoeid zijn met bepaalde technologieën, kan (de bereidheid voor) het gebruik plotseling inzakken.

Het is dus niet zeker dat de vierde industriële revolutie zoals beschreven door Schwab er ook echt komt. Desondanks kan het denken in dit soort samenhangende golven helpen om structuur in toekomstverwachtingen te brengen. Ook kan het helpen om te verwachtingen te temperen voor wat betreft technologieën die nog verder weg liggen.

2.3.1 Derde industriële revolutie: digitalisering

De vorige industriële revolutie, die van de introductie van ICT, had uiteindelijk verregaande digitalisering tot gevolg. Sensoren werden digitaal, net als transport en opslag van data. Data en informatie zijn praktisch overal toegankelijk en werkprocessen – ook die op gebied van bewaken en beveiligen, zijn sterk afhankelijk geworden van deze digitale informatie.

De beveiligingssector is massaal overgestapt op IP-technologie. Toegangscontrole werkt op basis van digitale passen met RFID. Beveiligingscamera's werden digitaal. Controlekamers zijn gedigitaliseerd, en beveiligingsmedewerkers zijn altijd en overal te bereiken middels smartphones en andere mobiele apparaten.

Deze golf gaat onverminderd door. Denk aan nieuwe ontwikkelingen zoals:

- Kleinere, gevoeligere, goedkopere sensoren (bijv. zoals gebruikt in smartphones).

- Kleinere energiezuinige en snellere draadloze communicatiemiddelen,
  - onder andere Bluetooth, ZigBee, Thread, LoraWAN, WiFi, NFC, 4G/5G,
  - deze worden ook voor Internet of Things (IoT) gebruikt; ook deels in smartphones.
- Wearable technologie (o.a. manieren om aan mensen te meten (sensing) direct op hun eigen lichaam of vanaf het lichaam van iemand in de omgeving, zoals de bodycam).

2.3.2 Golf 1: Platformtechnologie

Platformtechnologie koppelt aanbieders aan consumenten van diensten, waaronder allerlei informatiediensten. Doordat het elimineren van fysieke aspecten van marktplaatsen (zoals winkels, fysieke opslag en fysiek transport) in de commerciële sector tot grotere winsten leidt, wordt er wereldwijd en in hoog tempo aan platformtechnologie gewerkt. Internet (ADSL/VDSL, Fiber-to-the-Home, WiFi, 4G/5G) is uiteraard tegenwoordig de meest basale vorm van een platformtechnologie. Deze verbindt vrijwel alle domeinen met elkaar. Daar boven op gebeurt dit ook in meer gespecialiseerde vorm in allerlei domeinen: thuis (domotica), in de industrie (*smart industry*) en in steden (*Smart Cities*). Platformtechnologie wordt mogelijk gemaakt door de ontwikkeling van standaarden en nieuwe (maatschappelijke) “business modellen” voor allerlei (digitale) technieken.

In de beveiligingssector zijn bijvoorbeeld *Physical Security Information Management* (PSIM) systemen opgekomen. Dit zijn software platformen die allerlei veiligheid en beveiligingssystemen aan elkaar koppelen. Dit biedt een eenduidige gebruikersinterface. Het biedt ook de mogelijkheid om informatie snel te koppelen en om bepaalde (re)acties integraal (dus over verschillende systemen heen) te organiseren.

Platformtechnologie kan samenwerking met andere organisatieonderdelen en organisaties faciliteren. Ook kan platformtechnologie het mogelijk maken om diensten te centraliseren. Bijvoorbeeld om dreigingen te herkennen op basis van signalen van verschillende objecten, en bijvoorbeeld centrale commandovoering op fysieke beveiliging.

Voorbeelden van ontwikkelingen zijn:

- Toename van aantallen en soorten onlinediensten (bijv. cloud computing).
- Alerteringssysteem Terrorismebestrijding, LiveView en Camera in Beeld.
- Platformen voor *identity management* zoals bijvoorbeeld die het bedrijf 20FACE levert voor het beschikbaar stellen van gezichten (*informed* en expliciete consent) voor toegangscontrole.
- Communicatie- en encryptie varianten waarmee op veilige wijze toch afgeschermde informatie kan worden gebruikt zoals *multi-party computation*.
- *Smart cities* in de omgevingen van te beveiligen objecten die mogelijk relevante informatie of zelfs handelingsopties kunnen ontsluiten.

2.3.3 Golf 2: Big data & analytics

Big data (& analytics) is een verzameling technologieën die helpt bij het verzamelen, verwerken en ontsluiten van grote hoeveelheden (vaak complexe) gegevens. De omvang van de hoeveelheid data is niet (meer) het enige onderscheidende factor. Het gaat ook om de variatie van de datatypen en structuur,

en de snelheid waarmee deze verwerkt moet worden om waarde toe te kunnen voegen. Deze ontwikkeling vereist ICT, en heeft enorm baat bij het gebruik van platformtechnologie om data van producenten bij gebruikers te krijgen.

Deze ontwikkeling maakt bijvoorbeeld mogelijk:

- Het maken van een digitale representatie (een zgn. *digital twin*) van complexe systemen, zoals steden, of te beveiligen objecten om daarmee fictieve (toekomst)scenario's te analyseren.
- Harde en zachte[10] vormen van biometrie voor het authentiseren en terugvinden van personen.
- Het vinden van nieuwe patronen en trends die wijzen op nieuwe vormen van bonafide en van malafide gedrag in gebruiksdata.
- Intelligente sensoren die verdacht en afwijkend gedrag herkennen, zoals bijvoorbeeld indringers, of personen die een beveiligd object verkennen.
- Profileren van personen of situaties waarmee vroege signalen van (on)gewenste patronen ook live kunnen worden gesignaleerd. Zoals signalen van bezoekers of collega's die slordig of zelfs malafide met de beveiliging om gaan, of die wijzen op een gebrek aan integriteit.

2.3.4 Golf 3: Kunstmatige intelligentie

Kunstmatige intelligentie gaat over het in meer of mindere mate autonoom maken van bepaalde vormen van informatieverwerking zoals leren en besluitvorming. Er zijn verschillende routes om tot kunstmatige intelligentie te komen. Een veel gebruikte en effectieve manier is om grote hoeveelheden (big) data te gebruiken om de kunstmatige intelligentie te trainen.

Deze ontwikkeling maakt bijvoorbeeld mogelijk:

- Automatisch beheren van de kwaliteit van databronnen in relatie tot informatiebehoeftes. Als de kwaliteit van een databron (van anderen) onder het niveau zakt dat nodig is voor een mogelijke informatiebehoefte, dan kan automatisch worden bepaald wat daar de oorzaak van is. Vervolgens kunnen corrigerende acties worden voorgesteld, en, binnen grenzen, eventueel worden uitgevoerd. Hierdoor leveren databronnen vaker tijdig de benodigde kwaliteit.
- Automatische reactie op beveiligingsincidenten. Als er in een commandosysteem verdacht gedrag wordt gesignaleerd, dan kunnen er (semi-)autonoom acties in gang worden gezet, zoals het sluiten van deuren of hefbomen. Belangrijk aandachtspunt hierbij is dat het vaak ethisch en juridisch vereist is om ten alle tijden betekenisvolle menselijke controle te behouden.
- Autonome mobiele platformen, zoals drones en autonome voertuigen. Dit kan nuttig zijn voor (eenvoudige) surveillance taken rond objecten. Maar tegenstanders kunnen er ook gebruik van maken. Bijvoorbeeld om een object ongezien binnen te dringen, of om schade toe te brengen.

2.3.5 Vierde industriële revolutie: Cyber-physical systems: robots, cyborgs and augmented mensen

De vierde industriële revolutie over *cyber-physical systems* omvat, en bouwt voort op de derde revolutie (ICT) en de hierboven beschreven meer specifieke technologische golven. Deze vierde revolutie gaat over de toepassing van kunstmatige intelligentie in relatie tot de mens als biologisch en mentale entiteit. Het

[10] Zachte biometrie is het herkennen van personen op basis van veranderlijke eigenschappen zoals kleding, haarkleur, etc. (bijv. suspect search en digitaal aura).

gaat dan om de mens als werknemer, als bezoeker, maar ook de mens als tegenstander. Het gaat hier om technologieën die zich zeer dicht op of zelfs in het lichaam bevinden, en die zorgen dat mensen in veel meer soorten uitdagende omstandigheden normaal, of zelfs bovenmenselijk kunnen presteren.

Hier gaat om de volgende soorten ontwikkelingen:

- *Quantified self*: manieren om jezelf in data te beschrijven waarmee je jouw functioneren kunt verbeteren.
- Exoskeletten: technologie die mensen in staat stelt om uitzonderlijk fysieke prestaties te leveren in uitzonderlijke omstandigheden.
- Cognitieve *agents* (zowel in robot als “lichaamloos”) die complexe beveiligingstaken kunnen afhandelen.

Hier kan bijvoorbeeld worden gedacht aan systemen die complete aspecten van beveiliging min of meer autonoom verzorgen. Zoals een AI die alle aspecten van toegangscontrole verzorgt, inclusief autorisatieschema’s op basis van functies van mensen, authenticatie en toegangsverlening bij toegangen en het bepalen of er na een evacuatie nog mensen binnen zijn. Een andere vorm zou een persoonlijke uitrusting kunnen zijn voor te beveiligen personen en/of voor bewakers en beveiligers die hen in staat stelt om bovenmenselijke prestaties op gebied van bewaken en beveiligen te leveren.

Hoewel dit soort ontwikkelingen wel worden genoemd in technologieverkenningen, zijn ze nog pril, en nog niet zichtbaar in beveiliging. Deze ontwikkelingen worden daarom in deze studie verder niet meer gebruikt.

2.4 Value sensitive design voor bewaken en beveiligen

In reactie op de toenemende maatschappelijke en ethische impact van het gebruik van nieuwe technologie, is de beweging van *value sensitive design* ontstaan. Dit is het principe dat menselijke waarden zoals privacy en veiligheid gedurende de gehele levensduur van ICT systemen meegenomen moeten worden. Dus vanaf het eerste begin, tot en met het opruimen van dergelijke systemen (Van Rest, Boonstra, Everts, van Rijn, & Van Paassen, 2012).

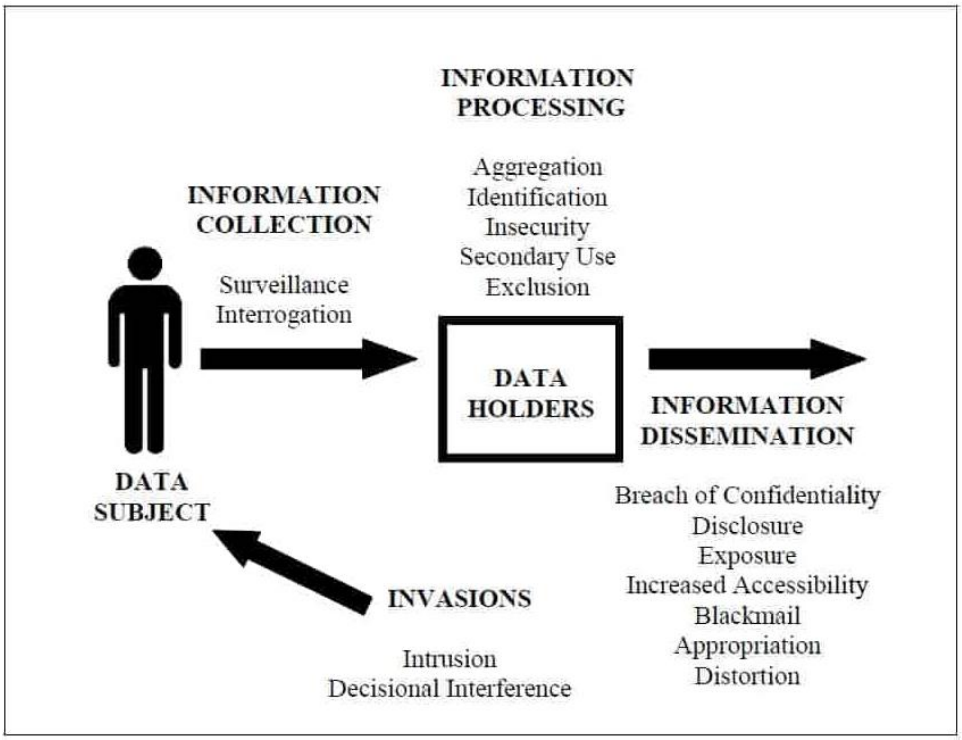
Een gerelateerd idee is dat technologie niet waarden-vrij kan zijn. De vorm waarin technologie beschikbaar is, en voorbeelden van gebruik door anderen, suggereren aan nieuwe gebruikers hoe de technologie gebruikt kan worden. Bijvoorbeeld, een systeem dat continu een knop in beeld heeft waarmee een bepaalde informatieverwerking gestart wordt, suggereert daarmee sterk aan de eindgebruiker dat die verwerking op enig moment plaat moet vinden. Dat idee wordt verder versterkt als de eindgebruiker ervaart dat zijn collega’s daar ook daadwerkelijk gebruik van maken.

Ook op gebied van bewaken en beveiligen zijn dit principe en dit idee relevant, aangezien ook hier intensiever gebruik wordt gemaakt van nieuwe technologie (zie vorige secties). Voor wat betreft het delen van data tussen beveiligers van nabije objecten, gaat het vooral om de menselijke waarden van “veiligheid” en van “privacy” – beiden in ruime zin. Dus zowel de aspecten van veiligheid die gaan over objectieve als over subjectieve veiligheid. En bij privacy zowel de aspecten die

gaan over de verwerking van persoonsgegevens, als die gaan over beslissingsinterferentie en het recht om met rust te worden gelaten.

Deze studie maakt wat privacy betreft gebruik van twee uitvoerige analyses die gedaan zijn in eerdere studies. Eén over de privacy impact van profileren (Van Rest, et al., 2020), en één over de privacy impact van het gebruik van niet-coöperatieve gezichtsherkenning (Van Rest, Attema, Timan, Den Hollander, & Van Voorthuijsen, 2021). Beide studies maken in een respectievelijke bijlage van de taxonomie van privacy dreigingen van Solove (Solove, 2005), van recente wetenschappelijke inzichten en van recente Nederlandse beleidsdocumenten om de impact van het gebruik van de betreffende technologie op bepaalde soorten privacy te duiden.

In hoofdstuk 3, sectie 3.3 worden specifieke technologieën geïntroduceerd die bij kunnen dragen aan federatieve beveiliging. Per technologie wordt daar ook beschreven hoe deze menselijke waarde privacy inherent helpt beschermen. Dat wordt gedaan door de privacy impact van de inzet van technologie te vergelijken met een alternatief dat hetzelfde veiligheidseffect zou bereiken, maar dan zonder de betreffende technologie. Daarvoor wordt de terminologie van Solove gebruikt (zie figuur 2).



Figuur 2 Taxonomie van privacy dreigingen (Solove, 2005).

2.5 Recente en actuele projecten

Als laatste onderdeel van dit hoofdstuk wordt een overzicht gepresenteerd van recente en actuele projecten waarbij TNO betrokken is die inzichten opleveren ten aanzien van technologieën rondom informatiedeling die relevant zijn voor deze verkenning. In tabel 2 staan de belangrijkste inzichten die zijn meegenomen in het

nieuwe beveiligingsconcept dat in het volgende hoofdstuk wordt beschreven. In bijlage B zijn enkele relevante recente projecten beknopt toegelicht.

Tabel 2 Inzichten uit recente en actuele projecten.

