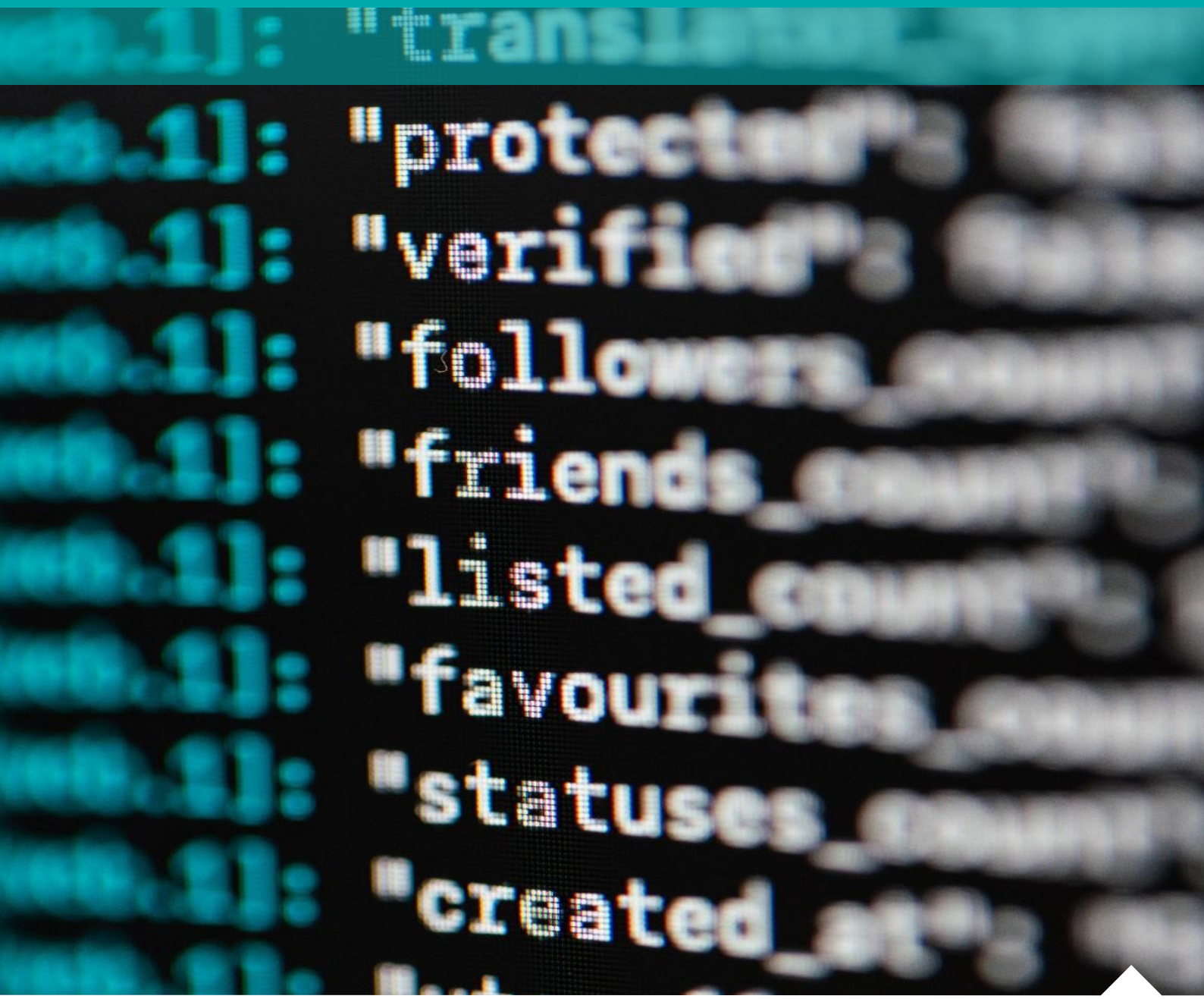
Informatie-uitwisseling tussen de Nationale Politie en particuliere veiligheidsorganisaties

Dr. Joery Matthys, Institute of Security and Global Affairs, Universiteit Leiden
Dr. Michiel de Weger, Century Consulting



Universiteit Leiden
Institute of Security and Global Affairs

COLOFON

Opdrachtgever

Nationale Politie

Staf Korpsleiding, Directie Operatiën, Cluster Onderzoek

Nieuwe Uitleg 1

2514 BP Den Haag

Onderzoekers

Het onderzoek is uitgevoerd door het Institute of Governance and Global Affairs van de Universiteit Leiden, samen met Century Consulting. De onderzoekers zijn Dr. Joery Matthys en Dr. Michiel de Weger.

Begeleidingscommissie Nationale Politie

Dr. Theo Jochoms, Ir. Joyce de Leij en Drs. André van Heel.

doi:10.5281/zenodo.10022917

INHOUDSOPGAVE

1. INLEIDING

1.1 Onderzoeksprobleem en onderzoeksvragen

De idee dat het alleen publieke organisaties zouden zijn die verantwoordelijk zijn voor publieke dienstverlening, werd reeds geruime tijd verlaten. Binnen de bestuurskundige literatuur wordt daarbij gebruik gemaakt van het adagium 'from government to governance'. Wat betreft veiligheidsvoorziening is dit niet anders. De politie is geëvolueerd van de bijna-monopoliehouder in het verstrekken van interne veiligheid naar één van de actoren in een intens veiligheidsveld. Men spreekt dan ook van 'plural policing'[1]. Sommige auteurs zien deze pluralisering als een teken dat hiërarchische relaties tussen veiligheidsactoren verdwijnen, en publieke actoren niet meer betrokken hoeven te worden bij veiligheidsvoorziening. Enkel wanneer zij voldoende meerwaarde leveren, worden ze betrokken. Dit wordt beschreven als 'nodal governance'[2]. Als theoretisch concept heeft dit een zekere aantrekkingskracht: elke veiligheidsactor wordt beoordeeld op de waarde die deze kan leveren, zodat steeds de meest geschikte partners een veiligheidsprobleem aanpakken. In de praktijk is deze setup echter weinig bruikbaar[3], alleen al wegens de geweldsbevoegdheden die uitsluitend aan de politie behoren. In de plaats daarvan kan een 'anchored pluralism' geobserveerd worden[4], waarbij de publieke sector, en met name de politie, een centrale rol blijft spelen in veiligheidsvoorziening, zonder dat de politie daarbij er als enige verantwoordelijk voor is. Een veelheid van andere actoren spelen tevens een rol maar telkens met de politie als een centrale actor.

Deze manier van werken leidt er wel toe dat de politie vaak moet steunen op andere veiligheidsactoren om op te treden, omdat de politie zelf niet meer overal aanwezig kan zijn. Informatiedoorstroming wordt dan van groot belang. Dit onderzoek concentreert zich op informatie-uitwisseling tussen de politie en particuliere veiligheidsactoren, met name particuliere beveiligingsorganisaties en recherchebureaus. Het doel van dit onderzoek is om een aantal projecten te identificeren die bijdragen tot een optimalisering van informatie-uitwisseling. De wettelijke omkadering hiervan wordt in de eerste plaats geregeld door de Wet Politiegegevens (WPG, voor politionele gegevens) en de Algemene Verordening Gegevensbescherming (AVG, voor de gegevens vanuit de particuliere veiligheidsactoren). Ook de Wet Particuliere Beveiligingsorganisaties en Recherchebureaus (WPBR) is van belang. Een wet die van belang kan worden als ze van kracht wordt, is de Wet Gegevensverwerking door Samenwerkingsverbanden (WGS).

We behandelen de volgende onderzoeksvragen:

1. Wat zijn de prioriteiten wat betreft informatie-uitwisseling voor zowel de Nationale Politie als particuliere veiligheidsactoren?
2. Wat zijn de wettelijke mogelijkheden voor het uitwisselen van informatie op basis van deze prioriteiten?
3. Welke concrete projecten worden binnen deze wettelijke contouren als wenselijk geacht door zowel de Nationale Politie als particuliere veiligheidsactoren?

1.2 Context

De relatie tussen de Nationale Politie en met name particuliere beveiligingsorganisaties en recherchebureaus opereert in een vrij specifieke context. Ten eerste is de behoefte aan informatie-uitwisseling niet symmetrisch:[5] de Nationale Politie heeft een algemene veiligheidsfunctie, en is steeds op zoek naar een verbetering van haar informatiepositie, om zo het publiek belang beter te dienen. Particuliere beveiligingsorganisaties en recherchebureaus hebben strikt gezien geen informatie van de politie nodig. Zij kunnen hun klanten bedienen en winst maken zonder deze informatie, hoewel ze dit wel beter kunnen doen indien zij deze informatie ter beschikking hebben, wat dan weer een netto positief resultaat geeft voor de samenleving. Ten tweede is er geen meldingsplicht voor de particuliere beveiligingsorganisatie of het recherchebureau om informatie uit te wisselen met de politie, in tegenstelling tot bijvoorbeeld de poortwachterfunctie van een notaris of een bank om verdachte geldstromen te melden. Andersom heeft de politie ook geen plicht om informatie te verstrekken aan deze particuliere actoren. Tenslotte is de informatie verzameld door de particuliere veiligheidsactor niet noodzakelijk ook eigendom van deze actor: het behoort vaak toe aan het individu of de organisatie die de particuliere veiligheidsactor heeft ingehuurd. Dat creëert een juridische problematiek wat er precies wel of niet kan gedeeld worden door de particuliere veiligheidsactor. Dat leidt dan weer tot terughoudendheid om informatie te delen.

1 Loader (2000).
2 Shearing (2005).
3 Boutellier & Van Steden (2011).
4 Loader & Walker (2006).
5 Hoogenboom (2004).

1.3 Relevantie

Dit project sluit aan bij de observatie binnen wetenschappelijk onderzoek dat informatie-uitwisseling tussen veiligheidsactoren weliswaar een sleutelwoord is binnen maatschappelijke veiligheidsvoorziening, maar dat zowel publieke als private actoren nog steeds sterk uitgaan van de traditionele scheiding tussen publiek en privaat in hun werking en hun interacties met elkaar.[6] Er is mede derhalve een institutionele drempel om effectief de stap te zetten tot informatie-uitwisseling. Dit project neemt aan dat dit voortkomt uit onbekendheid wat men precies aan elkaar kan bieden, onzekerheid over de haalbaarheid van uitwisseling en onzekerheid over de mate waarin informatie-uitwisseling ook past binnen het bestaande (wettelijke) kader van de publiek-private taakverdeling. Het is niet zo dat er een gebrek is aan onderzoek over publiek-private samenwerking in het algemeen of zelfs de noodzaak aan goede informatie-uitwisseling in het bijzonder. Maar het onderzoek dat initieel tijdens dit project naar boven kwam, bleef qua conclusies zeer sterk op het algemene en conceptuele niveau gericht, voornamelijk door er op te wijzen dat er kansen en risico's verbonden waren aan informatie-uitwisseling, en algemene aanbevelingen. Zie hiervoor hoofdstuk 4.1.

Door op zoek te gaan naar specifieke projecten in een Nederlands kader die door zowel de Nationale Politie als particuliere veiligheidsactoren als effectief, haalbaar en wenselijk geschikt worden gezien, kunnen deze drempels overwonnen worden en gaat dit onderzoek een niveau dieper. Ander onderzoek kan hier dan op voortbouwen om te analyseren of deze prioritering specifiek is aan de deelnemers in dit onderzoek en de Nederlandse context, of ook breder generaliseerbaar is. Het doel van het project is niet om uitputtend alle mogelijkheden voor informatie-uitwisseling te benoemen, maar door middel van een bevraging een aantal projecten te selecteren, om dan met een bijkomende analyse de meest geschikte projecten te selecteren en verder uit te werken. Ondanks het beperkte aantal deelnemers aan dit onderzoek bieden de uitkomsten een redelijk unieke, gedetailleerde kijk in de mogelijkheden voor en overwegingen bij (nieuwe) informatie-uitwisselingsvormen tussen de twee meest omvangrijke binnenlandse veiligheidsactoren die Nederland nu rijk is.

6 Nokleberg (2020).

2. THEORETISCH RAAMWERK

2.1 Politie en particuliere veiligheidsactoren

Het construeren van een goede definitie van de politie is niet eenvoudig. In de Angelsaksische literatuur wordt vaak een onderscheid gemaakt tussen "the police" langs de ene kant en "policing" langs de andere kant, wat vertaald zou kunnen worden als "de politie" en de "politiefunctie". Wanneer over de politie gesproken wordt, heeft men het over specifieke organisaties die een bepaalde mate van legitimiteit hebben, die een vastomlijnde structuur hebben, en die welbepaalde (veiligheids)taken uitvoeren.[7] Uit de legitimiteit komt een al dan niet gedeeld monopolie voort om bepaalde taken uit te voeren in naam van "de maatschappij". De politie moet ook over een professionele organisatie beschikken, die de mogelijkheid heeft om geweld te gebruiken (dit is wat er bedoeld wordt met "structuur" in de definitie hierboven). De uit te voeren taken vormen dan weer de link naar het "policing" aspect, de politiefunctie: de organisatie houdt zich bezig met ordehandhaving, criminaliteitsbestrijding[8] en hulpverlening. Dit is een eerste indeling van wat de politiefunctie behelst, meer differentiëring is ook mogelijk. Ordehandhaving kan bijvoorbeeld uitgesplitst worden in handhaving, noodhulp (inclusief een zorgfunctie als eerste hulpverlener) en signalerings- en adviesverlening, terwijl criminaliteitsbestrijding zowel signalering als opsporing omvat.[9] Door het uitvoeren van deze taken, is er tevens een afschrikkend effect: door de aanwezigheid van actoren die deze functies opnemen, verhoogt ook de veiligheid.[10]

Opvallend aan deze definitie van "de politie" is dat verschillende publieke organisaties onder deze definitie kunnen geplaatst worden, zolang ze over een bepaalde mate van legitimiteit beschikken, een vaste structuur hebben en bepaalde taken uitvoeren. Inlichtingendiensten en bijzondere opsporingsdiensten voldoen bijvoorbeeld ook aan deze voorwaarden.[11] Zelfs particuliere veiligheidsactoren worden niet uitgesloten.

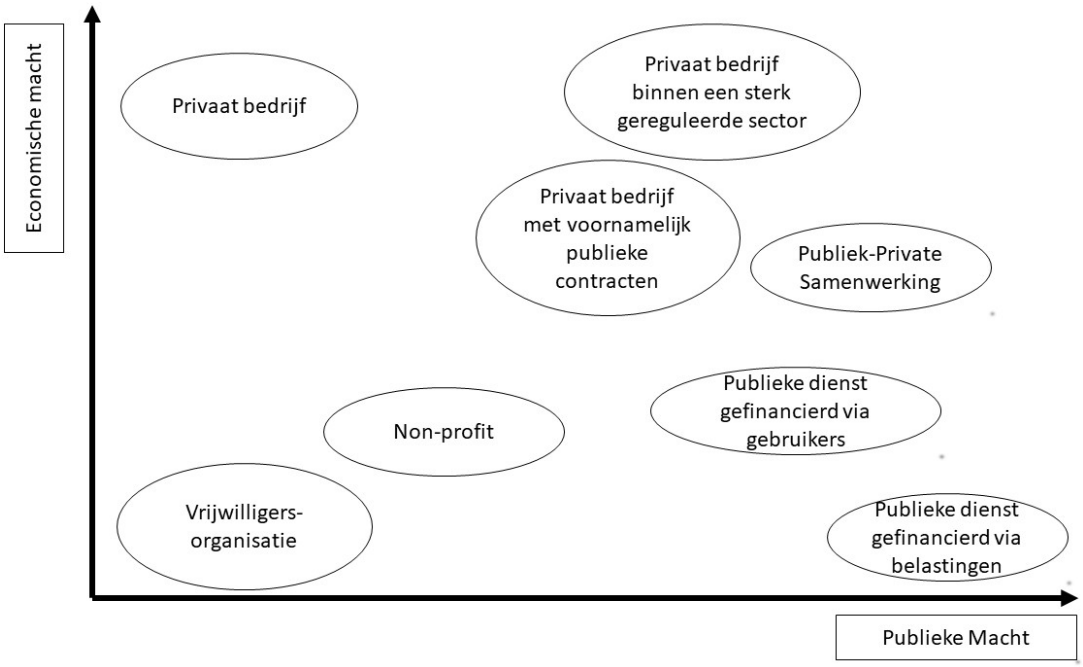
In het kader van dit onderzoek moet er echter wel een duidelijk onderscheid gemaakt worden tussen publieke en private actoren, tussen de politie en andere publieke veiligheidsactoren, en tussen particuliere veiligheidsactoren onderling.

2.1.1 Publieke en private actoren

In academische literatuur is er sprake van twee stromingen wanneer het gaat over de publieke en de private sector. Eén stroom ziet deze als functioneel identiek: bevindingen uit de private sector, zowel wat betreft algemeen management als HR, kunnen ook toegepast worden op organisaties binnen de publieke sector.[12] Andere auteurs wijzen op verschillen in een aantal essentiële gebieden. Publieke organisaties moeten hun goederen of diensten steeds kunnen leveren, en zijn dus minder onderhevig aan de vragen van de markt.[13] Vaak wordt ook gewezen op een intrinsieke motivatie van mensen die in de publieke sector werken, in tegenstelling tot de private werknemer die meer extern gemotiveerd zou zijn[14] (hoewel dit in de literatuur soms ook betwist wordt, en meer nadruk plaatsen op het overeenkomen van de waarden van de organisatie en de werknemer[15]). Daarenboven is er in de publieke sector een grotere vraag naar transparantie, zowel wat betreft financiën als wat betreft handelingsperspectieven.[16] En wanneer publieke en private actoren samenwerken, komt de verantwoordelijkheid naar de burger toe steeds bij de publieke partij te liggen, zelfs indien de private partij feitelijk verantwoordelijk zou zijn voor een onbevredigend resultaat.[17]

Hoewel er verschillen bestaan tussen publieke en private actoren, blijkt het in de praktijk niet steeds eenvoudig om een goed onderscheid te maken. Zo verwijst men vaak naar de functie van een organisatie, zoals veiligheidsvoorziening, maar publieke en private actoren voeren vaak vergelijkbare functies uit.[18]

7 Mawby (1990).
8 Mawby (2008).
9 Van Lakerveld et al. (2018).
10 Matthys (2009).
11 Cachet (1990).
12 Een voorbeeld hiervan is te vinden bij Mintzberg (1979), maar gaat zelfs terug tot Taylor (1911).
13 Anomaly (2015).
14 Perry & Hondeghem (2008).
15 Vandenabeele & Schott (2020).
16 Christensen et al. (2007).
17 Christensen et al. (2007).
18 Lienert (2009).



Figuur 1: economische macht - publieke macht matrix met voorbeelden.[19]

Eigenaarschap wordt ook naar voor geschoven, waarbij publieke organisaties eigendom zijn van de overheid. Ook hier kunnen organisaties in private eigendom toch als publiek gezien worden, zoals in het verleden de elektriciteitsbedrijven voor de liberalisering. Een andere mogelijkheid is controle, maar een minderheidscontrole vanwege de overheid kan toch grote gevolgen hebben voor een privaat bedrijf, waardoor de "publiekheid" van de organisatie toch groter wordt.[20] Tenslotte kan als enkelvoudige parameter ook de wet gebruikt worden, maar in verschillende landen kunnen publieke organisaties ook een privaatrechtelijke basis hebben.[21]

Bozeman stelt zelfs dat alle organisaties binnen de maatschappij tot op zekere hoogte publieke elementen bevatten.[22] Een overheid kan mogelijk een meerderheids- of minderheidsaandeel hebben. Door regulering kunnen organisaties verplicht worden om de overheid in bepaalde taken te ondersteunen, denk aan bijvoorbeeld bescherming van privacy door bedrijven die klantgegevens bewaren. Of ze kunnen verplicht worden om gegevens te delen met de overheid, zoals het geval is bij banken. Hij schuift dan ook de mogelijkheid naar voren om organisaties vanuit een matrix te bekijken, met als elementen economische macht en publieke autoriteit. Hoe meer economische macht een organisatie heeft, hoe meer het controle heeft over de eigen financiële bronnen. Hoe hoger de publieke autoriteit die wordt uitgeoefend op een organisatie, hoe meer de beslissingen van deze organisatie beïnvloed wordt door publieke/politieke actoren. Een organisatie die niet interageert met de overheid (dus ook geen contracten heeft met publieke actoren), waar weinig regulering voor bestaat, en die volledig op de markt gericht is, kan als volledig privaat gezien worden, terwijl publieke diensten gefinancierd door belastinggeld als volledig publiek zouden kunnen gezien worden. Alle andere organisaties vallen daar tussen.

Wanneer we de matrix van Bozeman gaan toepassen op de politie en particuliere veiligheidsactoren, kunnen we observeren dat er op deze laatste in grote mate regulering van toepassing is, waardoor ze dus over een zekere "publiekheid" beschikken. Meer interactie met publieke actoren en meer (niet-commerciële) informatie-uitwisseling zal deze "publiekheid" nog verder vergroten, omdat de relatie met de publieke sector versterkt wordt. Hetzelfde geldt echter niet voor de publieke veiligheidsactoren: hun economische macht wordt niet groter door interactie en informatie-uitwisseling met de private sector, en zij worden niet minder beïnvloed door publieke/politieke actoren.

19 Bozeman (1987).
20 Lienert (2009).
21 Lienert (2009).
22 Bozeman (1987).

2.1.2 Politie en andere publieke veiligheidsactoren

Wat betreft de publieke sector, onderscheidt de politie zich van andere veiligheidsactoren door vanuit een intern veiligheidsperspectief alle taken op zich te nemen: ordehandhaving, criminaliteitsbestrijding en hulpverlening. Hoewel de politiefunctie uitgeoefend wordt door een veelheid van actoren,[23] is de politie dus actief op alle vlakken van de politiefunctie, in tegenstelling tot enige andere veiligheidsactor. Bijzondere opsporingsdiensten vervullen bijvoorbeeld slechts een deel van de taken binnen de politiefunctie, gericht op specifieke sectoren (in casu criminaliteitsbestrijding). De Koninklijke Marechaussee vervult wel alle taken binnen de politiefunctie, maar enkel wat betreft Defensieonderdelen (en tot op zekere hoogte de luchthavens), en wordt daarom ook wel militaire politie genoemd (art. 4 Politiewet). Zij heeft daarnaast nog een aantal andere werkzaamheden, opgesomd in art. 4 Politiewet, maar daarbij vervult zij opnieuw niet alle taken van de politiefunctie. We denken daarbij bijvoorbeeld aan grensbeveiliging, waar opnieuw criminaliteitsbestrijding voorop staat. In Nederland zouden wellicht buitengewoon opsporingsambtenaren, wegens de uitbreiding van hun taken en bevoegdheden, nog als "politie" bestempeld kunnen worden, en in het verleden werd reeds in vraag gesteld of er al dan niet gesproken kan worden over een nieuwe vorm van gemeentepolitie.[24] Het valt echter buiten de scope van dit project om hier verder op in te gaan.

2.1.3 Particuliere veiligheidsactoren en andere private veiligheidsactoren

Wat betreft private veiligheidsactoren, maken we een onderscheid tussen private actoren die rond veiligheid werken vanuit een primair proces en vanuit een secundair proces.[25] Een primair proces draait rond de kernactiviteit van een organisatie, terwijl een secundair proces rechtstreeks ondersteuning biedt aan het uitvoeren van het primair proces. Wanneer een private actor als commerciële activiteit handhaving of recherche heeft, dan beschouwen we dit als een particuliere veiligheidsactor in het kader van dit onderzoek (e.g. particulier beveiligingsbedrijf dat ingehuurd wordt om een industrieterrein te bewaken). Wanneer een private actor wel activiteiten uitoefent die te maken hebben met veiligheidsvoorziening, maar deze activiteiten ondersteunend zijn aan de hoofdfunctie en dus secundair (e.g. een webshop die ook data moet beschermen van klanten), blijven zij buiten de scope van dit onderzoek.

2.2 Van government naar governance: een geankerd pluralisme voor veiligheidsvoorziening

2.2.1 Netwerken en informatiegestuurde politie

Het is belangrijk om het onderscheid publiek-privaat duidelijk aan te houden, juist omdat ontwikkelingen binnen het veiligheidsveld het beeld steeds diffuser maken, met complexe mengvormen tussen publieke veiligheid en private veiligheid.[26] Het beeld ontstaat dat de politie niet meer wordt dan een willekeurige actor onder vele verschillende veiligheidsactoren, een knoop in een complex netwerk zonder een specifieke eigenheid,[27] en zich daardoor ook meer terugtrekt uit taken die ook door andere actoren kunnen worden uitgeoefend. Dat staat echter haaks op de realiteit, waar de politie nog steeds gezien wordt als een belangrijke institutionele actor binnen de rechtsstaat, en een ankerfunctie heeft voor allerlei initiatieven en actoren rond veiligheid.[28] Eerder dan zich echt terug te trekken, lijkt de aandacht te liggen op het verbreden van de eigen activiteiten op meer indirecte manieren, vaak aangeduid als "steering not rowing".[29]

Het verbinding zoeken met andere actoren binnen het veiligheidsnetwerk en het aansturen van deze actoren ligt in lijn met het verbreden van de eigen activiteiten op een indirecte manier, gezien andere actoren aangespoord worden om ook verantwoordelijkheden op te nemen rond veiligheidsvoorziening, zonder dat daarbij de link met de politie verloren gaat.[30] Ook de principes van de gemeenschapsgerichte politiezorg, een politiemodel dat wereldwijd gehanteerd wordt en in Nederland vertaald werd naar het concept 'gebiedsgebonden politie' gaan uit van het leggen van een bepaalde verantwoordelijkheid voor ordehandhaving bij de maatschappij, in de vorm van burgers, welzijnswerkers, woningcorporaties, en andere private actoren.[31] Bij criminaliteitsbestrijding zien we dat er in de literatuur rond politiestudies de nadruk gelegd wordt op een informatiegestuurde politie: op basis van strategische en tactische trendanalyses kunnen profielen wor-

23 Van den Berg et al. (2012).
24 Eikenaar & Van Stokkom (2014).
25 Huckvale & Ould (1995).
26 Terpstra (2008a).
27 Johnston & (2003).
28 Loader & Walker (2006) en Boutellier & Van Steden (2011).
29 Barlow & Röber (1996).
30 Devroe (2015).
31 Terpstra (2008b).

den opgesteld die het mogelijk maken om hotspots en wellicht zelfs daders te identificeren.[32] Om deze analyses mogelijk te maken, is het noodzakelijk om zo veel mogelijk gegevens te ontsluiten.

Het ontwikkelen van een netwerkstructuur rond ordehandhaving betekent dus dat er meer interactie zou komen tussen publieke en private veiligheidsactoren, terwijl de nadruk op informatiegestuurde politie bij criminaliteitsbestrijding betekent dat er vanuit diverse bronnen informatie moet binnengebracht worden. Wat beide dus met elkaar gemeen hebben, is de wenselijkheid van informatie-uitwisseling tussen politie en andere veiligheidsactoren. Op zich is vooral de informatie die stroomt van de andere actoren naar de politie toe belangrijk, maar om die informatiestroom te optimaliseren, is het soms nodig om ook informatie de andere richting te laten stromen: de andere actoren moeten een duidelijke reden hebben waarom zij zich zouden committeren aan deze interactie. Indien de politie vooral aandacht geeft aan het 'nemen' aspect, verkleint dit uiteindelijk de feitelijke hoeveelheid informatie-uitwisseling.[33]

Tegelijkertijd wordt er voorbijgegaan aan de complexiteit van de problematiek indien er simpelweg gesteld wordt dat de oplossing ligt bij de wil die de politie moet hebben om tot informatie-uitwisseling over te gaan. Verschillende veiligheidsactoren hebben mogelijk een andere organisatiecultuur, hebben verschillende doelen en prioriteiten die hun wil om informatie uit te wisselen beïnvloeden, en heel belangrijk vaak ook verschillende juridische kaders die hun handelingen beperken. In voorgaand onderzoek[34] is al duidelijk geworden dat er reeds initiatieven zijn geweest in het verleden, met enthousiasme vanuit zowel de politie als andere actoren, om tot informatie-uitwisseling te komen, maar dat al vrij snel in het proces allerhande juridische vragen naar boven kwamen over de mogelijkheden tot dit soort uitwisseling, waarna het enthousiasme afkoelde. Een concreet voorbeeld is de pilot in samenwerking tussen particuliere onderzoeksbureaus met politie en Openbaar Ministerie.[35] De kwaliteit van het werk van de particuliere onderzoeksbureaus werd in de pilot als hoog beoordeeld, maar de evaluatie indiceerde dat er nauwelijks terugkoppeling was over de afhandeling van de zaken, dit (volgens de politie) wegens de beperkingen opgelegd door wet- en regelgeving, en dat er onduidelijkheid was over de doelen van de pilot. Het resultaat was dat ondanks de tevredenheid over initiële resultaten en de kwaliteit van de afhandeling, de pilot niet voortgezet werd.

2.2.2 Informatieverkrijging, -uitwisseling en -deling

Voordat er ingegaan wordt op het type van informatie dat uitgewisseld kan worden, moet eerst worden stilgestaan bij de term "uitwisseling". In de meest enge zin van het woord, is er enkel sprake van uitwisseling wanneer ten minste twee partijen informatie delen met elkaar.[36] In deze studie wordt echter de bredere definitie gebruikt die minder onderscheid maakt tussen uitwisselen (wederzijds) en informatiedeling (wat slechts van één kant komt).[37] Dat een van de partijen de ander informatie levert kan immers ook nuttig zijn, zonder dat er wederkerigheid is Naast deze twee vormen van uitwisseling kan er ook gesproken worden over samenwerking rond informatie, waarbij verschillende partijen vooraf met elkaar identificeren welke informatie, waarover geen van beiden beschikt, nodig is en er samengewerkt wordt om deze informatie te verzamelen.[38]

In dit onderzoek wordt er daarbij ook uitgegaan van twee typen informatie-uitwisseling tussen actoren: gegevens en kennis. Over het precieze onderscheid tussen de twee lijkt er in de literatuur weinig overeenstemming, maar in het algemeen kan gesteld worden dat gegevens meer ruwe data bevatten, terwijl bij kennisuitwisseling expertise werd toegevoegd aan de ruwe data, waardoor de waarde van de initiële gegevens verhoogd werd.[39] Ook hier is er geen eenvoudig dichotoom onderscheid te maken. Wanneer een private actor camerabeelden doorstuurt naar de politie, is er duidelijk sprake van gegevensuitwisseling. Wanneer de private actor met de politie ziet welke trends en evoluties zij zien in de nabije toekomst, is er duidelijk sprake van kennisuitwisseling. Maar wanneer een privaat onderzoeksbureau een aantal observaties maakt en deze bundelt in een rapport waarin op basis van de observaties een aantal conclusies getrokken worden, is te beargumenteren dat dit zowel onder gegevensuitwisseling kan vallen als onder kennisuitwisseling. Er moet daarom benadrukt worden dat het vanuit praktisch standpunt wellicht minder interessant is om een harde opdeling te maken tussen de twee. In de projecten die later opgesomd worden binnen dit onderzoek, komen zowel ideeën over gegevensuitwisseling

32 Tilley (2008).
33 Groenendaal & Helsloot (2014).
34 Staats et al. (2021).
35 Friperson et al. (2013) en Kuin & Wilms (2015).
36 Wang & Noe (2010).
37 Cabrera et al. (2006).
38 Talja & Hansen (2006).
39 Bartol & Srivastava (2002).

als over kennisuitwisseling naar boven, beide worden dus als waardevol ervaren.

2.3 Parameters voor informatie-uitwisseling

Wat zijn dan geschikte parameters om te oordelen over het al dan niet uitwisselen van informatie tussen politie en particuliere veiligheidsactoren? In de bestuurskunde wordt uitgegaan van drie brede maatstaven/waarden waar overheidshandelen aan kan worden getoetst.[40] In dit onderzoek gebruiken we dezelfde maatstaven binnen het beslissingskader om al dan niet tot dit handelen over te gaan:

- Sigma-waarden: hier draait het voornamelijk om efficiëntie en effectiviteit. Zorgt de informatie-uitwisseling ervoor dat de verschillende actoren beter presteren, dat ze de activiteiten die ze willen uitvoeren met zo weinig mogelijk middelen ook bewerkstelligen (of meer activiteiten uitvoeren met dezelfde middelen)? Hier gaat het om de kortetermijndoelen van de actoren, de *output* die ze creëren. Maar vraag is ook of het lange termijn doel bereikt van de informatie-uitwisseling wordt, namelijk dat de maatschappelijke veiligheid verhoogd wordt, de bedoelde *outcome* van het overheidshandelen.[41]

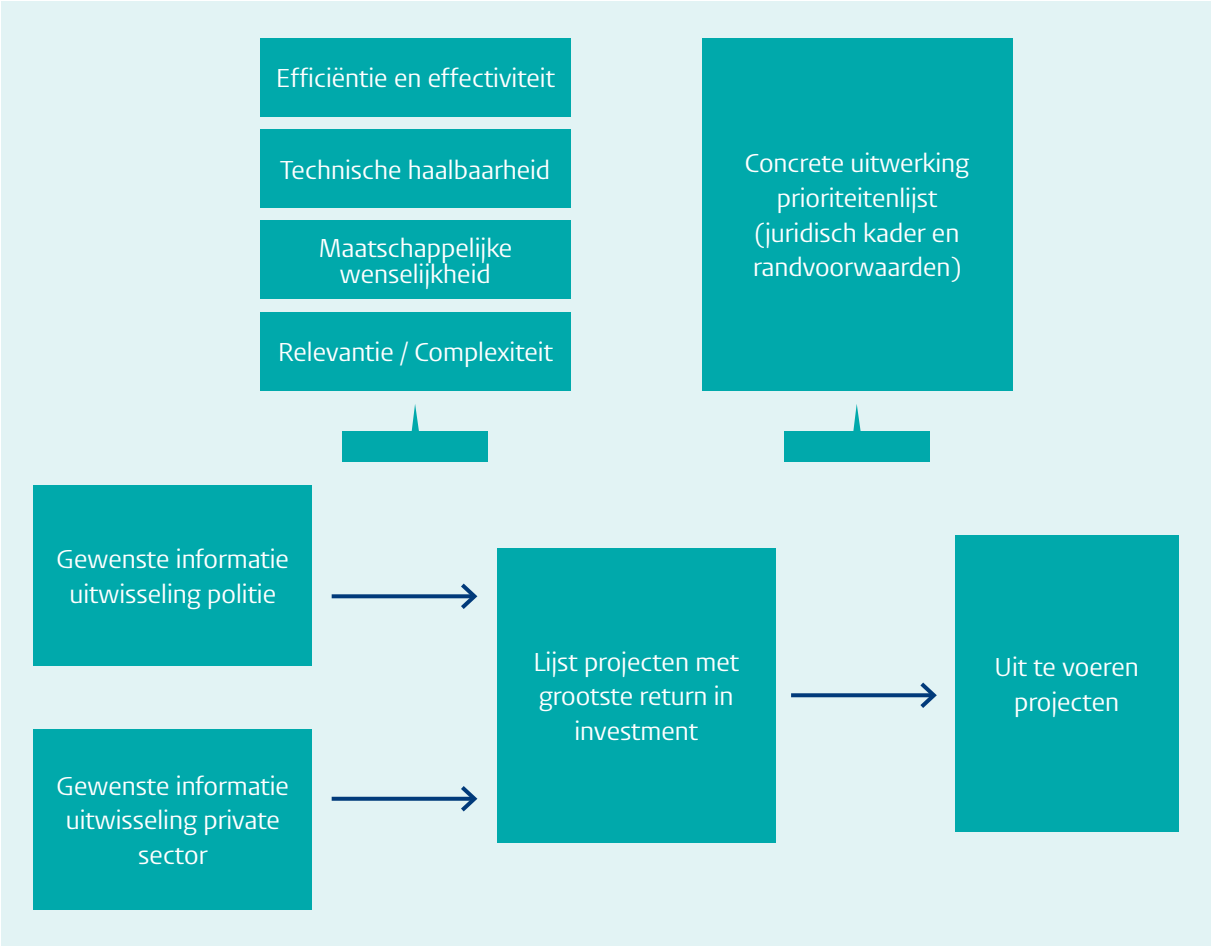
- Lambda-waarden: deze maatstaf legt de nadruk op veerkracht en robuustheid, wat in dit onderzoek vertaald wordt naar de (technische) haalbaarheid om informatie-uitwisseling op te zetten en ook voor een langere periode aan te houden. De haalbaarheid van een project wordt hoger naarmate het aantal veto-punten daalt. Veto-punten zijn momenten in het beslissingsproces waar het mogelijk is dat de beslissing wordt gemaakt om niet verder te gaan met een lopend proces.[42] Het aantal stappen binnen een beslissingsproces en het aantal actoren die deelnemen aan de uitvoering ervan, zijn daarbij bepalende factoren. Als daarenboven ook een extern beslissingsproces moet toegevoegd worden, zoals bijvoorbeeld een wetswijziging, dan verlaagt dit de kans dat het systeem kan worden opgezet of volgehouden.

- Theta-waarden: deze maatstaf draait om rechtvaardigheid. Dit is een moeilijk te definiëren concept, omdat het op verschillende manieren geïnterpreteerd kan worden. Een vrij eenvoudige versie van rechtvaardigheid legt een directe link met de wet en het wetgevend stelsel. Indien een handeling wettelijk is, is ze gerechtvaardigd, en indien overheidsoptreden of nieuwe wetten passen binnen het bestaande wettelijk stelsel, kunnen ze gezien worden als moreel.[43] Een andere interpretatie van rechtvaardig handelen is meer utilitair van aard. Handelen brengt zowel positieve als negatieve gevolgen met zich mee. Handelingen zijn dan moreel rechtvaardig indien de positieve gevolgen van de handeling groter zijn dan de negatieve gevolgen.[44] Tenslotte kan ethiek ook gezien worden vanuit het standpunt van de bescherming van een aantal waarden of deugden, dus vanuit maatschappelijke wenselijkheid. Indien met deze waarden rekening gehouden wordt, kan de handeling als rechtvaardig worden gezien.[45] Elk van deze interpretaties is mogelijk waardevol voor dit onderzoek. Zeker wat betreft beleid, heeft utilitaire rechtvaardigheid een zekere aantrekkingskracht: beleid moet meer voordelen dan nadelen met zich meebrengen. Echter, in het kader van dit onderzoek gebruiken we de maatschappelijke wenselijkheid als uitgangspunt. Dit geeft aan dat beleidsmakers breder moeten nadenken over welk beleid te voeren, niet alleen in termen van voordelen en nadelen, maar ook in termen van de bescherming van fundamentele waarden, in het kader van dit onderzoek specifiek het recht op privacy. Bovendien wordt utilitaire rechtvaardigheid al deels gecapteerd door de Sigma-waarden: het efficiënt en effectief behalen van de doelen.

40 Hood (1991).
41 Van der Knaap et al. (2020).
42 Immergut (1990).
43 Raz (1979).
44 Mulgan (2007).
45 Rachels & Rachels (2012).

3. METHODOLOGIE

3.1 Research design



Figuur 2: onderzoeksdesign project.

Om de verschillende onderzoeksvragen te kunnen beantwoorden, werd het project opgedeeld in drie fasen. In een eerste fase werd kort ingegaan op academische literatuur rond het onderwerp, op beleidsstukken en professionele literatuur. Tevens werd aandacht besteed aan Nederlandse casuïstiek van vorige samenwerkingen, waaruit mogelijke succesfactoren en randvoorwaarden kunnen blijken. Dit werd gevolgd door een aantal interviews met sleutelpersonen binnen de Nationale Politie en particuliere veiligheidsactoren om tot een preliminaire lijst te komen van gewenste projecten rond informatie-uitwisseling. De interviews vormden de basis voor deze preliminaire lijst, de (vak)literatuur en beleidsstukken vormden input voor de interviewvragen. Deze eerste fase was derhalve inventariserend en exploratief van aard. Een deel van de waarde van deze studie is dan ook dat een groot aantal suggesties voor meer informatie-uitwisseling wordt verzameld - die eveneens door politie en particuliere veiligheidsorganisaties verder zouden kunnen worden uitgewerkt en mogelijk ingevoerd, buiten dit onderzoek om.

In een tweede fase werd de lijst van gewenste projecten verder gerangschikt op basis van de onafhankelijke variabelen efficiëntie en effectiviteit (Sigma-waarden), haalbaarheid (Lambda-waarden), maatschappelijke wenselijkheid (Theta-waarden) en als losstaande factor complexiteit/relevantie voor het onderzoek (zie uitleg fase 2). Dit gebeurde door vragenlijsten te sturen naar experts door middel van een (gedeeltelijke) toepassing van een Delphi-methodiek[46], om zo tot een beperkte lijst van top-prioriteiten te komen. De top-prioriteiten werden dus gekozen op basis van een afweging van de onafhankelijke variabelen, waarbij elke variabele als evenwaardig beschouwd werd (zelfde weging). We vertaalden dit naar de afhankelijke variabele, die we identificeerden als de "uit te voeren projecten".

46 Linstone & Turoff (1975).

In de laatste fase werd een seminar georganiseerd waar de top-prioriteiten gepresenteerd werden aan zowel de Nationale Politie als particuliere veiligheidsactoren, en waar de onderzoekers preliminaire opties schetsten hoe deze samenwerking te concretiseren. Van daaruit werden verschillende randvoorwaarden uitgewerkt.

3.2 Datavergaring en -analyse per fase

3.2.1 Fase 1: Literatuurscan, interviews en opmaak prioriteiten

De literatuurscan bestond uit zowel academische als professionele literatuur, inclusief documenten van betrokken organisaties, over het onderwerp informatie-uitwisseling. Er werd gebruik gemaakt van de Mediatheek van de Politieacademie, de bibliotheek van de Universiteit Leiden en van Google Scholar. Gezocht werd op de volgende *keywords*: *information exchange* & *police*, informatie-uitwisseling & politie, politie & publiek-private samenwerking, *police* & *public private partnership*. Daarnaast werd geput uit de kennis van de literatuur van beide onderzoekers, en werd het netwerk van beide onderzoekers ingeschakeld om nog meer relevante literatuur te vinden. De zoekresultaten uit de zoekmachines werden doorgelicht wat betreft relevantie.

Tijdens het verzamelen van literatuur werd tevens een aanvang genomen met het afnemen van interviews bij verschillende sleutelpersonen binnen de private commerciële veiligheidssector en de Nationale Politie. Er werd gebruik gemaakt van semi-gestructureerde interviews, waarbij de volgende vragen leidend waren voor het gesprek:

- Welke mogelijkheden tot al dan niet geautomatiseerde informatie-uitwisseling ziet u tussen de politie en private commerciële veiligheidsactoren?
- Met welke initiatieven in het verleden bent u bekend wat betreft informatie-uitwisseling?
- Hebt u kennis van documenten vanuit uw organisatie, of documenten vanuit organisaties bij u bekend, die een positie innemen over informatie-uitwisseling? Indien ja, is het mogelijk om toegang te verkrijgen tot deze documenten?

De informatie verkregen uit de literatuurscan werd gebruikt om follow-up vragen te stellen, en om de geïnterviewden uit te dagen verder na te denken over mogelijkheden tot informatie-uitwisseling, wat vertaald werd in projecten. Deze werden toegevoegd aan hoofdstuk 3.3. Indien een project door verschillende geïnterviewden werd aangehaald, werd dit aangegeven in voetnoten in het betreffende hoofdstuk. In deze fase werd nog geen prioriteitenlijst opgesteld, maar alle ideeën werden onder elkaar weergegeven. Wel werd een eerste schifting gemaakt door de onderzoekers zelf: er werden geen projecten opgenomen die een uitbesteding betekenen van taken van de politie aan particuliere veiligheidsactoren. Wanneer bijvoorbeeld voorgesteld zou worden dat informatie die nu door de politie verzameld wordt, zou overgenomen worden door een particuliere veiligheidsactor,werd dit niet opgenomen, omdat het de bedoeling is dat de politie de eigen informatiepositie verbetert.

3.2.2 Fase 2: Analyse prioriteiten

Na het afronden van de eerste fase werden de verschillende mogelijkheden genoemd in de interviews onder elkaar gezet, en werden een aantal categorieën gebruikt om een prioriteitenlijst te creëren. Er werd daarbij gedeeltelijk gebruik gemaakt van een Delphi-methode. Deze methode is erop gericht om experts een complexe problematiek voor te leggen om tot een consensus te komen, zonder dat daarbij een groepsdynamiek begint te spelen die onafhankelijk oordeel zou kunnen beletten. Experts werden eerst gevraagd over hun inzichten in het onderwerp, wat hier is gebeurd door middel van interviews in fase 1 van dit onderzoek. Deze interviews werden op semi-gestructureerde wijze gehouden. Zie voor een overzicht van de vragen ANNEX I. In totaal werden 11 sleutelpersonen bevraagd, voor de lijst zie ANNEX II. Bij een Delphi-methode wordt vervolgens gebruik gemaakt van een vragenlijst die opgesteld wordt op basis van de inzichten die in de interviews verkregen werden, wat binnen dit onderzoek in fase 2 gebeurd is. De groep van sleutelpersonen werd hier wel uitgebreid: er werden een aantal extra personen aangeschreven, en aan de sleutelpersonen werd gevraagd om de vragenlijst nog naar één andere persoon door te sturen. In principe wordt bij een Delphi-methode de stap met de vragenlijst dan nog twee keer herhaald om de resultaten te verfijnen, maar deze herhaling werd in dit onderzoek niet gebruikt. In de plaats daarvan gingen de onderzoekers aan de slag met de resultaten van de vragenlijst, en werd de analyse van deze resultaten dan voorgelegd aan de sleutelpersonen in een seminar, zie hierna fase 3. Deze werkwijze werd gekozen om een belangrijke potentiële tekortkoming van de Delphi-methode te voorkomen. In deze methode is de rol van de onderzoekers zelf en hun analyse/moderatie van de resultaten vrij groot, waardoor er minder ruimte is voor perspectieven van anderen. Door de top-prioriteiten toch opnieuw voor te leggen aan sleutelpersonen, werden deze andere visies wel meegenomen in het eindresultaat.

Voor de vragenlijst werd gebruik gemaakt van de drie waarden/maatstaven zoals beschreven in het theoretisch kader: efficiëntie/effectiviteit, haalbaarheid en maatschappelijke relevantie. Deze werden op gelijke hoogte geplaatst met elkaar, dus zonder weging. Dit werd bewust gedaan, omdat weging een politieke keuze is, geen academische. We voegden tevens een vierde categorie toe, namelijk complexiteit/relevantie voor het onderzoek. Hoe meer wijzigingen nodig zijn aan de interne organisatie van een actor of hoe meer externe randvoorwaarden vervuld zijn,[47] hoe interessanter het is om in het kader van dit onderzoek het project uit te diepen. Deze categorie laat dus toe om laaghangend fruit wel op te nemen in de preliminaire lijst van projecten, maar de lijst met top-prioriteiten te beperken met projecten die niet eenvoudig door de politie zelf kunnen geïmplementeerd worden zonder dat daarvoor verdere uitwerking nodig is.

- **Efficiëntie en effectiviteit (Sigma-waarden)**: in hoeverre wordt de mogelijkheid tot informatie-uitwisseling als voordelig gezien door de betrokken actoren? Met andere woorden, in hoeverre zien zij de uitwerking van de informatie-uitwisseling als congruent met hun doelen en de doelen van de maatschappij? De wenselijkheid kan verder uitgesplitst worden tussen:
  - Output: in hoeverre brengt het iets op voor de betrokken partijen? Hoe hoger de score, hoe meer het waarde heeft voor de partijen zelf.
  - Outcome: wat is de inschatting van de toegevoegde waarde voor de maatschappelijke veiligheid?
- **Haalbaarheid (Lambda-waarden)**: in hoeverre is het mogelijk dat deze manier van informatie-uitwisseling opgezet en uitgevoerd wordt? Dit kunnen we opdelen in:
  - Aantal veto-punten bij de invoering: in welke mate is het nodig om meerdere actoren te betrekken bij de invoering van de informatie-uitwisseling? Moeten verschillende partijen zich akkoord verklaren met de informatie-uitwisseling? Hoe groter het aantal veto-punten bij de invoering, hoe lager de haalbaarheid.
  - Passendheid binnen het huidige regulatieve en wettelijke kader: wanneer het nodig is om wijzigingen aan te brengen aan het wettelijk of regulatief kader, betekent dit dat er ook extern een beslissingsproces nodig is, wat meer veto-punten met zich mee brengt.
- **Maatschappelijke wenselijkheid (Theta-waarden)**: in hoeverre wordt het systeem gepercipieerd als rechtvaardig? We beperken ons hierbij tot rechtvaardigheid gebaseerd op waarden, en meer specifiek de waarde respect voor privacy. Wanneer de informatie-uitwisseling zich beperkt tot informatie die reeds bij tenminste één van de actoren bekend was, is de impact op privacy niet zo groot . Er wordt namelijk geen nieuwe informatie verzameld, enkel bestaande uitgewisseld. Wanneer in het kader van informatie-uitwisseling zich ook een verrijking van de data voordoet, is de potentiële impact op privacy groter.
- **Complexiteit/Relevantie**: hoe interessant is het om de mogelijkheid tot informatie-uitwisseling verder uit te werken binnen het kader van dit onderzoek? Dit is een zoals eerder gesteld een aparte categorie om ervoor te zorgen dat de tijd besteed aan dit onderzoek zich zou richten op de meer complexe projecten. We toetsen complexiteit/relevantie door te kijken naar:
  - Externe context: hoe veel randvoorwaarden moeten vervuld worden om het project te realiseren? Suggesties waarbij de externe context vrij eenvoudig is, kunnen eenvoudig door politie en/of particuliere veiligheidsactoren zelf ingevuld worden, en zijn dus minder interessant om uit te werken binnen dit onderzoek.
  - Interne context: in hoeverre moeten partijen hun interne processen aanpassen om de informatie-uitwisseling mogelijk te maken? Ook hier geldt dat informatie-uitwisseling waar weinig tot geen wijzigingen nodig zijn, eigenlijk eenvoudiger door de partijen zelf kunnen opgenomen worden, en geen behoefte hebben aan een diepere analyse in het kader van dit onderzoek.

De preliminaire lijst met projecten werd voorgelegd met de vraag om voor elk (deel)criterium een score van 1 tot en met 5 te geven. Elk criterium en elke optie werd eerst uitgelegd, zodat er geen onduidelijkheden konden zijn over de scores. De antwoorden van de participanten komende uit de politie en de participanten komende uit de particuliere veiligheidsactoren werden door de onderzoekers ook apart gecontroleerd. De lijst die in de survey bevraagd werd, is niet één op één dezelfde als beschreven op basis van de interviews. Verduidelijkingen werden aangebracht, maar de kern van de suggestie is wel dezelfde gebleven, in lijn met de Delphi-methodiek.

47 Bryson (2018).

De verschillende voorgelegde projecten kunnen gevonden worden in ANNEX III. De vragen gesteld in de survey kunnen gevonden worden in ANNEX IV. De eerste twee vragen behandelen efficiëntie en effectiviteit, de score daarvoor wordt bekomen door het gemiddelde te nemen van de antwoorden op de eerste twee vragen. De derde en vierde vraag gaan over haalbaarheid. Om de gezamenlijke score voor haalbaarheid te bekomen, wordt tevens het gemiddelde genomen van de antwoorden op vragen 3 en 4, maar hier geldt dat hoe hoger de scores zijn, hoe lager de haalbaarheid, zodat de score hier omgekeerd moet worden, dus vijf minus de bekomen score. De vijfde vraag gaat over de maatschappelijke wenselijkheid, waarbij opnieuw geldt dat hogere scores staan voor lagere wenselijkheid, dus de eindscore voor wenselijkheid wordt bekomen door het bekomen cijfer af te trekken van 5. Vragen 6 en 7 tenslotte behandelen de relevantie in het kader van het project. Hoe hoger de score, hoe hoger de relevantie, dus hier is het gemiddelde voldoende.

3.2.3 Fase 3: Brainstormsessie

De personen die waren uitgenodigd voor het invullen van de vragenlijst, werden ook op de brainstormsessie uitgenodigd, in lijn met de Delphi-methode. Uiteindelijk waren er 7 personen van publieke en private organisaties beschikbaar, wat voor het doel van de brainstormsessie voldoende was. Aan hen werd een beperkte lijst van prioriteiten voorgesteld. Deze bestonden uit de hoogst gerangschikte suggesties[48] op basis van efficiëntie/effectiviteit, haalbaarheid en maatschappelijke wenselijkheid, rekening houdende met de prioriteiten van politie enerzijds en particuliere veiligheidsactoren anderzijds, en de complexiteit/relevantie voor het onderzoek. Op basis van de geuite zorgen over een project, werd elk project apart besproken om te bezien hoe deze zorgen weggenomen konden worden, zodat de kans op succesvolle implementatie zo hoog mogelijk is.

Na de brainstormsessie werden de resultaten door de onderzoekers verwerkt in een consensusdocument: enkel indien de deelnemers van het seminar het eens waren met elkaar, werd dit in het document opgenomen. Dit document werd nog eens rondgestuurd naar alle deelnemers om onnauwkeurigheden of materiële fouten te vermijden. Dit vormde tenslotte input voor praktische en juridische randvoorwaarden voor elk van de opgestelde prioriteiten. Hoewel het seminar dus een belangrijke input hiervoor vormde, willen de onderzoekers benadrukken dat de opgestelde voorwaarden hun verantwoordelijkheid zijn, niet die van de deelnemers.

48 Zie begin hoofdstuk 5.1 voor een aanvulling hierop, omdat de rangschikking van de gebruikte lijst uiteindelijk niet overeenkwam met de hoogste scores voor elk van de onderdelen.

4. FASE 1: LITERATUURSCAN EN OPMAAK PRIORITEITEN

4.1 Academische literatuur

In academische literatuur wordt er voornamelijk op een meer abstracte wijze gepleit voor informatie-uitwisseling, of worden gevaren daarvan uitgelicht, vaak vanuit het belichten van publiek-private samenwerking in meer algemene zin. Van Goethem & Easton[49] bijvoorbeeld stellen dat samenwerking tussen publieke en private actoren efficiëntie en effectiviteit ten goede kan komen, strategische en operationele voordelen kan hebben, onderlinge relaties verbeteren, en leiden tot een groter lerend vermogen. Private actoren die succesvol verbinding vinden met de publieke sector, hebben daarenboven een competitief voordeel, wat hun bereidheid tot informatie-uitwisseling verhoogt. Het specifieke voordeel voor de politie ligt bij een vergroting van het informatiebereik, en bij het betrokken zijn bij de ontwikkeling van instrumenten van informatieverzameling, waardoor de politie mogelijk hier ook sturend kan optreden. Hier schuilen uiteraard ook gevaren in. Schuilenburg & Van Steden wijzen op een mogelijke erosie van rechtsbescherming bij informatie-uitwisseling tussen zowel publiek-publiek,[50] denk bijvoorbeeld aan politie en gemeenten,[51] en publiek-privaat.[52] Een concreet voorbeeld is het gebruik van camera's door private actoren, waarbij de informatie nadien wordt doorgespeeld aan de politie.[53] Niet zelden is publiek-private samenwerking ook een poging tot bezuiniging,[54] wat kan betekenen dat ook informatie-uitwisseling kan leiden tot het minder verzamelen van eigen data en het meer steunen op informatie komende uit de private sector, een evolutie die de positieve gevolgen van informatie-uitwisseling teniet zou doen. In de literatuur wordt ook de vrees geuit dat samenwerking zou kunnen leiden tot rechtsongelijkheid, de capaciteit tot onderzoek wordt eigenlijk "ingekocht" door de private actor, die op deze manier kan wegen op de keuze van onderzoeksprioriteiten van de politie.[55]

Toch worden ook een aantal concrete handvatten gegeven om tot meer optimale interactie te komen tussen publieke en private actoren. Maurits geeft aan dat de politie zelf voldoende interne kennis in huis moet houden om inhoudelijk afspraken te kunnen maken met de private sector, de personen die de afspraken maken rond informatie-uitwisseling moeten in staat zijn om de gemaakte afspraken ook elk intern af te dwingen, en diezelfde personen moeten voldoende zicht hebben op de noden en werkwijzen van de verschillende actoren die samen willen gaan werken (dus niet enkel van de eigen organisatie).[56] Daarbij is het noodzakelijk dat er binnen de eigen organisatie voldoende steun is voor de interactie met andere actoren. Een echo daarvan vinden we terug bij Staats et al., die het ook heeft over de noodzaak van wederzijdse belangen en een gedeeld doel van zowel de organisaties in het algemeen als de specifieke individuen die betrokken zijn bij de uitwerking.[57] Daarbij speelt ook verwachtingsmanagement een grote rol: actoren moeten bekend zijn met wat er mogelijk is maar ook wat er niet mogelijk is binnen een samenwerking, waardoor frustraties vermeden worden.[58] Op deze manier kan vertrouwen worden opgebouwd tussen de verschillende actoren.

Eén specifiek handvat ligt gedeeltelijk buiten de interne mogelijkheden van de betrokken actoren: de juridische mogelijkheden van informatiedeling, natuurlijk met respect voor de relevante grondrechten. Een geopperde mogelijkheid is het verruimen van het beroepsgeheim, zodat ook private actoren hieronder vallen, en er dus een verder juridisch instrument is om informatie binnen bepaalde kanalen te houden, en te bestraffen wanneer dit niet gebeurt.[59] Tegelijkertijd ligt dit handvat ook gedeeltelijk binnen de mogelijkheden van de betrokken actoren: vaak is men niet voldoende op de hoogte van de mogelijkheden tot informatie-uitwisseling, en kiest men om niet of minder samen te werken uit vrees de wet te overtreden, terwijl er wel mogelijkheden tot samenwerking zijn.[60] Tenslotte kunnen ook de verschillende rollen die de politie speelt ten opzichte van de particuliere sector een temperende rol spelen. In Nederland bijvoorbeeld is de politie zowel een mogelijke partner als een toezichthouder op de particuliere sector.[61]

In academische literatuur werden tevens specifieke deelgebieden geïdentificeerd waar informatie-uitwisseling expliciet als een meerwaarde naar voren wordt geschoven.

49 Van Goethem & Easton (2021).
50 Schuilenburg & Van Steden (2014).
51 Salet (2019).
52 Ponsaers (2005).
53 Engberts & Copini (2016).
54 De Waard & Scheepmaker (2012).
55 Van Hoorn et al. (2020).
56 Sanders (2021).
57 Staats et al. (2021).
58 Van der Meulen & Sanders (2020).
59 Van Steden et al. (2018).
60 Meerts et al. (2022).
61 Van Hoorn et al. (2020).

- Interne financieel-economische criminaliteit: reeds afgewerkte onderzoeksrapporten door private actoren kunnen worden aangereikt aan de politie. In ruil kan de private actor feedback krijgen over hoe de verzamelde informatie al dan niet past in het bredere kader van een mogelijk opsporingsonderzoek, zonder dat hierbij precieze details vrij worden gegeven.[62] Er is ook parallelle informatie-uitwisseling mogelijk, dus terwijl zowel de private actor als de politie met een onderzoek bezig is. Dit kan gaan van het afstemmen van acties op elkaar tot het eenvoudig doorsturen van verzamelde gegevens door de private actor aan de politie.[63]
- Cybersecurity: de cyberwereld is een op zich interessante context, omdat in de offline wereld de private sector weliswaar een goede informatiepositie heeft, maar de politie toch eerder als betrouwbare partner of anker gezien wordt. In cybersecurity is het echter tevens de private sector die vaak de tools en expertise heeft, en niet de politie. Nog meer dan enkel informatie-uitwisseling, is publiek-private samenwerking hier vaak een noodzaak. Hagenaar & Bonnes stellen voor dat hierbij heldere doelstellingen worden bepaald, dat samenwerking gericht moet zijn op de lange termijn, en dat er best gebruik gemaakt wordt van beproefde methoden met voldoende middelen vanaf het begin. Zij sluiten potentiële *conflicts of interest* ook niet uit, maar stellen voor om daarom communicatielijnen kort te houden. Een interessante vaststelling is dat zij ook voorstellen om zo snel mogelijk de juridische beperkingen te exploreren. Anders zorgt dit op termijn voor frustraties bij de partners, omdat bepaalde verwachtingen dat iets juridisch mogelijk was, plots niet correct ingeschat bleken te zijn.[64]
- Veiligheidsvoorziening in havens: dit kan uitgebreid worden naar alle andere geografische locaties waar verschillende actoren over een langere periode samenwerken. Informatie-uitwisseling kan worden gedaan door een gezamenlijk opgezette centrale actor, die de informatie weer verder verspreidt. Een voorbeeld is het Expert Center Harbor in de haven van Rotterdam. Dit is een voorbeeld van publiek-publieke informatie-uitwisseling, maar het model kan mogelijk uitgebreid worden met private actoren.[65]

Veiligheidsvoorziening in een gemeentelijke context: in de openbare ruimte van gemeenten komen zowel publieke als particuliere veiligheidsactoren elkaar vaak (incidenteel) tegen. Dat gaat zowel over de politie als over gemeentelijke veiligheidsactoren (zoals buitengewoon opsporingsambtenaren), maar ook over politie en particuliere beveiliging en zelfs particuliere recherche. Informatiedeling gebeurt spontaan en informeel, vaak op basis van persoonlijke contacten. Meer structuur kan leiden tot meer waardevolle en langdurende partnerschappen.[66]

Tenslotte wordt er in de literatuur ook op gewezen dat samenwerking en informatie-uitwisseling tussen politie en particuliere veiligheidsactoren reeds bestaat, zowel in informele zin alsook op basis van meer formele verbintenissen, vaak in de vorm van pilotprojecten.[67] Een vaak gehoorde klacht is dat dit soort samenwerking incidenteel/ad hoc gebeurt, en dus vaak geen lang leven beschoren is, terwijl de literatuur laat zien dat langdurige en bestendige samenwerking meer voordelen heeft. De vraag kan echter gesteld worden of elke samenwerking langdurend moet zijn. Waar wel behoefte aan is, is een vaste werkwijze om tot samenwerking over te gaan, zodat er niet steeds opnieuw moet geëxperimenteerd worden. Wanneer er een vaste template voor samenwerking is, is het minder belangrijk dat er op een langere termijn wordt samengewerkt, deze kan ook incidenteel zijn.[68]

62 Vynckier (2019).
63 Meerts et al. (2022).
64 Hagenaars & Bonnes (2015).
65 Marks, Van Sluis, Vervooren & Zeer (2012).
66 Cools & Pashley (2018).
67 Van Hoorn et al. (2020), Kuin & Wilms (2015) en Meerts et al. (2022).
68 Meerts et al. (2022).

4.2 *Professionele literatuur en beleidsstukken*

4.2.1 Bestaande vormen

In de professionele literatuur en beleidsstukken worden een aantal bestaande vormen van informatie-uitwisseling genoemd. Daarbij is veelal niet duidelijk of deze inmiddels nog bestaan, wat precies wordt uitgewisseld, hoeveel dit wordt gedaan en hoeveel meerwaarde dit voor partners heeft. De bestaande vormen van informatie-uitwisseling worden in het vervolg van deze studie niet meer apart en als mogelijkheid voor de toekomst behandeld. Wel werden in de interviews vergelijkbare projecten, of projecten die verder bouwen op onderstaande ideeën, als toekomstmogelijkheid genoemd. Genoemd worden (alfabetisch):

- **Bedrijventerrein.** Om de veiligheid op bedrijventerreinen te vergroten wordt op verschillende manieren informatie uitgewisseld. Particuliere veiligheidsactoren voeren observaties uit op bedrijventerreinen en sturen digitaal of via rapportages meldingen aan de wijkagent/politie. De politie stuurt per bedrijventerrein informatiebulletins met modus operandi, hotspots en hot times, gebruikte vervoermiddelen en gereedschappen, signalementen, kentekens en trends aan particuliere veiligheidsactoren. Periodiek wordt overlegd (in het kader van het Keurmerk Veilig Ondernemen of een Bedrijfs Investerings Zone), tussen de politie, en particuliere veiligheidsactoren (ook de ' Parkmanager').[69]
- **Briefings en overleggen.** In deze samenwerking worden door de politie briefings gegeven in (handhavings)overleggen met verschillende veiligheidsactoren. Ook worden berichten gestuurd aan particuliere meldkamers over winkelcentra, stadscentra, horeca- en uitgaansgebieden.[70]
- **Gestolen voertuigen.** Particuliere veiligheidsactoren sturen wanneer zij die aantreffen of vermoedens hebben dat zij die zien informatie, rapporten of track&trace-informatie over gestolen voertuigen aan de politie.[71]
- **Geld- en waardetransport.** De politie deelt informatie over modus operandi, signalementen, gebruikte vervoermiddelen en gereedschappen van overvallers met particuliere veiligheidsactoren, in dit geval geld- en waardetransportbedrijven. Dit gebeurt in overleggen en 'via communicatiemiddelen'.[72]
- **LiveView.** Dit is een systeem om camerabeelden van onder andere particuliere alarmcentrales en geldtransporten door te verbinden naar de meldkamer van de politie (en ambulance en brandweer).[73]
- **Project Oog en Oor** (Haven Rotterdam). Binnen dit project wordt via een beveiligde website opsporingsinformatie uitgewisseld tussen de Zeehavenpolitie en twee particuliere veiligheidsactoren.[74]
- **Samen Alert 24/7.** Dit is een project in Twente, waarbij onder andere daderspecifieke informatie, plaatsen en kentekens, worden uitgewisseld. Ook werken politie en particuliere veiligheidsactoren samen tegen jeugdoverlast, geweld, drugs, overvallen, inbraken en onveilig verkeer. De samenwerking vindt plaats met strategische overleggen, briefings door de politie en een beveiligde webpagina voor politie en deelnemende bedrijven.[75]

4.2.2 Professionele literatuur

In de professionele literatuur worden ook een aantal aanbevelingen gevonden voor nieuwe, extra vormen van informatie-uitwisseling tussen politie en particuliere beveiliging. Sommige aanbevelingen die in de professionele literatuur gevonden werden, werden uiteindelijk ook als mogelijk project naar voor geschoven tijdens de interviews. De onderstaande lijst bevat de aanbevelingen die uiteindelijk niet pasten binnen de door de onderzoekers gestelde parameters voor projecten relevant in het kader van dit onderzoek (alfabetische volgorde):

69 Nederlandse Veiligheidsbranche (2014) en Document 1.
70 Nederlandse Veiligheidsbranche (2014) en Document 1.
71 Nederlandse Veiligheidsbranche (2014).
72 Nederlandse Veiligheidsbranche (2014). In de tekst staat niet welke communicatiemiddelen worden gebruikt.
73 Mehlbaum e.a. (2014).
74 Nederlandse Veiligheidsbranche (2014).
75 Nederlandse Veiligheidsbranche (2014).

- **Bestaande systemen**: Burgernet, CollegaNet en Compronet.[76] De suggestie wordt gedaan om particuliere veiligheidsactoren (meer) toegang te geven en te laten deelnemen in bestaande politie- of overheidsinformatie-uitwisselingssystemen. Overigens is moeilijk publiek informatie te vinden of als tweede en derde vermelde systemen nog bestaan of worden gebruikt.
- **Digital Security Operations Center.** De politie zou kunnen deelnemen in particuliere meldkamers voor digitale incidenten (cyber security).[77]
- **Federatieve beveiliging**. Federatieve beveiliging is een organisatievorm, een manier van werken en bijbehorende technologie voor organisaties met beveiligde objecten waarvan de observatiegebieden elkaar fysiek raken of overlappen. Voor bijzondere locaties, evenementen of gebieden zou het nuttig kunnen zijn dat publieke en private partijen, inclusief politie en betrokken veiligheidsactoren, via deze organisatievorm informatie uitwisselen. Daarbij kan worden gedacht aan 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. Hiermee wordt tegemoet gekomen aan privacy-regels en ~wetten.[78]
- **Vermiste veroordeelden.** De politie kan met particuliere veiligheidsactoren informatie delen over vermiste veroordeelden, zodat zij kunnen kijken of zij die waarnemen. De bedrijven kunnen die informatie ook internationaal in hun organisaties delen.[79]
- **Webruimte**. Een gezamenlijke, deels gesloten webruimte waar politie en particuliere beveiliging als community of practice kunnen samenkomen en samenwerken. Simeone noemt als onderdelen: e-mail, web-portal (openbaar, statische tekst), web forum (besloten, discussie ruimte) en het gaan gebruiken van Microsoft Groove ('secure workspace, share information, work on a joint document or project').[80]
- **Zwarte lijst**. Hierbij gaat het om het door politie en particuliere veiligheidsactoren samen opstellen en delen van een lijst van verdachte personen.[81]

4.2.3 Documenten

De verschillende organisaties waaruit voor dit onderzoek leidinggevenden of experts zijn geïnterviewd, hebben een aantal studies, documenten en presentaties gedeeld, waarin nog aanvullende mogelijkheden voor informatie-uitwisseling staan. Sommige van deze werden ook besproken tijdens de interviews en daarin als mogelijk project naar voor geschoven. Onderstaande mogelijkheden werden uiteindelijk niet genoemd als project (alfabetisch):

- **Alerteren beveiligers**. De regionale meldkamer (van de politie) voor een GSM-cel-gebied de mogelijkheid geven daar particuliere beveiligers te alerteren.
- **Bedrijventerrein analyses.** Door particuliere veiligheidsactoren laten maken en aan politie geven.
- **Best practices.** Publieke en particuliere veiligheidsactoren kunnen kennis uitwisselen over hoe het best misdaad te voorkomen en te bestrijden.
- **Co-locatie meldkamers**. Co-locatie realiseren van particuliere collectieve beveiliging (camera) meldkamers met gemeentelijke toezicht meldkamers waar ook de politie al (altijd) aanwezig is.
- **Informanten**. De politie recherche zou (meer) informanten kunnen rekruteren onder particuliere beveiligers(kader).
- **Locatie tracker**. De regionale meldkamer (van de politie) een locatie tracker geven van mobiele surveillancewagens van particuliere beveiliging, zodat die indien nodig om assistentie kunnen worden gevraagd.
- **RIEC**. Particuliere veiligheidsactoren in verschillende gebieden opnemen in de Regionale Informatie- en Expertise Centrum (RIEC)-samenwerking die de politie nu al met verschillende externe partners heeft.

76 Mehlbaum e.a. (2014).
77 Theuns & Wannee (2015).
78 TNO (2021).
79 Https://benefitsecurity.nl/beveiligingsbedrijven-doen-tweede-kamer-voorstellen-voor-samenwerking-met-politie , bezocht 5 april 2022. De Waard (2020) noemt 'combating cross-border crime' meer in het algemeen als terrein met kansen voor meer samenwerking.
80 Simeone (2007). De systemen genoemd in deze oude publicatie, zoals Microsoft Groove, zijn ten dele achterhaald, maar er zijn nu veel andere applicaties met dezelfde functies beschikbaar.
81 Van Rooij (2017).

- **SMART safe-data.** Vanuit de door bedrijven aan ondernemers geleverde *SMART safes* ongebruikelijke transacties laten melden en analyses leveren aan de politie/Fiscale Inlichtingen- en Opsporingsdienst.[82]

4.3 Interviews met sleutelpersonen

4.3.1 Betere samenwerking

In de interviews werden een aantal suggesties gedaan die volgens de geïnterviewden wel de samenwerking tussen de politie en particuliere veiligheidsactoren zouden verbeteren, betrekking hebben op relaties met derden en/of indirect meer informatie-uitwisseling zouden opleveren, maar niet in hoofdzaak richten op meer (operationele) informatie-uitwisseling tussen beide. Deze suggesties kunnen waardevol zijn, maar zijn niet het primaire doel van deze studie, omdat het niet gaat om concrete projecten rond informatie-uitwisseling. Genoemd werden (alfabetisch):

- **Betrouwbare veiligheidsactoren.** De politie zou zelf een register kunnen bijhouden van (on)betrouwbare particuliere veiligheidsactoren, waarmee (geen) informatie kan worden gedeeld. Deze kwalificatie zou na een extra screening van het bedrijf en op basis van incidenten/ervaring van de politie kunnen worden gegeven.[83]
- **Budgetten**. Politiedistricten zouden een klein budget moeten krijgen om kleine taken door particuliere veiligheidsactoren te laten uitvoeren, waarover dan intensiever informatie kan worden uitgewisseld en die in het algemeen de relatie en informatie-uitwisseling versterkt. Te denken valt aan het langsrijden van hotspots, het reageren op kleine aanrijdingen, uitvoeren van kleine rechercheonderzoeken en inhuur van medewerkers vanuit de bedrijven (voornamelijk om capaciteit schokken op te kunnen vangen). De politie zou landelijk beleid moeten maken welke vergoeding constructies en maximale betalingen hiervoor toegestaan zijn. Dit budget kan ook samen met gemeenten worden opgezet.[84]

  Er kan ook gedacht worden aan het verstrekken van informatie door de particuliere sector aan de politie als commercieel product, maar de particuliere sector lijkt in eerste instantie toch meer te denken aan het uitvoeren van een aantal taken.[85] Ook landelijk zou de politie een budget kunnen vastleggen voor innovatieve samenwerking pilots. De particuliere veiligheidsactoren zouden financieel evenveel moeten inbrengen. Over de pilots en een eventueel vervolg moet gezamenlijk worden besloten. Belangrijk is om pilots goed te (laten) evalueren. Mogelijk zou hiervoor een gezamenlijke stichting moeten worden gebruikt.[86]
- **Gezamenlijke patrouilles**. In navolging van bijvoorbeeld voorlichtingssessies kunnen ook gezamenlijke activiteiten georganiseerd worden, zoals bijvoorbeeld een gezamenlijke patrouille. De bedoeling is hier eerder om een betere verstandhouding en *goodwill* te creëren tussen mensen op het veld.[87]
- **Grensgebieden.** De politie, in de zin van de Koninklijke Marechaussee, zou in het kader van haar in de Politiewet genoemde taak van Mobiel Toezicht Veiligheid in grensgebieden structureel kunnen samenwerken en informatie uitwisselen met particuliere veiligheidsactoren, zoals verdachte voertuigen en personen. Deze intensievere samenwerking bestaat al wel voor havens, luchthavens en waardetransport, maar voor zover bekend niet voor grensgebieden.[88]
- **Horecaverboden.** Een aantal gemeenten heeft systemen waarin (online) kan worden gezien wie in die gemeenten een horecaverbod opgelegd heeft gekregen. Gemeenten verlenen hiertoe toegang, onder andere aan (horeca)ondernemers. Particuliere veiligheidsactoren die in de gemeente in de horeca werken, zouden ook toegang kunnen worden gegeven tot het systeem. Beveiligers zouden dan bij overtredingen van een horecaverbod sneller of vaker de politie kunnen inschakelen.[89]

82 Document 2.
83 Respondent 7.
84 Respondent 5 en Respondent 7.
85 Respondent 5.
86 Respondent 9.
87 Respondent 5
88 Respondent 5.
89 Respondent 2.

- **Informatieplicht**. In de WPG staat welke en wanneer de politie informatie mag delen met derden, niet wanneer zij dat moet. Het zou particuliere veiligheidsactoren helpen in hun werk, vergroten van veiligheid, als in deze wet of de WPBR als plicht zou staan welke en wanneer de politie informatie moet delen, zodat hierover meer duidelijkheid komt en minder subjectiviteit of toeval een rol speelt.[90]
- **Klantenpanel.** Particuliere veiligheidsactoren voeren in contracten vastgelegde taken uit voor hun klanten. Hun klanten zijn eigenaar van de informatie die ze daarvoor nodig hebben en die ze daarmee verzamelen. In die zin zou de politie met de klanten moeten overleggen over verbetering van de informatie-uitwisseling tussen politie en particuliere veiligheidsactoren. Het zou goed zijn als de politie om ervaringen te bespreken en verbetervoorstellen te ontwikkelen, een panel met grote klanten van de particuliere beveiligingsbranche zou hebben - zoals dit in de vitale infrastructuur en cyber security wel (meer) bestaat. Het zou goed zijn ook departement(en) hierin op te nemen.[91]
- **Kwaliteitsreviews.** Organisaties zoals de Kamer van Koophandel en het Centrum voor Criminaliteitspreventie en Veiligheid zouden een lijst van kwaliteitsindicatoren voor particuliere veiligheidsactoren kunnen ontwikkelen, individuele bedrijven daarop scoren en de resultaten publiceren. De politie zou over indicatoren kunnen adviseren en onderzoeken of de WPBR of WPG toelaat dat zij ook informatie levert voor de individuele scores. Ook als dit laatste niet wordt gedaan zou voor politie-eenheden de gepubliceerde score duidelijk maken wat betrouwbare bedrijven zijn, waarmee makkelijker - maar binnen de wet - informatie kan worden gedeeld.[92]
- **Leegstaande panden**. Juist omdat daar veel overlast en criminaliteit (kan) plaatsvinden, zouden politie en veiligheidsactoren plaatselijk adressen van leegstaande panden kunnen delen. Deze kunnen dan door beide meer in de gaten worden gehouden.[93]
- **Ondergrens publiek belang** bij particuliere zaken definiëren. Een probleem wat aan de kant van de commerciële actoren gemerkt wordt, zeker de recherchebureaus, is dat de zaken waar zij mee te maken krijgen, moeilijk begrepen worden door de politie. Het gaat veel vaker over fraude, witteboordencriminaliteit, het toe-eigenen van private data, etc. Vanuit de politie is er de cultuur om 'de crimineel' te pakken te krijgen, en deze mensen zijn geen goede 'fit' voor dat beeld. Er is dus ook behoefte aan meer begrip vanuit de politie dat deze personen ook criminele activiteiten verrichten die schadelijk zijn, en er ook prioriteit moet gegeven worden aan dit soort misdrijven.[94] Daar komt ook nog eens bij dat de eigen procedures van de politie niet zijn ingesteld op de snelheid waarop gerekend wordt bij de (klanten van) private commerciële actoren. Ook daardoor is er vertrouwensverlies. Het eerder beschreven aangiftesysteem kan daarbij helpen, maar dat kan alleen als er ook opvolging wordt gegeven aan dit systeem, en dat betekent investeren in capaciteit en expertise binnen de politie.[95]
- **Onderzoek i.o.v. rechter-commissaris.** Indien private recherchebureaus niet in PPS-constructies kunnen werken, is er ook een mogelijkheid om hen bij private onderzoeken bepaalde daden te laten stellen, indien daarvoor toestemming wordt verkregen bij de rechter-commissaris. Dan blijft er een publieke controle op de daden.[96]
- **Operationele opvolging.** Het komt vaak voor dat particuliere veiligheidsactoren bij de politie of meldkamers melding doen van een acute, gevaarlijke situatie en verzoeken om politie-assistentie. Vaak blijft dan onduidelijk wanneer de politie ter plaatse zal komen, wat bij betrokken beveiligers extra spanning veroorzaakt. Het zou wenselijk zijn als de politie (geautomatiseerd) kan aangeven wanneer hulp ter plaatse kan worden verwacht.[97]
- **Particuliere Beveiligingsautoriteit** (PBA)**.** Nu levert een particuliere veiligheidsactor informatie aan de politie voor screening en toestemming in het kader van de WPBR.