Project	**Inzichten**
'Voorkomen Aanslagen' (Schwedersky, Weima, Stolk, & van Rest, 2020)	• Het is mogelijk om inhoudelijk overzicht te bieden over de verschillende taken en rollen in het domein van contra-terrorisme. • Capabilities en functies zijn vaak voor meerdere taken nuttig. Bij het verbeteren daarvan is het nodig om dit vanuit een breed perspectief te doen.
Internationale Zone (The Hague Security Delta, 2019)	• Op papier lijkt een meer gebiedsgerichte veiligheidsbenadering wenselijk. • Verbeteren van samenwerking ten behoeve van efficiëntere en effectievere respons en daarmee het creëren van een betere 'overall security'. • Het is technisch en operationeel haalbaar om een Shared Security Information Platform (SSIP) te ontwikkelen en gebruiken voor het uitwisselen van informatie tussen beveiligingsorganisaties. Hierdoor kunnen organisaties een bijdrage leveren aan elkaars beveiliging. • Hierdoor zijn beveiligingsmanagers o.a. minder afhankelijkheid van hun persoonlijke connecties. • Er blijken desondanks juridische en bestuurlijke bezwaren te zijn voor het rechtstreeks delen van informatie. Betrokken partijen zijn uiteindelijk alleen bereid dit te doen via de politie.
Digitale Perimeter (Digitale Perimeter, 2020)	• Gebruik van *privacy enhancing technologies* (zoals Multi Party Computation: MPC) om gevoelige data in vroeg stadium met elkaar te kunnen delen. • Het creëren van een meer gebiedsgerichte veiligheidsbenadering.
Visie ProRail	• Het meenemen van de wensen en doelen van andere partijen in het gebied bij het aanscherpen van het eigen veiligheidsbeleid.
PRoTECT (PRoTECT, 2020)	• Kwetsbaarheidsanalyse van een gebied kan helpen bij de inrichting van een samenwerking tussen beveiligingsringen, omdat het iedereen eenduidig inzicht geeft in de kwetsbaarheid van een gebied.
TRESSPASS (TRESSPASS, 2020)	• Het uitdrukken van organisatiedoelstellingen, om daarmee vervolgens risicoprofielen en informatiebehoeften uit te kunnen drukken. • Het ontwikkelen van risicoprofielen als modus om informatie te kunnen filteren. • Dynamische wijze van bewaken en beveiligen: aan de hand van nieuwe of verergerde dreigingen kan het concept worden aangepast.
Professioneel profileren (Van Rest, et al., 2020)	• Ontwikkel vanuit scenario's de risicoprofielen en op basis hiervan informatiebehoeftes. • Vertaal deze informatiebehoeftes in indicatoren die het partijen inzichtelijk maakt welke middelen (sensoren) ze kunnen verbinden of aan elkaar ter beschikking kunnen stellen.
Sensoren en systemen voor security (Van Rest & Weima, De toekomst van sensing voor veiligheid, 2018)	• Zeven richtinggevende principes voor het goed gebruik kunnen maken van technische sensoren voor veiligheid, waaronder voor de politie, en voor andere veiligheidsorganisaties.
TACTICS (TACTICS, 2013)	• Technologie kan helpen om in complexe situaties op gebied van veiligheid acute informatiebehoeftes te verbinden aan aanbod van (sensor)data.

3 Federatieve beveiliging

In dit hoofdstuk zal eerst het concept van federatieve beveiliging worden toegelicht. Vervolgens wordt beschreven welke voorbereidende stappen moeten worden ondernomen door de betrokken partijen om tot afspraken te komen voor de operationele inrichting van het concept. In paragraaf 3.3 worden innovatieve technologieën, waaronder *privacy enhancing technologies*, verkend die bij kunnen dragen aan de samenwerking en informatiedeling binnen een federatie en bestaande juridische en politiek-bestuurlijke barrières kunnen slechten. Tot slot zullen de kansen van dit concept worden toegelicht door te analyseren welke capabilities ten aanzien van bewaken en beveiligen door federatieve beveiliging worden versterkt.

3.1 Federatieve beveiliging

Federatieve beveiliging (FB) is een organisatievorm voor organisaties met beveiligde objecten waarvan de observatiegebieden elkaar fysiek raken of overlappen. De organisatievorm kan een aparte stichting zijn, of een onderdeel van een bestaande organisatie zoals een gemeente waarmee deelnemende partijen bepaalde afspraken kunnen maken.

In FB worden de intelligence *capabilities* van de betrokken partijen op elkaar aangesloten via de sub-capabilities “Verzamelen” en “Disseminatie & Integratie”[11]. Daartoe zijn werkprocessen nodig die kunnen worden ondersteund door moderne technologie.

Er zijn drie mogelijke juridische gronden voor de informatie-uitwisseling in een federatie:

- Als het een wettelijke taak is van een overheidsorganisatie. In deze context is dat typisch de WPG.
- Als het gebeurt door een private partij in opdracht van een overheidsorganisatie. Dan gaat het over AVG, artikel 6, lid e.
- Als het gebeurt door een private partij vanwege een gerechtvaardigd belang. Dat gaat over AVG, artikel 6, lid f.

Ieder van die gronden is specifiek voor een éénrichtingsverstrekking in een bepaalde situatie; géén van de gronden lijkt geschikt te zijn voor een algemene verstrekking van één partij naar (een verband van) meerdere andere partijen. Dat betekent dat de federatie alleen kan bestaan uit bilaterale verbanden, waarbij een recht van verstrekking de ene kant op, niet logischerwijs ook leidt tot een recht van verstrekking de andere kant op. Het principe van reciprociteit/wederkerigheid gaat hier dus niet op.

[11] Zie bijlage B1 voor het capability model ‘Voorkomen Aanslagen’.

De federatie moet dus zijn opgebouwd uit één of meerdere bilaterale éénrichtings-informatieverstrekkingsrelaties. Het maximale aantal van dergelijke relaties in een concrete samenwerking hangt af van het aantal partijen. De formule daarvoor is:

n = Aantal partijen in federatie
F (n) = F(n-1) + 2 * (n – 1)
F(2) = 2.

In een omgeving waar vijf organisaties objecten beveiligen, is het dus denkbaar dat er tot wel 20 van dergelijke relaties mogelijk zijn. Daar komt nog bij dat de relaties allemaal verschillen, omdat zowel de beschikbare soorten informatie en de informatiebehoefte per partij verschilt. Dat is zowel juridisch als organisatorisch complex, en kan een barrière vormen voor samenwerking in een dergelijke federatie.

Mogelijk kan een vorm van platformtechnologie helpen om dit beheersbaar en efficiënt te kunnen doen: om producten en consumenten van informatie veilig en efficiënt met elkaar te verbinden. Dat wordt verder beschreven in sectie 3.3.1

3.2 De werking van federatieve beveiliging

In deze sectie wordt beschreven hoe federatieve beveiliging kan worden ingericht. Dat wordt gedaan door de belangrijkste verschillen met “normale” objectbeveiliging te duiden. Onder inrichting wordt verstaan alle activiteiten die gaan over het zorgen dat het werk uitgevoerd kan worden. Er wordt hierin onderscheid gemaakt tussen de inrichting van de federatie als geheel, en de inrichting die per partij nodig is.

3.2.1 Inrichting van centrale loket

Om de inrichting en uitvoering per partij beheersbaar te houden is het nodig om voor de federatie als geheel een aantal centrale zaken te regelen. Dit moet achter een centraal contactpunt of loket worden georganiseerd waar deelnemende partijen zich kunnen aanmelden.

Ten eerste, het lijkt verstandig om de bilaterale samenwerkingsafspraken centraal te beheren. Dat vergemakkelijkt kwaliteitscontrole en traceerbaarheid van de afspraken.

Ten tweede, deelnemende partijen moeten weten waar anderen sensoren hebben, en wat hun eigenschappen zijn. Sommige steden hebben daar openbare registers voor, zoals soms onder de vlag van *smart cities* (Gemeente Amsterdam, 2019). Dit register kan ook worden gebruikt om aan burgers duidelijk te maken, eventueel op sensorniveau, welke informatiedeling er concreet plaats vindt.

Er kan een incentive ontstaan voor deelnemende partijen om pas laat hun sensoren te installeren, en eerst af te wachten wat andere partijen aan sensoren installeren. Dat kan goedkoper lijken. Of juist andersom, om zelf veel invloed te hebben op de selectie en configuratie van de sensoren. Het kan daarom nodig zijn om hier aparte afspraken over te maken.

Ten derde, achter het centrale loket kan een functie zitten om de kwaliteit van sensordata te monitoren en acties te suggereren als deze kwaliteit buiten marges dreigt te komen, gesteld door afnemende partijen.

Ten vierde, achter het loket kan een functie zitten om toekomstverwachtingen over het observatiegebied te bepalen. Die kunnen gebruikt worden om proactief en gericht waarschuwingen naar deelnemende partijen te sturen, en meer concreet, om suggesties te geven voor deelnemende partijen om eenmalig bepaalde informatie met elkaar te delen.

3.2.2 Inrichting per objectbeheerder

De volgende stappen moeten per deelnemende partij worden uitgevoerd, in aanvulling op de normale beveiliging.

Bij het ontwerp van de dreiging is het nodig om te bepalen hoe variabel die is, en waar (geografisch gezien) vroege signalen van die dreiging mogen worden verwacht. Die informatie is nodig om later te bepalen of en waar maatregelen nodig zijn (in de openbare ruimte).

Nadat ook de kans en de impact van een risico zijn geëvalueerd, kan worden bepaald of maatregelen nodig zijn en hoe sterk die moeten zijn. In principe kan een beveiliger gebruik maken van eigen maatregelen in de openbare ruimte door zich te beroepen op artikel 6 lid f van de AVG (zie sectie 2.1.1.2). In FB komen daar, op basis van hetzelfde artikel[12], de opties via de federatie bij. Ten eerste het stelselmatig verkrijgen van informatie van naburige partners, en ten tweede het ad hoc krijgen van dergelijke informatie.

Het initiatief voor een concrete samenwerking ligt dus bij de informatie behoevende partij. Zonder hun juridisch onderbouwde behoefte is er immers geen grondslag voor informatiedeling.

Als de dreiging op de één of andere manier repeterend is, dan is het wellicht nodig om stelselmatig informatie uit te wisselen en deze op te werken tot bruikbare intelligence per casus. Bijvoorbeeld als de dreiging uitgaat van voorbijgangers, bezoekers, of van bepaalde evenementen die zich frequent voordoen. Daarvoor is het nodig om te profileren.

De objectbeheerder stelt profielen op, op basis van indicatoren. Van die indicatoren bepaalt de beheerder vervolgens welke databronnen nodig zijn om ze per casus te vullen. Hiervoor kan de methode Professioneel Profileren (zie bijlage B) worden gebruikt.

Na het bepalen van het observatiegebied, moet worden achterhaald of er reeds databronnen van anderen beschikbaar zijn om de indicatoren mee te vullen die kwalitatief voldoen (tijdigheid, beschikbaarheid, nauwkeurigheid, etc.). Dat kan bij het loket van de federatie opgevraagd worden. Het is daarbij van belang dat de

[12] Er lijken ook mogelijkheden te zijn voor overheidspartijen om deel te nemen in een dergelijke federatie indien ze zich daarbij kunnen beroepen op artikel 6 lid f. Bijvoorbeeld de beveiliging van een regulier politiebureau valt vermoedelijk niet onder het Stelsel Bewaken & Beveiligen. En wellicht is er ook een grondslag te vinden om deel te nemen in FB voor partijen die wel onder dat Stelsel vallen. In deze sectie wordt dat onderscheid verder niet gemaakt.

databron van de verzendende partij op een veilige manier met de rest van het profiel van de ontvangende partij wordt gecombineerd.

3.3 Technologie

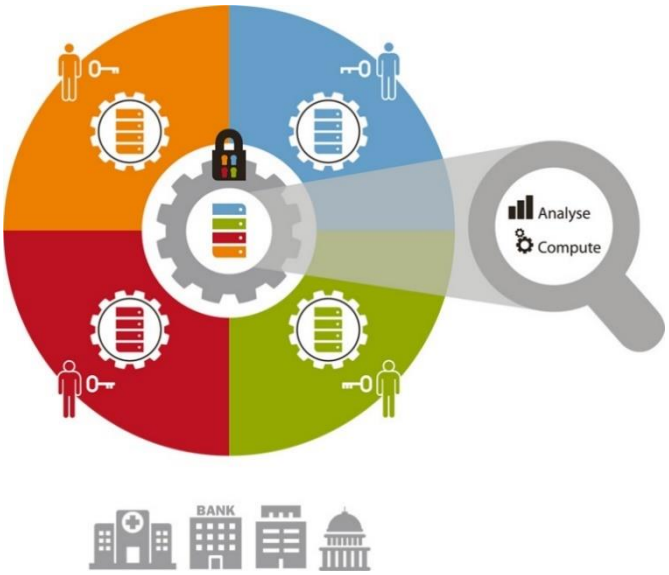
Deze sectie is een invulling van de onderzoeksvraag “Welke kansen biedt innovatieve technologie, wat zijn eventuele barrières om die in te zetten en hoe kunnen die worden overwonnen?” (zie sectie 1.4). Hier horen specifiek ook technologieën en ontwikkelingen bij die nu nog niet operationeel inzetbaar zijn.

3.3.1 Platformtechnologie: Secure Multi-Party Computation

Het combineren van verschillende datasets leidt tot nieuwe inzichten en betere besluitvorming. Echter niet alle datasets kunnen of mogen wettelijk worden gedeeld. Vaak willen (delen van) organisaties dit ook niet, wegens interne processen of beheersmaatregelen. Ook willen organisaties vaak voorkomen dat gevoelige informatie in verkeerde handen valt. Tot nu toe wordt voor dit soort problemen vaak een vertrouwde derde partij gebruikt. Echter, dit is juridisch gezien niet altijd mogelijk, het is organisatorisch gezien complex en vertrouwen in deze derde partij kan over tijd veranderen.

(Secure) Multi-party Computation (MPC) is een relatief nieuwe oplossing voor het genereren van de functionaliteit van een gedeelde database zonder de gegevens aan elkaar te hoeven onthullen. MPC is een gereedschapskist van versleutelingstechnieken waarmee verschillende partijen gezamenlijk gegevens kunnen berekenen, net alsof ze een gezamenlijke database hebben. Het is geschikt voor situaties waarin twee of meer partijen ieder gevoelige gegevens hebben die ze niet met anderen willen delen.

Er worden versleutelingstechnieken gebruikt om de gegevens te beschermen, zodat ze kunnen worden gedeeld op een manier die voorkomt dat de betrokken partijen ooit de gegevens van anderen kunnen bekijken. De deelnemende partijen bepalen tijdens de ontwerpfase wie de uitkomst van de berekening mag inzien (Evans, Kolesnikov, & Rosulek, 2017) (TNO, 2020) (Bomhof & Giezeman, 2019). Een eenvoudig voorbeeld waarbij twee partijen een beslissing kunnen nemen, zonder elkaars input te kunnen inzien, is te zien in het filmpje “Multi-Party Computation (MPC) uitgelegd” (TNO, 2020).



Figuur 3 Secure Multi-party Computation maakt het mogelijk om gezamenlijk verwerkingen te doen zonder de brondata met elkaar te delen (TNO, 2020).

Een concreet voorbeeld op gebied van fysieke beveiliging is de MPC voor niet-coöperatieve gezichtsherkenning dat in het project Digitale Perimeter is ontwikkeld (Digitale Perimeter, 2020). Daarmee kunnen gezichten van passanten op een relatief veilige wijze worden vergeleken met een volglijst. Dit gebeurt op zodanige wijze dat de beheerder van de volglijst niet de beschikking krijgt over de gezichten, en de beheerder van de biometrische camera's niet over de volglijst. Daarbij is het ook mogelijk dat een derde partij een procesmatig afschrift krijgt van de verwerking, waarmee eventueel misbruik kan worden gesignaleerd (Van Rest, Attema, Timan, Den Hollander, & Van Voorthuijsen, 2021).