90 Respondent 7.
91 Respondent 7.
92 Respondent 9.
93 Respondent 5.
94 Respondent 4.
95 Respondent 4.
96 Respondent 4.
97 Respondent 2.

Dit is een taak belegd bij districten, die ook met particuliere veiligheidsactoren samenwerken (en in strategische zin om taken concurreren). Het zou beter zijn om hiervoor, net als in andere/buurlanden, een nationale organisatie buiten de politie zelf op te zetten. Zo'n PBA zou bijvoorbeeld binnen de Nationaal Coördinator Terrorismebestrijding en Veiligheid kunnen worden gepositioneerd. Deze zou ook toezicht moeten houden op overheidsorganisaties die beveiligingstaken hebben, zoals de Rijksbeveiligingsorganisatie, Dienst Vervoer en Ondersteuning, Defensie Beveiligingsorganisatie, Koninklijke Marechaussee en de politie zelf. Het beste zou zijn deze PBA middels een (nieuwe) wet taken te geven, waarbij ook de mogelijkheid of verplichting voor particuliere veiligheidsactoren wordt geregeld om bij vermoedens van ontoelaatbaar gedrag informatie aan de PBA voor herscreening te geven, wat nu arbeidsrechtelijk niet mag.[98]

- **Publiciteit.** De politie en de particuliere veiligheidsactoren kunnen vaker voorbeelden van goede samenwerking en informatieuitwisseling publiceren, op websites, persberichten, in vakbladen en wetenschappelijke publicaties. Belangrijk is dat hierdoor 'buitenom' ook breed binnen de eigen organisaties informatie wordt gedeeld over hoe goed kan worden samengewerkt en welke informatie-uitwisseling daarvoor nuttig is[99].
- **Route-informatie.** (Waarde)transportbedrijven zouden van de politie (of Nationaal Crisiscentrum of Rijkswaterstaat) informatie moeten krijgen welke routes of plaatsen zij op bepaalde tijd beter kunnen mijden of waar zij voorzichtig of opmerkzaam moeten zijn. Te denken valt aan buitenlandse VIP/staatsbezoeken.[100]
- **Samenwerking in WPBR.** In de wet zou kunnen worden opgenomen hoe de politie en de particuliere veiligheidsactoren samenwerken en informatie uitwisselen. Hiervoor kan de vergelijkbare Belgische wet als voorbeeld dienen.[101] Ook de nieuwe WGS kan mogelijk hiervoor worden gebruikt.
- **Seponeringsregime**. Nu wordt vaak ('8 van de 10 keer') een door een particulier rechercheburo onderzochte zaak na aangifte door het OM geseponeerd. Als eerste zou het seponeringsbeleid hiervoor kunnen worden aangescherpt, zodat minder wordt geseponeerd.[102] In combinatie met het aangiftesysteem kan dan een terugkoppeling gebeuren wat er met een zaak gebeurt. En indien men tot een seponering overgaat, is het voor rechercheburo's belangrijk om te weten waarom. Indien het gaat om ontbrekende elementen in de aangifte, kan daarop voortgebouwd worden. Heel vaak wordt nu ofwel geen of een standaard antwoord verstuurd. Dat laatste is soms nog erger, omdat het de idee heeft van een zekere wereldvreemdheid vanuit de politie (e.g.: niet genoeg elementen om het onderzoek voort te zetten, terwijl heel veel info werd meegegeven).[103]
- **Speciale beveiligers.** De politie zou individuele beveiligers kunnen trainen in samenwerking en informatie-uitwisseling met de politie. Deze speciale beveiligers kunnen dan meer worden vertrouwd en meer informatie delen. Omdat hun afstand tot de politie nu groter is, zou hiervoor eerder aan beveiligers dan particuliere rechercheurs kunnen worden gedacht, die nu al vaak van de politie afkomstig zijn. Voor deze groep komen bijvoorbeeld ook oud-politiemensen eerder in aanmerking. Het zou goed zijn deze groep speciale beveiligers ook een wettelijke basis te geven.[104]
- **Software-ontwikkeling**. Een gezamenlijk, PPS-kenniscentrum van de politie en de particuliere beveiligingssector over software voor opsporing of veiligheid.[105]
- **Strategisch overleg**. Om informatieuitwisseling te vergemakkelijken zouden strategisch leidinggevenden van de politie, particuliere veiligheidsactoren en het vakdepartement elkaar met enige regelmaat, vrij informeel, moeten kunnen spreken. Het zou goed zijn

98 Respondent 7.
99 Respondent 9.
100 Respondent 3.
101 Respondent 9.
102 Respondent 1.
103 Respondent 4.
104 Respondent 5.
105 Respondent 1.

zo'n regelmatig strategisch overleg in de wet/WPBR, vast te leggen.[106] De suggestie werd ook gedaan om op deelterreinen, zoals *intelligence,* een dergelijk overleg, een 'trusted community' op te zetten, om nieuwe mogelijkheden voor samenwerking en informatie-uitwisseling te verkennen.[107] Ook een platform voor open gesprekken voor langere termijn samenwerking, innovatie en organisatieverandering zou waardevol kunnen zijn.[108]

- **Terugkoppelingsbeleid**. Particuliere veiligheidsactoren krijgen vaak geen reactie, terugkoppeling of bedankje als zij informatie of tips geven aan de politie. Dit demotiveert om het vaker te doen. Daardoor loopt de politie (veel) informatie mis. Het zou goed zijn als de politie beleid ontwikkelt wanneer, in welke soorten gevallen, altijd terugkoppeling moet worden gegeven, en hoe dit moet gebeuren. Dit beleid landelijk invoeren.[109] Ook dit kan mogelijk via een digitaal platform. Belangrijk is dat het om een gebruiksvriendelijk platform gaat.[110]
- **Veiligheidsdata**. Particuliere veiligheidsactoren slaan veel data op van de verschillende soorten incidenten die zij bij hun klanten constateren. Deze zou de politie of andere delen van de overheid kunnen gebruiken. Dit zou ervoor kunnen zorgen dat er een beter zicht komt op 'dark numbers' rond criminaliteit. Levering zou dan een commerciële transactie kunnen zijn, een soort abonnement dat de politie heeft. Databestanden kunnen bijvoorbeeld jaarlijks worden geleverd. Particuliere veiligheidsactoren mogen deze data aan de overheid geven als hun klanten hiervoor toestemming geven. Om redenen van privacy zou informatie daarvoor niet meer naar klantorganisaties en personen herleidbaar moeten zijn.[111]
- **Vitale sector**. Om meer en makkelijker informatie te kunnen uitwisselen met de politie, zou het goed kunnen zijn om ook (delen van) de particuliere beveiligingsbranche (wettelijk) aan te wijzen als maatschappelijk vitale sector.[112]
- **Voorlichtingssessies**. Laat de politie regelmatig (bijvoorbeeld: per kwartaal) voorlichting geven, een paar dagen per beveiliger, over wanneer de politie te informeren of te benaderen, hoe dit te doen, waar de politie wil dat door particuliere beveiligers op wordt gelet etc.[113] Beveiligers die deze voorlichting hebben gekregen, kunnen dan mogelijk een certificaat krijgen. Dat zou ook kunnen gebruikt worden voor de 'speciale beveiligers' (zie hierboven).

4.3.2 Suggesties voor informatie-uitwisseling

Tenslotte werden in de interviews ook suggesties gedaan die in lijn waren met het doel van dit onderzoek, met als kern het starten van nieuwe informatie-uitwisseling naar of tussen politie en particuliere veiligheidsactoren. Deze vormden de basis voor de projecten die nadien door de onderzoekers voorgelegd werden door middel van de survey. De volgende suggesties werden genoemd (alfabetisch):

1. **Aangiftesysteem.** Het komt (regelmatig) voor dat particuliere veiligheidsactoren ter plaatse of via e-mail informatie aan de politie geven met als doel dat daarvan een melding in het politie(aangifte)systeem wordt gedaan, maar dat dit niet wordt gedaan. Naast dat vaak onbekend blijft waarom dit niet gebeurt, dus ook niet door de bedrijven kan worden geleerd en verbeterd, is ook niet (makkelijk) te achterhalen hoe vaak iets met de informatie wordt gedaan en of hiertoe een juiste beslissing wordt genomen. Het zou goed zijn om hiervoor een apart meldings/aangiftesysteem te maken, waarin de bedrijven zelf gevallen kunnen invoeren, en gelogd, gevolgd, geleerd en gecontroleerd kan worden.[114] De invoering kan gebeuren nadat de commerciele actor het onderzoek heeft afgerond. Zeer waarschijnlijk moet die informatie dan wel telkens opnieuw geverifieerd worden door de politie, maar dan is er op zijn minst ook een

106 Respondent 7.
107 Respondent 8.
108 Respondent 9.
109 Respondent 5.
110 Respondent 5
111 Respondent 4 en Respondent 7. De mogelijkheid om plaatselijke en landelijke data te leveren staat ook in Document 2.
112 Respondent 7.
113 Respondent 5. Deze mogelijkheid staat ook in van Steden et al. (2018), gericht op het herkennen van de dreiging van een aanslag zoals in Denemarken, en in Document 2, gericht op herkenning van ondermijning.
114 Respondent 2.

basis.[115] De perceptie bij private commerciële bedrijven is dat hun klanten vrij negatief staan tegenover aangifte wegens teleurstellingen uit het verleden hoe er met hun klachten is omgegaan. Een aangiftesysteem dat gebruik maakt van specifieke personen met hogere *clearance*, en een feedback systeem heeft, kan voor een opbouw van vertrouwen zorgen.[116] Belangrijk is dan nog dat de informatie ook correct doorstroomt van het centraal/landelijk punt naar de regionale teams, zodat er ook relatief snel aan de slag kan worden gegaan met de informatie. Want ook de snelheid is van belang voor het vertrouwen van de klanten.[117]

2. **Bedreigingsdossiers.** Particuliere veiligheidsactoren leggen in de regel per klant een dossier van de bedreiging en mogelijke bedreigers aan, vooral om dit te analyseren en intern te verspreiden. Hierin staat vaak ook redelijk specifieke informatie, zoals namen, naam-adres-woonplaats, Internet Protocol-, kenteken- en telefoonnummers. Deze informatie is openbaar verkregen informatie en gezien de vaak externe dreiging geen eigendom van de specifieke klant. Deze dossiers worden niet standaard, zelfs niet vaak, met de politie gedeeld, wat de particuliere veiligheidsactoren wel zouden kunnen doen.[118] Hier gaat het dus niet om een aangifte, maar het dossier kan wel relevante informatie bevatten voor de politie.

3. Samenwerken met **beveiligingssoftware leveranciers**. Particuliere veiligheidsactoren gebruiken bepaalde softwarepakketten om informatie over hun klanten, locaties en incidenten in te registreren en deze informatie intern te delen. Een aantal van deze pakketten wordt door veel particuliere veiligheidsactoren gebruikt, alsook door een aantal Nederlandse gemeenten. De politie zou met de (Nederlandse) leveranciers van deze pakketten kunnen uitzoeken hoe via deze software informatie naar (en vanaf) beveiligers kan worden gestuurd.[119]

4. Real-time uitwisselen van informatie in een specifiek **evenementen systeem.** Bij veel (openbare) evenementen zijn zowel politie als particuliere veiligheidsactoren betrokken. Vaak zijn bij de politie of de beveiligers, vooraf of juist tijdens het evenement, personen bekend waar extra op moet worden gelet. Vaak worden deze niet of met gebrekkige informatie-uitwisseling gedeeld. Het zou nuttig zijn als hiervoor een systeem komt, dat per evenement, bijvoorbeeld door meldkamercentralisten, maar ook via PDA door agenten en beveiligers, kan worden gebruikt.[120] Een centrale persoon kan de info krijgen en dan relevante informatie doorsturen naar de PDA's. Dit kan via een gedeelde meldkamer.

5. Doorgeven **gevaarsindicatie** aan particuliere veiligheidsactoren. Bij bedreigingen hebben particuliere veiligheidsactoren (persoonsbeveiligers) vaak een vermoeden wie de bedreiger is. Of en hoe gevaarlijk deze daadwerkelijk is, is hen vaak niet duidelijk. Daardoor wordt soms teveel, soms te weinig beveiliging geleverd. Het zou voor veiligheidsactoren en hun klanten wenselijk zijn als zij bij een vaste contactpersoon bij de politie kunnen vragen of er gevaarsindicatie is, bijvoorbeeld of de persoon bekend is om wapenbezit. De politie zou een gevaarsniveau kunnen aangeven, zonder verdere informatie te verstrekken. Voordeel voor de politie zou zijn dat zij mogelijk extra informatie krijgt en door de melding de optie om zelf in te grijpen.[121] Voor de gevaarsindicatie alleen zou een nieuwe versie van een stoplichten convenant met de particuliere beveiligingssector, kunnen worden gebruikt.[122] Deze gevaarsindicaties kunnen ook uitgebreid worden naar bedreigingen langs een route die door private actoren gebruikt wordt voor bijvoorbeeld transport (zie ook: route-informatie). Dit kan aangevuld worden met open source informatie rond

115 Respondent 4. Deze mogelijkheid lijkt overeen te komen met het 'mini-proces verbaal' in Document 2.
116 Respondent 4.
117 Respondent 4.
118 Respondent 2.
119 Respondent 5. Een vergelijkbare optie staat ook in Document 2. Zie ook de meer algemene suggestie voor het door de politie ter beschikking te stellen foto's, kentekens en signalementen in https://nos.nl/artikel/277333-teeven-politiekennis-uitwisselen, bezocht 5 april 2022.
120 Respondent 2.
121 Respondent 2 en respondent 7.
122 Respondent 9. De Autoriteit Persoonsgegevens heeft in 2017 het gebruik van een dergelijk convenant met verhuurders van o.a. woningen afgewezen, waarna de Nationale Politie gestopt is deze organisaties te 'adviseren'. Belangrijkste bezwaar was het ontbreken van een wettelijke grondslag. Zie: https://www.tomlow-advocaten.nl/nieuws/politie-trekt-stekker-stoplichtconvenanten/, geraadpleegd 29-6-2022.

onder andere wegenwerken. Een gedeeld informatieplatform geeft ook feedback aan de politie over potentieel gevaarlijke situaties die door private bewakers geobserveerd worden.[123] Net zoals bij het aangiftesysteem, bedreigingsdossiers en evenement Smoelenboek is het belangrijk dat er sleutelpersonen zijn (bijvoorbeeld: veiligheidsofficier[124]) die een groter overzicht hebben over de informatie, en dan beslissen welke informatie relevant is om te delen met anderen.

6. **Heterdaad omgevingssensoren.** De politie zou graag vaker camerabeelden en andere sensorinformatie krijgen van particuliere veiligheidsactoren (of hun klanten) uit alarm- en heterdaad situaties, met name ook opnames uit straten/publieke omgeving van de woning of gebouw waar deze situatie zich voordoet. Dit mag binnen de huidige wetgeving en kan bijvoorbeeld met hoger (op daken) geplaatste camera's en andere sensoren. Particuliere veiligheidsactoren kunnen dergelijke systemen met hun klanten aanleggen, wat nu nog zelden gebeurt. Met deze systemen kan in voorkomende gevallen meer waardevolle informatie worden uitgewisseld.[125]

7. **Meld Misdaad Anoniem** (MMA). Particuliere veiligheidsactoren, hun medewerkers, hebben vaak vermoedens van criminele activiteiten. Daar wordt lang niet altijd aangifte voor gedaan, omdat mogelijk te weinig concreet bewijs verzameld is, klanten geen aangifte willen doen of dat men sceptisch is of de zaak door politie/Justitie wordt opgepakt. Particuliere veiligheidsactoren (of hun klanten) zouden vaker tips kunnen geven aan MMA.[126] Hier blijft dan wel het probleem dat met de misdrijven waar bijvoorbeeld recherchebureaus mee te maken hebben, er weinig voeling mee is vanuit de politie. Dat leidt tot het onvoldoende doorgeven van het belang van de aangifte aan het OM, wat dan weer leidt tot de seponeringen. Dus opnieuw moet hier de voeling van de politie met het onderwerp omhoog (zie ook: ondergrens publiek belang).[127]

8. Gebruik informatie vanuit **mobiele sensing-platforms.** Waardetransportbedrijven (maar ook andere particuliere veiligheidsactoren) hebben een groot wagenpark dat heel veel in Nederland rondrijdt. Ze kunnen aanbieden dat de politie (en andere overheidsdiensten) sensoren op hun wagens plaatsen om te controleren en handhaven. Te denken valt aan illegale radiozenders, verlopen APK-status en kwaliteit van wegen/asfalt. Maar ook andere informatie, zoals waarnemingen van beveiligers op de openbare weg/mobiele surveillance, kunnen aan de politie, gemeente of andere overheidsorganisaties worden gemeld, juist omdat de particuliere veiligheidsactoren in de publieke ruimte geen klanten hebben.[128]

9. **Opsporingsindicatie.** Bonafide particuliere veiligheidsactoren willen geen nieuwe klanten helpen waarbinnen criminele activiteiten plaatsvinden. In sommige gevallen zouden zij de nieuwe klant beter kunnen helpen als zij weten dat binnen de klant criminaliteit plaatsvindt. Het zou voor beide doelen helpen als particuliere veiligheidsactoren de politie zouden kunnen vragen om aan te geven of er een opsporingstraject loopt - niet zo zeer op wie en wat dit zich richt.[129] Ook hiervoor zou een nieuwe versie van een 'stoplichten-convenant', in dit geval met de particuliere beveiligingssector, kunnen worden gebruikt.[130]

10. De **Proeftuin PPS** met particuliere recherchebureaus opnieuw starten, met verbeteringen.[131] Er zijn enige documenten hierover beschikbaar, die zijn opgevraagd bij de Nederlandse veiligheidsbranche.[132] Bij de PPS-constructies is het voordeel dat de politie het onderzoek niet volledig uit de hand

123 Respondent 3.
124 Https://www.nvoans.be/nl/private-ondernemingen/veiligheidsofficier
125 Respondent 9.
126 Respondent 1.
127 Respondent 4.
128 Respondent 3 en Respondent 7. De mogelijkheid om ANPR-camera-detectie te plaatsen op wagens van particuliere veiligheidsactoren staat ook in Document 2. Engberts en Copini (2016) noemen mogelijkheden voor sensing van geluiden, gebeurtenissen, bewegingen, temperaturen en gewicht. Als sensor- systemen worden laserguns, voelplaten, warmtesensoren, *automatic number plate recognition* (ANPR)-camera's en richtmicrofoon genoemd.
129 Respondent 7.
130 Respondent 9. De Autoriteit Persoonsgegevens heeft in 2017 het gebruik van een dergelijk convenant met verhuurders van o.a. woningen afgewezen, waarna de Nationale Politie stopte deze organisaties te 'adviseren'. Belangrijkste bezwaar was het ontbreken van een wettelijke grondslag. Zie: https://www.tomlow-advocaten.nl/nieuws/politie-trekt-stekker-stoplichtconvenanten/, geraadpleegd 29-6-2022.
131 Respondent 1.
132 Respondent 4.

geeft, maar zelf een grote regierol blijft hebben. Er is ondersteuning van private commerciële partners, maar niet een overname.[133] Het mogelijke nadeel aan de PPS-constructies zit in het financiële element. Tegenover vrij veel inzet vanuit de commerciële actoren staat doorgaans een vrij lage financiële input vanuit de publieke sector. Er leeft het gevoel bij de commerciële actoren dat men langs de kant van de publieke sector niet echt goed weet hoe veel dingen normaal kosten.[134] En ook hier was het in het verleden vaak eenrichtingsverkeer wat betreft informatie. Dat frustreert, indien er zelfs geen informatie komt of de aangeleverde data nuttig was of niet.[135] Vanuit de politie werd aangegeven dat men graag in een *trusted community* verder zou verkennen waar behoefte en mogelijkheden zijn voor informatie-uitwisseling.[136]

11. **Sensing-aanvraagpunt**. De politie beschikt over mobiele sensor (ANPR-)camera's en de software om sensing door camera's van particuliere organisaties te laten plaatsvinden. Deze worden op slechts een beperkt aantal particuliere terreinen gebruikt. Particuliere veiligheidsactoren hebben soms klanten waar zij aanwijzingen hebben dat (veel) criminaliteit plaatsvindt of hoge (maatschappelijke) veiligheidsrisico's zijn. Het is nu zeldzaam dat de politie op dit soort locaties nu sensing installeert. Particuliere veiligheidsactoren kunnen een uitgebreid dossier van de risico's aanleggen. Deze zouden zij aan een vast, nationaal punt willen kunnen overleggen, bij politie of het Openbaar Ministerie (OM), om sensing te vragen.[137] De overheid zal dan wel zelf de afweging moeten maken of inzet van sensing aan eisen van ethiek, legitimiteit, proportionaliteit en subsidiariteit voldoet. Ook moet geen wederkerigheidsrelatie ontstaan en zelf kunnen worden besloten wanneer weer wordt gestopt.[138]

12. **Stimuleren privaat-private samenwerking**. Op sommige terreinen heeft de politie er belang bij dat verschillende soorten private organisaties gaan samenwerken. Zo zou het goed zijn als verzekeringsbedrijven kentekennummers van gestolen auto's aan particuliere veiligheidsactoren doorgeven. Dit hoeft de politie dan niet zelf te doen. Particuliere veiligheidsactoren kunnen via (hun) camera's bij klanten met software zoeken naar deze kentekens. Als deze op een locatie wordt geconstateerd dient de politie te worden geïnformeerd. Voor de politie zou dit mogelijk veel concrete meldingen opleveren.[139]

13. **Trends delen.** De politie zou aan particuliere veiligheidsactoren analyses en notities kunnen sturen. De organisaties kunnen ook samen analyses opstellen voor intern gebruik, zoals over nieuwe modus operandi, nieuwe soorten incidenten, nieuwe daderprofielen etc. Deze kunnen de bedrijven dan binnen hun werkzaamheden op gaan letten en daartegen optreden. De politie kan op deze manier uiteraard ook leren van en reageren op trends die het eerst door bedrijven worden opgemerkt.[140]

14. **Veiligheidsofficier.** Een particuliere veiligheidsactor zou één vaste, op hoog niveau door de overheid gescreende voor veiligheid verantwoordelijke functionaris moeten hebben, liefst op directieniveau, die door de politie of andere overheidsorganisaties meer kan worden vertrouwd en waarmee makkelijker en meer informatie kan worden uitgewisseld. Het zou goed zijn dat deze een wettelijke status heeft, en dat/welke particuliere veiligheidsactoren verplicht zijn zo'n medewerker te hebben (in de woorden van respondent 5: "iedereen kan een beveiligingsbedrijf oprichten").[141] Hier moet wel een even deskundige persoon aan de kant van de politie worden gezet, die bekendheid heeft met het soort zaken waar private commerciële actoren mee te maken hebben. De twee kanten moeten als het ware dezelfde taal kunnen spreken.[142]

133 Respondent 4.
134 Respondent 4.
135 Respondent 5
136 Respondent 8.
137 Respondent 7.
138 Respondent 6. Zie Engberts en Copini (2016) voor een bredere schets van mogelijkheden van sensing-samenwerking.
139 Respondent 9.
140 Respondent 5 en Respondent 9. Dit idee staat uitgewerkt in Saxion Hogeschool (2019) onder de naam 'fusion centers', zoals deze in de Verenigde Staten bestaande samenwerking centra heten.
141 Respondent 3, respondent 5 en respondent 7. In Document 2 staat de mogelijkheid om de politie recherche vaste contactpersonen te geven bij de (grote) particuliere recherchebureaus.
142 Respondent 4.

15. **Verstrekkingsregime verruimen**. Particuliere recherchebureaus kunnen veel meer zaken (helpen) oplossen als zij meer informatie hebben. Voor gecertificeerde particuliere recherchebureaus zou het beleid om informatie te geven kunnen worden verruimd. Hierbij gaat het om concrete vragen aan de politie, maar ook de Rijksdienst voor het Wegverkeer en Justis (voor Verklaring Omtrent Gedrag-informatie). Nu wordt informatie soms informeel door de politie gedeeld.[143]

16. **Voorvallenregistratie.** Er werd in het verleden door particuliere recherchebureaus een lijst met antecedenten bijgehouden, zodat er kon worden vastgesteld of een persoon reeds in het verleden het voorwerp van een onderzoek was geweest. Bij de implementatie van AVG werd dit pad verlaten. Er kan nagedacht worden of een vergelijkbaar systeem wel in overeenstemming met de AVG kan worden gebracht. Tegelijkertijd moet er ook toegegeven worden dat er weinig resistentie was tegen het afschaffen van het systeem: het werd niet zo goed bijgehouden.[144] Een dergelijk systeem zou voor de politie interessant zijn. Aangegeven werd dat de politie wel geïnteresseerd zou zijn in met name een register van fraude en financiële criminaliteit, bijgehouden door particuliere recherchebureaus, dat ongemerkt door de politie kan worden geraadpleegd, ook om op basis daarvan extra informatie te vorderen.[145]

17. **Quid pro quo samenwerking.** Een mogelijk voorstel is nog dat informatie-uitwisseling tussen politie en private commerciële actoren deel uitmaakt van een voorwaardelijk systeem (eventueel in combinatie met hierboven geschetste structuren zoals aangiftesysteem, veiligheidsofficieren, etc.). De commerciële private actor zou dan informatie kunnen krijgen van de politie indien op het einde van het onderzoek alle onderzoeksresultaten terug overgeleverd worden aan de politie. De politie kan dan zelf beslissen of er verder wordt gewerkt op de resultaten van het dossier. Omdat dit in principe niet kan zonder toestemming van de klant (die vaak eigenaar is van de resultaten), wordt dit best geregeld via een wettelijke verplichting.[146] De commerciële actor heeft dan nog steeds een keuze: onderzoek doen zonder input vanuit de politie, of input krijgen van de politie en op het einde de onderzoeksresultaten delen.

4.4 Juridisch kader

4.4.1 Wetgeving inzake informatie-uitwisseling

In Nederland kunnen we een aantal wetten onderscheiden die van belang zijn voor informatie-uitwisseling tussen publieke en private (veiligheids-)actoren, en niet verwonderlijk gaat het daarbij vaak over bescherming van privacy en persoonlijke gegevens. De projecten verder in dit rapport tonen aan dat dit niet noodzakelijk de enige relevante wetten zijn; afhankelijk van het soort informatie-uitwisseling en de betrokken actoren, moet er ook naar andere wetten gekeken worden. Maar in eerste instantie gaat het over de volgende:

- **Politiewet**: hoofdstuk 2 van deze wet zet de krijtlijnen voor het uitvoeren van de politietaak. Informatie-uitwisseling gebeurt steeds binnen het kader van deze bevoegdheden.
- **Wet Particuliere Beveiligingsorganisaties en Recherchebureaus**): dit is de tegenhanger van de Politiewet, omdat deze de bevoegdheden kadert van particuliere beveiligingsorganisaties en recherchebureaus. Tegelijkertijd is het niet toevallig dat in dit rapport gesproken wordt over particuliere veiligheidsactoren, en de definitie die uit het theoretisch kader hierover komt, breder is dan de categorieën besproken in de WPBR. De politie kan informatie rond veiligheid uitwisselen met vele actoren, die veiligheidsvoorziening zowel als primaire als secundaire taak hebben. In dit project wordt geconcentreerd op actoren die veiligheidsvoorziening als primaire taak hebben, waarvoor we de benoeming "particuliere veiligheidsactor" gebruiken. Dan nog zijn er particuliere veiligheidsactoren die mogelijk niet vallen onder de WPBR, we denken dan bijvoorbeeld aan bedrijven die financiële audits uitoefenen om fraude op te sporen, of bedrijven die zich specialiseren in cyber security. Vaak hebben deze bedrijven wel een vergunning als particulier recherchebureau, maar het is duidelijk dat de WPBR niet geheel afgestemd is op de huidige noden van de maatschappij en de diensten die nu aan-

143 Respondent 1 en Respondent 4.
144 Respondent 4. Het aanleggen van zo'n register om te delen met de politie staat ook in Document 2.
145 Respondent 8.
146 Respondent 4.

geboden worden in het veld. Een diepgaande analyse van de WPBR valt buiten de scope van dit onderzoek, maar dient zich in deze wel aan.

- **Wet Politiegegevens**: informatie die door de politie of door andere actoren voor de politie verzameld wordt, valt onder de WPG. Paragraaf 2 van deze wet concentreert zich op de verwerking van gegevens door de politie zelf, dus hoe deze geanalyseerd mogen worden, mogelijk gecombineerd met andere gegevens ter verrijking, etc. Paragraaf 3 stelt de regels op in welke omstandigheden politiegegevens ook gedeeld kunnen worden met andere instanties. Artikelen 18, 19 en 20 zijn hierbij het meest relevant in het kader van dit project, namelijk het structureel, incidenteel of in het kader van een samenwerkingsverband delen van gegevens met derden. Er worden daarbij veel mogelijkheden gegeven aan de verwerkingsverantwoordelijke, in casu de politie, natuurlijk onder een aantal voorwaarden: een zwaarwegend algemeen belang, en met specifieke doeleinden in gedachten. Overleg met het bevoegde gezag, zijnde burgemeester, officier van justitie of Minister van Justitie en Veiligheid, is wel steeds wettelijk noodzakelijk. Deze artikelen lijken informatie-uitwisseling in het veld vaak af te schrikken. Meermaals wordt er gewaarschuwd dat informatie-uitwisseling "moeilijk is binnen de contouren van de WPG", maar in werkelijkheid blijkt er wel veel mogelijk te zijn, mits toestemming gekregen wordt van verschillende instanties. De wil van de verwerkingsverantwoordelijke, zijnde de politie, blijft echter een centrale rol spelen, een gegeven dat duidelijker mag gemaakt worden in het veld.
- **De Wet Justitiële en Strafvorderlijke Gegevens (WJSG)**: deze wet is van toepassing op een bijzondere categorie van gegevens, namelijk de gegevens die deel uitmaken van een strafrechtelijke procedure of het resultaat ervan zijn (bijvoorbeeld een veroordeling). Belangrijk hier is dat er in deze wet geen equivalent bestaat van de artikelen 18, 19 en 20 binnen de WPG: het delen van deze gegevens met derden is in principe geheel onmogelijk, ook niet voor het Openbaar Ministerie. Dat is een scherp contrast met politiegegevens, waar de verwerkingsverantwoordelijke wel uitgebreide mogelijkheden heeft tot delen met derden, zolang toestemming verkregen wordt van de bevoegde autoriteit. De WJSG laat wel een beperkte ruimte om alsnog tot informatie-uitwisseling te komen van deze bijzondere categorie van gegevens, namelijk art. 14 van de wet. Deze bepaalt dat de Minister van Justitie en Veiligheid in bijzondere gevallen (zwaarwegend algemeen belang en bijzondere doeleinden) toestemming kan geven. Uiteraard is dit een zware barrière voor uitwisseling.
- **Algemene Verordening Gegevensbescherming en Uitvoeringswet Algemene Verordening Gegevensbescherming**: de AVG is een Europese Richtlijn (in het Engels: General Data Protection Directive of GDPR) die in Nederland rechtstreeks van toepassing is, maar wel een aantal keuzes overlaat aan de Europese Lidstaten. Deze keuzeruimte is in Nederland ingevuld door de UAVG. Private actoren, inclusief de particuliere veiligheidsactoren waarvan sprake in dit project, zijn in het algemeen gehouden aan de beperkingen tot gegevensverzameling binnen de AVG en UAVG. Relevant hier zijn paragrafen 3.1 en 3.2. van de UAVG, die bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard behandelen. De regel is hier dat deze gegevens niet mogen verzameld worden, tenzij onder zeer specifieke gevallen (bijvoorbeeld bij strafrechtelijke gegevens indien de persoon over wie het gaat, hier uitdrukkelijk toestemming voor gegeven heeft of de gegevens zelf openbaar gemaakt heeft). Indien een particuliere veiligheidsactor dus gegevens verzamelt, zijn de AVG en UAVG van toepassing. Indien echter de gegevens verzameld worden in het kader van een samenwerkingsverband met de politie, is het mogelijk (en zelfs aannemelijk) dat het om gegevens gaat die vallen onder de WPG. Dat is een belangrijk onderscheid om te maken.

- **Wet Gegevensverwerking door Samenwerkingsverbanden:** het is moeilijk om de precieze impact of waarde van deze wet in te schatten, omdat ze nog het wetgevend proces aan het doorlopen is. De laatste activiteit hier rond is het voorlopig verslag van de Vaste Commissie voor Justitie en Veiligheid, vastgesteld op 18 februari 2022,[147] en de laatste versie van het wetsvoorstel dateert reeds van 17 december 2020.[148] Daarin worden een aantal kritische kanttekeningen gemaakt over de waarborgen voor het uitwisselen van informatie, die tot op heden niet beantwoord werden. Het voorstel kan mogelijk wel van belang zijn omdat het een juridische grondslag voorziet voor het systematisch delen en verwerken van persoonsgegevens binnen samenwerkingsverbanden. Algemene Maatregelen van Bestuur ter uitvoering van deze wet zouden dan de samenwerkingsverbanden identificeren die vallen onder de wet, het zwaarwegend algemeen belang dat zij dienen, de persoonsgegevens die binnen het verband verwerkt worden, en hoe deze verwerking gebeurt.[149] Bijzonder aan het wetsvoorstel is dat er vier samenwerkingsverbanden reeds impliciet in behandeld worden: het Financieel Expertisecentrum, de Infobox Crimineel en Onverklaarbaar Vermogen, de Regionale Informatie- en Expertisecentra, en de Zorg- en Veiligheidshuizen. De vraag kan gesteld worden of het niet nuttiger zou zijn een algemeen kader uit te werken in de wet, en dan via aparte algemene maatregelen van bestuur alle samenwerkingsverbanden te identificeren die onder de wet vallen. De onderliggende gedachte van de wetgeving is echter wel zeer nuttig: het samenbrengen van de regels voor en mogelijkheden binnen samenwerkingsverbanden tussen publieke en private actoren, met bijzondere aandacht voor de uitwisseling van gegevens tussen beide.

4.4.2 Wetgeving inzake de marktpositie van particuliere veiligheidsactoren die informatie krijgen

Er zijn twee mogelijkheden die moeten worden beschouwd wanneer een particuliere veiligheidsactor informatie uitwisselt met de Nationale Politie. De eerste is dat de uitwisseling resulteert in een economische machtspositie van één of meerdere particuliere veiligheidsactoren. In tegenstelling tot wat er vaak gedacht wordt, is het bekomen van een economische machtspositie op zich juridisch niet problematisch. Een normale marktwerking kan ertoe leiden dat een beperkt aantal actoren een groot deel van de markt beheersen. Enkel wanneer deze positie bekomen werd door overnames of fusies, stelt de Mededingingswet (MW) in art. 29 e.v. dat de Autoriteit Consument en Markt over een concentratietoezicht beschikt, waarbij boetes kunnen opgelegd worden. Wat wel strafbaar is onder art. 24 MW, is een misbruik van de economische machtspositie, waarbij het concurrentievermogen aangetast wordt. Voorbeelden daarvan zijn te hoge prijzen, koppelverkoop, verkoop van producten onder de kostprijs, etc.[150] Ook hier heeft de Autoriteit Consument en Markt een toezichtstaak om dit soort misbruik op te sporen en te bestraffen. Maar wat betreft informatie-uitwisseling, is het dus niet zo dat deze rechtstreeks en automatisch kan leiden tot ongeoorloofd gedrag vanwege de particuliere veiligheidsactor. Er kan een economische machtspositie verkregen worden, maar alleen indien deze ook misbruikt wordt, is er juridisch een probleem. Een veiligheidsactor die extra kosten voor het verkrijgen van informatie van de politie aan klanten doorberekent zou volgens deze redenering dus niet strafbaar zijn, de politie ook niet voor het leveren van deze informatie. Er mogen alleen geen onterecht hogere prijzen in rekening worden gebracht en de informatie mag niet gebruikt worden om concurrenten actief van de markt te weren.

147 Https://www.eerstekamer.nl/9370000/1/j9vvkfvj6b325az/vlqkofsu4ipm/f=y.pdf
148 Https://www.eerstekamer.nl/behandeling/20201217/gewijzigd_voorstel_van_wet_5/document3/f=/vlf9cih018x4_opgemaakt.pdf
149 Https://www.eerstekamer.nl/wetsvoorstel/35447_wet_gegevensverwerking_door
150 Https://www.rijksoverheid.nl/onderwerpen/mededinging/misbruik-van-een-economische-machtspositie

De tweede mogelijkheid is een grotere barrière om tot uitwisseling te komen: de informatie-uitwisseling kan ook gezien worden als staatssteun, wat in principe verboden is onder art. 107 lid 1 van het Verdrag betreffende de Werking van de Europese Unie (VWEU). Bij verboden staatssteun krijgt een bedrijf een economisch voordeel, maar dit voordeel hoeft niet noodzakelijk de vorm te hebben van een geldbedrag; het verkrijgen van informatie kan er dus onder vallen. Voor verboden staatssteun moet er aan vijf voorwaarden voldaan worden. Ten eerste moet de steun verleend worden aan een onderneming die een economische activiteit verricht, wat hier het geval is. De tweede voorwaarde is dat de steun door staatsmiddelen bekostigd wordt. Omdat de informatie door de politie verzameld werd op basis van activiteiten door hen uitgevoerd, kan gesteld worden dat het om staatsmiddelen gaat. Ten derde moet de maatregel de potentie hebben om de Europese mededinging op een ongunstige manier te beïnvloeden. Dit is enkel het geval indien particuliere veiligheidsactoren zonder vestiging in Nederland (maar wel met een vergunning zoals vastgelegd in art. 2, eerste lid WPBR) uitgesloten worden van de mogelijkheid tot informatie-uitwisseling. Dit is een keuze die zou kunnen gemaakt worden. Het huidige wettelijke kader maakt geen onderscheid tussen binnenlandse of buitenlandse derden, maar wat betreft particuliere veiligheidsactoren kan door de politie de keuze gemaakt worden om enkel met Nederlandse bedrijven informatie uit te wisselen. Het valt aan te raden dit niet te doen, want dan kan er al geen sprake meer zijn van verboden staatssteun, maar we bespreken toch ook de andere cumulatieve voorwaarden. De vierde voorwaarde is dat de staatsmiddelen een economisch voordeel verschaffen dat niet via normale commerciële weg zou zijn verkregen (non-marktconformiteit). Deze voorwaarde kan vervuld worden onafhankelijk of de particuliere veiligheidsactor bij de informatie-uitwisseling betaalt voor de informatie, betaald wordt voor de informatie, of de informatie om niet verkrijgt. Indien de particuliere veiligheidsactor betaald wordt, kan de betaling als non-marktconform gelden indien niet via een aanbestedingsprocedure gewerkt werd. Indien de particuliere veiligheidsactor betaalt, kan dit non-marktconform zijn indien de betaling niet evenredig is aan het ontvangen voordeel, tenzij alle bedrijven (niet enkel particuliere veiligheidsactoren) hetzelfde voordeel kunnen bekomen. En indien de uitwisseling om niet gebeurt, kan dit opnieuw als non-marktconform gezien worden indien niet alle andere bedrijven ook van deze mogelijkheid gebruik kunnen maken. Tenslotte is er nog de vijfde voorwaarde, namelijk dat de maatregel selectief is: het geldt voor één of een beperkte groep van ondernemingen, of een specifieke sector. Dus opnieuw, indien enkel particuliere veiligheidsactoren de voordelen krijgen, kan er sprake zijn van verboden staatssteun.

Er moet op gewezen worden dat voor verboden staatssteun aan alle vijf hier geschetste voorwaarden voldaan moet zijn. De eerste twee voorwaarden zijn altijd voldaan, maar afhankelijk van de manier waarop een project rond informatie-uitwisseling opgezet wordt, zijn er voldoende manieren om te vermijden dat de uitwisseling op basis van de andere drie voorwaarden als verboden staatssteun wordt gezien. Desalniettemin moet hier rekening mee gehouden worden bij de opzet.

4.4.3 Wetgeving inzake de verplichtingen van klant of particuliere veiligheidsactor om informatie te leveren

Zoals in het begin van het onderzoek gesteld, is het mogelijk dat informatie waar de particuliere veiligheidsactor over beschikt en die nuttig is om te delen met de politie, niet de eigendom is van de particuliere veiligheidsactor, maar van diens klant. Bij afwezigheid van enige contractuele afspraken, is er geen eigendomsoverdracht van deze informatie. Meer nog, art. 13 lid 1 WPBR voorziet dat werknemers van particuliere veiligheidsactoren die gegevens verkrijgen tijdens hun werkzaamheden waarvan ze weten of redelijkerwijs vermoeden dat ze vertrouwelijk zijn, verplicht deze gegevens ook geheim te houden, wat opnieuw toont dat de wetgever het eigendom van deze gegevens bij de klant heeft gelaten. De toestemming van de klant is dus nodig om deze informatie te delen. De uitgewerkte projecten verder in het rapport tonen steeds de meerwaarde aan voor de klant wanneer dit relevant is. De idee erachter is dat wanneer een meerwaarde kan aangetoond worden, de klant een incentive heeft om via de contractuele overeenkomst met de particuliere veiligheidsactor akkoord te geven dat deze de relevante informatie kan delen. Er kunnen echter alternatieve redenen zijn waarom een klant, zelfs indien er voordelen verbonden zijn aan informatie-uitwisseling, ervoor kiest om informatie niet met de politie te delen. In dat geval kan het nuttig zijn dat de klant of de particuliere veiligheidsactor op één of andere manier wettelijk gehouden is tot het meedelen van informatie aan de politie.

Deze verplichting wordt in het huidige wettelijke kader niet voorzien, zelfs niet indien het gaat om strafbare feiten. Dit terwijl art. 13 lid 1 wel voorziet dat de geheimhoudingsplicht er niet is wanneer een wettelijk voorschrift de bekendmaking van de gegevens verplicht. In tegenstelling tot bijvoorbeeld België, waar art. 30 van het Wetboek van Strafvordering alle bur-

gers verplicht om misdaden (met uitzondering van kleinere overtredingen) aan te geven aan de politie wanneer zij daarvan getuige zijn, is dit in Nederland veel meer een mogelijkheid in plaats van een verplichting. Wat betreft burgers geldt in Nederland art. 161 Sv., dat bepaalt dat burgers bevoegd zijn om aangifte te doen. Een verplichting wordt enkel opgelegd bij moord of doodslag, verkrachting, en terrorisme, dit op basis van art. 160 Sv. Ook binnen de WPBR wordt een mogelijkheid geopend om informatie met een vertrouwelijk karakter toch aan de politie te geven indien de gegevens betrekking hebben op een strafbaar feit, dit in art. 13 lid 3. Opnieuw gaat het om een bevoegdheid, niet om een verplichting. Hoewel dit niet expliciet in de WPBR staat, kan er aangenomen worden dat de uitzonderingen in art. 160 Sv., waardoor er wel een verplichting ontstaat, ook hier gelden. Dit betekent niet dat er in Nederland buiten art. 160 Sv. voor burgers geen verplichtingen bestaan om gegevens te verstrekken aan de politie. Wanneer zij als getuige verhoord worden, zijn burgers op basis van art. 215 Sv. gehouden om de waarheid te vertellen. Enkel een verdachte kan zich beroepen op het zwijgrecht voorzien in art. 29 lid 2 Sv. Beide geldt dus ook voor medewerkers van particuliere veiligheidsactoren wanneer zij werken voor hun klant.

Een verhoor vindt echter plaats in het kader van een opsporingsonderzoek, dus de politie moet al op de hoogte zijn van het bestaan van mogelijk strafbare feiten. Het zou beter zijn indien er op de particuliere veiligheidsactoren wel een verplichting zou vallen om strafbare feiten aan te geven, zelfs indien deze vertrouwelijk zijn, en het eigendom ervan formeel bij de klant ligt. Indien art. 13 lid 3 WPBR aangepast wordt van een bevoegdheid naar een verplichting, kan dit de particuliere veiligheidsactor uit deze huidige lastige omstandigheid helpen. Want op dit moment zal de politie enerzijds verwachten dat er aangifte zal gedaan worden van alle strafbare feiten waar de werknemers van particuliere veiligheidsactoren weet van krijgen, omdat zij bevoegd zijn om dit te doen. Anderzijds zal de klant mogelijk verwachten dat er niet naar de politie gestapt wordt, omdat er op de particuliere veiligheidsactor geen verplichting rust. Door wel een verplichting in te voeren, kan er met de klant overlegd worden hoe de informatie zal doorgespeeld worden naar de politie (de particuliere veiligheidsactor kan de klant hierin dan begeleiden), maar hoeft niet langer de vraag gesteld worden of de informatie doorgespeeld mag worden.

5. FASE 2: RESULTATEN VRAGENLIJST

5.1 Keuze top-prioriteiten

De antwoorden op de vragenlijsten werden na ontvangst geanalyseerd. Daaruit kwamen de resultaten in onderstaande tabel naar voren. Links de tabel met projecten gerangschikt op een combinatie van de criteria efficiëntie/effectiviteit, haalbaarheid en maatschappelijke wenselijkheid. Rechts staan de projecten gerangschikt naar complexiteit/relevantie. Zoals de tabel toont, leek er in het algemeen vrij veel convergentie tussen de inhoudelijke criteria en de complexiteit/relevantie voor het onderzoek. Het sensing-aanvraagpunt staat wel een stuk lager in de complexiteit/relevantie voor het onderzoek, maar werd ogenschijnlijk zowel door de politie als door particuliere veiligheidsactoren zeer hoog gescoord op basis van de inhoudelijke criteria, en werd daarom toch meegenomen. De projecten "heterdaad omgevingssensoren" en "stimuleren privaat-private samenwerking" (geel) staan in deze tabel hoog bij de inhoudelijke criteria, maar vrij laag bij de complexiteit/relevantie voor het onderzoek, en er werd daarom besloten om de eerstvolgende projecten op de lijst mee te nemen in plaats van deze. Het project "beveiligingssoftware leveranciers" (oranje) had een hoge complexiteit/relevantie voor het onderzoek, maar scoorde volgens de oorspronkelijke berekeningen lager op de inhoudelijke criteria. De projecten in het groen zijn de top-prioriteiten die zijn geselecteerd door de onderzoekers. Gekozen is om deze te beperken tot vijf projecten, zodat de deelnemers aan het seminar in de volgende fase zich konden focussen op een beperkt aantal projecten.

Inhoudelijke criteria		Complexiteit/Relevantie voor het onderzoek
Sensing-aanvraagpunt (11)		Gevaarsindicatie(5)
Mobiele sensing-platforms (8)		Beveiligingssoftware leveranciers (3)
Heterdaad omgevingssensoren (6)		Mobiele sensing-platforms (8)
Evenementen systeem (4)		Evenementen systeem (4)
Stimuleren Privaat-Private samenwerking (12)		Opsporingsindicatie (9)
Gevaarsindicatie (5)		Bedreigingsdossiers (2)
Opsporingsindicatie (9)		Veiligheidsofficier (14)
Bedreigingsdossiers (2)		Proeftuin PPS (10)
Meld Misdaad Anoniem (7)		Aangiftesysteem (1)
Veiligheidsofficier (14)		Heterdaad omgevingssensoren (6)
Proeftuin PPS (10)		Sensing-aanvraagpunt (11)
Beveiligingssoftware leveranciers (3)		Stimuleren Privaat-Private samenwerking (12)
Verstrekkingsregime verruimen (15)		Meld Misdaad Anoniem (7)
Quid pro quo samenwerking (17)		Quid pro quo samenwerking (17)
Trends delen (13)		Verstrekkingsregime verruimen (15)
Aangiftesysteem (1)		Voorvallenregistratie (16)
Voorvallenregistratie (16)		Trends delen (13)

Tabel 1: projecten gerangschikt volgens inhoudelijke criteria en complexiteit/relevantie voor het onderzoek, eerste berekening.

Bij het samenstellen van het eindrapport werden de gemaakte berekeningen wat betreft efficiëntie/effectiviteit, haalbaarheid, maatschappelijke wenselijkheid en complexiteit/relevantie nog een laatste keer nagekeken. Daarbij kwam aan het licht dat een fout bij het instellen van Excel ertoe geleid heeft dat de verschillende projecten wat betreft haalbaarheid en maatschappelijke wenselijkheid van laag naar hoog waren gerangschikt en niet van hoog naar laag (zoals bij efficiëntie/effectiviteit en complexiteit/relevantie). De rangschikking wat betreft complexiteit/relevantie bleef ongewijzigd. Een herberekening kwam tot een nieuwe rangschikking, waarbij het doorgeven van de gevaarsindicatie en het *real-time* doorgeven van informatie tijdens events nog steeds tot de top-prioriteiten behoren, maar deze verder bestond uit publiek-private recherche samenwerking, het creëren van een apart meldings/aangiftesysteem voor particuliere veiligheidsactoren, en het creëren van veiligheidsofficieren binnen particuliere veiligheidsactoren. Dit komt ook sterk overeen met de top-prioriteiten indien enkel naar de scores wordt gekeken vanuit de politie of vanuit particuliere veiligheidsactoren. De hoogst scorende projecten op basis van inhoudelijke criteria door de politie tonen wel dat er ook interesse is in het verkrijgen van klantendossiers, terwijl de particuliere veiligheidsactoren meer selectief willen zijn in het kiezen welke gegevens zij willen delen met de politie, en dit ook gedeeltelijk anoniem willen doen. Zie ANNEX V voor een vergelijking.

Bij deze berekening waren er ook grotere verschillen tussen inhoudelijke criteria en complexiteit/relevantie voor het onderzoek. De hoogst gerangschikte projecten wat betreft inhoudelijke criteria hadden net een vrij lage complexiteit. Dit creëert opportuniteiten om deze projecten op korte termijn te implementeren. Een aantal projecten met een hoge complexiteit scoorden net laag op inhoudelijke criteria, en deze zijn dus minder interessant om in de praktijk uit te werken (zelfs al zijn ze binnen dit project wel verder geanalyseerd). Op basis daarvan werd onderstaande tabel opgebouwd.

Inhoudelijke criteria		Relevantie voor het onderzoek
Trends delen (13)		Gevaarsindicatie (5)
Verstrekkingsregime verruimen (15)		Beveiligingssoftware leveranciers (3)
Voorvallenregistratie (16)		Mobiele sensing-platforms (8)
Gevaarsindicatie (5)		Evenementen systeem (4)
Veiligheidsofficier (14)		Opsporingsindicatie (9)
Proeftuin PPS (10)		Bedreigingsdossiers (2)
Aangiftesysteem (1)		Veiligheidsofficier (14)
Evenementen systeem (4)		Proeftuin PPS (10)
Meld Misdaad Anoniem (7)		Aangiftesysteem (1)
Stimuleren Privaat-Private samenwerking (12)		Heterdaad omgevingssensoren (6)
Quid pro quo samenwerking (17)		Sensing-aanvraagpunt (11)
Heterdaad omgevingssensoren (6)		Stimuleren Privaat-Private samenwerking (12)
Beveiligingssoftware leveranciers (3)		Meld Misdaad Anoniem (7)
Opsporingsindicatie (9)		Quid pro quo samenwerking (17)
Bedreigingsdossiers (2)		Verstrekkingsregime verruimen (15)
Sensing-aanvraagpunt (11)		Voorvallenregistratie (16)
Mobiele sensing-platforms (8)		Trends delen (13)

Tabel 2: projecten gerangschikt volgens inhoudelijke criteria en complexiteit/relevantie voor het onderzoek, herberekening.

Uit de scores zelf, te vinden in ANNEX V, kunnen nog een aantal interessante observaties gemaakt worden. Zo zagen de particuliere veiligheidsactoren in het algemeen meer efficiëntiewinsten in de verschillende projecten dan de politie (de gemiddelde score voor efficiëntie/effectiviteit lag hoger), terwijl diezelfde particuliere actoren de technische haalbaarheid van de projecten gemiddeld ook hoger inschatten. Ook de spreiding lag verschillend: bij de politie kon een grote middenmoot onderscheiden worden samen met enkele zeer hoge en zeer laag gescoorde projecten, terwijl bij de particuliere veiligheidsactoren de scores dichter bij elkaar lagen. Bij de maatschappelijke wenselijkheid vinden we hogere scores terug bij de politie, en opnieuw een bredere spreiding van de scores voor de projecten, inclusief enkele zeer lage scores. Dat betekent niet noodzakelijk dat de particuliere veiligheidsactoren minder waarde hechten aan maatschappelijke wenselijkheid, maar indiceert wel dat de politie toch een grotere maatschappelijke wenselijkheid ziet in het uitvoeren van projecten die informatie-uitwisseling bevorderen. Bij de complexiteit/relevantie voor het onderzoek komt dezelfde balans naar voren als bij de technische haalbaarheid: de politie geeft gemiddeld hogere scores, wat betekent dat zij geloven dat de uitvoering van het project een grotere mate van complexiteit heeft (maar daarom ook meer relevant is om het in het kader van dit onderzoek verder te analyseren), en er is een grotere spreiding van de scores.

De materiële fout had gevolgen voor de keuze van de uitgewerkte projecten, maar niet op de methodologie of op de manier waarop randvoorwaarden gecreëerd kunnen worden (dus door gebruik te maken van een brainstormsessie en door de zorgen in de survey verder uit te werken). Het is dus mogelijk om de 3 projecten die met de correcte berekening wel de top 5 zouden gehaald hebben, op dezelfde manier uit te werken. Tegelijkertijd is het interessant om aan te tonen dat projecten die ook lager scoorden op de inhoudelijke criteria, via een analyse van de zorgen verder uitgewerkt kunnen worden. Uiteindelijk werd beslist om de oorspronkelijk geanalyseerde top 5 te behouden, en zo het project niet verder uit te stellen. Het tonen van de werking van de methodologie stond derhalve voorop, zeker bij de drie projecten die uiteindelijk inhoudelijk lager bleken gescoord te hebben.

5.2 *Geuite zorgen in de vragenlijst*

In de vragenlijst werd tevens de kans gegeven aan de experts om per project een aantal zorgen te uiten. Onderstaand is een overzicht van deze geuite zorgen, en bij welke projecten deze geuit werden. Omdat de survey gegevens anoniem uit het systeem kwamen, kon van antwoorden zoals 'zie opmerking bij vorig punt' niet worden achterhaald op welk additioneel project deze geuite zorg van toepassing was. Hierdoor zijn een aantal zorgpunten vaker in de survey genoemd dan in deze analyse kon geattribueerd worden. Sommige zorgen werden ook door meer dan één gesurveyerde bij één voorstel genoemd. In deze gevallen is de zorg maar één keer in het overzicht opgenomen. Ook dit resulteert in een lichte ondervertegenwoordiging. In een klein aantal gevallen kon in een opmerking bij een surveyvraag niet duidelijk een zorg worden herkend. Deze opmerkingen zijn niet verzameld en gebruikt.

De geuite zorgen worden gegroepeerd in verschillende categorieën. Deze vormen ook de input om voor de top-prioriteiten in het volgende hoofdstuk de randvoorwaarden te bespreken.

5.2.1 De informatie zelf moet voldoende waardevol zijn

1. Het is noodzakelijk dat informatie die wordt uitgewisseld, ook actueel is.[151]
2. Er zijn situaties waar het delen van informatie tot nadelen leidt die disproportioneel zijn tegenover de voordelen ervan, en dus moet er ook een keuze zijn om geen informatie te delen.[152]
3. Er moet op één of andere manier kunnen aangetoond worden (op termijn) dat de informatie-uitwisseling ook effectief, onveiligheid, criminaliteit, etc, vermindert.[153]
4. Het moet duidelijk zijn welke informatie als relevant gezien wordt door betrokken partijen, zodat er geen niet-bruikbare informatie wordt ontvangen en er teleurstelling ontstaat.[154]

151 Deze zorg werd geuit bij voorstel 2 (Bedreigingsdossiers).
152 Deze zorg werd geuit bij de voorstellen 6 (Heterdaad omgevingssensoren) en 11 (Sensing-aanvraagpunt).
153 Deze zorg werd geuit bij de voorstellen 1 (Aangiftesysteem), 2 (Bedreigingsdossiers), 3 (Beveiligingssoftware leveranciers), 7 (Meld Misdaad Anoniem), 14 (Veiligheidsofficier) en 16 (Voorvallenregistratie).
154 Deze zorg werd geuit bij de voorstellen 2 (Bedreigingsdossiers) en 10 (Proeftuin PPS).

5. De kwaliteit van de informatie moet voldoende hoog zijn. Dat betekent mogelijk dat er moet gescreend worden of de informatie wel geschikt is voor het doel het gedeeld zou worden, of mogelijk moet opgeschoond worden.[155]
6. De uitgewisselde informatie mag geen onnodige details bevatten.[156]
7. Er moet opgepast worden voor function creep, waardoor er steeds meer informatie uitgewisseld wordt, zonder dat de meerwaarde daarvan ook steeds duidelijk is.[157]
8. Er mag geen overload aan informatie zijn, want dan kan de uitgewisselde informatie niet correct geduid worden.[158]
9. Er mag niet gefixeerd worden op informatie-uitwisseling als instrument. Soms kan inhuur van capaciteit door de politie een betere optie zijn.[159]
10. De uitgewisselde informatie mag geen onnodige details bevatten die de particuliere beveiliging niet wil of moet weten.[160]
11. Informatie-uitwisseling kost ook tijd en mogelijk geld, wat mogelijk niet vergoed wordt. Op één of andere manier moet het wel waard zijn voor de politie en particuliere veiligheidsactoren om deze tijd toch te besteden.[161]
12. Er moet een manier zijn om de credibiliteit van de informatie te verifiëren, zelfs als deze anoniem verstrekt werd.[162]

5.2.2 Er moet gewaakt worden voor oneigenlijk gebruik

1. De focus van de informatie-uitwisseling moet liggen op het vergroten van de publieke veiligheid. Particuliere veiligheidsactoren mogen aan hun medewerking geen andere belangen koppelen die daar niet toe bijdragen.[163]
2. De particuliere veiligheidsactoren waar informatie gedeeld mee wordt, mogen daarmee geen bevoordeelde marktpositie krijgen.[164]
3. Er moeten waarborgen zijn dat uitgewisselde gegevens niet gebruikt worden voor andere processen of door andere delen van de ontvangende organisatie.[165]
4. Er moeten beschermingen ingebouwd worden zodat enkel geautoriseerde personen bij de gedeelde informatie kunnen.[166]
5. Het maken van kosten door particuliere veiligheidsactoren om informatie ter beschikking te stellen, mag er niet toe leiden dat er wederkerigheid ontstaat in de relatie.[167]
6. Informatie-uitwisseling moet steeds bewust gebeuren, er mag geen informatie onbedoeld gedeeld worden.[168]

5.2.3 De juiste actoren moeten betrokken worden

1. Er moet mee rekening gehouden worden dat er ook andere organisaties/bedrijven kunnen zijn dan particuliere veiligheidsactoren waar informatie mee kan gedeeld worden.[169]
2. De informatie-uitdeling hoeft niet noodzakelijk (alleen) met de politie te zijn, er zijn ook mogelijke andere actoren zoals het Openbaar Ministerie, de burgemeester of de rechter-commissaris, met wie contact kan worden gezocht of een samenwerking opgezet kan worden.[170]
3. De informatie moet niet noodzakelijk van de particuliere veiligheidsactoren komen, maar mogelijk ook van particulieren, bijvoorbeeld de eigenaars van een locatie, de bedreigde of de klant die beveiliging heeft ingehuurd, etc.[171]

155 Deze zorg werd geuit bij de voorstellen 5 (Gevaarsindicatie), 8 (Mobiele sensing-platforms) en 16 (Voorvallenregistratie).
156 Deze zorg werd geuit bij voorstel 9 (Opsporingsindicatie).
157 Deze zorg werd geuit bij de voorstellen 10 (Proeftuin PPS) en 12 (Stimuleren Privaat-Privaat samenwerking).
158 Deze zorg werd geuit bij voorstel 6 (Heterdaad omgevingssensoren).
159 Deze zorg werd geuit bij voorstel 8 (Mobiele sensing-platforms).
160 Deze zorg werd geuit bij voorstel 9 (Opsporingsindicatie).
161 Deze zorg werd geuit bij de voorstellen 1 (Aangiftesysteem), 2 (Bedreigingsdossiers), 7 (Meld Misdaad Anoniem), 10 (Proeftuin PPS) en 13 (Trends delen).
162 Deze zorg werd geuit bij voorstel 3 (Beveiligingssoftwareleveranciers).
163 Deze zorg werd geuit bij de voorstellen 1 (Aangiftesysteem), 7 (Meld Misdaad Anoniem) en 10 (Proeftuin PPS).
164 Deze zorg werd geuit bij de voorstellen 4 (Evenementen systeem), 5 (Gevaarsindicatie) en 6 (Heterdaad omgevingssensoren).
165 Deze zorg werd geuit bij de voorstellen 2 (Bedreigingsdossiers) en 17 (Quid pro quo samenwerking).
166 Deze zorg werd geuit bij voorstel 4 (Evenementen systeem).
167 Deze zorg werd geuit bij voorstel 11 (Sensing-aanvraagpunt).
168 Deze zorg werd geuit bij voorstel 4 (Evenementen systeem).
169 Deze zorg werd geuit bij voorstel 7 (Meld Misdaad Anoniem).
170 Deze zorg werd geuit bij voorstel 11 (Sensing-aanvraagpunt).
171 Deze zorg werd geuit bij voorstel 8 (Mobiele sensing-platforms).

4. De toestemming van de klant moet vaak ook bekomen worden. Deze is in vele gevallen de eigenaar van de informatie (bijvoorbeeld bij camerasystemen).[172]

5.2.4 Geen negatieve impact op de werkzaamheden van de betrokken actoren

1. Het delen van informatie met particuliere veiligheidsactoren mag andere activiteiten van de politie niet hinderen, verstoren of onmogelijk maken.[173]
2. Het delen van informatie mag niet leiden tot meer risicovol gedrag door werknemers van particuliere veiligheidsactoren, waardoor zij ook taken gaan uitvoeren die voorbehouden moeten zijn aan de politie.[174]
3. De klanten van particuliere veiligheidsactoren kunnen mogelijk de informatie-uitwisseling beletten, omdat dit niet in hun belang is omwille van ongewenste publiciteit, meer administratieve/managementtijd, etc.[175]
4. De informatie-uitdeling mag niet leiden tot een beïnvloeding van de objectiviteit van een onderzoek/werkzaamheden.[176]
5. De informatie-uitwisseling mag geen strafrechtelijke onderzoeken in gevaar brengen. Indien de politie of de particuliere veiligheidsactor bijvoorbeeld verplicht wordt om personen over wie informatie gedeeld wordt, te informeren, dan is dit een risico.[177]
6. Klanten van de particuliere veiligheidsactoren mogen niet benadeeld worden door de uitwisseling van informatie.[178]

5.2.5 Geen negatieve impact op de reputatie van de betrokken actoren

1. Particuliere veiligheidsactoren moeten opletten dat hun reputatie bij burgers niet geschaad wordt door het delen van informatie met de politie.[179]
2. De informatie-uitwisseling kan de relatie tussen de particuliere veiligheidsactor en de klant/markt mogelijk schaden.[180]
3. De verhouding/relatie tussen politie en burger mag niet aangetast worden door de informatie-uitwisseling.[181]

5.2.6 Het systeem moet voldoende waarborgen bevatten en bruikbaar zijn

1. De particuliere veiligheidsactoren of hun medewerkers zouden anoniem moeten kunnen blijven bij het aangeven van informatie aan de politie.[182]
2. Informatie-uitwisseling moet voorbehouden worden aan betrouwbare partners. Er moet dus een mogelijkheid tot uitsluiting zijn in het informatiesysteem.[183]
3. Indien er al een bestaand systeem manier van informatie-uitwisseling voorhanden is, is het nuttig om indien mogelijk hier gebruik van te maken bij de nieuwe vorm van informatie-uitwisseling.[184]
4. Een informatie-uitwisselingssysteem moet ook voldoende eenvoudig zijn om bruikbaar te zijn. Er is een gevaar dat indien informatie constant moet gefilterd worden op beschikbaarheid, de instellingen te complex worden.[185]

172 Deze zorg werd geuit bij de voorstellen 2 (Bedreigingsdossiers), 11 (Sensing-aanvraagpunt) en 13 (Trends delen).
173 Deze zorg werd geuit bij voorstel 5 (Gevaarsindicatie).
174 Deze zorg werd geuit bij de voorstellen 3 (Beveiligingssoftwarel everanciers) en 5 (Gevaarsindicatie).
175 Deze zorg werd geuit bij de voorstellen 1 (Aangiftesysteem) en 2 (Bedreigingsdossiers).
176 Deze zorg werd geuit bij voorstel 16 (Voorvallenregistratie).
177 Deze zorg werd geuit bij voorstel 2 (Bedreigingsdossiers).
178 Deze zorg werd geuit bij voorstel 8 (Mobiele sensing-platforms).
179 Deze zorg werd geuit bij voorstel 7 (Meld Misdaad Anoniem).
180 Deze zorg werd geuit bij voorstel 1 (Aangiftesysteem).
181 Deze zorg werd geuit bij voorstel 1 (Aangiftesysteem).
182 Deze zorg werd geuit bij voorstel 3 (Beveiligingssoftware leveranciers).
183 Deze zorg werd geuit bij de voorstellen 3 (Beveiligingssoftware leveranciers) en 15 (Verstrekkingsregime verruimen).
184 Deze zorg werd geuit bij de voorstellen 6 (Heterdaad omgevingssensoren), 7 (Meld Misdaad Anoniem), 11 (Sensing-aanvraagpunt), 14 (Veiligheidsofficier) en 16 (Voorvallenregistratie).
185 Deze zorg werd geuit bij voorstel 13 (Trends delen).

5. In de mate van het mogelijke zou informatie-uitwisseling geautomatiseerd moeten verlopen, om werknemers niet van hun reguliere werkzaamheden af te houden.[186]

6. De uitwisseling van informatie moet steeds traceerbaar zijn, het moet vastgelegd worden wat er gedeeld werd.[187]

7. Systemen die gebruikt worden voor informatie-uitwisseling moeten steeds verder geoptimaliseerd worden. Indien het om elektronische systemen gaat, zou het goed zijn om automatische updates te krijgen.[188]

8. Het is noodzakelijk een bewaartermijn te hebben voor de gedeelde informatie.[189]

9. Het is mogelijk dat er meer dan één informatie-uitwisselingssysteem is, waardoor de betrokken actoren op de verschillende systemen moeten worden aangesloten, of er een apart protocol moet uitgewerkt worden.[190]

10. Niet alleen de informatie-uitwisseling zelf moet op een veilige manier kunnen gebeuren, ook de opslag van de informatie nadien moet veilig zijn.[191]

11. Het uitgewerkte systeem moet noodzakelijk zijn om informatie te krijgen, zeker vanuit de politie. Deze heeft reeds een aantal andere mogelijkheden om informatie te verzamelen. Indien het op een andere manier kan, heeft het weinig nut een heel systeem op te zetten.[192]

5.2.7 Er moet voldoende kennis/ expertise aanwezig zijn

1. De specifieke mogelijkheid/het project van informatie-uitwisseling moet voldoende bekend zijn bij alle betrokken partijen.[193]

2. Ontvangen informatie moet op een discrete manier gebruikt worden.[194]

3. Er moet ook specifieke expertise aangetrokken worden bij zowel politie als particuliere veiligheidsactoren om op een correcte manier informatie uit te wisselen.[195]

4. Het moet duidelijk zijn met wie (tot op het niveau van de werknemer) er informatie kan gedeeld worden, dit door zowel politie als particuliere veiligheidsactor. Een speciale status of veiligheidspas kan hier helpen.[196]

5. Er moet voldoende kennis zijn welke informatie vooral wel mag gedeeld worden met elkaar. Nu gaat men vaak uit van het tegengestelde (dat er nauwelijks tot geen informatie mag gedeeld worden).[197]

6. Er zou een vaste contactpersoon moeten zijn bij de betrokken partijen, met back-ups.[198]

5.2.8 Er moet voldoende capaciteit aanwezig zijn

1. Er moet voldoende capaciteit zijn bij de politie om (goed) gebruik te maken van de extra informatie die de uitwisseling met de particuliere veiligheidsactoren oplevert, en voldoende tijd om (realtime) informatie toe te voegen.[199]

186 Deze zorg werd geuit bij voorstel 10 (Proeftuin PPS).
187 Deze zorg werd geuit bij voorstel 4 (Evenementen systeem).
188 Deze zorg werd geuit bij voorstel 10 (Proeftuin PPS).
189 Deze zorg werd geuit bij de voorstellen 4 (Evenementen systeem) en 8 (Mobiele sensing-platforms).
190 Deze zorg werd geuit bij de voorstellen 9 (Opsporingsindicatie), 11 (Sensing-aanvraagpunt) en 13 (Trends delen).
191 Deze zorg werd geuit bij de voorstellen 1 (Aangiftesysteem), 2 (Bedreigingsdossiers), 4 (Evenementen systeem), 9 (Opsporingsindicatie), 10 (Proeftuin PPS), 11 (Sensing-aanvraagpunt) en 17 (Quid pro quo samenwerking).
192 Deze zorg werd geuit bij de voorstellen 2 (Bedreigingsdossiers), 4 (Evenementen systeem), 7 (Meld Misdaad Anoniem) en 13 (Trends delen).
193 Deze zorg werd geuit bij voorstel 1 (Aangiftesysteem).
194 Deze zorg werd geuit bij voorstel 5 (Gevaarsindicatie).
195 Deze zorg werd geuit bij voorstel 12 (Stimuleren Privaat-Privaat samenwerking).
196 Deze zorg werd geuit bij voorstel 14 (Veiligheidsofficier).
197 Deze zorg werd geuit bij de voorstellen 4 (Evenementen systeem) en 9 (Opsporingsindicatie).
198 Deze zorg werd geuit bij de voorstellen 1 (Aangiftesysteem), 3 (Beveiligingssoftware leveranciers) en 14 (Veiligheidsofficier).
199 Deze zorg werd geuit bij de voorstellen 1 (Aangiftesysteem), 2 (Bedreigingsdossiers), 3 (Beveiligingssoftware leveranciers), 4 (Evenementen systeem), 7 (Meld Misdaad Anoniem) en 11 (Sensing-aanvraagpunt).

2. Er moet voldoende budget zijn voor samenwerking en informatie-uitwisseling.[200]

3. Indien er systemen/toestellen moeten geleverd worden om de informatie-uitwisseling mogelijk te maken, moeten deze ook voldoende voorradig zijn.[201]

5.2.9 Er moet voldoende en een volgehouden wil aanwezig zijn

1. Particuliere veiligheidsactoren zullen tot op zekere hoogte hun concurrentie met elkaar moeten kunnen overstijgen, anders kan er niet samengewerkt worden.[202]

2. Er kan enkel door alle betrokken personen belang gehecht worden aan uitwisseling van informatie indien de informatie ook effectief van verschillende kanten komt.[203]

3. De informatie-uitwisseling moet nut hebben; het mag geen overbodige exercitie worden.[204]

4. Indien het nodig is voor de klant om toestemming te geven om informatie te delen, is er een risico dat dit enkel zal gebeuren indien de klant voldoende ingedekt is. Dit kan leiden tot ongelijke verhoudingen.[205]

5. Het is nodig om aan verwachtingsmanagement te doen. Niet elke zaak waar informatie over uitgewisseld wordt, zal ook even hoge prioriteit krijgen van de politie. Indien er geen correct verwachtingsmanagement is, zal dit leiden tot onrust bij de particuliere veiligheidsactoren. [206]

6. Het uitwisselen van informatie mag niet op zichzelf staan, er moet een follow-up zijn die ook bewaakt wordt door alle betrokken actoren.[207]

7. Er moet een zekere bestendigheid zijn in het uitwisselen van de informatie. Naar alle waarschijnlijkheid zullen zowel politie als particuliere veiligheidsactoren tijd en middelen besteden aan het opzetten van systemen, dat heeft minder nut indien daar slechts een korte tijd gebruik van gemaakt wordt.[208]

5.2.10 Het juridisch kader moet voldoende duidelijk zijn

1. Het huidige wettelijke kader moet voldoende duidelijk zijn en ook waarborgen bieden dat informatie-uitwisseling niet zal leiden tot een aantasting van de democratische rechtsstaat.[209]

2. Er moeten duidelijk afspraken zijn over de informatie-uitwisseling.[210]

3. De informatie-uitwisseling moet altijd gebeuren met respect voor zowel privacy van individuen als vertrouwelijkheid van (bedrijfs)gegevens.[211]

200 Deze zorg werd geuit bij de voorstellen 9 (Opsporingsindicatie), 11 (Sensing-aanvraagpunt) en 17 (Quid pro quo samenwerking).
201 Deze zorg werd geuit bij voorstel 11 (Sensing-aanvraagpunt).
202 Deze zorg werd geuit bij voorstel 10 (Proeftuin PPS).
203 Deze zorg werd geuit bij de voorstellen 2 (Bedreigingsdossiers), 7 (Meld Misdaad Anoniem) en 17 (Quid pro quo samenwerking).
204 Deze zorg werd geuit bij voorstel 8 (Mobiele sensing-platforms).
205 Deze zorg werd geuit bij voorstel 17 (Quid pro quo samenwerking).
206 Deze zorg werd geuit bij voorstel 1 (Aangiftesysteem).
207 Deze zorg werd geuit bij voorstel 3 (Beveiligingssoftware leveranciers).
208 Deze zorg werd geuit bij voorstel 9 (Opsporingsindicatie).
209 Deze zorg werd geuit bij de voorstellen 1 (Aangiftesysteem), 8 (Mobiele sensing-platforms), 9 (Opsporingsindicatie), 11 (Sensing-aanvraagpunt), 13 (Trends delen) en 14 (Veiligheidsofficier).
210 Deze zorg werd geuit bij de voorstellen 2 (Bedreigingsdossiers) en 7 (Meld Misdaad Anoniem).
211 Deze zorg werd geuit bij de voorstellen 1 (Aangiftesysteem), 2 (Bedreigingsdossiers), 5 (Gevaarsindicatie), 6 (Heterdaad omgevingssensoren), 7 (Meld Misdaad Anoniem), 11 (Sensing-aanvraagpunt), 13 (Trends delen) en 14 (Veiligheidsofficier).

6. FASE 3: RESULTATEN BRAINSTORMSESSIES

6.1 Inleiding

De deelnemers aan het seminar werden vooraf geïnformeerd over de inhoud van de verschillende te bespreken projecten, en over de zorgen die in de vragenlijst over elk van de projecten geuit werden. Tijdens de sessie werden de randvoorwaarden voor het uitvoeren van de projecten besproken mede naar aanleiding van de geuite zorgen. De bedoeling was om naar de meest optimale, kansrijke 'formule' te zoeken voor iedere top-prioriteit. Tijdens de sessie zelf werd er geconcentreerd op de geuite zorgen die in de vragenlijst naar voor kwamen. Na de brainstormsessie werd op basis van literatuur en een analyse van de relevante wetgeving verder gewerkt om de randvoorwaarden verder uit te werken. Dit gebeurde op basis van de 10 categorieën van zorgen die in fase 2 waren geïdentificeerd.

6.2 Algemene consensuspunten

Voorafgaand aan het bespreken van de top-prioriteiten, worden onderstaande nog enkele punten gedeeld waar alle deelnemers van het seminar het over eens waren, maar die niet gerelateerd waren aan de projecten zelf of aan de categorieën van geuite zorgen.

1. Het bijeenbrengen van de publieke en private sector zorgt voor een goede discussie en een aangename dynamiek. Dit soort discussiedagen/avonden kunnen ook buiten het kader van een specifiek project georganiseerd worden, en zorgen voor kennisuitwisseling en potentieel innovatieve ideeën.
2. Hoewel het een goed idee was om de focusgroep te organiseren met verschillende deelsectoren binnen de publieke (handhaving, recherche, strategie, …) en de private (private opsporing, beveiliging, cyberveiligheid, …) sector, zou het voor gedetailleerdere discussie goed zijn om de top-prioriteiten meer per deelsector te bevragen en te bekijken. Bij meer heterogene groepen gaat de discussie breed, en bij meer homogene groepen kan de discussie net dieper gaan. Publieke en private actoren die met vergelijkbare materie bezig zijn, kunnen zo nog beter met elkaar gematched worden, waardoor ook de top-prioriteiten beter afgestemd zullen worden per deelsector. Methodologisch zou het dan goed zijn om op een vergelijkbare manier via een Delphi-methode te werken, maar verschillende seminars te organiseren waar publieke en private sectoren met kennis rond een specifieke deelsector samengebracht worden om de top-prioriteiten te bespreken die zij geïdentificeerd hebben.
3. Hoewel de top-prioriteiten die uit dit onderzoek kwamen zeker relevant zijn, is het zeker ook nuttig om andere projecten te bekijken die naar voor werden geschoven (17 projecten), omdat ook daar nuttige informatiedeling uit voort kan komen. Waar bijvoorbeeld verschillende keren op teruggekomen werd, was de suggestie dat particuliere partijen vaker onderzoeks/zaakdossiers aan de politie kunnen leveren. Er werd nadrukkelijk geadviseerd ook andere voorstellen verder te onderzoeken en mogelijk te implementeren. (Aanwezige) organisaties kunnen daar uiteraard ook zelf het initiatief toe nemen: niet alle initiatief hoeft van de Korpsleiding Staf te komen.
4. In het verlengde van de vorige suggestie, kwam het project rond de creatie van veiligheidsofficieren ook verschillende keren naar voren als mogelijke algemene randvoorwaarde voor het uitwisselen van informatie binnen andere projecten. Ook de algemene geuite zorgen die in hoofdstuk 6 vermeld staan, maken gewag van de noodzaak om bruggenbouwers en betrouwbare vaste partners te hebben bij alle betrokken actoren. Veiligheidsofficieren kunnen die rol vervullen.
5. De deelnemers in de focusgroep hadden de indruk, zeker ook gebaseerd op praktijkervaring in buurlanden, dat in Nederland de 'afstand' tussen publieke en particuliere veiligheidsorganisaties groter is dan in vergelijkbare andere landen.
6. Binnen de politie en daarbuiten zijn er al een aantal informatiesystemen en samenwerking die (deels) doen wat in dit onderzoek als nieuwe suggesties worden gepresenteerd. Dit kan omdat deze niet publiek, of zelfs binnen de politie, bekend zijn of nog maar kort bestaan. Het zou dus kunnen dat sommige van de projecten, ook uit de preliminaire lijst, kunnen worden meegenomen in deze trajecten. Sommige bestaande samenwerkingen zijn ook informeel of plaatselijk. Deze zouden structureel kunnen worden gemaakt. Een interne bevraging van de politie zou ook kunnen leiden tot een beter intern zicht wat er al

plaatsvindt, ook op informele en plaatselijke basis.