MPC helpt om diverse privacy dreigingen te beschermen ten opzichte van een situatie waarbij informatie "onveilig" wordt gedeeld. Ten eerste is *aggregatie* in te perken. MPC staat immers alleen maar de specifieke vergelijking toe, maar geen andere. Ook is *dual use* beter te signaleren indien afschriften van een verwerking (zonder inhoudelijke gegevens) naar een toezichthouders worden gestuurd. *Onveiligheid* is te voorkomen doordat gegevens überhaupt niet bij andere partijen terecht komen. Daarmee is ook de privacy dreiging *inbreuk op vertrouwelijkheid* beter te beheersen: partijen krijgen alleen gegevens indien ze dat echt nodig hebben.

MPC is nu maatwerk. Daar is wel "confectiewerk" van te maken binnen de context van (federatieve) beveiliging, zoals voor gezichtsherkenning is gedaan in het project Digitale Perimeter. Dat vereist aanvullend onderzoek.

3.3.2 Big data & analytics: Profileren

Profileren is de data analyse methodiek die het mogelijk maakt om bij repeterende casussen om te gaan met onzekerheid. De functie van profileren is om onderscheid aan te brengen in groepen casussen op basis van de inschatting van een verborgen kenmerk. Bijvoorbeeld, als het verdacht is als iemand binnen enkele dagen meerdere rondjes rijdt rond een beveiligd object, dan kunnen voorbijrijdende auto's daar dus op geprofileerd worden.

Een profiel bestaat uit indicatoren, operatoren daarop en wegingsfactoren. Bijvoorbeeld kan een indicator van een verdacht voertuig zijn: “de tijd sinds de vorige keer dat het voertuig in de buurt gezien is”. Profileren is een krachtig instrument dat ook misbruikt kan worden. Daarom is het van belang dat het terughoudend en zorgvuldig wordt ingezet. TNO heeft op basis van meerdere projecten de methodiek “Professioneel Profileren” ontwikkeld (Van Rest, et al., 2020).

Om zonder profileren eenzelfde veiligheidseffect te bereiken, is het typisch nodig om *alle* gevallen een bepaalde controle te laten ondergaan. Bijvoorbeeld om bij alle voorbijgangers een identiteitscontrole uit te voeren. De mogelijkheid die profileren biedt, is om op basis van andere informatie (bijv. gedrag) een onderscheid aan te brengen en alleen die voorbijgangers te controleren die een match hebben met een bepaald “malafide” profiel. Of andersom, om die voorbijgangers te laten passeren, die een match hebben met een bepaald “bonafide” profiel (en geen match met een malafide profiel). Indien goed gebruikt, draagt dit bij aan het recht om rest te worden gelaten – een kernwaarde van privacy.

Profileren heeft inherent een aantal forse privacy risico’s. Deze worden uitvoerig behandeld in eerder genoemd rapport. Daaronder zijn o.a. het risico op *aggregatie*, van *onveiligheid*, van *secondair gebruik* en van *inbreuk op vertrouwelijkheid*. Door in federatieve beveiliging, profileren technisch alleen via *multi-party computation* (zie vorige sectie) mogelijk te maken worden deze risico’s deels beheerst.

Profileren maakt gebruik van analysesoftware en gebruikt grote hoeveelheden data om goed getraind te worden. Profileren is nu maatwerk. Daar is wel “confectiewerk” van te maken binnen de context van federatieve beveiliging. Dat vereist aanvullend onderzoek.

3.3.3 Big data & analytics: Digital Twinning

In het algemeen wordt (tot nu toe) *digital twinning* gezien als een digitaal model, een simulatie, die gekoppeld is aan een fysiek object, zoals bijvoorbeeld een brug. Er is ook een meer algemene definitie: een *digital twin* is een dynamische digitale representatie van een fysiek object of een systeem, over de hele levenscyclus van dat object of systeem (Grieves, 2016) [13]. De typische functie van een *digital twin* is om te simuleren hoe een systeem zich onder bepaalde echte of fictieve condities zou gedragen, waaronder ook in een mogelijke toekomst. Dan gaat het dus om het maken en analyseren van verwachtingen.

Voor een *digital twin* zijn een accuraat model van het object nodig en grote hoeveelheden (i.e. *big*) data die de werking van het model onder verschillende omstandigheden beschrijven. Er bestaan digitale modellen van steden en gebouwen en ook van verkeersstromen (TNO, 2020) die mogelijk gebruikt kunnen worden voor fysieke beveiliging.

[13] Een *digital twin* wordt soms verward met *command & control* (C2) of *physical security information management* (PSIM) systemen die 3d gebruikersinterfaces hebben. Het verschil is dat een digital twin geen koppelingen heeft met daadwerkelijke sensoren en actuatoren, en dat een command & control systeem geen simulaties van alternatieve scenario’s doet. Een combinatie van de twee kan natuurlijk wel.

In de context van federatieve beveiliging zijn verschillende functies denkbaar voor de technologie van *digital twinning*. Bijvoorbeeld is het wellicht mogelijk om de effecten van beveiligingsmaatregelen te voorspellen in relatie tot de fysieke omgeving van het te beveiligen object. Dat kan nuttig zijn voor conceptontwikkeling (zoals deze studie), bij de inrichting van complexe omgevingen (zoals een binnenstad met veel beveiligde objecten) en ook in de operationele fase om operationele besluitvorming te ondersteunen (zoals de beslissing om een compartiment te sluiten). Daarbij zal het modelleren van het gedrag van vriendelijke en neutrale partijen uitdagend zijn. Extra moeilijk zal zijn om het gedrag van menselijke tegenstanders ook enigszins representatief te voorspellen. Er zijn wel modellen die juist daar ook in gespecialiseerd zijn. Bijvoorbeeld modellen die de reactie van (groepen van) personen op een prikkel modelleren (Patentnr. EP2754089A1, 2012).

Ook kan een *digital twin* mogelijk worden gebruikt om de operationele toestand van bevriende partijen te simuleren. Hiermee is het mogelijk om op hun behoeftes te anticiperen en daar proactief op in te spelen. Bijvoorbeeld door proactief te opperen om bepaalde soorten informatie te delen.

Een *digital twin* maakt in principe geen gebruik van persoonsgegevens. Nieuwe privacy dreigingen liggen bij het gebruik van *digital twins* dus niet voor de hand. Een *digital twin* kan mogelijk op lange termijn helpen om de noodzaak voor praktijkexperimenten (met echte mensen) enigszins te verkleinen, maar dat vereist modellen van menselijk gedrag van hoge kwaliteit.

Een *digital twin* met de functionaliteit zoals beschreven in deze verkenning lijkt nog niet te bestaan voor beveiliging.

3.3.4 Kunstmatige intelligentie: Managed analytics

De correcte verwerking van sensordata hangt af van meerdere technische en operationele factoren zoals afstand tot de scene, occlusie, oriëntatie van objecten (zoals gezichten of kentekenplaten) ten opzichte van de sensor, resolutie en belichting. Dat geldt zowel voor menselijke verwerking als voor automatische “intelligente” verwerking.

Als die factoren bekend zijn, dan kan er worden ingegrepen als ze buiten operationele marges dreigen te raken (bijv. als het donker wordt automatisch bijlichten), en kan de verwachting over de prestaties worden bijgesteld op basis van modellen die voorspellen hoe goed de interpretatie werkt onder uitdagende omstandigheden. Uiteraard moet daarbij worden opgelet dat er geen technieken worden gebruikt die niet-bestaande data “invullen”.

Technologie kan helpen om technische en operationele factoren die de kwaliteit van de verwerking beïnvloeden, automatisch te bepalen. Technologie kan vervolgens ook automatisch acties uitvoeren om die kwaliteit binnen gewenste marges te houden.

TNO heeft een raamwerk voorgesteld onder de noemer *managed analytics* die bovenstaande functies verenigt (TRL3). Dit raamwerk zou als het ware “om” reguliere analytics heen kunnen worden toegepast als een soort management-laag. Mogelijk kan dit helpen om een analytics systeem semi-automatisch te beheren

(Den Hollander, et al., 2017), waardoor het onder allerlei uitdagende omstandigheden met een van tevoren bepaalde minimale accuratesse zou blijven werken.

In FB kan dit mogelijk helpen om het probleem uit de inleiding te verhelpen, waarbij de ontvangende partij juist als het er om spant, zich moet bezig houden met de kwaliteit van sensordata van anderen (of van zichzelf). Managed Analytics zou bijvoorbeeld een dienst kunnen zijn van het centrale loket waar deelnemende partijen gebruik van maken.

Managed analytics gebruikt in principe geen persoonsgegevens, maar vooral gegevens over de operationele omstandigheden zoals afstand tot de scene, occlusie, oriëntatie van objecten (zoals gezichten of kentekenplaten) ten opzichte van de sensor, resolutie en belichting. Het kan helpen om de privacy dreiging van *vervorming* te verkleinen, specifiek van foutieve matches op volglijst en op profielen.

Managed analytics bestaat in de beschreven vorm alleen nog op papier. Een duidelijk afgebakende use case op een nuttige vorm van analytics, zoals het terugvinden van personen of voertuigen, is een zinvolle richting voor vervolgonderzoek.

3.4 Principes achter federatieve beveiliging

Het concept van federatieve beveiliging is gebaseerd op de zeven principes die TNO in 2018 publiceerde over sensing in het veiligheidsdomein (Van Rest & Weima, De toekomst van sensing voor veiligheid, 2018). De principes worden uitvoerig toegelicht in die publicatie. In deze sectie wordt per principe toegelicht hoe die in het concept Federatieve Beveiliging is uitgewerkt.

Sensing waarderen op effecten: een onderbouwde en expliciete noodzaak voor sensing in relatie tot een beveiligingsdoel is het startpunt voor iedere use case binnen federatieve beveiliging.

Privacy by design en security by design voor sensing: de primaire motivatie voor federatieve beveiliging is dat mensen zo veel mogelijk met rust moeten worden gelaten. Dat maatregelen waar mogelijk alleen werkzaam moeten zijn indien de situatie daar reden toe geeft, en dus niet zomaar altijd of voor iedereen. Als gevolg daarvan is de kern van het concept opgebouwd uit privacy beschermende maatregelen waaronder *multi-party-computation*.

Metadateren en filteren bij de bron: om te bepalen welke informatie potentieel relevant is voor een naburige objectbeveiliger, is het nodig om sensordata direct bij de bron te metadateren. Daarmee kan immers worden voorkomen dat ruwe, ongefilterde sensordata hoeft te worden gedeeld.

Sensordata van voldoende kwaliteit: Het moet worden verwacht dat de sensoren bij naburige objecten gericht zijn op het waarnemen van bepaalde soorten dreigingen en situaties. Die komen vermoedelijk niet helemaal overeen met de dreigingen en situaties die relevant zijn voor beveiligers van naburige objecten. Het is dus nodig om de factoren die de kwaliteit van sensordata bepalen (zoals opnamehoek,

resolutie, belichting, etc.) automatisch te monitoren en beheersen. Daarmee kan de kwaliteit van de verwerking van sensordata vanaf het begin worden verzekerd. Het risico van foutieve *matches* kan daarmee worden ingeschat en beperkt.

Sensing slechts als het nodig is: het delen van gevoelige informatie gebeurt slechts als er een *match* is op een volglijst of een profiel. Eerder dan dat moment wordt er geen betekenisvolle informatie gedeeld.

Gebruikmaken van andermans sensoren: het is efficiënter, flexibeler en vaak meer proportioneel om gebruik te maken van beveiligingssensoren die elders al beschikbaar zijn – en dus van anderen zijn, dan om daar zelf eigen sensoren bij te plaatsen.

Nieuw sensingconcept ontwikkelen: federatieve beveiliging is niet slechts een interne efficiëntieslag. Het heeft significante impact op de omgeving waarin het wordt toegepast. Daarom is het verstandig om bij de verdere ontwikkeling voldoende belanghebbenden vroeg te betrekken. Dat omvat ook partijen die de benodigde technologie moeten leveren.

4 Use cases

Dit hoofdstuk beschrijft een aantal use cases die de werking van federatieve beveiliging illustreren. De use cases zijn niet van elkaar afhankelijk, en kunnen dus los van elkaar gelezen worden.

4.1 Het scenario en de personas

De use cases van de volgende secties maken telkens gebruik van dezelfde uitgangssituatie, partijen en personas[14].

Er zijn twee beveiligde objecten, met beheerders Ben en Jerry. Ben is typisch de beheerder met een informatiebehoefte. Jerry is typisch de beheerder met sensoren die de informatiebehoefte kunnen vervullen.

Er is ook een lokale federatie opgericht door de gemeente, waar zowel Ben als Jerry lid van zijn. De naam van deze federatie is “de Veilige Zone”, afgekort tot VZ. De gemeente heeft voor de bemensing en bepaalde technische diensten van de VZ een contract afgesloten met een private beveiligingsorganisatie. Zij leveren Kurt aan de VZ.

In principe hoeft de VZ zelf geen inhoudelijke gegevens te verwerken. Maar in voorkomende gevallen moet de VZ, in de persoon van Kurt dus, kunnen adviseren op basis van inhoudelijke informatie. De private beveiliger verwerkt dan persoonsgegevens op basis van AVG artikel 6 lid e.

4.2 Use case informatiebehoefte melden bij federatie

Ben heeft een dreiging vastgesteld en daarbij een observatiegebied en een informatiebehoefte.
Vervolgens heeft hij bij de VZ zijn informatiebehoefte geregistreerd en gevraagd welke andere partijen daarin sensoren hebben staan waarmee in zijn informatiebehoefte wordt voorzien. Dat blijkt de organisatie van Jerry te zijn. De VZ brengt Ben en Jerry met elkaar in contact en suggereert een bilateraal samenwerkingsconvenant waarin alle details al zijn ingevuld. Na digitale ondertekening door beiden, wordt het convenant door VZ opgeslagen en worden het technische koppelvlak door VZ ter beschikking gesteld aan Ben.

4.3 Use case MPC met kentekens

Ben heeft vastgesteld dat extremistische actievoerders voor zijn object een reële dreiging vormen. Hij heeft daarom een lijst opgesteld met voertuigen die in bezit zijn van bekende actievoerders en met foto’s van hun gezicht. Als de auto’s in de buurt zijn, dan wil hij zijn medewerkers een bericht sturen met de foto van het gezicht van de betreffende actievoerder.

[14] Een persona is een fictief persoon die een bepaalde rol in een use case vertegenwoordigd. Het gebruik van personas is een onderdeel van *user centred design*.

Ben meldt zijn informatiebehoefte aan bij VZ en krijgt uiteindelijk het technische koppelvlak door VZ ter beschikking gesteld.

Ben stelt een volglijst samen. Deze wordt via MPC gecombineerd met de live kentekens die bij Jerry langsrijden. Ben krijgt binnen enkele minuten een melding van iedere match. De VZ krijgt een melding dat er een match was, maar geen inhoudelijke informatie. Jerry krijgt achteraf van de VZ een geaggregeerd overzicht van het gebruik van zijn sensordata.

4.4 Use case Profileren

Ben heeft vastgesteld dat er een forse dreiging zit op één van de medewerkers in zijn object. Als werkgever wil zijn organisatie daar haar verantwoordelijkheid in nemen. Ben heeft vastgesteld dat een mogelijke aanslag vooraf kan worden gegaan door een verkenning met een voertuig in de buurt. Ben heeft géén informatie over kentekens van specifieke voertuigen. Ben wil bereiken dat als er een verdacht voertuig in de buurt rondrijdt, de betreffende medewerker naar een safe room gaat, en dat de politie een melding krijgt met het betreffende kenteken, locatie en tijdstip van de passage.