7. De deelnemers in de focusgroep gaven verder aan dat over (nieuwe) informatie-uitwisseling ook niet te ingewikkeld en defensief moet worden gedacht, omdat er dan uiteindelijk vaak niets wordt gedaan. De basis implementeren zou als startpunt moeten worden genomen: implementeer gewoon eerst de simpelste variant van het systeem, en bouw daar later verder op door.

6.3 *Prioriteit 1: Sensing-aanvraagpunt*

6.3.1 Uitleg project

De politie beschikt over mobiele sensor (ANPR-)camera's, en heeft ook manieren om informatie te krijgen van privé-camera's, maar deze worden slechts zelden gebruikt op particuliere terreinen. Particuliere veiligheidsactoren hebben soms klanten waar zij aanwijzingen hebben dat (veel) criminaliteit plaatsvindt of dat er hoge (maatschappelijke) veiligheidsrisico's zijn. Een sensing aanvraagpunt zorgt ervoor dat de particuliere bedrijven een aanvraag kunnen indienen bij de politie of het OM om mobiele politiecamera's te installeren, of om toe te laten dat bestaande camera's beelden doorsturen naar de politie (met andere woorden aangesloten worden op hun netwerk). Dit geldt ook voor mogelijk andere sensing-apparatuur.

Uit de beantwoording van de survey en de discussie in de Focusgroepbijeenkomst bleek dat de crux van dit voorstel niet scherp genoeg naar voren is gekomen, vandaar dat het noodzakelijk is nog iets meer achtergrond te geven. De politie plaatst op dit moment reeds sensing-apparatuur, zoals camera's, op openbare plaatsen. Het zou nuttig zijn indien particuliere veiligheidsactoren, die locaties kennen waar serieuze vermoedens van criminaliteit, agressie of dreiging zijn, via een centraal, landelijk sensing-aanvraagpunt bij de politie een verzoek kunnen indien voor het plaatsen van sensing apparatuur op bepaalde plaatsen, ook op particuliere terreinen, of een aanvraag kunnen indienen om de politie mee te laten kijken met de door de particuliere veiligheidsactor geplaatste sensing-apparatuur. De aanvragen worden geëvalueerd door speciaal hierop gerichte (politie)medewerkers op het centrale niveau. Dit project gaat niet uit van wijzigingen aan de huidige bevoegdheden van de politie (deze is bevoegd om sensing apparatuur te plaatsen en heeft de mogelijkheid mee te kijken met private sensing-apparatuur).

6.3.2 Scores inhoudelijke criteria en complexiteit

Het sensing-aanvraagpunt bleek bij de herberekening na de materiële fout niet meer tot de top-prioriteiten te behoren. Wat betreft efficiëntie/effectiviteit scoorden de politie en de particuliere veiligheidsactoren ongeveer hetzelfde, maar door de gemiddeld hogere scores gegeven door de particuliere veiligheidsactoren, kwam het lager in de ranking terecht. Hetzelfde zien we bij de technische haalbaarheid, waar het aanvraagpunt wel hoger in de ranking staat bij de politie, maar een lagere score krijgt dan bij de particuliere veiligheidsactoren door de algemeen lagere scores bij de politie. De politie geeft een heel lage score aan de maatschappelijke wenselijkheid van dit project. Hoewel de score bij de particuliere veiligheidssector wel hoger ligt, is er wel eensgezindheid over de ranking, het project wordt bij beide zeer laag ingeschaald. Hetzelfde zien we tenslotte bij complexiteit, waar de politie wel een hogere mate van complexiteit vaststelt, maar de ranking van beide ongeveer overeenkomt.

6.3.3 Bereikte consensus in de brainstormsessie

Over een aantal zorgen werd een consensus bereikt tijdens de brainstormsessie. Deze consensus werd ook verwerkt in hoofdstuk 6.3.4, dat de randvoorwaarden per zorg uitstippelt. In eerste instantie werd gesproken over de vraag of er wel voldoende commerciële interesse zou zijn vanuit de particuliere veiligheidsactoren. Er zijn verschillende mogelijkheden om die interesse duidelijk te maken of aan te wakkeren. De sensing apparatuur helpt bijvoorbeeld tevens bij het verlenen van gevaarsindicaties (zie project 4) aan de commerciële actor, die daardoor ook meer gericht/beter advies kan verlenen aan de eigen werknemers om hun veiligheid te borgen. De aanvraag kan ook gepaard gaan met een hogere prioritering van meldingen/aangiften van de klant (waar de sensing-apparatuur zich zal bevinden). Dat betekent dat de commerciële partner meer kans maakt om een contract te verkrijgen indien het bij een centraal aanvraagpunt is aangemeld, en dat het waarschijnlijker is dat de klant ook toestemming geeft voor de plaatsing van de sensing apparatuur. Ook is het mogelijk dat de politie zelf interesse heeft in het opvolgen van wat de sensing-apparatuur gemeten heeft, maar zelf niet in staat is middelen hiervoor in te zetten. Op dat moment kan de commerciële actor door de politie vergoed worden om deze opvolging te doen, en de resultaten ervan doorgeven aan de politie. Dit op basis van een aparte contractuele relatie met de politie als klant. En tenslotte is het zeer waarschijnlijk dat het registreren van verdachte situaties zal leiden tot

een vraag voor verdere opvolging van de situatie door de klant, of op zijn minst een vraag om de sensing zelf over een langere periode verder te zetten. Ook dit is een commercieel interessante vraag voor de commerciële actor.

Een tweede beantwoorde zorg betrof privacy, oftewel de informatie die uit de sensing-apparatuur wordt gehaald. Er was eensgezindheid dat die voornamelijk door de politie moet kunnen worden gebruikt, niet door de commerciële partners. Hier werden verschillende ideeën naar voor geschoven, Sensing-apparatuur betekent in eerste instantie niet noodzakelijkerwijze camera's. Het kan nuttig zijn om apparatuur te plaatsen die enkel meet wat men specifiek wil meten (bijvoorbeeld: beweging), in plaats van een camera te plaatsen die alles meet, en er dan data afgeschermd moet worden. Tegelijkertijd was er hier ook geen volledige consensus: er werd geopperd dat men soms ex post wel degelijk een volledig beeld wil krijgen, bijvoorbeeld in het kader van een opsporingsonderzoek. Ten tweede kunnen technologische oplossingen gevonden worden voor het versterken van privacy (*privacy enhancing technology*). Zo kan bijvoorbeeld de informatie in een black box verzameld worden, en kan de politie enkel gerichte vragen stellen aan de *black box* (bijvoorbeeld: kwam een auto met een specifieke nummerplaat in beeld?). Zo wordt vermeden dat de politie onmiddellijk over alle informatie beschikt. Een variant hierop is *multiparty computation*. In dit geval blijft de data bij de eigenaar van het camerasysteem (dus de klant of de commerciële partner), en kan de politie enkel specifieke gegevens opvragen. Tegelijkertijd weet de klant of commerciële partner ook niet welke informatie opgevraagd wordt. Met deze verschillende manieren om privacy te verbeteren, kan mogelijk ook gedifferentieerd worden. Een vraag om informatie te verkrijgen vanuit de politie kan verschillende classificaties krijgen, gaande van enkel toegang tot zeer gerichte data tot full access. De ernst van een veiligheidsincident kan ertoe leiden dat een hogere classificatie gebruikt wordt (en de politie dus meer toegang krijgt tot gegevens).

Tijdens de brainstormsessie werd ook consensus bereikt over de zorg rond capaciteit, zekere langs de kant van de politie, omdat het gebruik van dit systeem betekent dat er meer informatie naar de politie zal stromen (wat ook de bedoeling is van informatie-uitwisseling). Ook hier werden technologische oplossingen naar voor geschoven. Ook kan capaciteit voor het uitkijken of analyseren van beelden bij commerciële partijen worden 'ingehuurd'.

Er werd tenslotte ook over juridische aspecten gesproken. Er werd overeengekomen dat het mogelijk zou moeten zijn om gebruik te maken van convenanten tussen de politie en geïnteresseerde commerciële partners, die zich dus zouden aanmelden via een centraal meldpunt). Dit lijkt al in sommige gevallen te gebeuren met het Live View-programma. Het is daarom nuttig om ook na te gaan of de reeds bestaande samenwerkingen (en de convenanten waar ze op gebaseerd zijn) opgeschaald kunnen worden naar het nationale niveau, om zo tot wat meer uniformiteit te komen.

6.3.4 Randvoorwaarden op basis van de geuite zorgen

Zorg 1: de informatie zelf moet voldoende waardevol zijn

Deze zorg werd niet besproken in de brainstormsessie zelf, omdat deze minder speelt in dit specifieke geval. De beoordeling van de waarde van de informatie wordt gemaakt door de politie of de gemeente, het gaat immers om een aanvraag door de commerciële actor. Het enige wat nodig is, is dat het systeem om sensing-apparatuur aan te vragen, voldoende ruimte laat om de aanvraag te motiveren, zodat de waarde van de informatie ingeschat kan worden.

> Randvoorwaarde: het aanvraagsysteem moet de mogelijkheid geven om te motiveren waarom het nuttig is dat sensing-apparatuur geplaatst moet worden of bestaande camera's aangesloten moeten worden op het systeem van de politie.

Zorg 2: er moet gewaakt worden voor het mogelijk oneigenlijk gebruik van de uitgewisselde informatie

Deze zorg kwam wat betreft oneigenlijk gebruik van de informatie zelf wel aan bod tijdens de brainstormsessie, en zoals hierboven gesteld, werd er voornamelijk gewezen op technologische oplossingen (*privacy enhancing technology*), waarbij camerabeelden kunnen worden gemanipuleerd, zodat de beelden geen informatie opleveren die een persoon identificeert, en enkel tonen wat er aan het gebeuren is (bijvoorbeeld: een auto passeert, maar de nummerplaat is niet zichtbaar en de kleur van de auto wordt zelfs aangepast, of er is enkel een silhouet van een persoon). Er wordt nu al geëxperimenteerd met dit soort technologie. Identificeerbare informatie kan verkregen worden wanneer dit expliciet in het systeem opgevraagd wordt, mogelijk na tussenkomst van een rechter-commissaris. Dit gaat ervan uit dat de informatie reeds eigendom is van de politie. Een variant hierop is *multiparty com-*

putation, waarbij de informatie verzameld wordt met camera's van de private partij, en de politie gegevens kan opvragen. Door gebruik te maken van *multiparty computation* weet de private actor niet welke informatie opgevraagd wordt door de politie, terwijl de politie enkel de gegevens krijgt waar ze expliciet om vraagt, wat de privacy verhoogt.

Een andere manier, minder gericht op bijkomende technologie, is om de gebruikte technologie af te schalen, en niet met camera's te werken die alles registreren en waarbij data dan afgeschermd moet worden. Er is bijvoorbeeld ook apparatuur die enkel meet of er beweging is of enkel patronen identificeert. Hier kan wel tegen in gebracht worden dat meer informatie dan strikt noodzakelijk ook nuttig kan zijn indien verdachte acties gevonden worden, want dan is er bij een camera een keuze om op te schalen en meer informatie te vragen. Zo kan men komen tot verschillende classificaties en kan de toegang van de politie tot de informatie variëren, van toegang tot zeer gerichte data tot *full access* (bijvoorbeeld bij een ernstige kans op een terroristische aanslag).

Het oneigenlijk gebruik kan zich echter nog op een tweede manier manifesteren, namelijk door particuliere veiligheidsactoren een meer directe toegang te geven tot de politie, en zo meer aanspraak te laten maken op de gelimiteerde capaciteit. Dit werd naar voor gebracht als een risico in de brainstormsessie zonder dit expliciet verder te behandelen, eerder als een aandachtspunt. Omdat er al manieren bestaan om sensing/camera's aan te vragen, lijkt dit risico vrij laag te zijn. Het komt neer op een evaluatie van de motivering voor de aanvraag. Dat heeft meer te maken met de vraag of er voldoende middelen besteed kunnen worden aan het systeem.

Randvoorwaarde: de informatie moet afgeschermd worden door gebruik te maken van privacy-verhogende technologie, of er moet kunnen gedifferentieerd worden welke sensing apparatuur aangevraagd kan worden in het systeem.

Zorg 3: De juiste actoren moeten betrokken worden bij de informatie-uitwisseling

Dit werd niet expliciet behandeld in de brainstormsessies. Uit de juridische analyse, zie later, komt echter naar voren dat, afhankelijk van de situatie ofwel de politie ofwel de gemeente verantwoordelijkheden heeft voor het plaatsen van de camera (en niet het OM). Bovendien wordt ervan uitgegaan dat de particuliere veiligheidsactor telkens het mandaat heeft van de klant om de sensing-apparatuur aan te vragen. Dit moet echter expliciet geregeld zijn.

Randvoorwaarde: de particuliere veiligheidsactor moet een mandaat hebben om de sensing-apparatuur aan te vragen (e.g.: de sensing apparatuur wordt geplaatst op locaties die eigendom zijn van de particuliere veiligheidsactor; het contract met de klant bevat clausules die deze mandatering mogelijk maken; etc.)

Randvoorwaarde: zowel politie als gemeenten moeten aangesloten zijn op het aanvraagsysteem.

Zorg 4: de informatie-uitwisseling mag geen negatieve impact hebben op de werkzaamheden van de betrokken actoren

Deze zorg is voor dit specifieke project minder relevant, omdat de keuzevrijheid bij alle actoren om al dan niet tot een aanvraag over te gaan. In de brainstormsessie werd er ook niet verder op ingegaan. De particuliere veiligheidsactor en hun klant kunnen een mogelijke negatieve impact inschatten, en ervoor kiezen om niet tot de aanvraag over te gaan. De politie kan het gebruik van sensing-apparatuur afwijzen, zodat mogelijke onderzoeken die al geïnitieerd werden niet in gevaar komen zonder daarbij een reden op te geven. Een verdere randvoorwaarde is niet noodzakelijk.

Zorg 5: de informatie-uitwisseling mag geen negatieve impact hebben op de reputatie van de betrokken actoren

Hier geldt hetzelfde als bij de vorige zorg: binnen dit project is het minder relevant, en het werd ook niet besproken tijdens de brainstormsessie, omdat het om een een systeem gaat waar elke actor een keuze maakt om al dan niet een aanvraag te doen, zodat de actoren zelf het best kunnen inschatten om dit al dan niet te doen. Het opzetten van het systeem zelf brengt geen reputatieschade mee, waardoor dit geen randvoorwaarde is. Bij Zorg 9 wordt wel de zorg behandeld dat de klant mogelijk geen interesse heeft om deel te nemen wegens reputatieschade.

Zorg 6: Het systeem waardoor informatie uitgewisseld wordt, moet voldoende waarborgen bevatten en bruikbaar zijn

Zowel de waarborgen als de bruikbaarheid van het systeem werden behandeld tijdens de brainstormsessie. Wat waarborgen betreft, gelden de reeds bestaande limieten van het plaatsen van een camera door publieke actoren, zowel incidenteel als permanent (zie later bij de juridische zorgen). Voor het laten aansluiten van een bestaande camera op de systemen van de politie bestaat evenzeer al een regelgevend kader voor aanvraag en opslag van data dat gevolgd kan worden.

Beide bieden voldoende waarborgen. Tijdens de brainstormsessie werd ook beargumenteerd dat de aanvraag zelf op een veilige manier moet verlopen, omdat de motivering voor de aanvraag vertrouwelijke informatie kan bevatten.

Wat de bruikbaarheid betreft werden verschillende elementen besproken. Voor camera's die aangesloten worden op de systemen van de politie werd er tijdens de brainstormsessie op gewezen dat er reeds twee systemen bestaan die dit faciliteren: Camera in Beeld en Live View. Het eerste systeem is minder interessant, omdat het niet om een live meekijken gaat, maar om het registreren van camera's, waardoor het gemakkelijker wordt om beelden nadien op te vragen.[212] Live View is een systeem waarbij beelden eerst geëvalueerd worden in een particuliere meldkamer, en deze dan nadien bij een incident doorgestuurd worden naar de politiemeldkamer.[213] In het op te zetten systeem kan deze stap behouden worden, of kunnen de beelden ook rechtstreeks gedeeld worden met de politiemeldkamer. Om de complexiteit van het gebruik van verschillende systemen en verschillende software te vermijden, kan de tussenstap van een particuliere meldkamer ook nuttig zijn, omdat er uniform kan gecommuniceerd worden naar de politiemeldkamer zonder dat deze de verschillende standaarden moet integreren. Een alternatief is dat de politie een makkelijk en breed toepasbare standaard configuratie kiest, en deze oplegt aan de gebruikers van het systeem. Tijdens de brainstormsessie werd aangeraden om aan te sluiten op Live View, zonder dit te veel te gaan wijzigen. Indien er al een systeem bestaat, vergemakkelijkt dit de implementatie.

Een meer algemene problematiek betreft de kosten van het opzetten en in stand houden van het systeem, wat ook samenhangt met de capaciteit, zoals hieronder besproken. Vooral indien het systeem populair zou worden, moeten er voldoende middelen beschikbaar zijn om aanvragen te evalueren en om camerabeelden live te bekijken. Indien dit niet gewaarborgd kan worden, en er bijvoorbeeld lange wachttijden zouden komen, verkleint dit drastisch het draagvlak voor en effect van dit project. Dit kan echter niet een initiële start van het project in de weg staan. Een regelmatige evaluatie van het systeem is op termijn wel noodzakelijk, zodat er ook beoordeeld kan worden of er aanpassingen in capaciteit moeten plaatsvinden.

Randvoorwaarde: gebruik wat betreft het meekijken van de politie met private sensing-apparatuur het reeds operationele systeem van Live View, zonder initieel wijzigingen in de setup aan te brengen.

Randvoorwaarde: voorzie voldoende middelen om aanvragen te verwerken.

Randvoorwaarde: voorzie regelmatige evaluatiemomenten voor het systeem. Om dit mogelijk te maken, is het nuttig om vanaf het begin de doelen van het systeem SMART te formuleren. Vooral bij een meer regelmatig gebruik van het systeem, is het mogelijk dat de middelen de doelen voorbij schieten, maar dit moet op strategisch niveau geëvalueerd worden.

Zorg 7: er moet voldoende kennis/expertise aanwezig zijn bij alle betrokken actoren

Deze zorg werd niet verder besproken wat betreft dit project, omdat het niveau van expertise niet zeer hoog is. Het gaat om informatie die ofwel binnen de politie blijft en dan is de expertise reeds aanwezig, ofwel informatie die vanuit de private actor naar de politie gaat en dat gaat via een reeds operationeel systeem. De belangrijkste zorg lijkt hier eerder de kennis van het bestaan van het aanvraagsysteem zelf te zijn. Wanneer dit gelanceerd wordt, moet er duidelijke informatie worden verleend wat het doel is van het aanvraagpunt, hoe de aanvraag gedaan kan worden en hoe de verwerking gebeurt.

Randvoorwaarde: zet een campagne op bij de lancering van het aanvraagpunt, met een website met voldoende uitleg in de vorm van filmpjes, voorbeelden en een FAQ.

212 Https://hetccv.nl/onderwerpen/high-impact-crimes/hic-preventiewijzer/overvallen/camera-in-beeld/
213 Https://www.politie.nl/informatie/wat-is-live-view.html

Zorg 8: er moet voldoende capaciteit aanwezig zijn bij alle betrokken actoren

Naast de middelen die besteed moeten worden aan de opzet en de implementatie van het systeem, zijn er mogelijke capaciteitsbeperkingen bij de politie in de verwerking van de informatie en voldoende sensing-apparatuur.

Het doel van het opzetten van dit project is uiteindelijk dat er meer informatie naar de politie stroomt via de sensing-apparatuur. Maar deze informatie moet ook verwerkt en geanalyseerd worden. Dit impliceert ofwel een zekere automatisering via AI, wat nog in een vroeg ontwikkelingsstadium is, of meer personeel. Live View toont reeds aan dat er een tussenstap kan gemaakt worden naar particuliere actoren, waardoor enkel de meest relevante informatie de politie bereikt. Analysecapaciteit kan derhalve verhoogd worden door gebruik te maken van particuliere inhuur. Wat niet geoutsourced kan worden is de reactie op incidenten die zichtbaar worden via de sensing-apparatuur: dit moet door de politie zelf gedaan worden. De beschikbare capaciteit moet daar op afgestemd worden.

Sensing-apparatuur zelf moet ook voldoende beschikbaar zijn. Om deze zorg weg te nemen zou de politie gebruik kunnen maken van een goede planningsmethode. Op basis van trends in aantallen aanvragen, percentages, gemiddelde inzetduur, slijtage/verlies, onderhoudswerk etc. kunnen lange wachttijden goeddeels voorkomen worden , althans zolang het aantal aanvragen binnen de perken blijft. Bij een grote populariteit van het systeem kan het gebruik opnieuw geëvalueerd worden, zoals aangegeven bij de vorige zorg.

Randvoorwaarde: voorzie voldoende capaciteit voor de verwerking van de informatie, eventueel door externe inhuur/outsourcing.

Randvoorwaarde: zorg ervoor dat routines/ patrouilles afgestemd zijn op het reageren op incidenten voor de nieuwe sensing punten. Zorg er dus voor dat het politiemanagement van de regio op de hoogte is en dit integreert in de operationele beslissingen.

Randvoorwaarde: voorzie een goede planningsmethode en voldoende voorraad voor sensing-apparatuur. Evalueer continu om te kunnen anticiperen op toekomstige pieken in aanvragen.

Zorg 9: er moet voldoende en een volgehouden wil tot informatie-uitwisseling aanwezig zijn bij alle betrokken actoren, wat betekent dat de meerwaarde voor iedereen duidelijk moet zijn

Potentieel zijn bij dit project drie actoren betrokken: politie, particuliere veiligheidsactoren en klanten. Elk van de drie moet een voldoende en volgehouden wil hebben. Bij de politie zorgen de voorheen opgestelde randvoorwaarden dat er voldoende meerwaarde is om in te stappen in het systeem; de voordelen zijn daarbij duidelijk. De voordelen voor de particuliere veiligheidsactoren zijn in eerste instantie minder duidelijk, blijkt uit de brainstormsessie. Toch kunnen een aantal voordelen geïdentificeerd worden. Ten eerste helpt de sensing-apparatuur om mogelijke gevaren te identificeren voor de eigen werknemers (zie ook project 4). Ten tweede kan het gebruik van het systeem als een meerwaarde naar voren geschoven worden in contractbesprekingen met (potentiële) klanten. Zeker wanneer het systeem na een tijd geëvalueerd wordt en het duidelijk wordt dat er voordelen verbonden zijn aan het gebruik ervan, kan een particuliere veiligheidsactor een aansluiting op het systeem aanbieden als een voordeel voor de klant waar concurrenten mogelijk niet over beschikken. Dit impliceert wel dat er een manier moet zijn om duidelijk te maken dat een particuliere actor aangesloten is op het aanvraagsysteem (bijvoorbeeld met een certificaat of logo). Tenslotte zou het gebruik van het systeem er ook toe moeten leiden dat er een grotere vraag komt van klanten om geïdentificeerde incidenten verder op te volgen. Ook dit is een commercieel interessante vraag voor particuliere veiligheidsactoren.

De hierboven besproken voordelen gelden ook voor de klant van de particuliere veiligheidsactor (identificatie van gevaren, evaluatie van contracten, opvolging van incidenten). Wat de wil van klanten bijna paradoxaal wel in negatieve zin kan beïnvloeden is een te grote efficiëntie van de sensing-apparatuur, waardoor er veel incidenten blootgelegd worden. Dit kan er in resulteren dat de klant als een problematisch bedrijf wordt beschouwd door anderen; een reputatie die het wil vermijden. Om deze reden moet het mogelijk zijn voor de klant aan te vragen dat het gebruik van de sensing apparatuur stopgezet wordt. Op basis van publieke belangen moet uiteraard de politie of het OM besluiten of dan daadwerkelijk gestopt wordt.

Randvoorwaarde: zorg voor een logo of certificaat dat door de particuliere veiligheidsactor gebruikt kan worden om te tonen dat zij gebruik maken van / aangesloten zijn op het aanvraagsysteem voor sensing apparatuur.

Randvoorwaarde: laat toe dat enige actor op gelijk welk moment kan aanvragen dat de sensing stopgezet wordt.

Zorg 10: het juridisch kader waarbinnen de informatie-uitwisseling gebeurt, moet voldoende duidelijk zijn

We kunnen bij dit voorstel onderscheid maken tussen twee juridische kaders, maar geen van beiden zijn op zich problematisch. Het eerste is een bestaand kader waarbij de politie op basis van de algemene bevoegdheden vastgelegd in art. 3 van de Politiewet incidenteel camerabewaking mag opzetten, of de gemeente op basis van art. 151c van de Gemeentewet regulier cameratoezicht mag opzetten. Hoewel het hier over camera's gaat, is dit kader ook van toepassing op sensing-apparatuur. Onafhankelijk van wie de sensing-apparatuur opzet, is de politie de verwerkingsverantwoordelijke en vallen de verzamelde gegevens onder de WPG. Één en ander hierover is uitgewerkt binnen de beleidsregels cameratoezicht van het College Bescherming Persoonsgegevens.[214] De route van incidenteel toezicht door de politie is op zich interessanter, omdat regulier toezicht door de gemeente enkel mogelijk is indien het om niet op zichzelf staande maatregelen gaat. Het moet dus gekoppeld worden aan andere veiligheidsverhogende maatregelen, zoals betere straatverlichting. Incidenteel toezicht is mogelijk indien er een concrete aanleiding bestaat, wat de vorm kan krijgen van een gemotiveerde aanvraag tot sensing. Wanneer een aanvraag binnenkomt, moet de verwerker van de aanvraag (een politiemedewerker) de noodzaak van de plaatsing van de sensing-apparatuur evalueren, inclusief of minder verregaande maatregelen (bijvoorbeeld geen camera maar een apparaat dat minder informatie opvangt) tot hetzelfde resultaat kunnen leiden.

Wanneer de noodzaak aangetoond kan worden, moet een data protection impact assessment (DPIA) worden uitgevoerd. In het huidige juridische kader is dit de verantwoordelijkheid van de korpschef, maar dit zou via het aanvraagpunt ook op een hoger niveau kunnen gebeuren. Het plaatsen van sensing-apparatuur moet tenslotte samen gaan met het kenbaar maken van het toezicht, en het wijzen op de rechten van betrokkenen. Dit kan door bijvoorbeeld een bord op te hangen. Het is dus niet toegestaan om zonder aankondiging cameratoezicht te starten (maar men hoeft niet expliciet aan te duiden waar de camera's hangen). Wanneer wegens capaciteitsuitbreiding het nodig is om externe verwerkers in te schakelen, dan moeten zij met de politie een verwerkersovereenkomst afsluiten.[215]

Het tweede juridische kader is evenzeer een bestaand kader: dat van Live View, een publiek-private samenwerking. Wat betreft privacy en dataverwerking is de UAVG van toepassing, gezien de sensing-apparatuur door of bij een private partij wordt geïnstalleerd. Dit betekent dat de sensing-apparatuur enkel gebruikt mag worden voor de bescherming van eigendommen, werknemers en klanten, en dat er geen beelden mogen gemaakt worden van eigendom van andere personen of de openbare weg. Ook hier is het verplicht aan te duiden dat er sensing-apparatuur aanwezig is (maar niet precies waar die hangt).[216] Het Live View-systeem werkt tenslotte met private meldkamers, die controleren of aan de voorwaarden voldaan is om informatie/beelden door te sturen naar de politiemeldkamer. Er kan aangenomen worden dat dit op basis van een convenant gebeurt, hoewel het uit de publiek toegankelijke informatie niet geheel duidelijk is hoe dit functioneert.

Randvoorwaarde: maak gebruik van de reeds bestaande juridische kaders rond incidenteel cameratoezicht door de politie en Live View, en pas deze aan om te werken met een centraal aanvraagpunt. Hierbij kan het nodig zijn dat taken die nu op een lager niveau liggen (bijvoorbeeld bij de korpschef) op te schalen.

214 Https://wetten.overheid.nl/BWBR0037591/2016-02-02#Circulaire.divisie_Circulaire.divisie_1
215 Https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/foto-en-film/cameratoezicht-op-openbare-plaatsen#faq
216 Https://www.politie.nl/binaries/content/assets/politie/onderwerpen/live-view/liveviewnl-def.pdf

6.4 *Prioriteit 2: Gebruik informatie vanuit mobiele sensing-platforms*

6.4.1 Uitleg project

Particuliere bedrijven hebben vaak een groot wagenpark dat heel veel in Nederland rondrijdt. Er kunnen contracten afgesloten worden tussen een aantal particuliere bedrijven en de politie (en/of andere overheidsdiensten) om sensoren op deze wagens te plaatsen om controles uit te voeren. Te denken valt aan illegale radiozenders, verlopen APK-status, kwaliteit van wegen/asfalt (niet aan de politie), etc. De sensoren zijn eigendom van de publieke sector, worden door hen ook onderhouden, en informatie kan niet uitgelezen worden door de private partner.

6.4.2 Scores inhoudelijke criteria en complexiteit

Ook dit project was uiteindelijk volgens de herberekening geen top-prioriteit. De score voor efficiëntie/effectiviteit ligt bij de particuliere veiligheidsactoren weliswaar wat hoger, maar in de ranking zit het project zeer laag ingeschaald. Diezelfde actoren plaatsen het project wat betreft technische haalbaarheid wel in de bovenste helft, terwijl dit niet het geval is bij de politie. Waar er wel eensgezindheid over bestaat, is de maatschappelijke wenselijkheid: zowel de politie als de particuliere veiligheidsactoren geven aan dit project de laagste score. De complexiteit tenslotte toont dat de particuliere veiligheidsactoren en de politie het wel eens zijn over de score zelf, maar gezien de verschillende spreiding, betekent dit voor de politie dat het project qua complexiteit een middenmoter is, terwijl het bij de particuliere veiligheidsactoren als het meest complex wordt gezien.

6.4.3 Bereikte consensus in de brainstormsessie

Een groot deel van de consensus-opmerkingen over de vorige prioriteit, gelden ook hier, zeker diegene rond privacy. De commerciële interesse is voor deze prioriteit wel duidelijker, omdat er een vergoeding gevraagd kan worden voor het rondrijden met de sensing-platforms. Ook moeten de kosten van de inbouw van de apparatuur en het onderhoud ervan vanuit de publieke sector komen.

En ook hier zijn er zorgen rond capaciteit, omdat er veel extra informatie naar de politie vloeit. Om dit te verkrijgen, kunnen ook hiervoor commerciële partners ingeschakeld worden. In plaats van continu informatie door te sturen, kan er aan de werknemers gevraagd worden om enkel informatie te registreren die volgens hen de moeite waard is om te versturen, zeker indien het gaat om verdachte handelingen (dit is minder relevant voor bijvoorbeeld nummerplaatregistratie). *Mogelijk kunnen AI-systemen hier nuttig zijn, die getraind kunnen worden door de werknemers (registratie van wanneer iets als verdacht wordt gezien, waardoor de AI nadien zelf beslissingen kan nemen over verdachte handelingen). Risico hier is wel dat de AI met verkeerde data getraind wordt, waardoor het principe 'garbage in, garbage out' geldt.*

Deze prioriteit kan ook gecombineerd worden met prioriteit 4 (leveren gevaarsindicatie). In dat geval zou er, in tegenstelling tot wat eerder werd aangegeven, wel een terugkoppeling komen naar de commerciële partner. Niet in de vorm van verwerkte informatie, maar bijvoorbeeld in de vorm van een algemene threat assessment. Dit verhoogt de waarde van het instappen in dit systeem voor de commerciële partner, omdat zij op deze manier de veiligheid van hun eigen werknemers beter kunnen borgen.

Tenslotte werd de vraag gesteld of particuliere veiligheidsactoren de beste partners zijn voor dit project. Ook andere commerciële actoren (bijvoorbeeld: pakjesverdelers) rijden constant rond, en komen overal. Uitgezocht zou moeten worden 'wie-wanneer-waar' rijdt, en welke partner(s) voor de politie als sensing-platform meerwaarde bieden. Er kan uiteraard worden gekozen om met meerdere soorten organisaties te gaan werken.

6.4.4 Randvoorwaarden

Zorg 1: de informatie zelf moet voldoende waardevol zijn

Dit project heeft een andere natuur dan het eerste project, waarbij een aanvraag gedaan wordt om op een bepaalde plaats sensing-apparatuur te installeren. Project 2 werpt een breder net, waardoor er meer kans is dat een deel van de informatie niet als waardevol gezien wordt. Deze zorg werd besproken in de brainstormsessie, en er werd tevens een consensus over bekomen. Het gaat ook samen met de zorg rond voldoende capaciteit voor het verwerken van de informatie, maar we nemen bij deze aan dat het capaciteitsprobleem gaat over het verwerken van die informatie die reeds als voldoende waardevol wordt gezien. Een manier om enkel waardevolle informatie door te sturen, is om het project aan te passen, en de werknemer van de particuliere veiligheidsactor wel toegang te geven tot de informatie. De werknemer kiest dan in om enkel informatie te registreren die volgens hen de moeite waard is om te versturen, zeker indien het gaat om verdachte handelingen (dit is minder relevant voor bijvoorbeeld nummerplaatregistratie). In tweede instantie werd

ook gesproken over AI-systemen, die initieel getraind kunnen worden door de werknemers (registratie van wanneer iets als verdacht wordt gezien, waardoor de AI nadien zelf beslissingen kan nemen over verdachte handelingen). Hier bestaat wel een risico dat de AI met verkeerde data getraind wordt, waardoor het principe 'garbage in, garbage out' geldt. Bovendien zou zo'n systeem nog volledig ontwikkeld moeten worden. Dat geldt dan weer niet voor nummerplaatherkenning, waar een script, gebaseerd op reeds bestaande software, voor kan ontwikkeld worden zonder menselijke interventie. Dus bij de opstart kan gewerkt worden met registratie door de werknemer van verdachte handelingen, terwijl meer gerichte informatie (zoals een bepaalde nummerplaat) automatisch kan verlopen.

Randvoorwaarde: differentieer tussen gerichte en niet-gerichte data. Gerichte data zoals nummerplaten kunnen via automatische herkenning verlopen, waarbij er geen actie van de werknemer verwacht wordt en de politie enkel waardevolle informatie krijgt. Niet-gerichte data zou door de werknemer zelf als relevant of niet-relevant beoordeeld moeten worden.

Zorg 2: er moet gewaakt worden voor het mogelijk oneigenlijk gebruik van de uitgewisselde informatie

Deze zorg geldt in vrij gelijke mate voor zowel het vorige project als dit project. Het gebruik van *privacy enhancing technology* kan gebruikt worden voor niet-gerichte data, en gerichte data kan afgeschermd worden van de particuliere veiligheidsactor door deze volledig af te schermen, zodat de gegevens enkel voor de politie beschikbaar zijn. De meer directe toegang tot de politie, een zorg die in het eerste project naar voor kwam, is hier minder relevant: het gaat om een contractuele relatie waarbij de particuliere veiligheidsactor tegen een vergoeding een dienst aanbiedt aan de politie. Dit leidt niet automatisch tot meer samenwerking en dit soort outsourcing is in de praktijk reeds langer aan de gang.

Randvoorwaarde: maak opnieuw een onderscheid tussen gerichte en niet-gerichte data. De particuliere veiligheidsactor heeft geen toegang tot de gerichte data, waardoor oneigenlijk gebruik niet kan gebeuren. Niet-gerichte data kan via privacy verhogende technologie beschermd worden. Omdat de sensing-apparatuur eigendom is van de publieke actor, kan deze de technologie zelf installeren.

Zorg 3: de juiste actoren moeten betrokken worden bij de informatie-uitwisseling

Dit is een belangrijke zorg bij dit project. De vraag is of de particuliere veiligheidsactoren de enige of juiste partij zijn om dit soort samenwerking mee op te zetten. Naast het feit dat politiewagens zelf constant rond rijden, en deze sensing-apparatuur dus ook daar op kan geïnstalleerd worden, zijn er legio andere private bedrijven, denk bijvoorbeeld aan pakjesdiensten, die een grote voertuigenvloot hebben. Toch kan een specifiek contract met particuliere veiligheidsactoren nut hebben. Werknemers van deze bedrijven zijn beter getraind in het identificeren van verdachte situaties. Verder is het plaats en tijd afhankelijk waar meer politiewagens of particuliere wagens komen. In algemene zin kan worden verwacht dat particuliere beveiliging vaker dan de politie aanwezig is op bedrijventerreinen en door-de-weekse nachten. Via marktconsultaties kan de politie te weten komen wanneer en met wie het plaatsen van mobiele sensing-apparatuur de meeste meerwaarde biedt. Dat kan van belang zijn in de keuze met wie een contract afgesloten wordt, of de hoogte van het vergoedingsbedrag.

Omdat kosten voor een dergelijk systeem voor een groot deel afhangen van de hoeveelheid gebruikte sensor-pods, niet waar en wanneer deze worden gebruikt, verdient het wel aanbeveling vergoedingen niet teveel naar gebieden en tijden te differentiëren, maar brede contracten met private bedrijven aan te gaan, al dan niet particuliere veiligheidsactoren. Het staat de politie uiteraard vrij om daarnaast ook op eigen voertuigen een dergelijk systeem (te gaan) gebruiken. Om kosten voor iedereen laag te houden verdient het ook aanbeveling om in publiek-private consortia marktverkenningen te doen en met geïnteresseerde leveranciers te praten, zodat die software en installaties aan kunnen bieden die voor zoveel mogelijk doelen en door zoveel mogelijk organisaties kunnen worden gebruikt.

Randvoorwaarde: analyseer voorafgaandelijk via marktconsultaties welke private bedrijven de grootste meerwaarde geven voor het installeren van de software. Ga daarbij uit van het afdekken van de grootste oppervlakte en de minste overlap tussen waar de politie (vaak) komt en waar de private bedrijven (vaak) komen. Hierbij kan wel een voorkeur gegeven worden aan particuliere veiligheidsactoren, omdat hun werknemers meer getraind zijn in het herkennen van verdachte situaties, maar dat is enkel van belang voor niet-gerichte data, dus dit speelt niet altijd een rol.

Zorg 4: de informatie-uitwisseling mag geen negatieve impact hebben op de werkzaamheden van de betrokken actoren

Deze zorg is net zoals bij het eerste project minder relevant. Voor de particuliere veiligheidsactor is er geen onderbreking in de normale uitvoering van de eigen werkzaamheden. Voor de politie is er wel een vraag rond capaciteit, maar dat wordt in een aparte zorg uitgewerkt. Een te realiseren randvoorwaarde is dus voor deze zorg niet nodig.