Ben heeft een profiel ontwikkeld dat gebruikmaakt van twee soorten indicatoren per voertuig. Ten eerste de tijdsduur sinds de vorige passage, met een maximaal geheugen van twee uur. Voertuigen die binnen die twee uur éénmaal langsrijden kunnen hiermee uitgezonderd worden. Ten tweede of het voertuig van een bezoeker van één van de lokale objecten is. Dit is een tijdelijke dreiging, waarvoor het observatiegebied volgens Ben tijdelijk groter zou moeten zijn. Ben heeft zijn indicatoren en observatiegebied aangemeld bij de VZ. De VZ stelt vast dat daarvoor de bezoekersregistratie en sensoren van Jerry nuttig zijn. Na registratie en ondertekening en koppeling van het technisch koppelvlak krijgt Ben de gewenste meldingen via MPC aangeleverd.

VZ, Ben en Jerry hebben zwart op wit vastgelegd welke data wordt verwerkt, waarom en onder welke condities de verwerking weer kan stoppen.

De profielen die Ben heeft bedacht blijken goed te werken. De VZ maakt er *templates* van die ze voor vergelijkbare behoeftes kan suggereren.

4.5 Use case Digital Twin

Kurt heeft een *digital twin* van het observatiegebied van de VZ draaien. Daartoe wordt gebruik gemaakt van openbare bronnen, en ook van de plannen en actuele operationele toestand van de deelnemende partijen. De Digital Twin helpt om tegelijkertijd en continu verwachtingen voor over twee uur, twee dagen en twee weken te geven. Die verwachtingen gaan over fenomenen die relevant zijn voor de deelnemers van de VZ, zoals de aanwezigheid en type van mensenmassa's, en over de verwachte toekomstige operationele toestand (zie sectie 2.1.3) van de deelnemende organisaties.

De *digital twin* geeft een verwachting dat over twee dagen een mensenmassa zal ontstaan naast het beveiligde object van Ben. Kurt stelt met behulp van de *digital twin* een rapportage op waarin de verwachting onderbouwd wordt beschreven,

inclusief de databronnen die daarvoor gebruikt zijn. Hij stuurt deze naar Ben, met als suggestie om tijdelijk een aantal extra informatiebehoeftes in te stellen op deze databronnen, zodat Ben zelf kan monitoren hoe de situatie zich de komende dagen ontwikkelt.

4.6 Use case Managed Analytics

Jerry beheert een object met een centrale ligging in de omgeving. Jerry heeft acht samenwerkingsrelaties waar zijn organisatie de databron levert. Op basis van maandelijkse rapportages van VZ weet Jerry dat er maandelijks honderden verwerkingen plaatsvinden, en dat er gemiddeld drie matches of hits zijn op volglijsten of profielen van zijn collega's in de buurt.

Het is voor Jerry niet eenvoudig om te monitoren of de kwaliteit van zijn sensoren nog past bij die acht informatiebehoeftes, en daar mag Jerry van zijn organisatie ook maar weinig capaciteit aan besteden.

Jerry neemt daarom de dienst *Managed Analytics* (MA) af. Toen de donkere maanden kwamen, gaf MA meldingen dat de beelden te donker werden voor twee van de informatiebehoeftes. Daar kwamen concrete suggesties bij voor extra verlichting die Jerry snel kon plaatsen.

Ook Ben neemt de dienst MA af. Toen Ben plotseling geconfronteerd werd met een overval, kon hij met behulp van MA en de VZ de sensoren in een ad hoc groter observatiegebied zoeken die voldoende bruikbare data leverden waarin een vluchtende dader kon worden gezocht.

5 Conclusie en aanbeveling

Dit hoofdstuk 5 geeft de beantwoording van de onderzoeksvragen (5.1), de conclusies (5.2) en de aanbevelingen (5.3). Veiligheidsorganisaties met specifieke taakstellingen kunnen bijlage C gebruiken om snel een beeld te vormen van het mogelijke nut van federatieve beveiliging voor hun specifieke taak.

5.1 Beantwoording onderzoeksvragen

1 Welke voorbeelden/casuïstiek van beveiliging zijn te identificeren (in de literatuur en in de praktijk), waarbij sprake is van overlappende beveiligingsringen?

Overlappende beveiligingsringen zijn op heel veel plekken te vinden. Overal waar organisaties objecten hebben die grenzen aan de openbare ruimte en die dicht bij elkaar staan, zal sprake zijn van overlappende beveiligingsringen. Het is door toenemende verstedelijking en industrialisatie te verwachten dat het aantal situaties dat zich leent voor federatieve beveiliging zal toenemen.

Voorbeelden uit eerdere projecten zijn treinstations met winkels er in of er naast en met vervoerders met rijdend materieel, industrieterreinen en -campussen waar meerdere bedrijven bij elkaar gevestigd zijn, stedelijke gebieden waar overheidsgebouwen naast elkaar en naast andere objecten staan, en ook woonwijken waar burgers woningen naast elkaar hebben. Een aparte categorie zijn terreinen waar vitale infrastructuur zich te midden van andere diensten en bedrijvigheid bevindt. Voorbeelden hiervan zijn grote logistieke en transport centra en havens en luchthavens.

2 Wat wordt bedoeld met federatieve beveiliging? Is daar een typering in aan te brengen?

Federatieve beveiliging (FB) is een organisatievorm, manier van werken en bijbehorende technologie voor organisaties met beveiligde objecten waarvan de observatiegebieden elkaar fysiek raken of overlappen.

In federatieve beveiliging delen beveiligers hun informatiebehoefte met hun fysieke buren, waarop zij kunnen intekenen met een aanbod aan sensordata. De daadwerkelijke informatieverwerking bestaat uit het toetsen van sensordata (zoals gezichten, kentekens, of beschrijvingen van gedrag) tegen volglijsten en profielen – zonder dat deze informatie met een andere partij wordt gedeeld. Daar wordt de technologie *multi-party-computation* voor gebruikt. Om te borgen dat de kwaliteit van de sensordata voldoende goed is en blijft, wordt deze aan de verzendende kant gemonitord en gemanaged met behulp van geautomatiseerde analyses. Daar wordt het concept *managed analytics* voor gebruikt. Om verwachtingen te maken voor toekomstige informatiebehoeftes van beveiligers, worden simulaties uitgevoerd van de omgeving van te beveiligen objecten. Hier wordt de technologie *digital twinning* voor gebruikt.

Een vorm van centrale ondersteuning hierbij lijkt nodig. Dat kan een aparte stichting zijn, of een onderdeel van een bestaande organisatie zoals een gemeente waarmee deelnemende partijen specifieke afspraken kunnen maken.

Het lijkt nuttig om de typering van soorten FB vooral af te laten hangen van de juridische grondslag voor het verzamelen van informatie voor beveiliging in de openbare ruimte. Daar komen drie grondslagen voor in aanmerking:

- Als het een wettelijke taak is van een overheidsorganisatie. In deze context is dat typisch de WPG.
- Als het gebeurt door een private partij in opdracht van een overheidsorganisatie. Dan gaat het over AVG, artikel 6, lid e.
- Als het gebeurt door een private partij vanwege een gerechtvaardigd belang. Dat gaat over AVG, artikel 6, lid f.

3 Wat zijn de voornaamste kansen en barrières (juridisch, technologisch, procesmatig) voor de totstandkoming van federatieve beveiliging?

a. Wat zijn de belangrijkste juridische kaders? Welke gronden voor het delen van informatie zitten daar in, en welke barrières?

De belangrijkste grondslag lijkt AVG artikel 6 lid f te zijn. Die wordt door de AP expliciet als mogelijke grondslag voor de verwerking van persoonsgegevens voor beveiliging geopperd. Daar worden wel voorwaarden aan gesteld.

De wet schrijft voor dat voor een verwerking, inclusief een informatiedeling, op basis van dit artikel, er sprake moet zijn van een echte, reële dreiging. Voor de verzendende partij kan het echter moeilijk zijn om te bepalen of iets een dreiging vormt op de ontvangende partij. Voor de ontvangende partij kan het zonder de betreffende informatie moeilijk zijn om te bepalen of de dreiging echt is. Dat levert dus mogelijk een barrière op om informatie over echte dreigingen te delen.

Een andere barrière is dat er geen grondslag lijkt te zijn voor 1:N of N:N informatiedeling. Daardoor zijn alleen bilaterale relaties mogelijk in één richting per relatie. Bij situaties waar meerdere organisaties samen willen werken, leidt deze beperking tot een complexere organisatie en benodigde techniek.

Bij het ontwerpen van het concept voor federatieve beveiliging is gebruik gemaakt van deelconcepten uit eerdere projecten die conform de principes van *value sensitive design* zijn ontwikkeld. De belangrijkste ontwerpbeslissingen in die context zijn om profileren technisch te koppelen aan *multi-party computation*, en om *managed analytics* voor te stellen om onnodige foutieve *matches* te voorkomen. Dat betekent dat de proportionaliteits- en subsidiariteitsafwegingen – een belangrijk onderdeel van het juridisch kader – wellicht anders kunnen uitvallen dan wanneer deze technische waarborgen niet gebruikt zouden worden. Een gevolg hiervan kan zijn dat federatieve beveiliging de “drempel” om profileren in te zetten, kan verlagen. Dat komt in principe de veiligheid ten goede.

b. Wat zijn de belangrijkste procesmatige veranderingen voor de totstandkoming van een federatieve beveiliging?

Bij dit antwoord wordt er van uitgegaan dat objectbeveiligers al gebruik maken van profileren en van volglijsten. Voor federatieve beveiliging zullen objectbeveiligers bij het bepalen van de dreiging explicieter moeten maken waar deze dreiging -of vroege signalen daarvan- zich fysiek zou kunnen manifesteren. Daarmee kunnen ze inschatten op welke andere plekken ze sensoren nodig zouden hebben. Ook kunnen ze zelf sensoren aanbieden voor anderen om gebruik van te maken. Hiervoor is het nodig om een centraal loket op te zetten dat de juridische, organisatorische en technische complexiteit helpt beheersen.

c. Welke kansen biedt innovatieve technologie?

In relatie tot FB zijn vier soorten innovatieve technologie geopperd, die zijn verdeeld over drie families van “sleuteltechnologieën”. Het gaat om secure *multi-party computation*, profileren, *digital twin*, en *managed analytics*. Zij helpen om de effectiviteit, efficiëntie, en conformiteit met de wet te vergroten.

MPC kan helpen om informatie gezamenlijk te verwerken zonder dat de betrokken partijen gevoelige data hoeven uit te wisselen. Daarmee wordt ten opzichte van “onveilige” informatie uitwisseling de conformiteit met de wet- en regelgeving vergroot.

Profileren helpt om bij repeterende casussen (zoals passanten, bezoekers of evenementen) gevaarlijke gevallen te onderscheiden van ongevaarlijke gevallen. Profileren helpt ook om de noodzaak voor informatiedeling te beschrijven in termen van indicatoren, op basis waarvan andere partijen zelf kunnen inschatten welke informatie dan toegestaan kan zijn om te delen.

Een *Digital Twin* helpt om toekomstverwachtingen op te stellen van gebieden en/of van de operationele toestand van deelnemende partijen. Daarmee kunnen anderen zelf inschatten of het wellicht verstandig en toegestaan is om informatie gericht te delen.

Managed Analytics helpt om de kwaliteit van sensordata automatisch te beheersen. Daarmee kunnen partijen voor zichzelf en voor anderen tijdig (dus vóórdat een incident plaats vindt) de kwaliteit van sensordata op orde krijgen en houden.

d. Wat zijn eventuele barrières om die technologie in te zetten en hoe kunnen die worden overwonnen?

Zowel MPC als profileren zijn nu maatwerk. Daar is wel “confectiewerk” van te maken, zoals voor gezichtsherkenning is gedaan in de Digitale Perimeter. Dat vereist aanvullend onderzoek.

Een Digital Twin wordt soms verward met hoogwaardige *command & control* systemen. Een Digital Twin met de functionaliteit zoals beschreven in deze verkenning lijkt nog niet te bestaan voor beveiliging.

Managed Analytics bestaat in de beschreven vorm alleen nog op papier. Een duidelijk afgebakende use case op een nuttige vorm van analytics, zoals het terugvinden van personen of voertuigen, lijkt een zinvolle richting voor vervolgonderzoek.

Goede praktische voorbeelden in een coherent verband bestaan nog niet. Dit leidt tot de barrière “onbekend maakt onbemind”. Een demonstratie in een praktische omgeving zou die barrière kunnen beslechten.

e. *Hoe kunnen digitale modellen van fysieke objecten (‘digital twinning’) helpen bij federatieve beveiliging?*

Het koppelen van digitale modellen aan fysieke objecten kan helpen om verwachtingen over het observatiegebied rond beveiligde objecten op te stellen, en inhoudelijk te onderbouwen. Daarmee kunnen objectbeveiligers pro-actiever beveiligen. Ook kunnen informatiepartners dergelijke verwachtingen gebruiken om proactief (extra) informatie aan te bieden.

5.2 Conclusie

Beveiligingsconcepten gaan veelal uit van een ringenmodel waarin verschillende veiligheidsmaatregelen zijn opgenomen in verschillende ringen (die fasen en fysieke ruimten weergeven) waarbij het totaal een ‘waterdicht’ veiligheidssysteem betreft en aansluit op verschillende (dreigings)scenario’s. In veel gevallen is er echter sprake van overlappende beveiligingsringen door de complexiteit van stedelijke gebieden of openbaarvervoerslocaties. Daarnaast groeit de hoeveelheid te beschermen objecten en neemt de complexiteit van het bewaken en beveiligen in stedelijk gebied toe. In samenhang met de toename van ondersteunende ICT-systemen van beveiligingsringen, leidt dit naar de vraag naar een informatiegedreven beveiligingsconcept voor objecten.

In dit rapport is een Federatieve Beveiliging (FB) in concept beschreven. Dit is in meer detail beschreven in hoofdstuk 3, en in de beantwoording van onderzoeksvraag 1. Op basis van brainstorms, documentstudie en een interview lijkt het nuttig en veelbelovend. De technologieën zijn in vergelijkbare doch andere contexten in andere projecten deels ontwikkeld op TRL3-6. Daarmee lijkt federatieve beveiliging vooralsnog haalbaar, maar er zijn nog een aantal stappen te zetten (zie het antwoord op onderzoeksvraag 3 in sectie 5.1).

5.3 Aanbeveling

Het wordt aanbevolen aan de NCTV om samen met politie, KMar en OM, en welwillende uitvoerende beveiligingsorganisaties, waaronder mogelijk ook bepaalde vitale infrastructuur en relevante private (branche)organisaties, de wenselijkheid en haalbaarheid verder te verkennen. Het concept kan verder worden doorontwikkeld en geoperationaliseerd, om vervolgens te testen conform een CD&E benadering waarin verschillende stappen worden doorlopen.

Ten eerste workshops om het nieuwe beveiligingsconcept in een spelvorm toe te passen op een variëteit aan omgevingen en situaties: via *walk-throughs* en *what-if*

scenario’s wordt het concept verder ingevuld, kunnen behoeftes en benodigde capabilities van stakeholders verder worden geduid, op grond waarvan kansrijke (opkomende) technologieën worden geïdentificeerd.

Met deze informatie kan vervolgens een eerste basale werkbare variant van het concept worden gedefinieerd. De kern van federatieve beveiliging is gebaseerd op het slim gebruiken van reeds bestaande en gebruikte technologie. Desondanks zal het voor bepaalde technologische onderdelen nodig zijn om in enige mate technologie ontwikkeling, integratie en configuratie te doen. Dit lijkt prima te kunnen in samenwerking met industrie.

Hierop volgend kunnen proeven worden uitgevoerd, bijvoorbeeld met behulp van een simulatie-infrastructuur die reeds is ontwikkeld en getest in het kader van een recent afgerond Europees project (DRIVER+). Virtuele scenario’s kunnen worden ontwikkeld, waarbij huidige gebruikte technologische middelen gekoppeld kunnen worden aan (simulaties van) nog niet gebruikte nieuwe technologieën, en nieuwe manieren van samenwerken en informatiedelen getest. Vervolgens kunnen experimenten worden uitgevoerd in een afgebakende fysieke omgeving met een selectie van partners. Tenslotte kunnen testen/experimenten worden uitgevoerd in de werkelijke fysieke en operationele omgeving met alle relevante partners.

6 Referenties

AIVD. (2019). *Doelwitten in beeld: Vijftien jaar jihadistische aanslagen in het Westen. .* Algemene Inlichtingen- en Veiligheidsdienst.

Autoriteit Persoonsgegevens. (2019). *Normuitleg grondslag 'Gerechtvaardigd belang'.* Autoriteit Persoonsgegevens.

Bomhof, F. W. & Giezeman, P. (2019). *Data gebruiken zonder ze te krijgen of te zien: hoe we zonder privacyschending informatie verkrijgen in de zoektocht naar onvindbare veroordeelden.* Den Haag: Ministerie Justitie & Veiligheid.

Bovenkamp, E. G., Eendebak, P., Halma, A., Van der Mark, W. & Van Rest, J. (2012). *Patentnr. EP2754089A1.* Opgehaald van https://worldwide.espacenet.com/patent/search?q=pn%3DEP2754089A1

Coole, M., Corkill, J. & Woodward, A. (2012). Defense in Depth, Protection in Depth and Security in Depth: A Comparative Analysis Towards a Common Usage Language. *Proceedings of the 5th Australian Security and Intelligence Conference.*

Den Hollander, R. J., Bouma, H., Van Rest, J. H., ten Hove, J. M., Ter Haar, F. B. & Burghouts, G. J. (2017). Automatically assessing properties of dynamic cameras for camera selection and rapid deployment of video content analysis tasks in large-scale ad-hoc networks. *Counterterrorism, Crime Fighting, Forensics, and Surveillance Technologies (Vol. 10441, p. 1044108). International Society for Optics and Photonics*.

Digitale Perimeter. (2020). Opgehaald van Gemeente Amsterdam: https://www.amsterdam.nl/wonen-leefomgeving/innovatie/de-digitale-stad/digitale-perimeter/

Evans, D., Kolesnikov, V. & Rosulek, M. (2017). A pragmatic introduction to secure multi-party computation. *Foundations and Trends® in Privacy and Security, 2(2-3)*.

Garcia, M. (2008). *The Design and Evaluation of Physical Protection Systems.* Elsevier.

Gemeente Amsterdam. (2019). Opgehaald van Register Slimme Apparaten: https://slimmeapparaten.amsterdam.nl/

Grieves, M. (2016). *Origins of the digital twin concept.* Opgehaald van https://www.researchgate.net/publication/307509727_Origins_of_the_Digital_Twin_Concept.pdf

HCSS. (2017). *Grote bewegingen, grote impact.* Den Haag: HCSS.

NCTV. (2020). *Dreigingsbeeld Terrorisme Nederland 53.* Nationaal Coördinator Terrorismebestrijding en Veiligheid.

Nunes-Vaz, R., Lord, S. & Ciuk, J. (2011). A More Rigorous Framework for Security-in-Depth. *Journal of Applied Security Research 6*, (pp. 372-393).

PRoTECT. (2020). Opgehaald van Public Resilience using TEchnology to Counter Terrorism: https://protect-cities.eu/

Schwedersky, A., Weima, I., Stolk, D. & van Rest, J. (2020). *Eindrapport kennisopbouwprogramma 'Voorkomen aanslagen' 2018/2019. TNO 2019 R11837.* Den Haag: TNO.

Solove, D. J. (2005). A taxonomy of privacy. *U. Pa. L. Rev. 154*, 477.

TACTICS. (2013). *D3.1 Conceptual Solution Description.* TACTICS. Opgehaald van http://www.fp7-tactics.eu/

The Hague Security Delta. (2019). *Security Innovation in the International Zone*. Opgehaald van The Hague Security Delta: https://www.thehaguesecuritydelta.com/projects/project/37-integral-area-protection-the-hague-international-zone

TNO. (2020). *Multi-Party Computation (MPC) uitgelegd*. Opgehaald van YouTube: https://www.youtube.com/watch?v=JnmESTrsQbg

TNO. (2020). *Secure multi-party computation: jointly analysing sensitive data without sharing it*. Opgehaald van TNO.nl: https://www.tno.nl/mpc

TNO. (2020). *Urban Strategy brings planning effects into clear focus* . Opgehaald van TNO.nl: https://www.tno.nl/urbanstrategy

TRESSPASS. (2020). Opgehaald van robusT Risk basEd Screening and alert System for PASSengers and luggage: https://www.tresspass.eu/

Van der Steur, G. (2015, November 24). BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE (Nr. 594). Den Haag.

Van der Wiel, W., Hasberg, M., Weima, I. & W. Huiskamp, W. (2010). Concept Maturity Levels Bringing structure to the CD&E process. *Proceedings Interservice / Industry Training, Simulation and Education Conference (10105)*, (pp. 2547-2555).

Van Rest, J. & Weima, I. (2018). *De toekomst van sensing voor veiligheid.* Den Haag: TNO.

Van Rest, J., Attema, T., Timan, T., Den Hollander, R. & Van Voorthuijsen, G. (2021). *Privacy bescherming bij niet-cooperatieve gezichtsherkenning.* Den Haag: TNO.

Van Rest, J., Boonstra, D., Everts, M., van Rijn, M. & Van Paassen, R. (2012). Designing privacy-by-design. *Annual Privacy Forum*, 55-72.

Van Rest, J., Van Dijk, R., Peeters, M., Smits-Clijsen, E., Sternheim, A. & Wessels, M. (2020). *Professioneel profileren: een methode voor het ontwerp en gebruik van profielen door de politie.* Den Haag: TNO.

Weima, I., Schwedersky, A., van Vliet, H. & van Rest, J. (2019). *Technologie voor terrorismebestrijding: Overzicht van technologiegebieden om de gezamenlijke aanpak van contra-terrorisme, extremisme en radicalisering te versterken.* Den Haag: TNO.

World Economic Forum. (2016). *World Economic Forum Annual Meeting 2016: Mastering the Fourth Industrial Revolution.* World Economic Forum.

A Gebruikte afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene verordening gegevensbescherming
BNT	Politie Bureau Nationale Taken
CBB	Coördinator Bewaking en Beveiliging
CML	*Concept Maturity Level*
FB	Federatieve Beveiliging
ICT	Informatie en Communicatie Technologie
IP	*Internet Protocol*
IZ	Internationale Zone
KMar	Koninklijke Marechaussee
MPC	*Multi-party computation*
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
OV	Openbaar Vervoer
PRoTECT	Public Resilience using TEchnology to Counter Terrorism
RFID	*Radio Frequency Identification*
SGBO	Staf Grootschalig Bijzonder Optreden
TACTICS	Tactical Approach to Countering Terrorists in Cities
TRESSPASS	robusT Risk basEd Screening and alert System for PASSengers and luggage
TRL	*Technology Readiness Level*
WPG	Wet Politiegegevens

B Initiatieven rondom informatiedeling voor beveiliging

Separate beveiligingsringen overlappen elkaar vaak, zodat feitelijk sprake is van een “beveiligd gebied”, in plaats van een aantal afzonderlijk beveiligde objecten. Denk bijvoorbeeld aan de Internationale Zone in Den Haag, een druk stationsgebied of een omgeving rondom een stadion waar ook horeca en retail aanwezig is. Een concept van *federatieve beveiliging* bestaat op dit moment nog niet. Het idee achter een dergelijke federatie is geïnspireerd op recente initiatieven waar sprake is van beveiligings- / veiligheidsopgaven, waarbij gekeken is naar de kracht en potentie van informatiedeling tussen (semi-) publiek- en private partijen.

In de paragrafen hieronder zijn voorbeelden van initiatieven beschreven. Het betreft vooral initiatieven waar o.a. TNO bij betrokken is (geweest). Er zijn ook andere initiatieven (geweest) die mogelijk (zeer) relevante informatie en/of inspiratie kunnen bieden. Criminee in Eindhoven en Zwolle is een voorbeeld, en ook de Digitale Vertrouwensinfrastructuur. Er was over deze initiatieven geen expliciete informatie beschikbaar op het benodigde detailniveau.

Per initiatief wordt aangegeven wat het respectievelijke doel was, wat het concept inhoudt en het (beoogde) resultaat ervan is. De laatste paragraaf analyseert deze initiatieven en geeft aan welke inzichten uit deze initiatieven worden meegenomen in deze verkenning.

B.1 Voorkomen aanslagen

In 2018 en 2019 heeft TNO samen met de NCTV het kennisopbouwprogramma ‘Voorkomen Aanslagen’ uitgevoerd.

B.1.1 Aanleiding / doel

In dit programma is kennis en kunde ontwikkeld om bij te dragen aan de doelstelling van de NCTV, namelijk om met ketenpartners in staat te zijn proactief en continu te sturen op de versterking en ontwikkeling van de benodigde capabilities voor het voorkomen van aanslagen. Eén van de projecten binnen het programma richtte zich op de methodiekontwikkeling van capability-assessment en gap-analysis die bijdraagt aan het versterken van de gezamenlijke aanpak van terrorismebestrijding.

B.1.2 Concept

Het *capability-model* (zie figuur B.1) is ontwikkeld om overzicht te creëren van taken en vermogens die nodig zijn in de keten voor terrorismebestrijding. Het model heeft betrekking op het geheel van activiteiten die door ketenpartners dienen te worden afgedekt om aanslagen te voorkomen dan wel adequaat te reageren om een vervolgaanslag te voorkomen en/of gevolgen te beperken.

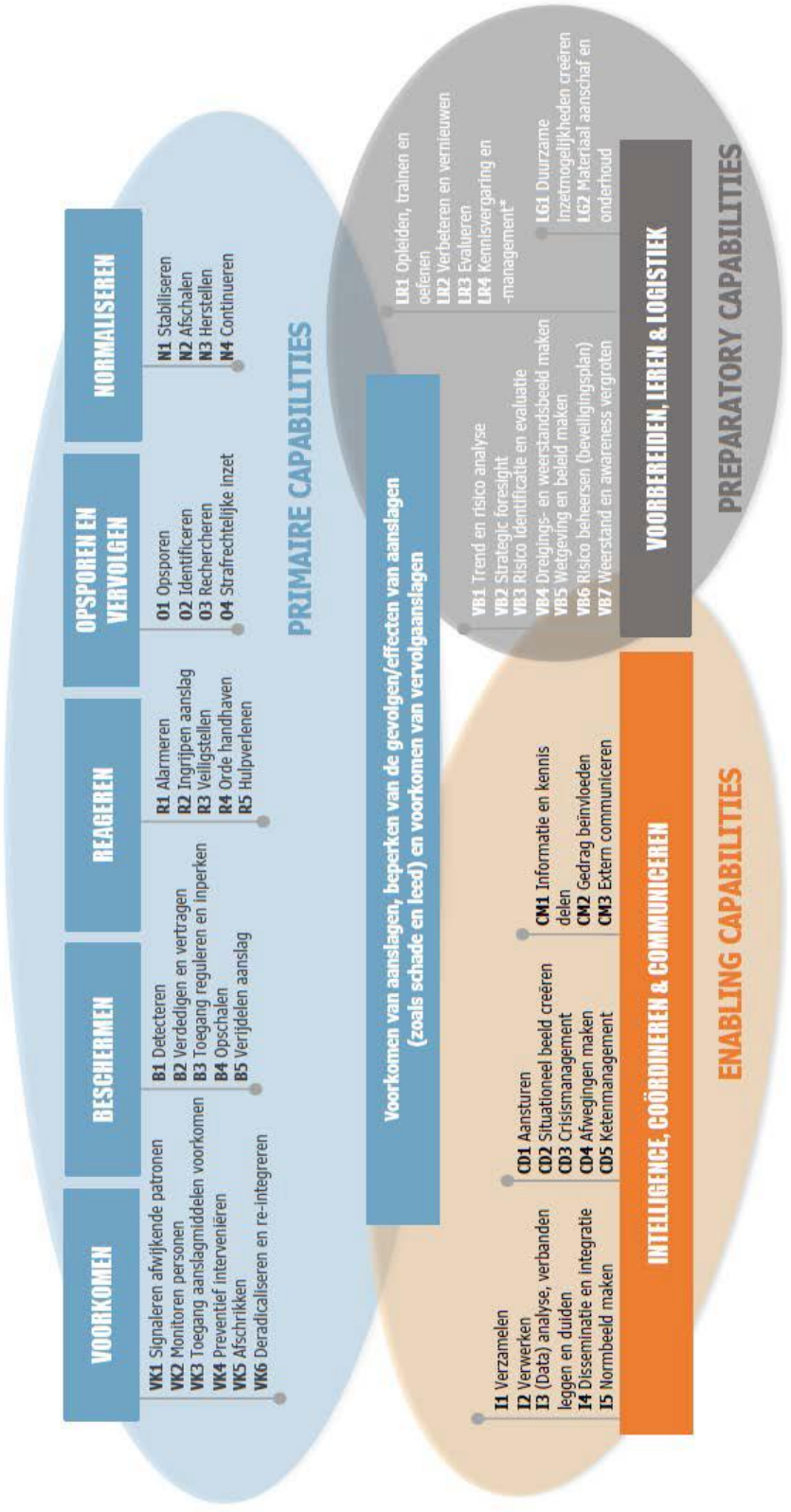
B.1.3 Resultaat

In het model zijn drie soorten *capabilities* onderscheiden: de *primaire*, de *enabling* (ondersteunende) en de *preparatory* (voorbereidende) *capabilities* (zie tabel B.1).

Tabel B.1 Typen capabilities.

Type *capability*	**Beschrijving**
Primair	Staan het meest dichtbij het direct voorkomen van aanslagen: voorkomen, beschermen, reageren, opsporen & vervolgen, en herstellen.
Enabling	Zorgen ervoor dat de andere *capabilities* beter kunnen functioneren: intelligence, coördineren en communiceren.
Preparatory	Zijn voorbereidend om alle andere *capabilities* beter uit te kunnen voeren: voorbereiden, leren en logistiek.

Iedere *capability* is opgedeeld uit meer specifieke *capabilities* (zie figuur B.1). Bijvoorbeeld, onder de *capability* “Voorkomen”, vallen zes *capabilities* waaronder “Signaleren afwijkende patronen”.



Figuur B.1 Capability model voorkomen aanslagen.

B.2 Internationale Zone

B.2.1 Aanleiding / doel

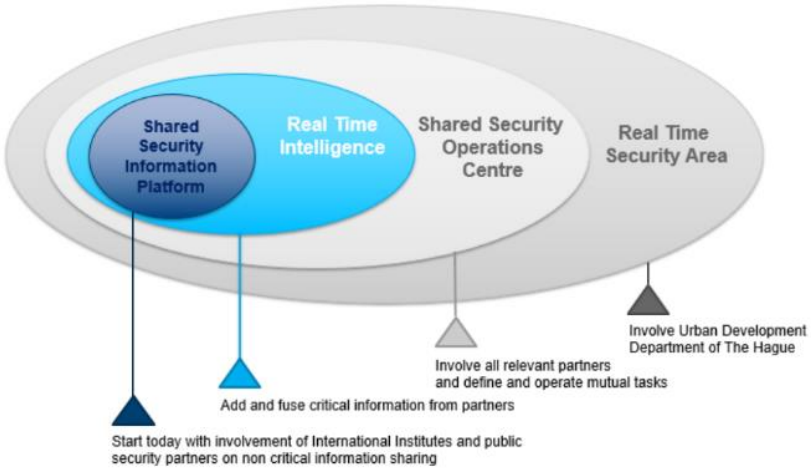
Met in het achterhoofd de opgave om de balans te vinden tussen veiligheid, attractiviteit en economische aantrekkingskracht was dit project gericht op het opzetten van een fieldlab in de Internationale Zone in Den Haag. Door het nemen van effectieve maatregelen moest de beveiliging en veiligheid binnen de Internationale Zone gewaarborgd worden, zonder in te boeten aan de toegankelijkheid van het gebied en de kwaliteit van leven voor de bewoners en bezoekers. Om dit te bewerkstelligen is een innovatief beveiligingsconcept onderzocht dat tegemoet komt aan deze ambitie. Het concept moest een robuust veiligheidsniveau creëren voor de organisaties en bewoners in het gebied. Centraal binnen het concept stond het ervaren en identificeren van de waarde van het delen van informatie. Ook werd stil gestaan bij de voorwaarden en functionaliteiten voor een ‘Shared Security Information Platform (SSIP)’.