Zorg 5: de informatie-uitwisseling mag geen negatieve impact hebben op de reputatie van de betrokken actoren

In tegenstelling tot het eerste project is deze zorg hier wel een aandachtspunt. Er zijn mogelijk negatieve gevolgen voor zowel de particuliere veiligheidsactor als voor de politie. Wat betreft de particuliere veiligheidsactoren, ziet een deel van de bevolking beveiliging(s-voertuigen) nu al - veelal ten onrechte - voor handhavers in de publieke ruimte. Veel burgers zien of kennen het verschil met een politiewagen niet. Vanuit de politie kan een mobiel sensing-systeem als een stap te ver gezien worden. Er is nu reeds aandacht en tegenstand tegen het gebruik van camera's in de openbare ruimte en hier gaat het om sensing-apparatuur die een nog groter bereik heeft.

Dit maakt deel uit van een maatschappelijk debat waar geen eenvoudig antwoord op bestaat. Wel kan via een voorlichtingscampagne duidelijk gemaakt worden om welke redenen de sensing-apparatuur gebruikt zal worden, wat deze precies doet, en (op termijn) welke meerwaarde het heeft gehad om gebruik te maken van dit systeem. Onduidelijkheden of desinformatie over het gebruik van dit systeem zullen de weerstand enkel vergroten. Bewuste keuzes om het systeem te gebruiken wanneer en waar de maatschappelijke veiligheidswaarde het grootst is, kunnen weerstand verkleinen.

> Randvoorwaarde: organiseer informatiecampagnes vooraleer het systeem in gebruik genomen wordt. Zorg er voor dat er voldoende informatie beschikbaar is, inclusief welke informatie verzameld wordt en hoe het systeem precies werkt.

Zorg 6: het systeem waardoor informatie uitgewisseld wordt, moet voldoende waarborgen bevatten en bruikbaar zijn

Wat betreft waarborgen voor dit project, is de grootste waarborg in dit geval dat het niet zozeer om een informatie-uitwisseling gaat, maar om het gebruik van materiaal van particuliere veiligheidsactoren door de politie om eigen sensing-apparatuur op te installeren. Er is met andere woorden maar één actor die over de informatie beschikt. Dat is nog steeds het geval indien bij niet-gerichte informatie de werknemer de beslissing kan nemen om informatie te registreren, want de informatie zelf komt nog steeds enkel terecht in het politiesysteem. En bij het verzamelen van gerichte informatie is er helemaal geen toegang.

Wat de bruikbaarheid betreft, hangt deze grotendeels samen, net zoals bij het eerste project, met de capaciteit om de informatie te verwerken. Dit wordt later behandeld. Wel kan gesteld worden dat deze problematiek mogelijk minder speelt, omdat bij het vorige project de aanvragen vanuit de particuliere veiligheidsactoren kwamen. Hier komt de vraag vanuit de politie zelf, waardoor zij beter kunnen inschatten welke capaciteit zij hebben en in hoeverre zij dit systeem willen gebruiken. Ook hier kan regelmatige evaluatie van het gebruik en de meerwaarde van het systeem leiden tot een meer intensief gebruik of mogelijk een afschaling.

> Randvoorwaarde: voorzie regelmatige evaluatiemomenten voor het systeem. Om dit mogelijk te maken, is het nuttig om vanaf het begin de doelen van het systeem SMART te formuleren.

Zorg 7: er moet voldoende kennis/expertise aanwezig zijn bij alle betrokken actoren

Expertise is niet noodzakelijk een probleem bij dit project. Het gaat om een outsourcing contract, wat in het verleden al geregeld gebeurd is, en alle apparatuur komt van de politie, zodat er kan aangenomen worden dat de relevante expertise aanwezig is. De enige expertise die mogelijk nog moet opgebouwd worden, is indien verdachte situaties geïdentificeerd moeten worden door de werknemers van een particuliere veiligheidsactor, zeker indien dit dan ook gebruikt wordt om een AI-systeem te voeden. Hier is mogelijk bijkomende praktische training voor gebruik van het systeem nodig, maar aangenomen kan worden dat personeel van particuliere veiligheidsactoren de vaardigheid van het herkennen van verdachte situaties (grotendeels) reeds moet bezitten.

> Randvoorwaarde: voorzie trainingen aan werknemers die potentieel verdachte situaties moeten identificeren.

Zorg 8: er moet voldoende capaciteit aanwezig zijn bij alle betrokken actoren

Capaciteit is een kernvereiste bij dit project, waarbij net zoals bij het vorige project een onderscheid gemaakt kan worden tussen een voldoende verwerking van de informatie en voldoende sensing-apparatuur. Ook hier

gaat het om een capaciteitsproblematiek bij enkel de politie; bij de particuliere veiligheidsactoren wordt er geen gebruik gemaakt van bijkomende middelen en is er dus ook geen bijkomende capaciteit nodig. Ook de antwoorden op deze zorgen blijven dezelfde: automatisering, meer personeel bij de politie of gebruik van particuliere inhuur voor verwerking van informatie en een goede planningsmethode voor voldoende aanwezigheid van apparatuur.

Randvoorwaarde: voorzie voldoende capaciteit voor de verwerking van de informatie, eventueel door externe inhuur/outsourcing.

Randvoorwaarde: voorzie een goede planningsmethode en voldoende voorraad voor sensing-apparatuur. Evalueer continu om te kunnen anticiperen op toekomstige piek-aanvragen.

Zorg 9: er moet voldoende en een volgehouden wil tot informatie-uitwisseling aanwezig zijn bij alle betrokken actoren, wat betekent dat de meerwaarde voor iedereen duidelijk moet zijn

Binnen dit project zijn slechts twee actoren actief: politie en particuliere veiligheidsactoren. Voor de laatste categorie is voldoende en volgehouden wil tot informatie-uitwisseling op zich duidelijk: er wordt een vergoeding gevraagd voor het rondrijden met de sensing-platformen. Om de kosten minimaal te houden, kan ook gestipuleerd worden dat alle kosten van de inbouw van de apparatuur en het onderhoud ervan vanuit de politie komen. Dit dekt indien breed berekend de risico's voor de particuliere veiligheidsactoren volledig af. Om het project nog interessanter te maken, kan er ook aan een combinatie gedacht worden met het leveren van een gevaarsindicatie, zie project 4. In dat geval is er een terugkoppeling naar de commerciële partner. Dit is niet in de vorm van verkregen ruwe informatie, maar bijvoorbeeld in de vorm van een algemene *threat assessment* voor de eigen werknemers. Dit kan een factor zijn in het bepalen van de vergoeding voor de dienst: hoe meer de particuliere veiligheidsactor alternatieve waarde haalt uit het systeem, hoe minder de vergoeding een rol speelt bij het bepalen van de wil om in het systeem te stappen. Een andere factor is de lengte van het contract: het installeren en onderhouden van sensing-apparatuur neemt tijd in beslag, die ook moet worden vergoed, maar het zou goed zijn als de dienst over een langere periode gegarandeerd is.

De meerwaarde voor de politie is zonder meer duidelijk, alleen willen we wel verwijzen naar zorg 5 rond de reputatie van de politie. Indien het maatschappelijk debat zich in negatieve zin ontwikkelt, kan dit een significante impact hebben op de wil van de politie om een dergelijk project te ontwikkelen.

Randvoorwaarde: neem de installatie en het onderhoud van de sensing-apparatuur op in het contract als een kost voor de politie.

Randvoorwaarde: zorg voor een contract met een voldoende lange looptijd.

Randvoorwaarde: bespreek binnen de contouren van de wet hoe de particuliere veiligheidsactoren ook alternatieve meerwaarde kunnen halen uit het project, om de kosten te drukken voor de politie.

Zorg 10: het juridisch kader waarbinnen de informatie-uitwisseling gebeurt, moet voldoende duidelijk zijn

We moeten wat betreft de juridische kaders ook hier een onderscheid maken tussen gerichte en niet-gerichte data. Het verzamelen van gerichte data valt ofwel onder het algemeen taakstellende art. 3 van de Politiewet, ofwel onder art. 126jj Sv, afhankelijk van hoe de verzamelde informatie bijgehouden wordt. Op basis van art. 126jj kunnen specifieke nummerplaten bijgehouden worden, en wordt er nadien door de politie informatie opgevraagd uit deze verzamelde database. Op basis van art. 3 van de Politiewet wordt er vooraf een selectie gemaakt van relevante data, bijvoorbeeld specifieke nummerplaten. Indien deze herkend wordt, levert dit een hit op, terwijl andere gegevens niet bijgehouden worden. De informatie verzameld op basis van art. 126jj Sv. mag slechts 28 dagen bijgehouden worden.[217]

Het huidige probleem met art. 126jj Sv. is dat het zich specifiek richt op nummerplaatherkenning, niet op andere mogelijk gerichte gegevens of andere sensing-platforms, en dat de gegevens enkel mogen geraadpleegd worden in het specifieke kader van een opsporingsonderzoek (dus bij bevel van een officier van justitie), terwijl het wat betreft dataverzameling wel meer mogelijkheden geeft. Het is aan te raden om in eerste instantie the path of least resistance te volgen, en te werken met art. 3 van de Politiewet, omdat deze als toereikend gezien wordt voor de inzet van opsporingsmethoden die niet meer dan een lichte inbreuk op de persoonlijke levenssfeer betekenen. Dat kan bewerkstelligd worden door secuur om te gaan met de gerichtheid van de informatie die men wil verzamelen, dus welke selectie vooraf gemaakt wordt en de reden waarom deze informatie wordt opgenomen in de selectie. Daarenboven zou ook hier de duur van het

217 Https://www.om.nl/binaries/om/documenten/publicaties/2022/02/23/anpr-op-basis-van-artikel-3-politiewet-2012-fotos-van-herkenbare-personen/Samenvatting+advies+WBOM+-+ANPR-foto%27s+artikel+3+Politiewet+2012.pdf

bijhouden van de informatie beperkt moeten worden gehouden, en wie tot deze informatie toegang heeft, bijvoorbeeld enkel een specifieke dienst. Op termijn kan dan ook gekeken worden naar het gebruik van art. 126jj Sv. als wettelijke basis, maar dit is enkel mogelijk indien er een uitbreiding van het artikel komt van nummerplaatherkenning naar ook andere identificerende gegevens van een object of persoon, en naar andere soorten van sensing, niet enkel camera's.

Voor niet-gerichte data kan er teruggevallen worden op de juridische basis die ook besproken werd in het eerste project. Opnieuw speelt art. 3 van de Politiewet hier de hoofdrol. Ter herinnering, de politie kan op incidentele basis sensing-apparatuur installeren indien hier een concrete aanleiding voor is, en indien er een evaluatie wordt uitgevoerd van de noodzaak tot plaatsing ervan, inclusief of minder ver gaande maatregelen tot hetzelfde resultaat kunnen leiden. Wanneer de noodzaak kan worden aangetoond, moet een data protection impact assessment (DPIA) worden uitgevoerd, en het toezicht moet tenslotte kenbaar gemaakt worden. Indien er gebruik gemaakt wordt van een systeem waarbij enkel verdachte situaties geregistreerd worden, ofwel omdat een medewerker overgaat tot registratie ofwel omdat een AI-systeem beslist om te registreren, kan aan het incidentele karakter voldaan worden, zelfs indien het outsourcing contract een langere doorlooptijd heeft. De noodzaak ligt moeilijker, maar ook hier zou er beargumenteerd kunnen worden dat de registratie van het incident noodzakelijk werd geacht, niet zozeer de installatie van de sensing-apparatuur zelf. Dit verschuift de vraag dus van "is het noodzakelijk dat er een camera is?" naar "was het noodzakelijk dat de camera een incident registreerde?". Zelfs indien de eerste vraag moeilijk positief kan beantwoord worden, kan het antwoord op de tweede vraag wel "ja" zijn. Deze redenering zou echter verder uitgewerkt moeten worden, en zal uiteindelijk ook een rechterlijke toets niet kunnen ontlopen. Er zou op basis hiervan ook kunnen geopteerd worden om in eerste instantie enkel te werken met het verzamelen van gerichte data.

Randvoorwaarde: maak gebruik van art. 3 van de Politiewet wat betreft gerichte data, met bijzondere aandacht voor de selectie van de informatie waar naar gezocht wordt, de duurtijd van het bijhouden van de informatie, en de personen die toegang hebben tot de informatie. Wat betreft het laatste punt, kan gedacht worden aan een gespecialiseerde dienst.

Randvoorwaarde: wat betreft niet-gerichte data, moet een sluitende analyse gemaakt worden over het incidenteel karakter, de noodzaak en de subsidiariteit van het systeem. In afwachting daarvan, kan er geopteerd worden om het systeem enkel van start te laten gaan met het verzamelen van gerichte data.

6.5 *Prioriteit 3: realtime uitwisselen info voor specifiek evenement*

6.5.1 Uitleg project

Bij (openbare) evenementen zijn vaak zowel politie als particuliere bedrijven betrokken. Zij zijn elk apart wel bekend met een aantal potentiële dreigingen of bedreigende personen, maar deze informatie wordt niet (steeds) uitgewisseld. Dit kan wel wanneer leidinggevenden langs beide kanten informatie filteren en aan elkaar doorgeven via een landelijk aangeboden, snel en eenvoudig te gebruiken software systeem.

6.5.2 Scores inhoudelijke criteria en complexiteit

Het realtime uitwisselen van informatie in het kader van een specifiek evenement is wel één van de top-prioriteiten, zelfs met de herberekening. De efficiëntie/effectiviteit wordt door zowel politie als particuliere veiligheidsactoren hoog gescoord, en hoog geplaatst in vergelijking met andere projecten. De technische haalbaarheid komt wat betreft de scores vrij goed overeen (en is niet heel hoog), maar de politie is wel positiever over de haalbaarheid in relatie met de andere projecten (het project staat hoger in de ranking). De maatschappelijke wenselijkheid verschilt wel vrij sterk: de politie is vrij positief hierover, bij de particuliere veiligheidsactoren kan een lagere score gevonden worden. Dat is enigszins verbazingwekkend, omdat uit gesprekken blijkt dat dit soort uitwisseling op informele basis reeds gebeurt. Er is geen follow-up gesprek hierover gehouden, maar eventueel zou dit in het kader van een bijkomende Delphi-ronde kunnen bevraagd worden, ook om te peilen hoe de maatschappelijke wenselijkheid vergroot kan worden. Tenslotte zijn alle actoren het er ook over eens dat het om een vrij complex proces gaat om dit project uit te voeren, waarbij de politie wel een aantal andere projecten ziet die mogelijk meer complex in de uitvoering zijn, terwijl de particuliere veiligheidsactoren dit project hoog inschalen wat betreft complexiteit.

6.5.3 Bereikte consensus in de brainstormsessie

Er werd voornamelijk consensus bereikt over een aantal juridische aspecten van het systeem, namelijk dat het mogelijk zou moeten zijn om het gebruik van een dergelijk systeem te integreren in de vergunning voor een evenement, omdat daarin ook afspraken staan welke informatie er gedeeld wordt. Ook kan dan gebruikgemaakt worden van opschaling-mogelijkheden in de vergunning. Als er bijvoorbeeld uit het systeem signalen komen dat de initiële inschatting van gevaar te laag ingeschat werd, dan kan er extra personeel (vanuit de politie of de commerciële actor) ingezet worden. In het ontwerp van het systeem kan geprobeerd worden zo veel mogelijk efficiëntie in te bouwen, zodat er in het algemeen minder menselijke capaciteit en interventie nodig is, van zowel politie als beveiligers. Wel is het nodig om wettelijk of in elk geval via regulering vast te leggen wanneer er gebruikgemaakt kan/moet worden van een dergelijk systeem. Een dergelijk systeem lijkt het meest geschikt voor kleinere veiligheidsincidenten op middelgrote of grote evenementen (bij grote veiligheidsincidenten moeten er andere beslissingen genomen worden, zoals het stilleggen van het evenement). De regulering kan dan tevens een template bevatten hoe er via de vergunning afspraken vastgelegd kunnen worden.

De deelnemers van de brainstormsessie geloofden tevens dat het systeem verder uitgebreid kon worden. Zo kan via open source internetmonitoring (bijvoorbeeld door een andere commerciële partner) *real-time* in de gaten gehouden worden of er daar signalen komen van incidenten die zich voordoen. Ook bezoekers van het evenement zouden, eventueel via een filtering door de organisator, informatie kunnen toevoegen aan het systeem. Veel evenementen beschikken op dit moment reeds over een app waar bezoekers dingen kunnen melden (soms zo banaal als “het WC papier is op in toilet X”). Deze app gaat naar de organisator, waardoor de informatie ook zou kunnen toegevoegd worden aan het systeem. Zo kan een dreigingsanalyse constant aangepast worden.

De datakwaliteit en dataretentie blijven wel aandachtspunten voor het gebruik van dit systeem. Zo werden zorgen geuit dat de commerciële actor de informatie bij zal houden en zal gebruiken buiten het evenement zelf. Opnieuw kan een regulerend kader hier duidelijkheid scheppen. En voor het delen van niet-privacy gevoelige informatie (bijvoorbeeld: er wordt gevochten op plaats X, het is heel druk en daardoor minder veilig op plaats Y) is er zeker geen issue, waarvoor via dit systeem ook een standaardisering van informatie-uitwisseling kan bereikt worden.

De deelnemers waren het er over eens dat ook dit project een mogelijke link heeft met prioriteit 4 (doorgeven gevaarsindicatie), omdat het systeem ook gebruikt kan worden om gevaar indicaties te geven aan de commerciële partner. Daarnaast kan er een systeem gekoppeld worden waarin de commerciële actoren in real time melden en zelfs aangifte kunnen doen (dus met persoonsgegevens), waarna een bijna onmiddellijke opvolging kan plaatsvinden, terwijl de informatie vanuit de politie naar de commerciële actoren op een hoger niveau kan liggen, en aangeven waar er mogelijke dreigingen en gevaren zijn, zonder dat personen aangeduid worden. Maar ook hier kan in een template een onderscheid gemaakt worden op basis van type dreiging: bij heel acute en grote dreiging kan er toch voor gekozen worden persoonlijke informatie te delen, zoals in geval van een dreigende terroristische aanslag op het evenement.

Tenslotte werd tijdens de brainstormsessie nog de vraag gesteld of het nodig is om dit systeem te koppelen met een meldkamer, of dat het beter is om een apart systeem uit te werken waar politie en commerciële partners (en eventueel anderen) toegang toe hebben. De deelnemers geloofden dat beide mogelijkheden zijn, waarbij ook moet gekeken worden hoe beveiligd een dergelijk systeem kan worden gemaakt, mede vanwege het risico op hacking.

6.5.4 Randvoorwaarden

Zorg 1: de informatie zelf moet voldoende waardevol zijn

Het antwoord op de eerste zorg zit verwerkt in de opzet van het systeem: omdat informatie in eerste instantie door leidinggevenden aan beide kanten gefilterd wordt, is de waarde van de informatie hoog. Wel moeten leidinggevenden voldoende expertise hebben om deze filtering door te voeren, wat in een andere zorg behandeld wordt. Specifiek voor de waarde van de informatie is er derhalve geen aparte randvoorwaarde die moet worden gerealiseerd.

Zorg 2: er moet gewaakt worden voor het mogelijk oneigenlijk gebruik van de uitgewisselde informatie

De informatie die live gedeeld wordt in het kader van het evenement, kan moeilijk oneigenlijk gebruikt worden. Wel is het mogelijk gebruik van de informatie buiten het kader van het evenement een zorg, althans het gebruik door de particuliere veiligheidsactor van informatie in het systeem die verkregen werd door de politie. Bij de politie kan alle verkregen informatie gezien worden als een melding, en het registreren

van een melding is niet problematisch. Maar indien een particuliere veiligheidsactor in het kader van het evenement informatie doorkrijgt van de politie om bijvoorbeeld uit te kijken naar een bepaalde persoon, en de commerciële actor houdt nadien deze informatie bij, dan treedt er wel een potentieel problematische situatie op. Dit kan in eerste instantie geremedieerd worden door de contractuele relatie die de particuliere veiligheidsactor heeft met de organisator, waar ook het gebruik van het systeem ingeregeld kan worden (zie hierover later). Het is echter mogelijk dat dit niet voldoende is, als er een gebrek is aan afdwingbaarheid van de in het contract opgenomen regels. In dat geval kan er ook gewerkt worden met de gebruiksvoorwaarden van het systeem, of met het uitwerken van een wettelijk kader.

Naast het oneigenlijk gebruik van de informatie zelf, bestaat de vrees dat het systeem zal leiden tot het opbouwen van een grotere vertrouwensrelatie tussen de politie en de specifieke particuliere veiligheidsactoren die gebruik maken van het systeem, waardoor deze actoren mogelijk een bevoorrechte positie krijgen. Dit kan vermeden worden door het systeem in zo groot mogelijke mate open te stellen, zodat er weinig restricties zijn welke particuliere veiligheidsactoren gebruik kunnen maken van het systeem. Indien een grotere vertrouwensrelatie opgebouwd wordt met een groot aantal particuliere veiligheidsactoren, is er geen sprake van een bevoorrechte positie, en het vergroten van vertrouwen tussen deze actoren kan zelfs als een bijvangst gezien worden. Bovendien geldt dat alleen misbruik, niet gebruik, van een verkregen marktpositie strafbaar is, zoals staat in art. 29 e.v. MW.

Randvoorwaarde: neem in het contract voor het evenement of in de gebruiksvoorwaarden van het systeem duidelijke regels op dat de de uitgewisselde informatie enkel mag gebruikt worden in het kader van het evenement, en moet verwijderd worden nadat het evenement afgelopen is.

Randvoorwaarde: zorg voor een duidelijk kader, bijvoorbeeld met een Algemene Maatregel van Bestuur of een Ministeriële Regeling, die aangeven wat er wel en niet mag gedaan worden met de informatie in het systeem.

Randvoorwaarde: creëer zo weinig mogelijk barrières voor particuliere veiligheidsactoren om gebruik te maken van het systeem.

Zorg 3: de juiste actoren moeten betrokken worden bij de informatie-uitwisseling

Naast de politie en de particuliere veiligheidsactoren kunnen mogelijk nog andere partijen toegang hebben tot het systeem, of op zijn minst mogelijkheden om het systeem te voeden. De organisatoren van het evenement hebben, mag worden aangenomen, in de regel geen behoefte aan het uitlezen van informatie, maar kunnen wel nuttige informatie toevoegen. Veel evenementen beschikken op dit moment reeds over een app waar bezoekers incidenten of zorgen kunnen melden aan de organisator(soms zo banaal als “het WC papier is op in toilet X”). Relevante informatie, bepaalde categorieën meldingen, uit deze app kan toegevoegd worden aan het systeem. Zo krijgt het systeem nog een mogelijk bijkomende dimensie, niet enkel het delen van informatie tussen politie en particuliere veiligheidsactoren, maar ook het meer algemeen uitwerken van een dreigingsanalyse, wat de meerwaarde van het systeem verder zou verhogen. Hierop verder gaand werd in de brainstormsessie nog naar voor geschoven dat er ook via open source internet monitoring data ingebracht kan worden in het systeem, waarbij het mogelijk is dat nog andere particuliere veiligheidsactoren betrokken worden. Op deze manier zou men dus *real time* in de gaten kunnen houden of er signalen komen van mogelijke incidenten, waardoor dreigingsanalyses *real time* kunnen worden aangepast.

Het bovenstaande betreft geen randvoorwaarden voor het gebruik van het systeem, ze maken het systeem wel nuttiger. Om een duidelijk onderscheid te maken tussen nut en randvoorwaarde, nemen we ze derhalve niet op in een kader.

Zorg 4: de informatie-uitwisseling mag geen negatieve impact hebben op de werkzaamheden van de betrokken actoren

Het invullen van informatie in een systeem, dat bijkomend gefilterd wordt door leidinggevenden, neemt tijd in beslag die niet besteed kan worden aan andere veiligheidswerkzaamheden. Er moeten dus manieren gevonden worden om deze tijd zo veel mogelijk te beperken. Zo kan er met gestandaardiseerde categorieën gewerkt worden in het systeem, waarbij enkele klikken volstaan om informatie te sturen naar de leidinggevende. Of het systeem kan met stemherkenning werken; gesproken tekst uittypen en doorsturen. Ook wat het ontvangen van informatie betreft kan er zo veel mogelijk gestandaardiseerd gewerkt worden; met een korte mededeling waar het over gaat en wat er van de politie of particuliere veiligheidsactor verwacht wordt. Gebruiksvriendelijkheid staat derhalve voorop.

Randvoorwaarde: hou het inbrengen van informatie in het systeem en het ontvangen van informatie zo simpel en kort mogelijk.

Zorg 5: de informatie-uitwisseling mag geen negatieve impact hebben op de reputatie van de betrokken actoren

Alle actoren op het evenement streven naar veiligheid van de aanwezigen. De kans op reputatieschade lijkt miniem. Een mogelijkheid is dat particuliere veiligheidsactoren te veel gezien worden als een uitbreiding van de politie, als dat al als reputatieschade beschouwd kan worden. Om deze, maar ook om andere redenen, is het beter dat interactie met personen die van illegale activiteiten worden verdacht, uitgevoerd wordt door de aanwezige politie.

Randvoorwaarde: maak duidelijke afspraken dat commerciële veiligheidsactoren input kunnen geven, maar dat interactie met verdachten voorbehouden blijft aan de aanwezige politie.

Zorg 6: het systeem waardoor informatie uitgewisseld wordt, moet voldoende waarborgen bevatten en bruikbaar zijn

Eén waarborg die het systeem moet bevatten, werd hierboven reeds aangegeven, namelijk dat het niet de bedoeling is dat de uitgewisselde gegevens in het systeem nadien behouden worden door de particuliere veiligheidsactoren. Deze voorwaarde kan in het contract opgenomen worden, in de gebruiksvoorwaarden of in een nog te ontwikkelen regulerend kader, indien de beide voorgaande manieren als onvoldoende gezien worden. Een tegenhanger van deze randvoorwaarde is dat het wel noodzakelijk is om alle informatie die in of door het systeem gedeeld wordt, ook te documenteren/loggen. Het systeem mag dus niet voorzien in het mondeling meedelen van informatie (tenzij er een audio-opname beschikbaar is van de mededeling) of in het verwijderen van informatie die ingebracht werd. Verder moeten nog waarborgen uitgewerkt worden in verband met de veiligheid van het systeem (bijvoorbeeld de mogelijkheid dat het systeem gehackt kan worden). Deze zorg zal in het ontwerp en de werking van het systeem praktisch moeten worden weggenomen. Zowel politie als particuliere veiligheidsactoren hebben hier ervaring mee, zodat het aanbeveling verdient dat de ontwikkeling van het systeem binnen een publiek-private samenwerking gebeurt, met een stuurgroep met verschillende relevante actoren.

Bovenstaande werkwijze kan ook een positieve weerslag hebben op de bruikbaarheid van het systeem. Zo werd al aangegeven dat standaardisering de bruikbaarheid vergroot. Maar er kunnen nog andere specificaties bedacht worden. Indien de stuurgroep die het systeem ontwikkelt niet alleen politie en particuliere veiligheidsactoren bevat, maar ook evenementenorganisatoren, kunnen zij door een gezamenlijke ontwikkeling een systeem uitbouwen dat aan (elk van) hun wensen voldoet. Eventueel kunnen ook gemeenten hieraan toegevoegd worden, omdat een systeem dat een dreigingsanalyse bevat voor hen van belang kan zijn. In de brainstormsessie werd ook de vraag gesteld of het goed zou zijn om het systeem te koppelen aan een meldkamer. Dit zou een vraag kunnen zijn die beantwoord wordt in de stuurgroep, waarbij functionaliteit en veiligheid van het systeem afgewogen worden.

Het valt aan te raden om het systeem niet onmiddellijk groot in te zetten, maar te werken met een langere pilotperiode, die verschillende inzichten kan geven. Tijdens de pilot kan het systeem zelfs getest worden door ethische hackers, die proberen toegang te verkrijgen.

Een laatste vergroting van de bruikbaarheid is om op voorhand te definiëren voor welke evenementen het gebruik van dit systeem het meest geschikt is. Een dergelijk systeem lijkt het meest geschikt voor middelgrote of grote evenementen. Een gemeente kan een afweging maken over deze geschiktheid en bijvoorbeeld het verlenen van een vergunning laten afhangen van het gebruik van het systeem.

Randvoorwaarde: zorg ervoor dat alle informatie die in het systeem wordt ingevoerd werd, ook gedocumenteerd wordt.

Randvoorwaarde: ontwikkel het systeem in samenwerking met de gebruikers ervan, dus zowel politie, particuliere veiligheidsactoren als evenement organisatoren, en eventueel ook gemeenten.

Randvoorwaarde: zet het systeem uit via een langere pilot, waarbij er eerst op kleinere schaal getest wordt, en initiële fouten uit het systeem kunnen gehaald worden vooraleer het breed ingezet wordt.

Randvoorwaarde: verwerk het gebruik van het systeem in de regulering rond vergunningen van evenementen. De keuze kan daarbij nog steeds gegeven worden aan de vergunningverlener om het gebruik al dan niet te verplichten.

Zorg 7: er moet voldoende kennis/expertise aanwezig zijn bij alle betrokken actoren

De kennis noodzakelijk voor het ontwikkelen van het systeem werd reeds in de vorige zorg behandeld, dus we concentreren ons hier op het gebruik van het systeem zelf. Er kan training voorzien worden aan de gebruikers om de functionaliteiten van het systeem te

belichten. De meeste aandacht gaat daarbij uit naar de leidinggevenden, die beslissen welke informatie er teruggekoppeld wordt naar de publieke en private personen aanwezig op het evenement. Daarbij gaat het niet om de relevantie van de informatie: vanuit hun positie zouden zij voldoende ervaring moeten hebben om dit te beoordelen. De vraag is welke gegevens er wel en niet mogen worden gedeeld. Een juridische training is dus nodig. Zie daarbij ook de conclusie over Zorg 10; er mogen vrij veel gegevens gedeeld worden, zolang dit duidelijk afgesproken wordt.

Randvoorwaarde: voorzie gebruikerstrainingen voor het systeem, en trainingen aan de leidinggevenden om hen duidelijk te maken welke gegevens juridisch gezien mogen gedeeld worden en welke niet.

Zorg 8: er moet voldoende capaciteit aanwezig zijn bij alle betrokken actoren

Deze zorg speelt in beginsel geen grote rol bij dit project. Uiteraard moet er voor afhankelijk van de grootte van het evenement meer of minder capaciteit voorzien worden, maar het voorgestelde systeem is zelfs een mogelijke hulpbron hierbij, niet een stoorfactor. Indien het systeem ook een *real-time* dreigingsanalyse bevat, zoals al eerder besproken, kan op basis daarvan beslist worden om op het moment zelf capaciteit te verhogen of terug te schalen, wat de efficiënte inzet van zowel politionele als private capaciteit verhoogt. Hier is geen randvoorwaarde aan gekoppeld.

Zorg 9: er moet voldoende en een volgehouden wil tot informatie-uitwisseling aanwezig zijn bij alle betrokken actoren, wat betekent dat de meerwaarde voor iedereen duidelijk moet zijn

Dit project moet potentiële meerwaarde bieden aan zowel de politie, particuliere veiligheidsactoren als de organisatoren van de evenementen. Voor de volledigheid kunnen ook de gemeenten vermeld worden waar het evenement georganiseerd wordt, maar in dit geval hebben zij dezelfde belangen als de organisatoren: een betere samenwerking tussen de verschillende veiligheidsactoren op het evenement leidt tot een verbeterde veiligheidssituatie. Ook de commerciële veiligheidsactoren hebben een duidelijk voordeel bij het gebruik van het systeem, omdat zij informatie krijgen van de politie, die in beginsel over een betere informatiepositie beschikt (de beschikking over politiegegevens, waardoor zij beter het gevaar kunnen inschatten dat uitgaat van bepaalde personen of situaties). Indien het systeem ook een gevaar-indicatie bevat, kunnen zij hun eigen personeel ook beter beschermen. De zoektocht naar de meerwaarde is dus het belangrijkst voor de politie. Welke informatie kunnen zij verkrijgen uit het systeem die zij moeilijk(er) op een andere manier kunnen verkrijgen?

Deze zorg zou kunnen worden weggenomen door voorafgaandelijk aan de invoering van het systeem gesprekken te voeren met de particuliere veiligheidsactoren en hen te bevragen over de informatie waarvan zij geloven dat het een meerwaarde vormt voor de politie. Op basis daarvan kan een beslissing genomen worden tot invoer van het systeem. Echter, zelfs zonder deze bevraging zijn er indicaties dat het systeem een meerwaarde vormt voor de politie. Indien het systeem ook een *real-time* dreigingsanalyse bevat, kan de politie de eigen capaciteit optimaliseren, zoals hierboven reeds besproken. En indien het systeem ook toelaat aan de particuliere veiligheidsactoren om niet alleen meldingen te maken, maar ook melding of aangifte doen van verdachte activiteiten, kan de politie sneller potentieel gevaarlijke situaties voorkomen of beëindigen.

Randvoorwaarde: organiseer een bevraging van de particuliere veiligheidssector om na te gaan welke informatie zij potentieel kunnen leveren binnen het systeem, zodat er kan geëvalueerd worden of dit als een voldoende meerwaarde gezien wordt door de politie.

Randvoorwaarde: zorg ervoor dat het systeem niet enkel informatie uitwisselt, maar ook een algemene gevaar-indicatie levert, zodat acties (en capaciteit) daarop afgestemd kunnen worden.

Randvoorwaarde: laat particuliere veiligheidsactoren toe om niet alleen eenvoudige meldingen te maken, met standaardisering en op de meest eenvoudige manier, maar ook om aangifte te doen, waarbij wel meer informatie meegedeeld wordt.

Zorg 10: het juridisch kader waarbinnen de informatie-uitwisseling gebeurt, moet voldoende duidelijk zijn

Voordat er ingegaan wordt op het juridische kader voor het gebruik van het systeem, herhalen we nog eens een belangrijk juridisch aspect dat als consensus naar voren is gekomen in de brainstormsessie. Om de kans op succesvol gebruik van het systeem te optimaliseren, zou het goed zijn om het te integreren in het systeem van vergunningen voor een evenement. Daardoor wordt tevens tegemoetgekomen aan een vereiste van één van de relevante juridische kaders, namelijk de WPG. Deze stelt dat informatiedeling door de politie mogelijk is in opdracht van het bevoegde gezag, wat in deze situatie (de politie treedt op in een gemeente ter handhaving van de openbare orde en ter uitvoering van de hulpverleningstaak) volgens art. 11 van de Politiewet de burgemeester is.

Dit brengt ons bij de juridische kaders. Er zijn verschillende informatiestromen aanwezig in het systeem. Politie en particuliere veiligheidsactoren voeren beide gegevens in, waarbij er geen toegang is tot de gegevens die door anderen worden ingevoerd. Het zijn de leidinggevenden van beide actoren die de gegevens ontvangen van hun respectieve werknemers. De leidinggevenden beslissen welke informatie ze aan elkaar doorgeven, en deze informatie wordt door de leidinggevenden dan weer ingevoerd in het systeem naar hun werknemers. De juridische problematiek situeert zich dus op twee vlakken: de informatie die de politie deelt met de particuliere veiligheidsactoren, en de informatie die de particuliere veiligheidsactor registreert in het systeem.

Op de informatie die de politie deelt met de particuliere veiligheidsactoren is de WPG van toepassing. Artikel 19 van deze wet stelt dat informatie-uitwisseling aan derden op incidentele basis mogelijk is indien er een voldoende zwaarwichtig algemeen belang is, indien de uitwisseling gebeurt in overeenstemming met het bevoegd gezag, in dit geval de burgemeester, en indien het bijdraagt aan een aantal specifieke doeleinden, waarvan hier het handhaven van de openbare orde relevant is. Mogelijk zou ook gebruik kunnen worden gemaakt van art. 20 van de WPG, dat structurele uitwisseling in het kader van een samenwerkingsverband voorziet. Dit artikel verduidelijkt de samenwerking verder, omdat er vastgelegd moet worden welk zwaarwegend algemeen belang speelt, het doel van het samenwerkingsverband, welke gegevens verstrekt worden, onder welke voorwaarden en met wie. De vraag kan gesteld worden of een vergunning waarbij deze elementen geregeld worden, als basis kan dienen voor een samenwerkingsverband. Als er in de vergunning kan vastgelegd worden welke informatie onder welke voorwaarden kan gedeeld worden, is het wellicht mogelijk om de informatiedeling te differentiëren afhankelijk van de situatie, waardoor bij meer ernstige of meer acute dreigingen (een extreem geval zou een mogelijke extremistische aanval zijn op het evenement) meer specifieke informatie kan gedeeld worden. Het is onzeker of art. 19 WPG zo'n differentiatie toelaat, althans zonder dat de burgemeester telkens afzonderlijk toestemming moet geven. Om dit mogelijk te maken, zou de wet gewijzigd moeten worden.

Wat betreft de informatie die de particuliere veiligheidsactor registreert in het systeem, geldt in beginsel de AVG en de uitvoeringswet daarvan. Art. 5 van de AVG stelt over gewone persoonsgegevens dat er van een regelmatige verwerking sprake is onder een aantal voorwaarden, waarvan de relevante hier is dat de betrokkene toestemming heeft geven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden, of dat de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang. Toestemming van de betrokkene kan opgenomen worden in de voorwaarden voor toegang tot het evenement, wat nu bijvoorbeeld al gebeurt om het filmen van aanwezigen te rechtvaardigen. Maar ook de vervulling van een taak van algemeen belang kan hier naar voor geschoven worden, zeker indien er sprake is van een samenwerkingsverband met de politie (via de vergunning). Daarnaast voorziet de AVG ook een aantal bijzondere categorieën van persoonsgegevens (art. 9). De enige bijzondere categorie die mogelijk relevant zou kunnen zijn in deze context, is ras of etnische afkomst. Aan te raden valt om deze niet te registreren in het systeem, en op een andere manier personen te identificeren.

Randvoorwaarde: bepaal of het systeem mogelijk valt onder art. 20 van de WPG. Indien dit het geval is, verwerk dan in de vergunning situaties of voorwaarden waarbij overgegaan kan worden tot het delen van meer specifieke informatie.

Randvoorwaarde: verwerk de toestemming tot het registreren van gegevens in het systeem in de toelatingsvoorwaarden van het evenement.

Randvoorwaarde: registreer in het systeem geen gegevens die vallen onder bijzondere categorieën van persoonsgegevens, zoals voorzien in art. 9 van de AVG.

6.6 *Prioriteit 4: doorgeven gevaarsindicatie aan particuliere veiligheidsactoren*

6.6.1 Uitleg project

Particuliere bedrijven hebben in hun zaken een goed idee waar dreiging van uitgaat (persoon of organisatie), maar beschikken vaak niet over informatie over die dreiging waar de politie wel over beschikt (bijvoorbeeld: beschikt de persoon over een wapen). Daardoor ontstaat een niet-optimale threat assessment. Indien de politie een algemene gevaarsindicatie kan geven wanneer dit wordt gevraagd door een particulier bedrijf, is dit zeer gewenst. Ook de politie kan hierbij gebaat zijn, omdat ze dan op het juiste moment kan worden ingeschakeld.