B.2.2 Concept

Het ontwikkelde concept bestaat uit vier fasen (zie figuur B.2), waarbij de SSIP de eerste fase beslaat. De SSIP is een communicatie platform voor het asynchroon uitwisselen van data (tekst, afbeeldingen, video’s) tussen (internationale) organisaties. De informatie van het platform zou in een volgende iteratie verrijkt kunnen worden met informatie uit open bronnen.

In de tweede fase wordt een Real Time Intelligence component toegevoegd aan de SSIP, dit wordt zodanig gedaan dat verrijkte informatie wordt gegenereerd en klaargezet wordt voor geschikt gebruik.

In een volgende fase zou de Real Time Intelligence worden uitgebreid met een Shared Security Operations Centre (SSOC) waarbinnen beveiligings- en veiligheidsactiviteiten binnen het gebied worden gemonitord en gecoördineerd. Wanneer tot slot ook gewerkt wordt aan de fysieke lay-out en het ruimtelijk ontwerp spreek je van een Real Time Security Area.

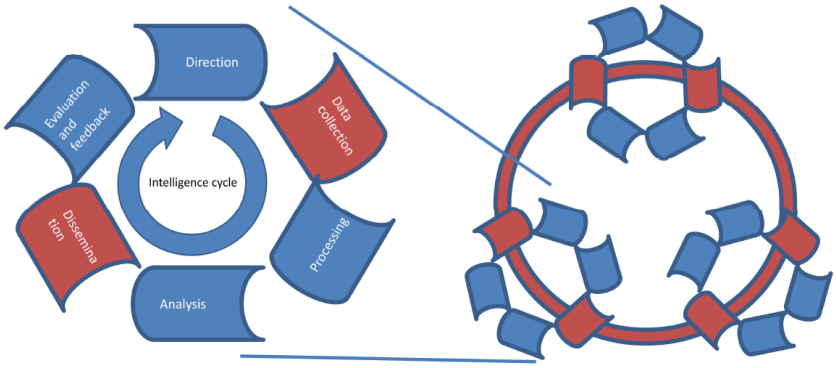


Figuur B.2 De vier fasen van het innovatieve concept voor gebiedsbeveiliging.

Wat betreft informatie is binnen het concept uitgebreid stilgestaan bij de principes van ‘need to know’ en ‘need to share’ en de nadelen hiervan[15]. Hier is een nieuw principe uit voortgekomen dat neergezet is als ‘We need to share what others need to know’. Om hier te komen moeten de doelen van de verschillende partijen die deelnemen aan de samenwerking duidelijk zijn: ‘I need to know what I need to share’.

Eén van de uitvloeisels uit deze insteek betreft het feit dat het concept gericht was op het delen van ‘bezorgdheid’ zonder daar gelijk veiligheids-sensitieve data bij te delen. Op basis van deze bezorgdheidssignalen kunnen de andere partijen bepalen welke informatie ze met de andere partij moeten delen.

Binnen dit concept werd nadrukkelijk gekozen voor het delen van informatie en niet het delen van intelligence. Het idee achter het concept was dat informatie werd gedeeld zodat de deelnemende partijen binnen hun eigen organisatie er intelligence van konden maken. Binnen dit intelligence proces van elke organisatie zitten twee stappen die te maken hebben met communicatie, te weten ‘data collection’ en ‘dissemination’, deze beide stappen worden door het SSIP ondersteund (zie figuur B.3). Hierdoor ontstaat een continue flow aan verrijkte veiligheidsinformatie.



Figuur B.3 De intelligence-cycli van verschillende organisaties (bijv. drie in deze figuur) versterken elkaar door informatie met elkaar te delen.

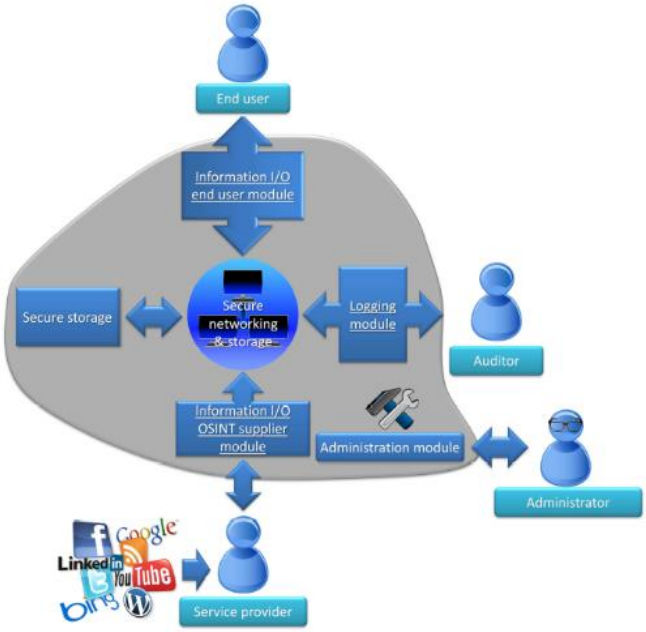
In het SSIP concept bij de IZ is bewust gekozen om het te laten dienen voor situaties die betrekking hebben op ‘dagelijkse gang van zaken’, ‘evenementen’, ‘gevaarlijke situaties’ en ‘verdachte situaties’. Niet opzettelijke en opzettelijke incidenten zijn buiten de scope van de SSIP gehouden, dit heeft invloed op het type scenario’s die met het SSIP kunnen worden afgehandeld.

B.2.3 Resultaat

In het onderzoek is een SSIP ontwikkeld dat gebruikt kan worden als een communicatie platform waarop veiligheidsinformatie tussen politie, gemeente en (internationale) organisaties met hoog risico-objecten gedeeld kan worden (zie

[15] ‘Need to know’ impliceert dat informatie enkel gedeeld wordt als het evident is dat een andere partner die informatie moet weten. Het risico van dit principe is dat een deel van de informatie niet bij andere partijen terecht komt die het wel nodig hebben en die partijen weten tevens niet dat de informatie bestaat. ‘Need to share impliceert dat alle informatie wordt gedeeld, het risico van dit principe is dat er te veel informatie gedeeld wordt, ook met partijen die de informatie niet nodig hebben en wellicht zelfs niet te vertrouwen zijn.

figuur B.4). De informatie kon worden weergegeven in verschillende formats: tijdlijn, geografisch, bulletin board type. Er is bewust gekozen voor het gebruik van off-the-shelf technologieën, die specifiek aangepast zijn voor de pilot binnen de Internationale Zone.



Figuur B.4 Functioneel ontwerp van het *Shared Security Information Platform.*

B.3 Digitale Perimeter Johan Cruijff Arena

B.3.1 Aanleiding / doel

Om zowel de veiligheid van bezoekers en medewerkers als de bezoekerservaring te verhogen is een digitale veiligheidsring rondom de Johan Cruijff ArenA ontwikkeld. Hiermee wil men op een innovatieve manier vorm geven aan service en veiligheid tijdens grote evenementen in de ArenA. Het onderzoek richt zich tevens op de vraag of de gebruikte technologieën hun doel dienen, makkelijk in gebruik zijn en of het gebruik daarvan ethisch verantwoord is.

B.3.2 Concept

De Digitale Perimeter beoogt een ‘virtueel hek’ te creëren door gebruik te maken van verschillende technologische toepassingen. Door de data uit deze toepassingen te combineren ontstaat een geïntegreerd, real-time beeld van de ArenA en de directe omgeving. Afwijkingen van de “normale” status kunnen automatisch worden gedetecteerd, zodat medewerkers snel kunnen ingrijpen bij incidenten. Het concept beoogt niet alleen de veiligheid van alle aanwezigen in en rondom de ruimte te verhogen, maar streeft ook een verbeterde bezoekerservaring na. De gebruikte technologieën kunnen namelijk worden ingezet om knelpunten in de mensenstroom weg te nemen (denk aan toegangscontroles).

Er wordt een digitaal track record gemaakt zodra een persoon het arenagebied binnenkomt. Alle data over een persoon worden gelezen, geanonimiseerd en verzonden naar een centraal datacenter. Daar wordt alle informatie verzameld en in kaart gebracht.

Eén deelproject gaat over niet-coöperatieve gezichtsherkenning (zie figuur B.5). Specifiek over de vraag of het mogelijk en nuttig is om live beelden en *enrollment* beelden gescheiden te verwerken en toch matches daartussen te kunnen vinden.

Figuur B.5 Infographic over privacy beschermende gelaatsherkenning bij de Digitale Perimeter.

B.3.3 Resultaat

Een digitale veiligheidsring rondom de Johan Cruijff ArenA waarmee ongewenst gedrag gedetecteerd kan worden, mensenstromen gemanaged kunnen worden en bezoekers op het bezit van wapens of vuurwerk kunnen worden gescand. De veiligheidsring maakt gebruik van onder andere camera's en sensoren.

B.4 FP7 TACTICS

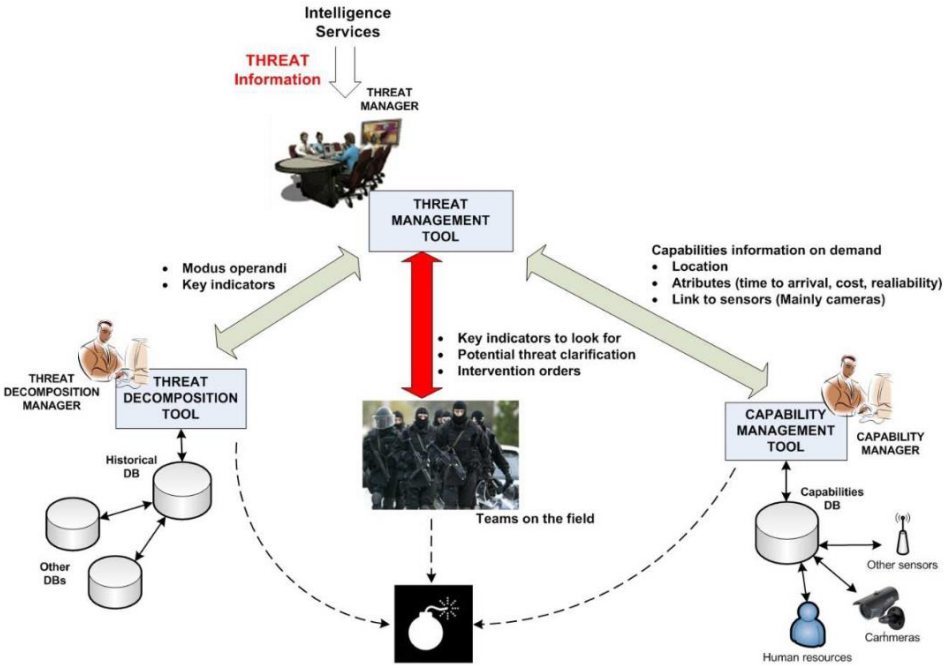
B.4.1 Aanleiding / doel

Mede naar aanleiding van diverse terroristische aanslagen in Europa publiceerde de Europese Commissie in 2010 een onderzoeksuitvraag in FP7 met daarin een onderwerp over contra-terrorisme in een stedelijke omgeving.

B.4.2 Concept

Een internationaal consortium met onder andere de politie, KMar en TNO voerde daarop het TACTICS (Tactical Approach to Countering Terrorists in Cities) project uit. Het kernidee van TACTICS was dat juist in een stedelijke omgeving kostbare tijd kon worden gewonnen door bij een duidelijke terroristische dreiging, op slimme en beheersbare wijze zo veel mogelijk gebruik te maken van reeds bestaande sensoren (TACTICS, 2013).

In dat concept werd gebruik gemaakt van een rol die "Capability Manager" heet. Diens rol bestond er uit om informatiebehoeften te koppelen aan aanbod van (sensor)data (zie figuur B.6).



Figuur B.6 TACTICS concept waarin de capability manager zorgde voor het combineren van informatiebehoeften aan aanbod van (sensor)data.

B.4.3 Resultaat

Het concept van TACTICS is beproefd middels *table top games* als onderdeel van de opleiding van commandanten van SGBO's.

B.5 Visie op Cameratoezicht Prorail

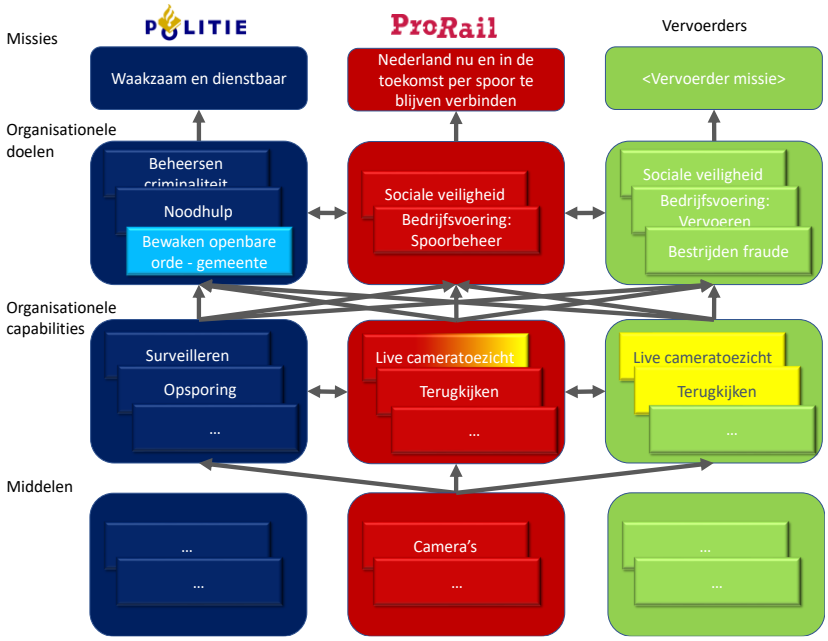
B.5.1 Aanleiding / doel

In 1993 zijn de eerste camera's op Nederlandse treinstations geplaatst. Door de tijd heen is de inrichting van stations veranderd, de problematiek waartoe de camera's dienen is veranderd en ook de technologie is aan grote veranderingen onderhevig. Vanwege onderhoud worden camera's regelmatig vervangen. ProRail wil dat cameratoezicht voor elk soort gebied op en rond de stations toegespitst moet zijn op de specifieke problematiek in dat gebied. Daarom moet het cameratoezicht op basis van actuele informatie en inzichten én op een systematische en logisch onderbouwde wijze worden ingericht en uitgevoerd. Eén van de belangrijkste aanleidingen voor de visie op cameratoezicht was een herziening van de doelen waarvoor cameratoezicht werd ingezet. ProRail wilde de doelen niet enkel vanuit de behoeften van de eigen organisatie maar juist ook kijken naar de samenwerking met ketenpartners en overige belanghebbenden die deels in dezelfde (semi-) openbare gebieden actief zijn, zoals de NS, politie en gemeenten. ProRail zocht daarom een visie op cameratoezicht waarin die andere behoeftes ook een plek kregen. Samengevat beschrijft de visie "Het waarom & waartoe van cameratoezicht bij treinstations".