6.6.2 Scores inhoudelijke criteria en complexiteit

Ook de gevaarsindicatie bleef na de herberekening een top-prioriteit. Bij efficiëntie/effectiviteit valt onmid-

dellijk de zeer hoge discrepantie op tussen de politie en de particuliere veiligheidsactoren, waarbij deze laatste het project met stip op 1 zetten, terwijl deze bij de politie bijna als laagste scoort. Dit terwijl beide het wel eens zijn over de score voor de technische haalbaarheid, en de politie deze zelfs vrij hoog inschat in vergelijking met de andere projecten. Indien de politie ook overtuigd zou worden van de efficiëntieslag die hier gemaakt kan worden, verhoogt dit de kans op selectie voor implementatie. Ook omdat de politie uiteindelijk de maatschappelijke wenselijkheid van het project wel hoog inschaalt, hoger zelfs dan de particuliere veiligheidsactoren. Wegens de mogelijke juridische belemmeringen die hieronder aan bod komen, zijn beide actoren het er wel over eens dat de implementatie vrij complex zou worden, met een aantal randvoorwaarden.

6.6.3 Bereikte consensus in de brainstormsessie

Dit project werd in de focusgroep als mogelijk zeer nuttig bestempeld. Er was wel overeenstemming dat het heel moeilijk met de privacy-richtlijnen te rijmen wordt wanneer de gevaarsindicatie ook persoonlijke informatie bevat (bijvoorbeeld: dreiging gaat uit van deze persoon, of kijk uit voor persoon met deze kenmerken). In dat geval is wettelijk ingrijpen noodzakelijk om een kader te creëren. Hiervan bestaat een mogelijk voorbeeld: in het kader van publiek-publieke informatie-uitwisseling staat bijvoorbeeld in de Wet Integriteitsbeoordeling door het Openbaar Bestuur (Wet Bibob) onder welke voorwaarden dit kan gebeuren. Hier kan inspiratie opgedaan worden hoe dat er voor publiek-private informatie-uitwisseling tussen de politie en particuliere beveiliging (of de bedreigde of klant) uit zou kunnen zien.

Waar er wel onmiddellijk (dus zonder verdere wetswijziging) veel mogelijkheden gezien worden, is het aangeven van een algemene gevaarsindicatie door de politie. Die kan gegeven worden aan de klant zelf, of aan de commerciële actor. In voorgaande prioriteiten werden ook mogelijke systemen aangereikt om die gevaarsindicatie door te geven (ook rechtstreeks aan de commerciële actor). Er lijkt hier sprake te zijn van een conflict van plichten: enerzijds is het geven van een gevaarsindicatie een manier om de veiligheid van een klant of de veiligheid van de werknemers van de commerciële actor te verhogen. Zodoende valt dit binnen zowel de wettelijke als morele taken van de politie. Anderzijds is er ook een plicht om grondwaarden, zoals privacy, van de bedreiger te vrijwaren. Wanneer er echter geen persoonlijke gegevens worden gedeeld, staat de verhoging van de veiligheid voorop. Hoe meer persoonlijke gegevens gedeeld worden, hoe meer de twee plichten in conflict komen met elkaar. Binnen dit dilemma kan ook worden gedacht over de noodzaak van opschaling: wanneer de veiligheid acuut in gevaar is, kan waarschijnlijk vaker of meer informatie over de dreiging worden gedeeld.

6.6.4 Randvoorwaarden

Zorg 1: de informatie zelf moet voldoende waardevol zijn

Er bestaat geen twijfel over de toegevoegde waarde van deze informatie. Meer nog; in de brainstormsessie werd duidelijk dat het geven van een gevaarsindicatie vaak samen kan gaan met andere projecten rond informatie-uitwisseling. Wanneer er reeds een communicatiekanaal open staat, is het gemakkelijker om ook gevaarsindicaties te delen. Wat betreft de inhoud van de gevaarsindicatie zijn er legio mogelijkheden. Dit moet in overleg afgestemd worden tussen de verschillende actoren. Om het systeem te optimaliseren is het nodig om eerst te weten te komen in welke omstandigheden een gevaarsindicatie gevraagd zal worden (door de particuliere veiligheidsactoren) en welke reactie als voldoende waardevolle informatie beschouwd wordt. De politie moet dan toetsen welke informatie zij kan/mag verstrekken. Zie hiervoor ook Zorg 2 (oneigenlijk gebruik), Zorg 4 (impact op werkzaamheden) en Zorg 10 (juridisch kader). Het opzetten van een beperkte pilot is hier nuttig, alsook continue evaluatie na de lancering van het project, om te blijven leren en verbeteren.

Randvoorwaarde: organiseer een bevraging naar de particuliere veiligheidsactoren om hun behoefte in kaart te brengen. Op basis daarvan kan bekeken worden welke mogelijkheden er zijn voor de politie om hieraan tegemoet te komen (bijvoorbeeld welk type gevaarsindicatie er gegeven kan worden).

Randvoorwaarde: zet het project in eerste instantie uit binnen een beperkte pilot, en voorzie een evaluatieperiode.

Randvoorwaarde: monitor het gebruik van het systeem op continue basis, om te leren en te verbeteren. Mogelijk kunnen op termijn ook nieuwe functionaliteiten (bijvoorbeeld gevaarsindicaties die meer informatie bevatten) toegevoegd worden.

Zorg 2: er moet gewaakt worden voor het mogelijk oneigenlijk gebruik van de uitgewisselde informatie

In de commentaren in de survey en in de brainstormsessie blijkt dit een grote zorg te zijn voor dit project. Oneigenlijk gebruik van de informatie zelf is waar-

schijnlijker naarmate meer gedetailleerde informatie gegeven wordt. Bij algemene gevaarsindicaties over een plaats of een situatie, is dit weinig waarschijnlijk, ook omdat de gevaarsindicatie naar alle waarschijnlijkheid zeer tijdelijk is: een plek die mogelijk gevaarlijk is op één moment, kan weer veilig zijn op een ander. Indien de gevaarsindicatie over een persoon gaat, is het gevaar van oneigenlijk gebruik groter, en zorg 10 laat ook zien dat de juridische situatie rond privacy in die omstandigheden complexer wordt. Mogelijk is zelfs een nieuw wettelijk kader hiervoor nodig. Het is daarom nuttig om bij de aanvang van dit project geen informatie over personen te delen, maar het te houden bij een indicatie van het gevaar van een plaats of situatie. Dat betekent niet dat de politie geen rekening houdt met personen, enkel dat er geen informatie over personen verstrekt wordt.

Naast het gebruik van de informatie zelf, vallen onder deze zorg nog een aantal andere aangehaalde punten. Net zoals in het vorige project, bestaat de vrees dat particuliere veiligheidsactoren die gebruik maken van een systeem van gevaarsindicaties door meer contact met de politie in een preferente positie komen, omdat een vertrouwensrelatie opgebouwd wordt. Een groei van vertrouwen tussen deze actoren is echter op zich geen negatieve evolutie. Indien er zo veel mogelijk openheid is over het gebruik van het systeem, speelt het bekomen van een preferente positie een kleinere rol. In zorg 2 behandelen we ook het punt of de politie wel de juiste actor is om de veiligheidsindicatie af te geven. Indien niet, komt dit aandachtspunt volledig te vervallen. Een ander aandachtspunt betrof de klant die mogelijk ook geholpen wordt bij een gevaarsindicatie (bijvoorbeeld wanneer het gaat over persoonlijke bescherming). Indien deze klant zelf criminele activiteiten ontplooit, is het dan de taak van de politie om ervoor te zorgen dat deze persoon beter beschermd wordt? De logica achter dit aandachtspunt is echter enigszins vreemd te noemen. Ten eerste hebben ook criminelen het recht op bescherming. Mogelijk kan er moreel geoordeeld worden dat criminele klanten het minder 'verdienen' om beschermd te worden, maar de wet voorziet geen categorieën van personen die meer of minder bescherming verdienen. Ten tweede wordt er door de gevaarsindicatie niet alleen meer bescherming gegeven aan de klant, maar ook aan de werknemers van de particuliere veiligheidsactor die voor de bescherming van de klant instaan (en de omgeving van de klant en beveiliger). Het hebben van een criminele achtergrond van een klant, maakt niet dat deze het minder verdient om beschermd te worden. Mogelijk kunnen de particuliere veiligheidsactoren hier wel zelf een rol spelen, door de klanten die zij hebben te screenen en contracten te weigeren. Dit gebeurt in de praktijk ook al, maar tegelijkertijd toont project 5 dat het moeilijk is om deze screening exhaustief uit te voeren.

Randvoorwaarde: zorg er voor dat bij de aanvang van dit project de gevaarsindicatie geen informatie over personen bevat, enkel over plaatsen of situaties. In een later stadium kan de inclusie van persoonlijke informatie onderzocht worden. Hier is mogelijk een nieuw wettelijk kader voor nodig.

Randvoorwaarde: hou het systeem zo open mogelijk, zodat een zo groot mogelijk aantal particuliere veiligheidsactoren er gebruik van kunnen maken. Zo wordt de kans op de ontwikkeling van preferentiële relaties geminimaliseerd.

Zorg 3: de juiste actoren moeten betrokken worden bij de informatie-uitwisseling

Het project gaat in eerste instantie uit van een gevaarsindicatie die door de politie wordt afgegeven aan particuliere veiligheidsactoren, maar dit hoeven niet de enige actoren te zijn die gebruik kunnen maken van een dergelijk systeem. Eén mogelijkheid is dat de gevaarsindicatie aan de klant gegeven wordt, en niet aan de particuliere veiligheidsactor. Dit kan om juridische redenen mogelijk een eenvoudigere route zijn, tenzij de klant expliciet toestemming geeft om de informatie ook door te geven aan de particuliere veiligheidsactor. Tegelijkertijd is deze omweg wellicht niet nodig, omdat er beargumenteerd kan worden dat de gevaarsindicatie niet over de klant gaat, maar over het gevaar voor de werknemers van de particuliere veiligheidsactor. Deze heeft dan een fiduciaire verantwoordelijkheid onder art. 5 van de Arbeidsomstandighedenwet om hen hierover in te lichten.

Niet alleen particuliere veiligheidsactoren hebben baat bij het krijgen van een gevaarsindicatie, maar ook veel andere organisaties. Dit mag niet geïnterpreteerd worden als een reden om dit project niet uit te voeren, maar eerder als aanmoediging om het systeem (mogelijk op een later tijdstip) ook voor andere soorten maatschappelijke organisaties aan te bieden.

Een laatste punt onder deze zorg is de vraag of de politie de juiste actor is om de gevaarsindicatie af te geven. Enerzijds voorziet art. 3 van de Politiewet dat de politie hulp verleent aan hen die deze behoeven, en er kan beargumenteerd worden dat een advies over het gevaar waarin iemand zich bevindt, daaronder valt. Anderzijds zijn er overheidsorganen die zich hebben gespecialiseerd in procedures rond screening, waarbij een afweging gemaakt wordt tussen de belangen van het individu (recht op privacy) en de belangen van de samenleving. Met name kan dan aan de screenings-

autoriteit Justis gedacht worden. Bij de verdere ontwikkeling van het systeem, indien een wettelijk kader voorziet in de mogelijkheid om ook informatie over personen toe te voegen aan het systeem, wordt de afweging van deze belangen nog belangrijker, en kan het dus nuttig zijn om met een gespecialiseerde dienst te werken.

Randvoorwaarde: onderzoek in hoeverre het systeem ook kan opengezet worden voor andere actoren dan particuliere veiligheidsorganisaties, inclusief burgers.

Randvoorwaarde: onderzoek of de politie de juiste actor is om de gevaarsindicatie af te leveren. Mogelijk is een actor zoals Justis hier meer geschikt voor, zeker indien op termijn ook afwegingen moeten gemaakt worden of er ook informatie over personen gedeeld kan worden.

Zorg 4: de informatie-uitwisseling mag geen negatieve impact hebben op de werkzaamheden van de betrokken actoren

De werkzaamheden van de politie kunnen eventueel beïnvloed worden indien veelvuldig gebruikgemaakt wordt van het systeem, maar dit punt wordt verder behandeld bij Zorg 8 (capaciteit actoren). Daarnaast kunnen de werkzaamheden van de politie ook in gevaar komen wanneer uit de gevaarsindicatie achterhaald kan worden op welke informatie gebaseerd werd om tot de indicatie te komen. Een voorbeeld is een lopend opsporingsonderzoek waarbij telecommunicatie afgeluisterd wordt. Zeker indien de gevaarsindicatie ook haar weg vindt naar diegenen die verantwoordelijk zijn voor het gevaar, wat altijd een mogelijkheid is, zijn hier significante risico's aan verbonden. De Dienst Landelijke Informatieorganisatie binnen de politie heeft hier in principe ervaring mee, gezien hun verantwoordelijkheid voor het opstellen van verschillende informatieproducten, van dreigingsmeldingen tot risicoanalyses,[218] binnen het Stelsel Bewaken en Beveiligen. Er kan van hun expertise gebruikgemaakt worden om dit risico te minimaliseren, of in te schatten welke informatie wel en niet gedeeld kan worden, nog onafhankelijk van de juridische mogelijkheid tot het delen van informatie.

De gevaarsindicatie kan ook een effect hebben op het gedrag van de werknemers van de particuliere veiligheidsactor. De indicatie kan een vals gevoel van veiligheid creëren of juist voor bijkomende stress zorgen, waardoor de werknemers mogelijk sneller overgaan tot het gebruik van fysiek geweld voorbehouden aan de politie. Hier is voorlichting belangrijk, en mogelijk kunnen ook bij het leveren van de gevaarsindicatie zelf instructies worden gegeven over hoe zich te gedragen. Een particuliere veiligheidsactor kan bijvoorbeeld bij een hogere gevaarsindicatie de eigen werknemers eraan herinneren dat het preventief gebruik van fysiek geweld nog steeds niet toegelaten is, onafhankelijk van de dreiging. Verder zou het goed zijn om op dit aspect gericht te evalueren. Als in een pilot of later blijkt dat in veel gevallen een gevaarlijke gedragsverandering plaatsvindt, zou dit reden moeten zijn om dit project stop te zetten.

Randvoorwaarde: Bespreek de mogelijkheden wat betreft het detailniveau van de dreigingsanalyse met de Dienst Landelijke Informatieorganisatie, gezien hun ervaringen binnen het Stelsel Bewaken en Beveiligen.

Randvoorwaarde: evalueer in een pilot en ook nadien op continue basis in hoeverre het geven van een gevaarsindicatie ook het gedrag van werknemers van particuliere veiligheidsactoren beïnvloedt. Werk een systeem uit van trainingen en instructies om deze gedragsbeïnvloeding te beperken.

Zorg 5: de informatie-uitwisseling mag geen negatieve impact hebben op de reputatie van de betrokken actoren

Deze zorg lijkt bij dit project minder relevant te zijn. De enige mogelijkheid dat de relatie tussen particuliere veiligheidsactor en klant geschaad kan worden is indien uit een gevaarsindicatie blijkt dat het contract met de klant grote veiligheidsrisico's met zich meebrengt. Maar het is net het doel van het project om dit te weten te komen, en dus geen reden om het project niet aan te vangen, of randvoorwaarden te ontwikkelen om deze zorg te vermijden.

Zorg 6: het systeem waardoor informatie uitgewisseld wordt, moet voldoende waarborgen bevatten en bruikbaar zijn

Bij zorg 2 werd reeds de waarborg ingebouwd dat in eerste instantie geen informatie over personen toegevoegd wordt aan de gevaarsindicatie. Op termijn zou dit wel onderzocht kunnen worden. Het juridische kader dat daarvoor uitgewerkt wordt, moet waarborgen bevatten om dit op een veilige manier te doen. Hierboven werd reeds gesproken over het afwegen van de rechten van het individu tegen de bescherming van de samenleving. Hier kan nog aan toegevoegd worden dat ook de bescherming van de werknemers van de particuliere veiligheidsactoren en hun klanten een

218 Art. 3.2 van de Circulaire met betrekking tot de bewaking en beveiliging van personen, objecten en diensten 2019.

rol speelt in deze afweging. Inspiratie kan mogelijk gehaald worden uit de Wet Bibob. Hoewel het hier gaat om informatie-uitwisseling tussen publieke actoren, zijn er parallellen te trekken. In het kader van deze wet kan er advies worden gevraagd aan het Landelijk Bureau Bibob (onderdeel van Justis), dat dan zonder te veel extra informatie te verstrekken, een indicatie kan geven over het al dan niet intrekken van een vergunning.

Er kan ook beargumenteerd worden dat dit project de waarborgen op het correcte gebruik van informatie vergroot. Uit de praktijk blijkt dat het geven van advies aan particuliere veiligheidsactoren door de politie reeds op informele basis veelvuldig gebeurt. Het formaliseren van deze informatie-uitwisseling geeft het een stevige basis en de mogelijkheid tot toezicht op een correcte uitvoering ervan. Formalisering optimaliseert ook de bruikbaarheid van het systeem, omdat er meer actoren toegang krijgen.

De bruikbaarheid hangt samen met het type van gevaarsindicatie dat de politie (of Justis) kan geven. Dat kan gaan om een punt op een schaal (weinig gevaarlijk tot heel gevaarlijk), maar ook om meer specifiek advies, zoals "de inzet van de politie is gewenst" of "het valt aan te raden de bescherming van de klant te verhogen" (of naar de klant toe; "we raden aan om uzelf beter te beschermen)". Bij Zorg 1 hebben we al een randvoorwaarde ontwikkeld om dit in kaart te brengen. Om de waarde van de gevaarsindicatie nog verder te verhogen, kan er ook onderzocht worden of er mogelijkheden zijn tot opschaling: meer acute dreigingen kunnen dan leiden tot meer gedetailleerde gevaarsindicaties. Dit past in het dilemma van het afwegen van verschillende belangen (privacy personen, bescherming samenleving, bescherming individuen).

Randvoorwaarde: onderzoek de waarborgen die zijn ingebouwd bij vergelijkbare systemen, zoals bijvoorbeeld de adviesaanvraag onder de Wet Bibob. Indien relevant, kunnen deze opgenomen worden in het nog verder uit te werken wettelijk kader.

Randvoorwaarde: onderzoek of het op termijn ook mogelijk is om te differentiëren in de informatie die de gevaarsindicatie bevat, waarbij meer acute dreigingen kunnen leiden tot meer informatie-uitwisseling.

Zorg 7: er moet voldoende kennis/expertise aanwezig zijn bij alle betrokken actoren

Hier gaat het in eerste instantie over de juridische expertise bij de actor die de gevaarsindicatie afgeeft: in hoeverre is de kennis aanwezig over wat wel en wat niet gedeeld mag worden. Zoals al eerder aangegeven bij Zorg 3, is het mogelijk dat een andere actor hier meer geschikt voor is, namelijk een gespecialiseerde dienst zoals Justis. Zelfs indien dit niet het geval is, is het nuttig om het leveren van een gevaarsindicatie door de politie ofwel te centraliseren, ofwel te beleggen bij specifieke diensten binnen elke politieregio. Aan deze centrale dienst of regionale diensten kunnen dan trainingen aangeboden worden.

Randvoorwaarde: beleg het verlenen van de gevaarsindicatie bij een specifieke organisatie buiten de politie (zoals Justis), of voorzie een centrale dienst of regionale diensten binnen de politie die de verantwoordelijkheid krijgen hierover. Voorzie juridische training aan deze diensten om duidelijk te maken wat er kan meegedeeld worden in de gevaarsindicatie.

Zorg 8: er moet voldoende capaciteit aanwezig zijn bij alle betrokken actoren

De capaciteit hangt samen met de expertise, waardoor ook dezelfde randvoorwaarde geldt. De verantwoordelijke diensten moeten voldoende bemand zijn om de aanvragen aan te kunnen. Afhankelijk van de populariteit van het systeem kan een opschaling of afschaling noodzakelijk worden.

Randvoorwaarde: monitor het aantal aanvragen voor gevaarsindicaties, en stel daar de capaciteit van de diensten verantwoordelijk voor het verlenen van de aanvragen op af. Dit kan tijdens een pilot gebeuren voor de initiële inschatting van de capaciteit, maar blijvende monitoring is nodig.

Zorg 9: er moet voldoende en een volgehouden wil tot informatie-uitwisseling aanwezig zijn bij alle betrokken actoren, wat betekent dat de meerwaarde voor iedereen duidelijk moet zijn

De meerwaarde voor de aanvragers van het systeem is duidelijk, maar de vraag is in hoeverre de politie meerwaarde haalt uit het in gebruik nemen van een dergelijk systeem. Nieuwe informatie wordt door hen in eerste instantie niet verkregen. Wel kan het zijn dat door de aanvraag vanuit de particuliere veiligheidsactor de politie meer zicht krijgt op situaties die mogelijk meer aandacht zouden moeten krijgen, dus de keuze kan maken om zelf actie te ondernemen. In afwezigheid van een aanvraag voor een gevaarsindicatie zou de politie naar alle waarschijnlijkheid in veel gevallen geen andere signalen gekregen hebben. Of dit voldoende is om als een echte meerwaarde te zien, is evenwel vooraf onduidelijk. Een argument om toch in te stappen is, zoals boven reeds beschreven, dat het geven van een

gevaarsindicatie valt onder de bredere noemer van de algemene politietaak zoals genoemd in art. 3 van de Politiewet; het verlenen van hulp aan hen die deze behoeven. Op die basis kan er geen sprake zijn van het uitsluiten van enige burger of bedrijf uit het systeem, omdat de politie gehouden is om deze dienst in principe aan iedereen aan te bieden. De enige mogelijke uitzondering daarop is wanneer er een testfase is voor de inwerkingtreding van een systeem. Een pilot moet dan wel de bedoeling hebben om de werking van het systeem te evalueren met als doel het toegankelijk te maken voor iedereen.

Opnieuw kan de oplossing liggen in het verschuiven van het verschaffen van de gevaarsindicatie naar een gespecialiseerde dienst zoals Justis, die aanvragen kan behandelen indien het juiste kader hiervoor gemaakt wordt. Dat is dan weer het nadeel van deze verschuiving, omdat het geven van een gevaarsindicatie vanuit de politie op zich geen nieuwe wetgeving behoeft, maar indien Justis deze moet verzorgen er wel een nieuwe wettelijke basis hiervoor nodig is Een bijkomend voordeel voor het gebruik van Justis is dat in dit geval de dienst ook betalend kan gemaakt worden, zoals bijvoorbeeld bij een VOG. Dit kan tevens een mogelijke overvraging van het systeem tegengaan. Het werpt een barrière op om zelfs zonder enige aanwijsbare reden een vraag voor gevaarsindicatie te stellen.

Randvoorwaarde: verplicht de politie tot het organiseren van het afleveren van gevaarsindicaties, op basis van de algemene politietaak zoals genoemd in art. 3 van de Politiewet.

OF

Randvoorwaarde: creëer een wettelijk kader waarbij Justis de verantwoordelijkheid krijgt om gevaarsindicaties te leveren, eventueel tegen betaling.

Zorg 10: het juridisch kader waarbinnen de informatie-uitwisseling gebeurt, moet voldoende duidelijk zijn

Zoals reeds eerder besproken, is het huidige juridische kader voor het geven van een gevaarsindicatie niet geheel duidelijk of aanwezig. Voor een algemene gevaarsindicatie zonder het delen van persoonsgegevens, zelfs indien deze gegevens door de politie gebruikt werden om tot de indicatie te komen, lijken er geen juridische bezwaren te zijn. De politie mag steeds een inschatting geven hoe (on)gevaarlijk zij een situatie vinden. Wanneer de gevaarsindicatie gericht is op een persoon, worden de mogelijkheden echter een stuk beperkter. Artikel 1 van de WPG ziet alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon als persoonsgegevens. Indien deze gegevens verwerkt zijn in het kader van de uitvoering van de politietaak, dan gaat het om politiegegevens die niet zomaar met derden kunnen gedeeld worden. Mogelijk kan art. 19 van de WPG een basis vormen voor het meedelen van deze politiegegevens, opnieuw met de redenering dat het gaat om het ‘ verlenen van hulp aan hen die dat behoeven’ (één van de legitieme doeleinden). Dan nog zou een zwaarwegend belang en overeenstemming met het bevoegde gezag, in dit geval de burgemeester, aangetoond moeten worden.

Deze omslachtige manier van werken kan gestroomlijnd worden door een specifieke dienst binnen de politie of een dienst buiten de politie (zoals Justis) verantwoordelijk te maken voor het verlenen van de gevaarsindicatie, en hiervoor een apart juridisch kader te ontwikkelen. Dit kader kan geïntegreerd worden in de WPG. Mogelijk inspiratiebronnen zijn Afdeling 5 van Wet Justitiële en Strafvorderlijke Gegeven (WJSG) s, die de verklaringen omtrent het gedrag regelt, of Hoofdstuk 4 van de Wet Bibob, die voorziet in adviezen vanuit een landelijk bureau.

Randvoorwaarde: kijk naar vergelijkbare wetgeving zoals de WJSG of de Wet Bibop om een juridisch kader te creëren waardoor een dienst binnen of buiten de politie verantwoordelijk gesteld wordt voor de gevaarsindicaties. Integreer dit in de WPG.

6.7 *Prioriteit 5: opsporingsindicatie*

6.7.1 Uitleg project

Particuliere veiligheidsactoren hebben er belang bij om te weten of er binnen nieuwe of bestaande klanten opsporingsonderzoeken lopen. Het is minder belangrijk om te weten tegen wie die gericht zijn, enkel of ze lopen. De politie kan op aanvraag informatie geven aan (vertrouwde) particuliere veiligheidsactoren. Met dat ‘signaal’ kunnen de bedrijven bij hun klant aandringen meer maatregelen tegen criminaliteit te nemen.

6.7.2 Scores inhoudelijke criteria en complexiteit

De opsporingsindicatie bleek bij de herberekening uiteindelijk niet tot de top-prioriteiten te behoren. Net zoals bij de gevaarsindicatie lopen de ideeën over efficiëntie/effectiviteit bij politie en particuliere veiligheidsactoren vrij ver uit elkaar, waarbij de particuliere sector een stuk enthousiaster is. Tegelijkertijd beseffen beide actoren dat de technische haalbaarheid van dit project moeilijk ligt, en de particuliere veilig-

heidsactoren geven het zelfs de laagste score van alle projecten. Over de maatschappelijke wenselijkheid is er dan wel weer een verschillende mening: hoewel de absolute scores dicht bij elkaar liggen, zien de particuliere veiligheidsactoren een grotere maatschappelijke wenselijkheid dan de politie in vergelijking met de andere projecten. De complexiteit van een opsporingsindicatie is volgens beide actoren ook vrij hoog, maar de politie ziet wel nog meer complexiteit bij een aantal andere projecten, terwijl dit project bij de particuliere veiligheidsactoren de top 5 haalt. Het valt wel op dat zowel politie als particuliere veiligheidsactoren de opsporingsindicatie als minder complex ervaren dan het implementeren van het project gevaarsindicatie, terwijl de opsporingsindicatie in principe in het huidige juridische kader meer mogelijkheden geeft (zie daarover de juridische analyse hieronder).

6.7.3 Bereikte consensus in de brainstormsessie

Vooraleer de politie een evaluatie kan maken of men dit soort informatie wil delen (onafhankelijk van de wettelijke mogelijkheden daartoe), is het noodzakelijk om per geval eerst duidelijkheid te verkrijgen waarom de commerciële actor deze informatie opvraagt.

De grootste vraag bij deze prioriteit is wat de politie eigenlijk kan delen over het al dan niet bestaan van opsporingsonderzoeken. Vaak zal dit niet het geval zijn, omdat de politie ook niet mag zeggen dat er een onderzoek gaande is (omdat dit het onderzoek kan schaden). Commerciële actoren komen zo in een lastig parket terecht: indien zij signalen krijgen (vaak ook gebaseerd op gut feelings) dat er iets niet in de haak zit, kunnen zij in sommige gevallen wegens reputatieschade beter weigeren om een opdracht van een klant te aanvaarden. Maar dit betekent dat opdrachten die de veiligheid potentieel kunnen verhogen, toch niet aanvaard zullen worden. In andere gevallen kan het juist een goede aanleiding zijn om een klant te helpen criminaliteit terug te dringen.

Mogelijk kan er op een andere manier toch dit soort informatie uitgewisseld worden. Daarvoor kan worden gedacht aan vrijwillige uitwisseling of uitwisseling op grond van een vergunning of convenant. In dit geval gaat het bijvoorbeeld om een vraag die gesteld wordt aan de politie door de commerciële actor, waarbij geen van beiden een overeenkomst met elkaar hebben. Indien dit soort uitwisseling wordt afgesproken in het kader van een publiek-private samenwerking, waardoor het ook duidelijk wordt welke doelen nagestreefd worden door deze informatie uit te wisselen, en hoe dit ook bijdraagt aan de doelen van de politie, dan is het waarschijnlijker dat men elkaar wel vindt. Maar dat is dus wel een andere opzet dan de vrijwillige uitwisseling waar de top-prioriteit initieel van uitging.

6.7.4 Randvoorwaarden

Zorg 1: de informatie zelf moet voldoende waardevol zijn

In tegenstelling tot het vorige project, was er hier minder eensgezindheid rond de precieze waarde van het verkrijgen van een opsporingsindicatie. Voor particuliere veiligheidsactoren kan het een rol spelen in het bepalen of men al dan niet een contractuele relatie wil aangaan of voortzetten met een (potentiële) klant, waarbij de beslissing zeker niet altijd negatief hoeft uit te vallen: nu werken particuliere veiligheidsactoren ook vaak voor organisaties waarvan ze weten dat er criminaliteit plaatsvindt. Of de klant wil weten of er al dan niet opsporingsonderzoeken lopen is ook vooraf niet eenduidig te beantwoorden, maar van een bonafide organisatie mag worden geacht dat zij in een opsporingsindicatie motivatie vindt om te proberen meer preventieve maatregelen te nemen. In bepaalde gevallen is het waardevolle informatie. Er moet worden onderzocht in welke situaties dit het geval is, of dit ook correspondeert met de gevallen waarin de politie bereid is een opsporingsindicatie aan te leveren en hoe gedetailleerd deze informatie mag zijn. Met andere woorden: welk niveau van detaillering is nuttig en is het mogelijk of zelfs wenselijk vanuit de doelstelling van criminaliteitspreventie om die informatie te geven? Hieruit kan worden geanalyseerd welke informatie in een aanvraag (en doorvraag) moet worden gevraagd en gegeven. Moet bijvoorbeeld de waarde van het opsporingsonderzoek of waarover het gaat, meegenomen worden in de evaluatie? Wat als het om een relatief kleine overtreding gaat, of als het opsporingsonderzoek nog loopt, maar op een dood spoor zit? Moet dit dan vermeld worden in het rapport van de opsporingsindicatie, of volstaat bijvoorbeeld de melding dat er geen ernstige opsporingsonderzoeken zijn of geen opsporingsonderzoeken van voldoende waarde?

Uiteraard is het goed dit in een pilot en na bredere invoering te blijven evalueren en verbeteren. De randvoorwaarden hier zijn derhalve gelijkaardig aan het vorige project, met de waarschuwing dat het animo voor dit project beduidend lager lag.

Randvoorwaarde: organiseer een onderzoek onder particuliere veiligheidsactoren om hun behoeften in kaart te brengen. Op basis daarvan kan bekeken worden welke mogelijkheden er zijn voor de politie om hieraan tegemoet te komen.

Randvoorwaarde: start een beperkte pilot, inclusief een evaluatieperiode.

Randvoorwaarde: monitor het gebruik van het systeem op continue basis, om te leren en te verbeteren.

Zorg 2: er moet gewaakt worden voor het mogelijk oneigenlijk gebruik van de uitgewisselde informatie

Net zoals bij het vorige project is dit een grote zorg. In de brainstormsessie werd opgemerkt dat het nodig was dat er per geval moest gemeld worden waarom de particuliere veiligheidsactor de opsporingsindicatie wil krijgen, uit bezorgdheid voor 'verkeerde' redenen. Opnieuw is het niveau van detail belangrijk. Het geven van informatie over personen lijkt hier helemaal uit den boze te zijn, zie daarvoor ook Zorg 10 rond het juridisch kader. Om het project enige kans van slagen te geven lijkt het dat het enkel mogelijk is om in de meest algemene termen de opsporingsindicatie te geven; lopen er wel of niet één of meerdere opsporingsonderzoeken? En zelfs dan zijn er wijzigingen nodig aan het huidige wettelijk kader om dit mogelijk te maken.

Het afleveren van een opsporingsindicatie in de meest algemene termen, moet wel samen bezien worden met zorg 5, waarvoor het nodig kan zijn om te variëren in de bewoordingen van een opsporingsindicatie. Bij een groot opsporingsonderzoek kan het nodig zijn om enkel aan te geven dat er een negatief advies gegeven wordt wat betreft de opsporingsindicatie Bij minder ernstige feiten kan de criminaliteitspreventie belangrijker zijn, en kunnen de bewoordingen aangepast worden om wel een meer duidelijke indicatie mogelijk te maken.

Randvoorwaarde: geef enkel in de meest algemene termen een opsporingsindicatie.

Zorg 3: de juiste actoren moeten betrokken worden bij de informatie-uitwisseling

Ook gelijkaardig aan het vorige project is de vraag of de aanvragen voor een opsporingsindicatie voorbehouden moeten worden aan particuliere veiligheidsactoren. Op zich is er geen specifieke reden waarom zij als enigen hier gebruik van zouden mogen maken. Ook de klant, zelfs al laat Zorg 1 zien dat daar mogelijk niet altijd interesse voor is, kan zelf de aanvraag doen. In de survey werd gesteld dat de eigenaar van het bedrijf waar de opsporing plaatsvindt zelfs de betere partij kan zijn die middels de opsporingsindicatie zou moeten worden geïnformeerd en geadviseerd. Criminaliteitsbestrijding kan hier als leidend principe gezien worden: de klant moet gemotiveerd worden om preventieve maatregelen te nemen, al dan niet met inschakeling van particuliere veiligheidsactoren. Een opsporingsindicatie, zeker naar een klant toe die welwillend is, maar nog niet veel aan criminaliteitspreventie doet, en/of erg voor haar reputatie vreest, kan de motor zijn tot preventieve maatregelen. De particuliere veiligheidsactor kan ook steeds de aanvrager zijn voor de opsporingsindicatie, bijvoorbeeld door dit op te nemen in het contract met de klant.

Verder speelt ook hier opnieuw de zorg of de politie de juiste actor is om de gevaarsindicatie af te geven. Bij project 4 hebben we al geduid dat er een afweging tussen de belangen van het individu en de belangen van de samenleving, en hoe meer gedetailleerd de informatie is, hoe meer de belangen van het individu (of in dit geval de rechtspersoon) spelen. De vraag of er een opsporingsonderzoek loopt tegen de rechtspersoon of werknemers ervan, is zeer gedetailleerde informatie, zelfs al worden er geen gegevens verspreid over het soort onderzoek. Indien een wettelijk kader ontwikkeld wordt dat deze informatie-uitwisseling mogelijk maakt, heeft het gebruik van een bestaande screeningsautoriteit zoals Justis voordelen tegenover het beleggen van deze taak bij de politie.

Tenslotte kunnen net zoals in het vorige project ook andere organisaties het nuttig vinden om opsporingsindicaties te krijgen over een bedrijf, bijvoorbeeld in het kader van een fusie of zelfs het al dan niet afsluiten van een contract. Ook hier kan de opsporingsindicatie mogelijk aan de andere partij gegeven worden, en kan het aanvragen ervan als voorwaarde gesteld worden om een relatie aan te gaan.

Randvoorwaarde: indien dit in het kader van criminaliteitspreventie beter is, maak dan de klant de standaard aanvrager voor een opsporingsindicatie.

Randvoorwaarde: onderzoek of de politie de juiste actor is om de gevaarsindicatie af te leveren. Een bestaande screeningsautoriteit zoals Justis is waarschijnlijk meer geschikt.

Randvoorwaarde: onderzoek in hoeverre het systeem ook kan opengesteld worden voor andere actoren dan particuliere veiligheidsorganisaties, inclusief burgers.

Zorg 4: de informatie-uitwisseling mag geen negatieve impact hebben op de werkzaamheden van de betrokken actoren

In tegenstelling tot het vorige project is hier weinig gevaar dat werknemers van de particuliere veiligheidsactor een vals gevoel van veiligheid zullen krijgen of bijkomende stress, want de opsporingsindicatie beschrijft waarschijnlijk niet een specifieke situatie in detail - de beveiliging kan uiteraard wel een rol spelen in de criminaliteit die bij de klant plaatsvindt, alsook de bestrijding daarvan. Wel kan er door de particuliere veiligheidsactor beslist worden om een contract niet af te sluiten indien een opsporingsonderzoek loopt, maar dat lijkt een legitieme impact te zijn op de werkzaamheden, en niet een zorg om weg te nemen.

De grootste zorg ligt dus bij de impact op de werkzaamheden van de politie, omdat er informatie vrij komt over een lopend opsporingsonderzoek waarvan de personen tegen wie het onderzoek loopt, nog niet in kennis gesteld zijn. Om dat te voorkomen, kunnen er twee maatregelen genomen worden. De eerste maatregel werd reeds hierboven als randvoorwaarde geschetst: enkel in de meest algemene termen een opsporingsindicatie afleveren. Op die manier is het niet mogelijk om te identificeren welk opsporingsonderzoek loopt. Dit moet wel opnieuw samen gezien worden met Zorg 5. Met een opsporingsindicatie in algemene termen lopen de beveiligers op de locatie ook geen duidelijk extra risico en zullen zij hun gedrag niet veranderen.

De tweede maatregel wordt al in het Wetboek van Strafvordering op verschillende momenten toegepast: wanneer een persoon in het kader van een opsporingsonderzoek kennis krijgt over dat onderzoek, bijvoorbeeld omdat ze werknemer zijn van een telecombedrijf en moeten assisteren bij een telefoontap, dan zijn zij gehouden tot geheimhouding over deze informatie. Er kan dus aan degene die de opsporingsindicatie verkrijgt, ook geheimhouding gevraagd worden. Dat betekent nog steeds dat door de daaropvolgende acties van die persoon of entiteit, bijvoorbeeld het niet aangaan van een contractuele verbintenis, kan afgeleid worden dat de opsporingsindicatie feiten naar boven bracht, maar dat lijkt te algemeen te zijn om gevolgen te hebben voor de werkzaamheden.

Randvoorwaarde: lever enkel in de meest algemene termen een opsporingsindicatie af.

Randvoorwaarde: voorzie geheimhouding van de opsporingsindicatie voor diegenen die deze verkrijgen.

Zorg 5: de informatie-uitwisseling mag geen negatieve impact hebben op de reputatie van de betrokken actoren

Dit is een belangrijke zorg voor de (potentiële) klant. De zorg wordt mede veroorzaakt door sommige van de randvoorwaarden voor het mogelijk maken van het project zelf, paradoxaal genoeg als enkel in de meest algemene bewoordingen een opsporingsindicatie wordt gegeven. Een bedrijf kan bijvoorbeeld zelf geen subject zijn van een opsporingsonderzoek, maar een werknemer wel, en toch zou dit kunnen zorgen voor een negatief rapport binnen een opsporingsindicatie, en dus tot extra onrust. Dit kan meegenomen worden in de overwegingen en de bewoordingen van het rapport. Onrust is niet noodzakelijkerwijze een slecht gevolg, het kan leiden tot meer preventieve maatregelen en dus criminaliteitsbestrijding. Er kan dus nog steeds gevarieerd worden in wat 'de meest algemene bewoordingen' betekent.