B.5.2 Concept

In de visie wordt ook informatiedeling genoemd. Zo worden de camera's beheerd door ProRail, maar kunnen de camerabeelden worden gebruikt door verschillende belanghebbende partijen, zoals Politie of vervoerders (zie figuur B.7). Deze partijen

hebben allemaal andere doelen, deze doelen bereiken ze door gebruik te maken van dezelfde informatie. Het vastleggen van deze doelen is een belangrijk uitkomst van de herziening van de visie op cameratoezicht.



Figuur B.7 De huidige samenwerking van cameratoezicht rond treinstations van ProRail.

B.5.3 Resultaat

De visie betreft een beschouwing van de uitdagingen op het gebied van veiligheid en beheer met betrekking tot cameratoezicht. Deze uitdagingen zijn bekeken vanuit ProRail zelf en vanuit door ProRail geïdentificeerde relevante andere belanghebbenden, zoals vervoerders, gemeenten en politie, op basis van gezamenlijke rollen en doelen voor cameratoezicht. De visie beschrijft ook in welke taken camera's kunnen ondersteunen om die doelen te behalen. Hierbij zijn camera's vaak een onderdeel van een breder pakket van maatregelen.

B.6 ISF PRoTECT

B.6.1 Aanleiding / doel

Het Europese project PRoTECT (Public Resilience using TEchnology to Counter Terrorism) heeft tot doel een kwetsbaarheidsanalyse tool te realiseren waarmee gemeentes in de Europese Unie met hun lokale partners kwetsbare plekken (zogenaamde soft spots) in hun openbare ruimtes kunnen opsporen. Een ander doel is het uitvoeren en testen van technologische innovaties om terroristische dreigingen te voorkomen.

B.6.2 Concept

Het concept van ProTECT gaat uit van het opsporen van kwetsbaarheden, om op basis daarvan te kijken welke technologieën deze kwetsbaarheden kunnen mitigeren. Het delen van informatie kan hierbij een mitigatie zijn van een bestaande kwetsbaarheid. Het werken met een dergelijke tool kan tevens inzicht geven of er een kwetsbaarheid ligt op het vlak van informatiedeling. Daarnaast kun je gezamenlijk het gesprek voeren wat voor informatie je nodig hebt om nog meer

inzicht te verkrijgen in je kwetsbaarheden óf welke informatie je nodig hebt om andere acties te kunnen ondernemen.

B.6.3 Resultaat

Eén van de resultaten van het project ProTECT betreft de manual van de EU Vulnerability Assesment Tool. De manual, die getest is met eindgebruikers, stelt gemeenten en betrokken veiligheidspartners in staat om een reeds uitgekozen gebied gezamenlijk te beveiligen.

B.7 H2020 TRESSPASS

B.7.1 Aanleiding / doel

TRESSPASS (robusT Risk basEd Screening and alert System for PASSengers and luggage) is een Europees (H2020) project dat zich richt op innovatie in het grenstoezichtdomein binnen alle drie de modaliteiten: lucht, maritiem en land. Op dit moment worden op basis van rigide richtlijnen controles op alle reizigers uitgevoerd, wat voor vertraging zorgt in het grenspassageproces. De verwachting van de Europese Commissie is dat het aantal reizigers in en uit Schengen zal toenemen over de tijd, waardoor deze vertragingen die ontstaan door de huidige manier van grenstoezicht ook zullen toenemen. Vandaar dat TRESSPASS zich toelegt om te helpen bij een transitie van de huidige (regelgestuurde) grenscontroles, naar risicogestuurd grenstoezicht. De doelen van TRESSPASS zijn hierbij onder andere om een risicogestuurd grenstoezichtconcept te ontwikkelen, en deze toe te passen in drie pilots om dit concept ook te beproeven.

B.7.2 Concept

Het idee achter het concept van risicogestuurd grenstoezicht is dat op basis van individuele risico-inschattingen van reizigers kan worden bepaald of zij nog in het grenspassageproces moeten worden gecontroleerd, of dat zij zonder tussenkomst van menselijke grenstoezicht Schengen kunnen betreden of verlaten. Hierbij moet een balans worden gezocht tussen de vier aspecten van grenstoezicht: de mate van effectiviteit van het grenstoezichtproces, de doorstroomsnelheid van reizigers, efficiëntie in de uitvoer van grenstoezicht, en de (privacy/ethische) impact van het proces op de individuele reiziger.[16]

Het kernprincipe achter risicogestuurd grenstoezicht is dat er op basis van informatie over de reiziger in verschillende fases van het reizigersproces kan worden besloten of de persoon voldoet aan een bepaald *risicoprofiel*: een profiel kwaadwillende reiziger die de doelen van het grenstoezicht in gevaar brengen (bijvoorbeeld irreguliere migranten of grensoverschrijdende criminaliteit), of juist profielen van reguliere reizigers.

Eén van de onderdelen van TRESSPASS is internationale samenwerking rond risicosturing. Dat kan worden ingevuld door informatie over reizigers(groepen) te delen. Maar hoe weet het ene land nu welke informatie het andere land nodig heeft? Dat kan mogelijk door profielen met elkaar te delen als onderbouwing van de informatievraag.

[16] Van Rest, J., Stolk, D., Weima, I. & Wessels, M. (2019). Deliverable 1.2: Conceptual Model. *Confidential*. TRESSPASS project.

B.7.3 Beoogd resultaat

TRESSPASS kent vele tussenresultaten waarbij verschillende technologieën of methoden worden ontwikkeld. Het hoofddoel van TRESSPASS is om te bestuderen in hoeverre een risicogestuurd grenstoezichtconcept kansrijk en haalbaar is.

B.8 Professioneel profileren

B.8.1 Aanleiding / doel

De politie doet aan profileren met behulp van ICT in een aantal landelijke diensten. De portefeuilles Intelligence en Digitalisering & Cybercrime van de politie wensten die *capability* ook te ontsluiten voor regionale eenheden. Daartoe was het nodig om een methode te ontwikkelen die de professionaliteit van het profileren helpt borgen.

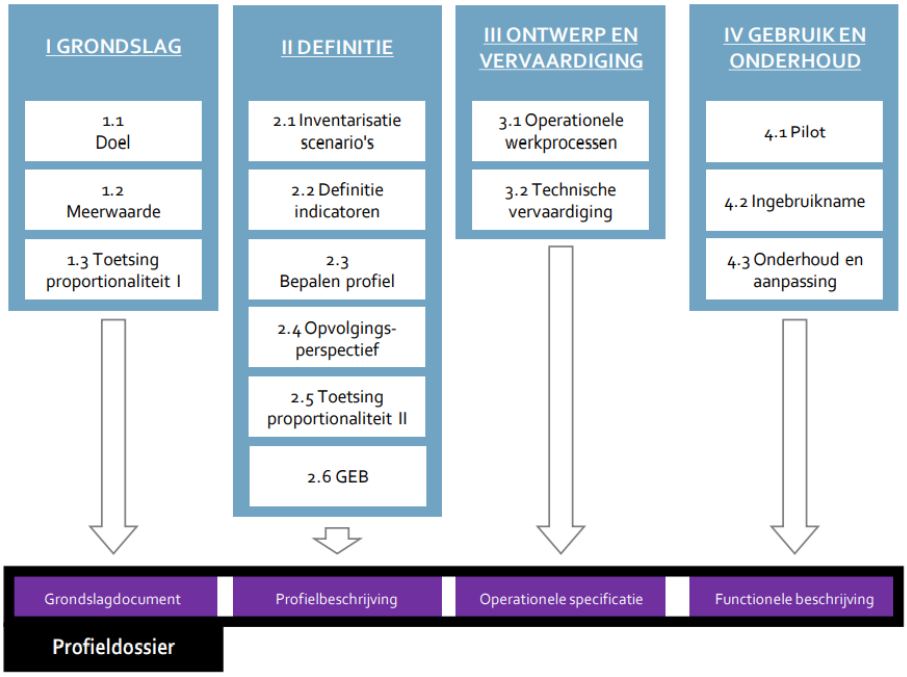
Het doel van profileren is om te helpen bepalen wat de beslissing over een opvolging is of moet zijn. Het gebruik van profielen (profileren) kan helpen om informatie uit datastromen gestuurd en automatisch te verwerken, vanuit vooraf gedefinieerde doelen. Het object van profileren, oftewel het type casus, kan een persoon, een ding en ook een situatie zijn. Profileren is per definitie geen meting of waarneming: het moet gezien worden als een aanname.

B.8.2 Concept

Bij profileren wordt een kenmerk van een casus (bijv. de kans op betrokkenheid bij een misdaad) ingeschat op basis van andere kenmerken van de betreffende casus (zoals bijvoorbeeld gedrag). De typische functie van profileren is om een verzameling van casussen (dingen, personen, situaties) te scheiden in twee of meer groepen. De functie van die scheiding hangt af van het toepassingsgebied (bijv. stoppen mobiel banditisme). Binnen het toepassingsgebied veiligheid wordt onderscheid gemaakt in preventie (vooraf), repressie (tijdens), opsporing en herstel (achteraf). De effectiviteit van profileren moet dus worden uitgedrukt in de mate waarin een verzameling casussen op zo'n manier kan worden onderscheiden dat die tot een opvolgingsbeslissing leidt die direct of indirect aan een veiligheidseffect (voor, tijdens of na een incident) bijdraagt. Kortom: profileren moet een nuttig onderscheid in een verzameling casussen opleveren.

B.8.3 Resultaat

Het resultaat van het project is een methodiek bestaande uit vier fasen (zie figuur B.8). In deze fases wordt bepaald wat de grondslag, de definitie, het operationeel ontwerp en het gebruik van het profiel inhouden:



Figuur B.8 De methodiek Professioneel Profileren bestaat uit vier fases. (Tussen)resultaten worden vastgelegd in het profieldossier.

B.9 Sensoren en systemen voor security

B.9.1 Aanleiding / doel

Van 2012 tot 2017 is een serie topsector projecten uitgevoerd. Het doel van deze projecten was om de Nederlandse high-tech industrie te helpen om relevante high-tech te identificeren, ontwikkelen en beproeven in het veiligheidsdomein.

Parallel daaraan, in 2015, publiceerde de minister van Justitie en Veiligheid een visie op sensing met de politie. Die vormde de basis voor het veranderprogramma Sensing bij de politie.

TNO publiceerde in 2018 op basis van een serie topsector-projecten in het veiligheidsdomein een visie op sensing voor veiligheid (Van Rest & Weima, De toekomst van sensing voor veiligheid, 2018). Daarin zijn zeven strategische principes gedefinieerd die kunnen helpen om een veiligheidsorganisatie op gebied van sensing te helpen richten.

B.9.2 Concept

De zeven principes van TNO zijn:

- Privacy by design en security by design voor sensing;
- Metadateren en filteren bij de bron;
- Sensordata van voldoende kwaliteit;
- Sensing slechts als het nodig is;
- Gebruikmaken van andermans sensoren;
- Nieuw sensingconcept ontwikkelen;
- Sensing waarderen op effecten.

B.9.3 Beoogd resultaat

De politie constateerde dat de visie uit 2015 verouderd raakte door voortschrijdend inzicht, nieuwe maatschappelijke trends, en ontwikkelingen bij de politie. TNO heeft in 2017 - 2019 in een apart project de politie geholpen om een startnotitie te schrijven voor een nieuwe visie op sensing voor de politie, mede gebaseerd op de zeven principes van TNO Dit is een compact startdocument geworden, specifiek voor de politieorganisatie.

C Effect van Federatieve Beveiliging op capabilities ten behoeve van Voorkomen Aanslagen

In deze bijlage worden de effecten van federatieve beveiliging geduid aan de hand van het capability model van (Schwedersky, Weima, Stolk, & van Rest, 2020). Dat capability model is gemaakt voor contra-terrorisme, en gebruikt daarom termen uit dat domein (terrorisme, CTER, aanslag). Die termen zijn hieronder vervangen door dreiging-neutrale termen. Het gaat hieronder nog steeds wel om een dreiging vanuit menselijke kant, waaronder terrorisme en criminaliteit.

C.1 Primaire capabilities

C.1.1 Voorkomen

Sub-capability	Functie / beschrijving	Kansen voor FB
Signaleren afwijkende patronen	Het signaleren van afwijkende patronen zoals gedrag dat niet past bij een situatie en mogelijk duidt op voorbereidende handelingen van een misdaad. Het gaat daarbij om reispatronen, financieringspatronen, gedragspatronen, routes en bewegingen en andere afwijkende situaties	Door het combineren van informatie van verschillende partijen en ringen ontstaat een completer beeld van de situatie. Dit biedt kansen wat betreft het signaleren van afwijkend gedrag in een situatie.
Monitoren	Het fysiek en/of digitaal monitoren van (verdachte) geradicaliseerde of verwarde personen en/of groepen.	Daar waar zonder federatie alle partijen de situatie separaat monitoren, kan een federatie kansen bieden om hier gezamenlijke afspraken in te maken.
Afschrikken	Het onaantrekkelijk maken van het plegen van een misdaad door het, vanuit het gezichtspunt van de dader(s) bezien, (a) vergroten van de nadelige gevolgen ervan ten opzichte van de potentiële voordelen, of (b) wegnemen van de voordelen. Bijvoorbeeld, wanneer kan worden verwacht dat een misdaad wordt gepleegd met als doel om media-aandacht te verkrijgen, kan het op voorhand wegnemen van media-aandacht als middel worden ingezet.	Om de capability afschrikken goed in te zetten is het nodig inzicht te hebben in de voordelen en nadelige gevolgen van potentiële misdaden. Een federatie biedt kansen om het inzicht hierin te vergroten en daarmee gericht interventies in te zetten.
Preventief interveniëren	Het interveniëren tijdens de voorbereidende handelingen van een misdaad. Het gaat daarbij om het verstoren, verhinderen en/of stoppen van deze voorbereidingen, maar ook kan gebruik worden gemaakt van infiltratie. Het onschadelijk maken, neutraliseren en in beslag nemen van (aanslag)middelen hoort hier ook bij.	Daar waar voorbereidende handelingen rondom een object plaatsvinden biedt een federatie kansen als het gaat om het vroegtijdig detecteren van deze voorbereidende handelingen waardoor hier preventief op geïntervenieerd kan worden.

C.1.2 Beschermen

Deze capability gaat over het klassieke beveiligen. Federatieve beveiliging is met name bedoeld om deze *capability* te verbeteren.

Sub-capability	Functie / beschrijving	Kansen voor FB
Detecteren	Het detecteren van (voorbereidingen op) een incident. Het kan daarbij gaan om detectie van een middel (zoals wapens) en detectie naar omgeving (verdachte situaties en gedrag, zowel digitaal als niet-digitaal).	Een federatie biedt kansen om aan de voorkant met de diverse deelnemende partijen gezamenlijk te bepalen wat er gedetecteerd moet worden en wie daar de juiste sensoren / bronnen voor beschikbaar heeft om deze uiteindelijk met elkaar te delen en zo toe te werken naar vroegtijdige detectie.
Verdedigen en vertragen	Het verdedigen en vertragen van een aanval. Dit kan bijvoorbeeld plaatsvinden door middel van fysieke beveiligingsmaatregelen waardoor de situatie voor de daders wordt bemoeilijkt	Door het delen van informatie tussen verschillende partijen kan het inzicht in de modus operandi verbeteren, hier kan op geanticipeerd worden door de maatregelen ten behoeve van verdedigen en vertragen aan te passen / aan te scherpen.
Toegang reguleren en inperken	Het reguleren en inperken van toegang tot gebieden en/of gebouwen voor zowel mensen als objecten. Het gaat hierbij om zowel digitale als fysieke maatregelen. Deze *capability* is van belang voordat een aanval plaatsvindt, maar ook tijdens een aanval en daarna. Een voorbeeld is het reguleren van de toegang voor verkeer, waarbij zware voertuigen zoals vrachtwagens niet meer worden toegestaan in een potentieel gevaarlijk gebied.	Informatie vanuit FB kan in de voorbereidingsfase van belang zijn, bijvoorbeeld om te bepalen welke toegangsregulerende maatregelen getroffen moeten worden. Deze informatie kan ook helpen wanneer er sprake is van de warme fase en aanvullende toegangsmaatregelen getroffen moeten worden.
Opschalen	Het verhogen van het niveau van alertheid door middel van opschaling. Dit kan worden gedaan aan de hand van een dreiging en wordt toegepast om een hoger niveau van alertheid te bereiken. Hierdoor kan ook een betere respons worden gegeven wanneer een aanval plaatsvindt. Dit impliceert dat bijvoorbeeld noodzakelijke maatregelen kunnen worden getroffen zoals het gereed stellen van ambulances en het voorbereiden van ziekenhuizen op een mogelijke toestroom van slachtoffers.	Een federatie kan zinvol zijn om op basis van een gedeeld informatiebeeld & dreigingsbeeld gezamenlijk een niveau van alertheid te bespreken.
Verijdelen aanslag	Het vroegtijdig reageren op een aanval met beschikbare middelen. Welke reactie dit is hangt af van de modus operandi en (daarmee) ook van de gebruikte middelen.	Een federatie biedt kansen door met behulp van een betere informatiepositie in een eerdere fase een aanval te kunnen verijdelen. Wanneer de federatie ook afspraken maakt over operationele inzet geeft dit ook kansen in de mogelijkheden van verijdeling.

C.1.3 Reageren

Sub-capability	Functie / beschrijving	Kansen voor FB
Alarmeren	Het alarmeren van eenheden en andere uitvoerende diensten, betrokkenen, omstanders en de samenleving in het algemeen.	Een federatie kan afspraken maken hoe men elkaar onderling informeert en alarmeert, separaat aan de reguliere opschalingslijnen naar uitvoeringsdiensten. Dit geeft kansen in de wijze waarop en de snelheid waarmee geschakeld kan worden.
Ingrijpen	Het ingrijpen bij een aanval omvat het actief stoppen en/of neutraliseren van de aanvallers. Ook het voorkomen van vervolgaanvallen valt hieronder. Op welke manier moet worden ingegrepen bij een aanval verschilt per aanslagmiddel en hangt verder af van de motivatie die een kwaadwillende heeft, en hoe een eventueel middel naar het doelwit is/wordt gebracht.	Door binnen een federatie niet enkel informatie te delen, maar aan de voorkant ook gezamenlijk te prepareren op scenario's kunnen afspraken gemaakt worden ten aanzien van het ingrijpen bij een aanval.
Veiligstellen	Het in veiligheid brengen van mensen, objecten, diensten en de omgeving. Na een explosie kan bijvoorbeeld instortingsgevaar ontstaan waardoor personen en objecten in veiligheid moeten worden gebracht. Ook kan het gaan om het omleiden van verkeersstromen of het veiligstellen van gebieden waar zich veel mensen bevinden.	Binnen een federatie kunnen in de preparatiefase voorbereidingen getroffen waarin per scenario gekeken kan worden naar locaties etc. waar veiligstelling eventueel mogelijk is. In de hete fase kan gerichte informatie uitwisseling uitsluitsel geven over de mogelijkheden wat betreft 'safe havens'.
Orde Handhaven	Het handhaven van de openbare orde. Hier vallen bijvoorbeeld crowd control en riot control onder.	Informatie-uitwisseling binnen een federatie biedt kansen voor het verkrijgen van een situatie beeld wat nodig is voor het handhaven van de orde.
Hulpverlenen	Het verlenen van hulp aan slachtoffers en omstanders. Het gaat daarbij om noodhulp zoals medische hulp (bijv. triage) maar ook het beveiligen van gebieden/personen, begeleiden van personen of zoeken van (mogelijke) slachtoffers.	In de preparatiefase kunnen aan de voorkant afspraken gemaakt worden wat betreft hulpverlening bij een aanval. In de hete fase kan informatie-uitwisseling middels de federatie bijdragen aan gerichtere hulpverlening.

C.1.4 Opsporen

Sub-capability	Functie / beschrijving	Kansen voor FB
Opsporen	Het opsporen van (verdachte) personen, middelen en/of strafbare feiten die mogelijk een relatie hebben met illegitieme handelingen.	Binnen een federatie is inzicht in de doelen, taken, verantwoordelijkheden en sensoren van alle betrokken partijen. Dit inzicht geeft kansen ten tijde van de opsporing van een strafbaar feit doordat hierdoor gerichter informatie opgevraagd kan worden, immers is bekend wie welke informatie beschikbaar heeft.
Identificeren	Het identificeren van (mogelijke) daders, middelen en betrokkenen bij illegitieme handelingen. Het gaat daarbij om zowel de digitale identificatie als fysieke identificatie.	Door de bundeling van krachten van diverse deelnemende partijen worden de kansen wat betreft identificatie van (mogelijke) daders vergroot.

C.1.5 Normaliseren

Sub-capability	Functie / beschrijving	Kansen voor FB
Stabiliseren	Het herstellen van de openbare orde en veiligheid na een dreiging of incident.	De federatie biedt kansen doordat het een beter situatiebeeld kan genereren wat gebruikt kan worden bij het herstellen van de openbare orde. Daarnaast biedt het kansen door aan de voorkant met de betrokken partijen afspraken te maken over ieders taken, rollen en verantwoordelijkheden bij het herstel.
Afschalen	Het onder bepaalde voorwaarden verlagen van het alerteringsniveau, zodat de van personele en materiële middelen kan worden teruggeschroefd. Dit betreft ook het intrekken van bijzondere bevoegdheden die tijdelijk zijn ingesteld.	Door aan de voorkant gezamenlijk af te spreken welke informatie nodig is om te bepalen of afschaling mogelijk is, kan gericht informatie ingewonnen en gedeeld worden waardoor het keuzeproces rondom afschaling gefaciliteerd wordt.

C.2 Ondersteunende capabilities

C.2.1 Intelligence

Sub-capability	Functie / beschrijving	Kansen voor FB
Verzamelen	Het verzamelen van data op basis van vooraf bepaalde criteria. Het gaat om het verzamelen van informatie over personen en groeperingen maar ook over (nieuwe) modi operandi en daarmee (aanvals- en verdedigings-) methoden en middelen	Door de criteria in de koude fase met meerdere partijen te delen, kan er door meer partijen gericht informatie verzameld worden. Hierdoor ontstaat er een breder inzicht in personen, groeperingen en modus operandi.
Verwerken	Het verwerken van data tot relevante informatie. Het gaat om zowel het verwerken van grote hoeveelheden (digitale en niet-digitale) informatie als kleine stukjes informatie.	Door aan de voorkant afspraken te maken over het type informatie dat wordt gedeeld (data, informatie of intelligence) kan door FB sprake zijn van een grotere verwerkingskracht.
Analyse	Het analyseren van reeds verwerkte informatie of data, het leggen van verbanden tussen deze informatie en het voorspellen op basis van deze resultaten.	Middels FB is het mogelijk om van verschillende partijen informatie of intelligence te verwerven, daardoor is het mogelijk een hogere kwaliteit te genereren in de analysefase
Disseminatie & integratie	Het verspreiden van kennis en informatie naar belanghebbenden in de keten van terrorisme- en criminaliteitsbestrijding en, wanneer van toepassing, het integreren in het besluitvormingsproces van organisaties in de keten.	Een federatie maakt het mogelijk kennis, informatie en intelligence op een snelle & gerichte manier te delen tussen belanghebbenden.
Normbeeld maken	Het maken van een normbeeld (wat is de normale situatie) is essentieel om intelligence op de juiste manier te kunnen plaatsen. Dit normbeeld kan bijvoorbeeld worden opgesteld aan de hand van informatie waarbij bekend is dat het gaat om vals-positieven.	Door de combinatie van informatie van diverse sensoren ontstaat een rijker beeld van de omgeving, dit geeft meer mogelijkheden bij het creëren van een normaal beeld.

C.2.2 Coördineren

Sub-capability	Functie / beschrijving	Kansen voor FB
Aansturen	Het aansturen van een organisatie-eenheid of -eenheden. Dit gaat om zowel de aansturing tijdens normale situaties als crisis- of noodsituaties.	Door aan de voorkant duidelijk te hebben wie, welke informatie nodig heeft om de aansturing zo optimaal mogelijk in te richten, kan hier binnen de federatie gericht informatie op worden gedeeld.
Situationeel beeld creëren	Het krijgen van overzicht over een situatie. Het kan daarbij gaan om een situatie voor, tijdens of na een (potentiële) aanval.	Een federatie maakt het mogelijk een situatie vanuit verschillende stakeholders te bekijken en samen te voegen, dit verrijkt het situationele beeld.
Crisismanagement	Het beheersen van een situatie waarvoor de reguliere risicobeheersingsmaatregelen niet toereikend zijn. Deze *capability* staat sterk in verbinding met de overige enabling capabilities; aansturen, het creëren van een situationeel beeld en het maken van afwegingen staan centraal bij het uitvoeren van crisismanagement.	Het is belangrijk als federatie om in de voorbereiding duidelijk te hebben hoe de rollen, taken en verantwoordelijkheden belegd zijn ten tijde van de crisis. Hier kan tevens een koppeling gemaakt worden naar welke partijen over welk type informatie uit de federatie mogen beschikken om hun rol in de crisisbeheersing te ondersteunen.
Afwegingen maken	Het kiezen tussen alternatieven. Bij ontwikkeling van deze *capability* hoort een duidelijk overzicht op basis van welke criteria een keuze moet worden gemaakt tussen deze alternatieven. Het gaat om het maken van afwegingen tijdens een normale, een crisis-of een noodsituatie.	Door in de voorbereidende fase de verschillende alternatieven voor te bereiden, kan ook gekeken worden welke informatie noodzakelijk is om hiertoe een keuze te kunnen maken. Hier kan het intelligenceproces binnen de federatie op worden ingericht.

C.2.3 Communiceren

Sub-capability	Functie / beschrijving	Kansen voor FB
Informatie en Kennis delen	Het delen van informatie en kennis met (keten)partners. Het kan daarbij gaan om nieuwe inzichten in (nieuwe) modi operandi en daarmee (aanvals- en verdedigings-)methoden en middelen, maar ook om informatie over personen, groepen of (potentiële) gebeurtenissen.	Een federatie is bij uitstek een vehicle dat het delen van kennis, informatie en intelligence zal ondersteunen en versterken.

C.3 Voorbereiding

Sub-capability	Functie / beschrijving	Kansen voor FB
Trend- en risicoanalyse	Het analyseren van trends en risico's over dreigingen met als doel om daar een betere inschatting van te kunnen maken.	Het delen van kennis en informatie binnen een federatie geeft een breder inzicht en heeft daarmee de potentie om een completer beeld van de trends en risico's op te stellen.
Risico beheersen	Het vaststellen van risico beheersingsmaatregelen en daarmee (vaak) het opstellen van een beveiligingsplan. Het beheersen van risico's gaat hand in hand met andere *capabilities* zoals trend- en risicoanalyse en risico-identificatie en -evaluatie.	Door gezamenlijk de risico's van het gebied vast te stellen, is het ook mogelijk om de beheersingsmaatregelen beter op elkaar aan te laten sluiten, dit kan verwerkt worden in de diverse separate beveiligingsplannen.
Weerstand en awareness vergroten	Het vergroten van de weerstand van de bevolking of specifieke groepen in de bevolking, maar ook van bedrijven en of (vitale) instellingen. Het kan specifiek gaan om het vergroten van de weerstand of awareness tegen een bepaald type aanval (bijvoorbeeld met CBRN-middelen), maar ook om aanvallen in het algemeen.	Een federatie zal de samenwerking tussen partijen intensiveren, dit geeft mogelijkheden wat betreft het vergroten van de alertheid van de diverse betrokken partijen.
Evalueren	Het evalueren van reeds voorgedane situaties (dreigingen en aanvallen) en de daarbij ingezette werkwijzen ene middelen alsmede het effect daarvan. Bijvoorbeeld om te bepalen wat wel of niet werkte, en wat beter kan. Het gaat daarbij zowel om normale als nood- of crisissituaties.	Informatie vanuit de federatie kan als input dienen bij het evalueren van reeds voorgedane situaties.

D Stellingen bij interview bureau nationale taken politie

Deze bijlage bevat de stellingen die zijn gebruikt het interview met Tamara Jopp (politie, bureau National Taken). Het ruwe uitgebreide verslag van dit gesprek is bij TNO beschikbaar op aanvraag. Dat ruwe verslag is op hoofdlijnen akkoord bevonden door Mevr. Jopp.

Aanwezig bij het interview waren Jordi Nahumury en Jeroen van Rest.

Per stelling is een beknopte conclusie geformuleerd door TNO, op basis van het interview.

Stelling: *Allerlei partijen (bijv. in de OV-sector) hebben een beveiligingsbelang bij de (semi-)openbare ruimte, op basis waarvan zij gebruik willen kunnen maken van de (beveiligings)infrastructuur van zichzelf, en van lokale partners.*
Ja, deze stelling is waar. Er zijn allerlei voorbeelden waarin dit het geval is. Het zou direct indruisen tegen de basis van iedere beveiligingsdoctrine om de omgeving van het te beveiligen object te negeren.

Stelling: *Een beveiligd (authenticatie, autorisatie en encryptie) informatieplatform waarop aangesloten partijen informatie kunnen delen is nuttig en technisch haalbaar.*
Deze stelling is beperkt waar. Ja, het is functioneel gezien nuttig en technisch haalbaar, maar het lijkt geen juridische grondslag te vinden voor beveiligingssituaties om een gemeenschappelijke informatieruimte te maken waar deelnemende partijen relatief vrij informatie in kunnen doen en uit kunnen halen.

Stelling: *Informatie kan direct van de ene objectbeheerder naar de andere gaan, zonder tussenkomst van politie.*
Deze stelling is beperkt waar, het hangt er van af. Voor veiligheidsinformatie levert dit in andere domeinen typisch juridische vragen op, en ook in het veiligheidsdomein. Het lijkt in specifieke gevallen met specifieke argumentatie wel mogelijk te zijn, maar in het algemeen niet. Overigens, het is ook niet zo dat het via de politie wel mag. Als iets eenmaal politiegegevens is, dan gelden er bepalingen waardoor het niet zomaar gedeeld mag worden.

Stelling: *Het is niet nodig om ruwe (sensor)gegevens met partners te delen, om toch samen conclusies uit de combinatie van die gegevens te kunnen trekken.*
Deze stelling lijkt waar. Er zijn bijvoorbeeld diverse samenwerkingsverbanden waarin de ene partij bepaalt welke informatie nuttig is voor de andere partij(en). Echter, daar kan in de praktijk nuttige informatie verloren gaan. Als het ook mogelijk is om dit technisch te ondersteunen waarbij er minder informatie verloren gaat, dan zal het vervolgens ook nodig zijn om dat juridisch goed te onderbouwen en vervolgens te communiceren.

Stelling: *Het kan effectief zijn om profielen te delen om daarmee een informatiebehoefte te onderbouwen.*
Deze stelling lijkt niet voldoende scherp, en lijkt (daarom slechts) ten dele waar. Door met buren te delen welke indicatoren relevant zijn, kan een informatiebehoefte

worden gecommuniceerd, maar niet worden gemotiveerd. Die motivatie is echter niet per se nodig naar de buren, maar naar de wetgever en handhaver van die wet.

Stelling: *Profileren is te standaardiseren.*
Deze stelling lijkt waar. Een verdeling in indicatoren, in gewichten per indicator en in profielen ligt voor de hand. Indien de indicatoren gestandaardiseerd worden, dan kunnen die betekenisvol gedeeld worden met buren. Die buren weten op basis van de standaardisatie welke soorten informatiebronnen nodig zijn om de indicatoren te vullen met sensordata.