De particuliere veiligheidsactoren zelf hebben te maken met een dubbel snijdend zwaard. In afwezigheid van een manier om een opsporingsindicatie te krijgen, maken sommige actoren de keuze, op basis van *gut feelings*, om niet met bepaalde klanten in zee te gaan, uit angst voor reputatieschade. Maar dit betekent ook dat opdrachten die de veiligheid potentieel kunnen verhogen, in ieder geval door deze veiligheidsactor op dat moment niet aanvaard zullen worden. Wanneer er echter wel een systeem bestaat om een opsporingsindicatie te leveren, maar er wordt een negatief rapport gegeven, kan dit evenzeer leiden tot een beslissing om geen contract af te sluiten, terwijl hulp van een particuliere veiligheidsactor kan leiden tot een verbeterde veiligheidssituatie. De oplossing is net zoals hierboven te vinden in de bewoordingen gebruikt in het rapport van de opsporingsindicatie, die algemeen moeten blijven, maar tegelijkertijd in zo groot mogelijke mate moeten leiden tot criminaliteitspreventie. Dat betekent ook dat indien het om ernstige feiten gaat binnen een lopend opsporingsonderzoek, particuliere veiligheidsactoren mogelijk moeten worden gevraagd om zich niet te engageren, omdat de politie zelf de verantwoordelijkheid voor veiligheidsvoorziening overneemt. De juiste bewoordingen kunnen er ook voor zorgen dat de particuliere veiligheidsactor wel bereid is om een contractuele relatie aan te gaan met een potentiële klant, maar alleen als die eerst een aantal maatregelen neemt omtrent criminaliteitspreventie. Ook dit levert dan een maatschappelijk gewenst effect op.

Randvoorwaarde: varieer de bewoordingen in het rapport van de opsporingsindicatie zodat in zo groot mogelijke mate aangespoord wordt tot criminaliteitspreventie.

Zorg 6: het systeem waardoor informatie uitgewisseld wordt, moet voldoende waarborgen bevatten en bruikbaar zijn

Reeds bij verschillende vorige zorgen werd gewaarschuwd voor het gebruik van de correcte bewoordingen in adviezen voor opsporingsindicaties, waardoor enerzijds criminaliteitspreventie verkregen wordt (bruikbaarheid) en anderzijds privacy-waarborgen gerespecteerd worden. In de survey werd ook gewezen op de noodzaak van goede datakwaliteit, wat zou moeten bewerkstelligd worden door een correcte evaluatie binnen een gespecialiseerde dienst, en maximale bewaartermijnen in het nog uit te werken wettelijk kader. Met bewaartermijnen wordt bedoeld hoe ver er terug in de tijd kan/moet gegaan worden voor de opsporingsonderzoeken, en hoe lang een opsporingsindicatie bewaard mag worden. Gaat het enkel om lopende onderzoeken, of kunnen onder bepaalde omstandigheden ook eerder onderzoeken meegenomen worden, zelfs indien deze niet geleid hebben tot een uiteindelijke veroordeling? Verder kan ook gekeken worden naar de procedure rond de VOG Rechtspersonen om te kijken welke waarborgen daar gebruikt worden om te verzekeren dat alleen relevante informatie gedeeld wordt. Er kan dan bijvoorbeeld gedacht worden dat bij de aanvraag duidelijk moet aangegeven worden (door de aanvrager) wat de reden is voor de aanvraag van de opsporingsindicatie. Afhankelijk van de reden voor een opsporingsonderzoek, kan dan beslist worden door de behandelende organisatie of dat opsporingsonderzoek relevant is voor de aanvraag of niet.

Randvoorwaarde: werk voldoende waarborgen, zoals datakwaliteit en maximale bewaartermijnen, uit in het te ontwikkelen wettelijk kader. Bekijk daarvoor ook vergelijkbare vragen tot informatie, zoals de VOG Rechtspersonen .

Randvoorwaarde: varieer de bewoordingen in het rapport van de opsporingsindicatie zodat in zo groot mogelijke mate aangespoord wordt tot criminaliteitspreventie.

Zorg 7: er moet voldoende kennis/expertise aanwezig zijn bij alle betrokken actoren

Net zoals bij het vorige project, werd ook hier aangegeven dat mogelijk een andere actor dan de politie meer geschikt is om verantwoordelijk te zijn voor de procedure tot het afgeven van een opsporingsindicatie, namelijk Justis. Indien ervoor wordt gekozen om de verantwoordelijkheid toch bij de politie zelf te leggen, zou dit binnen een gecentraliseerde dienst moeten gebeuren, of op zijn minst bij gespecialiseerde diensten binnen elke politieregio. Aan deze kunnen dan trainingen aangeboden worden.

Randvoorwaarde: beleg de verantwoordelijkheid voor het verlenen van een opsporingsindicatie bij een specifieke organisatie buiten de politie (zoals Justis), of voorzie een centrale dienst of regionale diensten binnen de politie die de verantwoordelijkheid krijgen hierover. Voorzie juridische training aan deze diensten om duidelijk te maken wat er kan meegedeeld worden en hoe dit verwoord moet worden.

Zorg 8: er moet voldoende capaciteit aanwezig zijn bij alle betrokken actoren

Deze zorg is niet anders dan bij het vorige project: de verantwoordelijke dienst moet voldoende bemand zijn.

Zorg 9: er moet voldoende en een volgehouden wil tot informatie-uitwisseling aanwezig zijn bij alle betrokken actoren, wat betekent dat de meerwaarde voor iedereen duidelijk moet zijn

In de eerste zorg werd reeds aangegeven dat de wil om van dit project gebruik te maken mogelijk niet zo hoog is wat betreft de particuliere veiligheidsactoren en hun klanten. Net zoals bij het vorige project is er evenzeer de vraag wat de meerwaarde is voor de politie, omdat zij geen bijkomende informatie krijgt, maar enkel aanlevert. Het is ook onzeker of een opsporingsindicatie ook onder art. 3 van de Politiewet zou kunnen vallen, omdat het niet zo duidelijk is dat er hulp verleend wordt aan derden. omdat er toch een wettelijk kader ontwikkeld moet worden, zijn er weinig tot geen redenen om aanvragen door de politie te laten behandelen en niet door Justis. Dan kan er ook onmiddellijk verkregen worden dat het om een betalende dienst gaat, zodat in elk geval gemaakte kosten gerecupereerd kunnen worden.

De enige andere route voor een volgehouden wil tot informatie-uitwisseling, is indien deze er komt in het kader van een veel bredere samenwerking met de publieke sector/de politie. In dit geval is er geen sprake van een klant waar een opsporingsindicatie van gevraagd wordt, maar gaat het om een publiek-private samenwerking in het kader van een contract of een convenant. Het delen van dit soort informatie aan de particuliere veiligheidsactor over andere bedrijven, gebeurt dan omdat er een gezamenlijke doelstelling is in het kader van de samenwerking. Dit gaat echter om

een geheel andere opzet dan informatie-uitwisseling waarvan sprake was bij de aanvankelijke beschrijving van dit project binnen dit onderzoek.

Randvoorwaarde: creëer een wettelijk kader waarbij Justis de verantwoordelijkheid krijgt om gevaarsindicaties te leveren, eventueel tegen betaling.

Randvoorwaarde: onderzoek of een opsporingsindicatie geleverd kan worden in het kader van een publiek-private samenwerking, waarbij duidelijk het nut en doel aangetoond kan worden waarom de particuliere veiligheidsactor zou moeten weten waarom tegen een actor een opsporingsonderzoek loopt.

Zorg 10: het juridisch kader waarbinnen de informatie-uitwisseling gebeurt, moet voldoende duidelijk zijn

Op dit moment bestaat er geen wettelijk kader voor dit soort informatie-uitwisseling. In tegenstelling tot het vorige project, is de WPG hier niet van toepassing. Het gaat namelijk niet om politiegegevens maar om strafvorderlijke gegevens; in dit geval is de WJSG relevant. In tegenstelling tot de WPG, bevat deze geen artikelen die het mogelijk maken om informatie uit te wisselen met derden. Wel staan er in de WJSG mogelijkheden om via Justis een VOG af te geven, ook wat betreft rechtspersonen. Lopende opsporingsonderzoeken lijken daarin mee te kunnen genomen worden, blijkens art. 35a WJSG waarbij er sprake is van 'strafbare feiten die zouden zijn of zullen worden gepleegd'. Alleen is een VOG niet hetzelfde als een opsporingsindicatie. Bij een VOG is er enkel sprake van het geven of weigeren ervan, terwijl een opsporingsindicatie informatie geeft over het bestaan van opsporingsonderzoeken. De WJSG zou dus uitgebreid moeten worden om dit soort informatie door Justis te laten verspreiden, inclusief onder welke voorwaarden dit mag gebeuren. Daarbij kan wel inspiratie worden gehaald uit de voorbeelden van de VOG, bijvoorbeeld dat de aanvraag voldoende gemotiveerd moet zijn en dat Justis enkel informatie over opsporingsonderzoeken kan geven die relevant zijn voor de aanvraag.

Randvoorwaarde: breidt de WJSG uit met een nieuw hoofdstuk rond het geven van een opsporingsindicatie. Kijk daarbij naar de voorwaarden gesteld aan het geven van een VOG.

7. CONCLUSIE

7.1 Conclusies

7.1.1 Belangrijkste concepten

Vooraleer we de verschillende onderzoeksvragen beantwoorden, schetsen we eerst de definities die we hebben gebruikt voor de belangrijkste concepten in dit rapport. Dit onderzoek richtte zich op het vinden van prioriteiten rond informatie-uitwisseling tussen de politie en particuliere veiligheidsactoren. Hoewel er in Nederland meerdere politionele actoren actief zijn, werd de Nationale Politie als centrale actor uitgelicht, zodat er geen aandacht besteed werd aan mogelijke informatie-uitwisseling met bijvoorbeeld de Koninklijke Marechaussee, bijzondere inspectiediensten of buitengewone opsporingsambtenaren. Dat betekent echter niet dat de in dit rapport ontwikkelde methodologie om voorstellen te ontwikkelen en prioriteiten te identificeren niet ook kan worden gebruikt voor projecten rond informatie-uitwisseling met deze actoren.

De tweede vernoemde partij zijn de particuliere veiligheidsactoren. Hier beperkten we het onderzoek tot private bedrijven die zich met als primair proces commercieel bezighouden met handhaving en/of recherche. Daarbij sloten we dus actoren uit die deze activiteiten uitoefenen als ondersteunende activiteit voor hun primaire proces, zoals een webshop die data beschermt over hun klanten, of zelfs een bank.

Wat betreft informatie-uitwisseling, hanteerden we in dit onderzoek een brede definitie van uitwisseling, waaronder ook informatiedeling valt (informatie gaat slechts één kant uit) en samenwerking rond informatie (partijen gaan samen op zoek naar informatie waar geen van beiden over beschikken).

Ook informatie zelf definiëren we in een vrij brede zin, waardoor binnen dit project zowel naar gegevens (ruwe data) als kennis (bewerkte data op basis van relevante kennis) gepeild werd. Tenslotte moest nog getracht worden om te komen tot een prioritering van mogelijke projecten rond informatie-uitwisseling. Dit werd bereikt door rekening te houden met drie maatstaven/waarden waar overheidshandelen aan kan worden getoetst: efficiëntie en effectiviteit, technische haalbaarheid en maatschappelijke wenselijkheid.

7.1.2 Antwoord op de eerste onderzoeksvraag

De eerste onderzoeksvraag luidde: "Wat zijn de prioriteiten wat betreft informatie-uitwisseling voor zowel de Nationale Politie als particuliere veiligheidsactoren?". Om deze vraag te beantwoorden, werd eerst academische en professionele literatuur geanalyseerd. Daar bleek slechts beperkte aandacht voor praktische vormen van (operationele) informatie-uitwisseling tussen politie en particuliere veiligheidsactoren. Er werd meer aandacht besteed aan algemene observaties, waarbij ook vaak verwezen werd naar mogelijke gevaren en barrières voor samenwerking en informatie-uitwisseling.

In de professionele literatuur en beleidsdocumenten werden een aantal bestaande vormen van informatie-uitwisseling genoemd. Daarbij was het niet geheel duidelijk in hoeverre deze nog in de praktijk uitgevoerd werden en indien wel, op welke schaal dit gebeurde. Documenten vanuit de sector zelf bevatten wel een groter aantal suggesties voor vormen en onderwerpen van informatie-uitwisseling tussen de politie en particuliere veiligheidsactoren.

Deze bronnen vormden de input voor de interviews met sleutelpersonen, waaruit uiteindelijk 17 concrete voorstellen konden worden gedistilleerd vanuit zowel de Nationale Politie als particuliere veiligheidsactoren. Deze werden in een survey bij elkaar gebracht. Uit de open tekst vragen in de survey konden 61 onderscheiden zorgen bij projecten voor informatie-uitwisseling tussen politie en particuliere veiligheidsactoren geïdentificeerd worden. Vele daarvan zijn van betrekkelijk praktische aard en kunnen bij het opzetten van implementatietrajecten vrij eenvoudig (als eis aan de oplossing) worden weggenomen, zoals ook in het voorgaande hoofdstuk door de onderzoekers voor vijf top-prioriteiten werd gedaan.

De zorgen werden door de onderzoekers in 10 brede categorieën gerangschikt: waarde van de informatie, oneigenlijk gebruik van de informatie, betrekken van de juiste actoren, impact op andere werkzaamheden, impact op reputatie, waarborgen en bruikbaarheid, kennis en expertise, capaciteit, wil tot samenwerken en juridisch kader. Het is belangrijk om bij elk project waar nodig randvoorwaarden te creëren voor het wegnemen van deze zorgen.

7.1.3 Antwoord op de tweede onderzoeksvraag

Voor het beantwoorden van de tweede onderzoeksvraag: "Wat zijn de wettelijke mogelijkheden voor het uitwisselen van informatie op basis van deze prioriteiten?" werd zowel een breder juridisch kader onderzocht als juridische randvoorwaarden voor de vijf concrete projecten die op basis van de derde onderzoeksvraag uitgewerkt werden. Over de juridische

randvoorwaarden voor de concrete projecten kan algemeen gesteld worden dat er veel mogelijk bleek zonder dat het nodig was om wetgeving te wijzigen. Het bredere juridische kader keek zowel naar wetgeving rond informatie-uitwisseling met de politie, wetgeving rond beïnvloeding van de marktpositie, en wetgeving rond de wettelijke informatieplichten van en aan de politie.

Het juridisch kader rond informatie-uitwisseling bleek verspreid te zijn over verschillende wetgevingen, met als belangrijkste de WPG en de WJSG indien het gaat om informatie waar de politie over beschikt, en de AVG en de UAVG wanneer het gaat om informatie van de particuliere veiligheidsactoren. De Politiewet en de WPBR gelden daarbij als kaderwetten, ze bepalen wel in algemene termen de mogelijkheden tot informatie-uitwisseling, maar de regels en beperkingen worden in de andere wetten gevonden. Het juridisch kader is door de spreiding niet steeds duidelijk. In de praktijk betekent dit dat er voorzichtig wordt omgegaan met mogelijkheden voor informatie-uitwisseling, waardoor er ook kansen gemist worden. Men gaat er namelijk ten onrechte van uit dat het juridisch kader de informatie-uitwisseling niet toelaat, terwijl er juist vrij veel mogelijk is rond de uitwisseling van politiegegevens en gegevens vanuit particuliere veiligheidsactoren indien de correcte procedures gevolgd worden. Tijdens het onderzoek werd tenslotte ook een betrekkelijk nieuw wetgevend initiatief bekeken; de WGS. Deze doorloopt nu het wetgevend proces; het is niet duidelijk wanneer en zelfs of de wet van kracht zal worden. Toch is het een interessant initiatief, omdat het een poging betreft om regels voor en mogelijkheden binnen samenwerkingsverbanden tussen publieke en private actoren systematisch samen te brengen, en zo het juridisch kader te vereenvoudigen. Er kan gedacht worden aan een gelijkaardig wettelijk initiatief om hetzelfde te doen rond informatie-uitwisseling buiten formele samenwerkingsverbanden. Dit zou de duidelijkheid van het wettelijk kader vergroten, en het ook eenvoudiger maken om in een later stadium aanpassingen te doen aan de wetgeving, zonder daarbij in verschillende juridische teksten te gaan ingrijpen.

Wat betreft de wetgeving rond beïnvloeding van de marktpositie, werden twee kaders als relevant gezien: wetgeving rond misbruik van machtspositie en wetgeving rond verboden staatssteun. Het bereiken van een machtspositie is op zich niet ongeoorloofd, bedrijven proberen continu marktaandeel van concurrenten te winnen. Informatie-uitwisseling met de politie is een mogelijke *sales pitch* naar huidige en toekomstige klanten. Wanneer echter die machtspositie misbruikt wordt, bijvoorbeeld door zeer te hoge prijzen te rekenen aan klanten (er even van uitgaand dat concurrenten geen mogelijkheid hebben om informatie uit te wisselen) of door informatie te gaan gebruiken om concurrenten actief te blokkeren, ontstaat er wel een juridisch probleem. Dan moet de Autoriteit Consument en Markt optreden.

Hetzelfde geldt als de informatie-uitwisseling vanuit het perspectief van verboden staatssteun bezien wordt. Hiervoor gelden vijf cumulatieve voorwaarden: de steun wordt verleend aan een onderneming die een economische activiteit verricht, de steun wordt door staatsmiddelen bekostigd, de steun moet de potentie hebben om de Europese mededinging op een ongunstige manier te beïnvloeden, de steun verschaft een economisch voordeel dat niet via normale commerciele weg zou zijn verkregen (non-marktconformiteit), en tenslotte de steun moet selectief zijn (enkel een beperkte groep ondernemingen of een bepaalde sector geniet er van). Ervan uitgaande dat er informatie vanuit de politie naar de particuliere veiligheidsactor gaat, wordt aan de eerste twee voorwaarden steeds voldaan. Er zijn echter legio mogelijkheden om niet te voldoen aan ten minste één van de drie laatste voorwaarden. Bij het uitwerken van een project rond informatie-uitwisseling moet hier dus wel rekening mee gehouden worden, maar het is twijfelachtig dat het een ernstige belemmering zou opleveren.

Het laatste relevante wetgevend kader is dat van de mogelijke verplichting van de klant of de particuliere veiligheidsactor om informatie te leveren aan de politie. In Nederland bestaat, behalve in uitzonderlijke gevallen (moord of doodslag, verkrachting, en terrorisme), deze verplichting niet. Burgers hebben wel de bevoegdheid om de politie in te lichten over strafbare feiten, maar enkel wanneer ze verhoord worden en zelf geen verdachte zijn, kunnen zij verplicht worden om informatie te geven (verdachten hebben zwijgrecht). Dit principe wordt uitgebreid in de WPBR, waar de particuliere veiligheidsactor de mogelijkheid gegeven wordt om vertrouwelijke gegevens toch aan de politie te geven indien het om strafbare feiten gaat, maar niet gehouden is dit te doen. Het valt aan te raden om deze regel te wijzigen. Er kan beargumenteerd worden dat in het kader van veiligheidsvoorziening particuliere veiligheidsactoren een hogere plicht hebben, en de vrijblijvendheid hier niet op zijn plaats is. Het verlicht ook de moeilijke spreidstand van deze actoren. De politie verwacht van hen dat ze van hun bevoegdheid gebruikmaken, terwijl de klant mogelijk verwacht dat zij discretie aan de dag leggen en de wensen van de klant respecteren. In afwezigheid van een wijziging van de WPBR, valt het aan te raden dat de informatie-uitwisseling met de politie contractueel vastgelegd wordt, en dat er in het uitwerken van de projecten steeds rekening gehouden wordt met meerwaarde voor de klant. Dit is sowieso een goed idee, omdat het verplicht le-

veren van informatie zelfs bij een wetswijziging in alle waarschijnlijkheid enkel zal beperkt blijven tot strafbare feiten.

7.1.4 Antwoord op de derde onderzoeksvraag

De derde onderzoeksvraag, "Welke concrete projecten worden binnen deze wettelijke contouren als wenselijk geacht door zowel de Nationale Politie als particuliere veiligheidsactoren?" werd beantwoord door het creëren van een methodologie om de 17 voorstellen die uit de beantwoording van de eerste onderzoeksvraag kwamen, op twee manieren te rangschikken. Vooral de eerste manier heeft nut voor de toekomst, de tweede methode was voornamelijk bedoeld om in het kader van dit onderzoek de wat complexere projecten meer diepgaand te bespreken.

In eerste instantie werden de projecten gerangschikt op de combinatie van efficiëntie/effectiviteit, technische haalbaarheid en maatschappelijke relevantie. Dit werd kwantitatief bevraagd in een survey, met ook een kwalitatief gedeelte om zorgen te uiten over het project. De survey werd gestuurd naar een aantal sleutelpersonen, die zelf gevraagd werden om deze door te sturen naar één andere persoon die ze als expert beschouwden. Er was verder geen sneeuwbalmethode; de tweede persoon werd niet gevraagd om de survey opnieuw door te sturen. De projecten werden gerangschikt rekening houdende met de antwoorden van alle respondenten, en dan een tweede en derde keer gerangschikt rekening houdende met de antwoorden van respondenten uit de politie en met de antwoorden van respondenten uit de particuliere veiligheidsactoren. Dit laatste werd gedaan om te toetsen of de antwoorden niet te ver uit elkaar lagen. In dit onderzoek heeft dit geleid tot een selectie van vijf verder uit te werken projecten. Echter, het is ook mogelijk om in plaats van onmiddellijk over te gaan tot een selectie, een nieuwe Delphi-ronde te organiseren met de deelnemers, en hen te confronteren met de verschillen in scores van de geaggregeerde data. Waren er significante verschillen wat betreft gemiddelde en spreiding over de projecten heen? Waren er binnen sommige projecten discrepanties, waarbij scores vrij ver uit elkaar lagen? Dit kan verdere relevante informatie opleveren over hoe de verschillende actoren aankijken tegenover de projecten, en hoe zij deze evalueren. Door dit boven tafel te krijgen, kan er mogelijk ook meer begrip gecreëerd worden voor elkaars standpunten, en deze wellicht zelfs dichter bij elkaar gebracht worden.

In het kader van dit onderzoek werd nog een tweede manier van rangschikken toegevoegd, gebaseerd op de complexiteit van het project (hoe complexer, hoe relevanter dat het project in dit onderzoek dieper uitgewerkt wordt). Door deze tweede rangschikking vielen eenvoudigere, maar toch mogelijk nuttige projecten af. Bij het maken van een keuze welke projecten in een later stadium uitgevoerd zullen worden, hoeft deze tweede rangschikking niet noodzakelijk gemaakt te worden, of kan er zelfs geopteerd worden ze in omgekeerde zin te gebruiken. Binnen dit onderzoek was het minder relevant om low hanging fruit uitvoerig te gaan bespreken, maar in de praktijk kan het nuttig zijn om net die projecten (hogere algemene wenselijkheid, lagere complexiteit) eerst uit te voeren. Projecten die ook bij de brainstormsessie expliciet aangeduid werden hierover, waren de mogelijkheid om het verstrekkingsregime voor informatie te verruimen en de mogelijkheid om een systeem me veiligheidsofficieren te ontwikkelen, wat ook ter ondersteuning kan dienen voor andere projecten, omdat zij kunnen fungeren als bruggenbouwers en betrouwbare vaste partners.

Uiteindelijk werden vijf projecten als meest interessant geselecteerd: sensing-aanvraagpunt, gebruik informatie vanuit mobiele sensing-platforms, realtime uitwisselen info voor specifieke evenementen, doorgeven gevaarsindicaties, en opsporingsindicaties.[219] Dit was eigenlijk het antwoord op de derde onderzoeksvraag, maar binnen het onderzoek werd nog een stap verder gegaan en werden de projecten ook verder uitgewerkt door randvoorwaarden toe te voegen aan elk project. Deze werden bekomen door rekening te houden met de geuite zorgen per project, de consensus die bereikt werd hierover tijdens de brainstormsessie, verdere discussies tijdens deze brainstormsessie, en een verdere analyse door de onderzoekers zelf.

7.1.5 Bijkomende bevindingen

Uit dit onderzoek kwamen nog een aantal andere bevindingen die niet passen onder de gestelde onderzoeksvragen, maar wel relevant zijn. Het bijeenbrengen van publieke en private actoren in een brainstormsessie werd als heel positief ervaren, zelfs indien dit niet leidde tot de uitvoering van een project met de aanwezigen als participanten. Kennisuitwisseling en de creatie van potentieel innovatieve ideeën werd op zich al als waardevol bestempeld. Er lijkt in Nederland

219 Zoals hierboven beschreven, bleek er een foute berekening aan de basis te liggen van de selectie van deze projecten. Gezien het uitwerken van de methodologie een belangrijk element was binnen dit rapport, werd uiteindelijk beslist, in samenspraak met de opdrachtgever, om de reeds uitgewerkte projecten te behouden.

een grotere kloof te bestaan tussen de politie en particuliere veiligheidsactoren dan in andere landen, en deze kan onder andere door dit soort bijeenkomsten overbrugd worden.

Tegelijkertijd was het niet mogelijk om in de brainstormsessie zeer gedetailleerd te werken, omdat er bij zowel de politie als bij de particuliere veiligheidsactoren participanten waren die uit verschillende deelsectoren kwamen (handhaving, recherche, cyber, etc.). Deze deelsectoren kunnen ook apart bevraagd worden en bij elkaar komen.

Een andere conclusie die kan getrokken worden, is dat er met de politie al een aantal informatiesystemen en samenwerkingsmechanismen ontwikkeld worden of bestaan die (deels) doen wat in dit onderzoek als nieuwe voorstellen werden gepresenteerd, omdat de onderzoekers niet konden achterhalen dat er reeds een implementatietraject bestaat of lopende is. Dit kan omdat deze niet publiek bekend zijn, nog maar kort bestaan, heel plaatselijk of heel informeel zijn. Een interne structurele bevraging bij de politie kan leiden tot een beter intern zicht wat er al plaats neemt, om deze ook te onderwerpen aan de toets uitgewerkt in dit project en indien gewenst uit te werken op een nationaal niveau (met het al lopende project wellicht als pilot).

Tenslotte kan de conclusie getrokken worden dat er over (nieuwe) informatie-uitwisseling ook niet te ingewikkeld en defensief moet worden gedacht, omdat er dan uiteindelijk vaak niets wordt gedaan. De basis implementeren zou als startpunt moeten worden genomen: implementeer gewoon eerst de simpelste variant van het systeem, en bouw daar later verder op door. Het volledig doordenken van een project zorgt voor een heel lang voortraject, waarbij enthousiasme ook verloren kan worden. Een stapsgewijze ontwikkeling met continu feedback van participanten en stakeholders zorgt voor onmiddellijke eerste resultaten, terwijl het systeem op termijn steeds beter wordt.

7.2 Aanbevelingen

Op basis van de bovenstaande conclusies komen we tot de volgende aanbevelingen:

1. Stimuleer als Nationale Politie dat **meer (wetenschappelijk) onderzoek** wordt gedaan naar en meer wordt gepubliceerd over samenwerking en informatie-uitwisseling met particuliere beveiligingsorganisaties. Zet hier bijvoorbeeld een (wetenschappelijke) stuurgroep op.
2. Maak in academische projecten meer gebruik van **actieonderzoek**, waardoor nieuwe kennis wordt gegenereerd terwijl de praktijk ook verbetert, bijvoorbeeld omdat een nieuw project uitgevoerd wordt. Zo kan men verder komen dan algemene observaties over informatie-uitwisseling.
3. Leg in professionele literatuur in grotere mate vast wanneer praktische vormen van informatie-uitwisseling plaatsvinden. **Documenteer** hun levensloop, evalueer tussentijds, en indien een concreet project beëindigd wordt, leg dan vast wat er goed en minder goed is gegaan.
4. Organiseer **thema-avonden/brainstormsessies** waarbij leden van de politie en particuliere veiligheidsactoren, ook per sector (handhaving, recherche/private opsporing, beveiliging, cyber security, strategie, etc.) samengebracht worden om te brainstormen over nieuwe en innovatieve ideeën. In dit onderzoek werd dit via interviews gedaan met sleutelpersonen, wat ook een adequate methode is. Maar deze is wel meer tijdrovend, en de brainstormsessie werd zeer goed onthaald. De ideeën moeten wel omgezet worden naar concrete projecten.
5. Overweeg de vijf hier diepgaand onderzochte nieuwe **informatie-uitwisselingsprojecten te implementeren**.[220] Besteed ook aandacht aan de inventarisatie van bestaande samenwerkingsvormen, ideeën uit de literatuur voor mogelijke samenwerking, de samenwerkingsvoorstellen die uit interviews naar voren kwamen, en de 12 projectvoorstellen die niet dieper geanalyseerd werden (die dus niet als top-prioriteiten geselecteerd werden). Het is niet omdat zij niet geselecteerd werden, dat zij niet voldoende waarde hebben, zeker omdat in dit onderzoek we voor de uitgewerkte onderzoeken ervoor gekozen hebben om geen *low hanging fruit* te selecteren. Het kan net interessant zijn om dit in de praktijk wel te doen.
6. Analyseer de concrete projecten aan de hand van de **toetsing** gebruikt tijdens dit onderzoek. Er werden binnen dit onderzoek concrete indicatoren ontwikkeld voor efficiëntie/effectiviteit, technische haalbaarheid en maatschappelijke relevantie. Indien gewenst

220 Onafhankelijk van het feit dat door de gemaakte fout de uitgewerkte projecten niet allemaal bovenaan stonden in de lijst, werden alle randvoorwaarden volledig uitgewerkt, zodat het nog steeds de moeite waard is om te bekijken of deze projecten ook effectief geïmplementeerd kunnen worden.

kan ook complexiteit/relevantie voor het onderzoek als aparte indicator meegenomen worden. Binnen dit onderzoek werd dit gedaan aan de hand van een survey. Dezelfde afweging kan echter ook gemaakt worden indien een brainstormsessie gehouden wordt met experts vanuit de politie en particuliere veiligheidsactoren. Het gebruik van een survey, net zoals de thema-avonden georganiseerd, ook per sector, wordt wel aangeraden om zo meer input te krijgen, zeker indien er ook de mogelijkheid wordt gegeven om zorgen te uiten over het project. Maak op basis van deze methodiek een keuze welke projecten verder uitgewerkt kunnen worden.

7. Werk voor de projecten **randvoorwaarden** uit. Indien tijdens de brainstorm of survey specifieke zorgen geuit worden, moeten deze in de randvoorwaarden verwerkt worden. Maar zelfs indien dit niet het geval is (er is bijvoorbeeld geen brainstormsessie geweest waar de projecten gerangschikt werden), kunnen de randvoorwaarden nog steeds gestructureerd uitgewerkt worden aan de hand van de 10 brede categorieën van zorgen: waarde van de informatie, oneigenlijk gebruik van de informatie, betrekken van de juiste actoren, impact op andere werkzaamheden, impact op reputatie, waarborgen en bruikbaarheid, kennis en expertise, capaciteit, wil tot samenwerken en juridisch kader.

8. Integreer indien mogelijk het **wettelijke kader** rond informatie-uitwisseling. Nu is dit verspreid over verschillende wetgevingen, voornamelijk de WPG voor de politie en de de UAVG voor de particuliere veiligheidsactoren (maar zeker niet de enige). De bestaande wetten moeten daarom niet gewijzigd worden. De WGS kan een inspiratiebron zijn. Het brengt wettelijke regels samen, iets wat ook mogelijk moet zijn voor informatie-uitwisseling. In afwachting daarvan, kan de gedachte gepromoot worden dat er onder het huidige wettelijke kader al veel mogelijk is. Dit is op dit moment niet de heersende gedachte, er is veel terughoudendheid.

9. Laat de Autoriteit Consument en Markt regulier **toezicht houden** op mogelijk misbruik van machtspositie. Het is niet mogelijk om alle eventualiteiten te controleren, er zijn andere overheidsdiensten die hier meer geschikt voor zijn.

10. Hou bij het uitwerken van een project er wel rekening mee dat ook informatie als **verboden staatssteun** kan gezien worden. Om hieronder te vallen, moet aan vijf voorwaarden cumulatief voldaan worden. Het lijkt het eenvoudigst om te vermijden dat een project de Europese mededinging op een ongunstige manier beïnvloedt, dat het project non-marktconform is, en dat de steun als selectief gezien wordt.

11. Informatie-uitwisseling **over strafbare feiten** zou eigenlijk bijna een automatisme moeten zijn, en kan de relatie tussen politie en particuliere veiligheidsactoren versterken. Het juridisch kader gaat echter uit van de mogelijkheid om dit te doen, maar niet de verplichting. Een wijziging aan art. 13 lid 3 WPBR zou deze vrijblijvendheid wegwerken en zou een discussie tussen de klant en de particuliere veiligheidsactor vermijden. In afwezigheid hiervan is het nodig dat particuliere veiligheidsactoren goede contractuele afspraken maken met hun klanten over het uitwisselen van informatie met de politie.

12. Het bijeenbrengen van publieke en private actoren in een brainstormsessie werd als heel positief ervaren, zelfs indien dit niet leidde tot de uitvoering van een project met de aanwezigen als participanten. Kennisuitwisseling en de creatie van potentieel innovatieve ideeën werd op zich al als waardevol bestempeld. Er lijkt in Nederland een grotere kloof te bestaan tussen de politie en particuliere veiligheidsactoren dan in andere landen, en deze kan onder andere door dit soort bijeenkomsten overbrugd worden.

13. Onderzoek binnen de politie welke projecten rond informatie-uitwisseling er **op dit moment** lopen. Dit kan in een interne (raadpleegbare) databank bijgehouden worden, waarbij er ook gestimuleerd wordt dat nieuwe projecten zich aanmelden bij de database. Dit vergroot kennisontwikkeling bij de politie, lerend gedrag, en kan ertoe leiden dat interessante projecten ook breder uitgezet worden. Een mogelijke inspiratie hiervoor zijn de projecten van Q-lab,[221] die ook in een interne database zijn samengebracht en die kunnen bekeken worden door alle leden van de politie.

14. Maak het begin van een project **niet te ingewikkeld**. Indien het bij het ontwikkelen

221 Https://www.politie.nl/informatie/welkom-bij-q.html

van de randvoorwaarden duidelijk wordt dat een beperkte start mogelijk is, doe dat dan. Het project kan zich dan stapsgewijs verder ontwikkelen en indien nodig toenemen in complexiteit. Maar als er te lang wordt nagedacht tot alle eventualiteiten theoretisch weggewerkt zijn, is het goed mogelijk dat het initieel enthousiasme voor het project alweer verdwenen is. Laat het project zo snel mogelijk resultaten opleveren, hoe beperkt ook, dat werkt net aanstekelijk.

7.3 Kritische reflectie op het onderzoek

Als onderzoekers kijken we terug op een pittig maar ook zeer interessant en relevant onderzoek. Tussen politie en particuliere veiligheidsactoren bestaat een veelbelovende, maar onvoldoende onderzochte (althans wat betreft praktijkgericht onderzoek) en ontwikkelde relatie. De maatschappelijke en wetenschappelijke relevantie was zodoende zeker hoog. Achteraf gezien hoeft het daarom niet te verbazen dat het onderzoek langer heeft geduurd dan oorspronkelijk voorzien, maar we raden toekomstige onderzoekers toch aan om realistisch te zijn in het uitwerken van een tijdslijn.

De lange doorlooptijd van het onderzoek heeft alvast gedeeltelijk te maken met het verkrijgen van informatie en voorstellen voor informatie-uitwisseling. Zowel binnen de politie als binnen de particuliere veiligheidsactoren bleken er minder analyse-documenten te bestaan over de relatie met de andere partij. Dit zou kunnen worden aangemoedigd. Ook viel het op dat tijdens de interviews de deelnemers vanuit de particuliere veiligheidsactoren meer ideeën en voorstellen hadden voor extra informatie-uitwisseling. Zij lijken hier dus meer behoefte aan te hebben dan andersom. Wellicht is ook informatie-uitwisseling uiteindelijk een verkeerde benaming gebleken, hoewel de definitie die we vanuit het theoretisch kader ontwikkeld hebben, dit enigszins heeft opgevangen. Verschillende voorstellen en projecten hadden geen wederkerig karakter. Informatie-levering lijkt daarom passender.

Een andere reden voor de doorlooptijd was het gebruik van de Delphi-methode. De combinatie van survey en brainstormsessie heeft mooie resultaten opgeleverd. Wat betreft de survey gaat het over interessante diepte- en detail inzichten. Tegelijkertijd was het aantal deelnemers uiteindelijk nog steeds beperkt. Zoals al aangegeven in de aanbevelingen, zou het interessant zijn om dit vaker en met meer deelnemers te doen, en om ze ook per sector te organiseren. We geloven dat de brainstormsessie één van de meest uitgebreide discussies heeft opgeleverd tussen politie en particuliere veiligheidsactoren van de voorbije jaren. Zulke bijeenkomsten zouden vaker moeten worden gehouden. Ook hier moeten we tegelijkertijd toegeven dat de tijd per project in de sessie uiteindelijk nog steeds beperkt was, en dat uit de analyse van de brainstormsessie door de onderzoekers ook nieuwe inzichten verkregen werden. Deze nieuwe inzichten werden verwerkt in dit onderzoek binnen de verschillende randvoorwaarden, maar het zou mooi zijn geweest indien er meerdere discussierondes waren geweest, de inzichten opnieuw hadden kunnen voorgelegd worden aan de deelnemers en opnieuw verwerkt door de onderzoekers. De meest uitgebreide vorm zou dan kunnen zijn dat deze iteratie zo lang doorgaat tot de deelnemers aangeven dat er geen nieuwe discussies of inzichten meer nodig/mogelijk zijn.

We willen in deze reflectie het zeker niet nalaten om op de materiële fout te wijzen die we als onderzoekers gemaakt hebben bij de keuze van de top-prioriteiten. De verkeerde ranking heeft ervoor gezorgd dat een aantal projecten diepgaander zijn uitgewerkt zonder dat dit gerechtvaardigd was vanuit de gebruikte methodologie. We willen niet zo ver gaan dat deze uitwerking daarom geen nut heeft: de manier van uitwerken kan inspiratie en richtlijnen geven voor toekomstige uitwerking van andere projecten. Tegelijkertijd lag het nut toch lager dan indien de juiste projecten waren geïdentificeerd. In dat opzicht moeten we toegeven dat ook de deelnemers aan het seminar benadeeld werden: zij zijn abusievelijk gevraagd hun tijd te besteden aan minder interessante opties. Dat neemt niet weg dat met de discussie tijdens de brainstormsessie en het door de onderzoekers moeten beschrijven van randvoorwaarden om ondanks zorgen deze projecten toch een succes te kunnen maken, meer inzicht in het vraagstuk van informatie-uitwisseling werd gekregen.

Afsluitend kan worden gesteld dat het verrichte onderzoek veel nieuwe opties voor en inzichten in het vraagstuk van informatie-uitwisseling tussen politie en de particulieren veiligheidsactoren heeft opgeleverd. Waarschijnlijk is deze studie de meest uitgebreide die in Nederland ooit is gedaan. Voor ons als onderzoekers was het een beroepsmatig plezier om te doen, ondanks de grote(re dan verwachte) inspanning. Zowel als naslagwerk als start van daadwerkelijke implementatieprojecten kan deze studie van grote waarde zijn voor de toekomst van politie, beveiligingssector en de samenleving.

REFERENTIELIJST

Anomaly, J. (2015). 'Public goods and government action.' *Politics, Philosophy & Economics 14(1)*: 109-128

Barlow, J. & Röber, M. (1996). 'Steering not rowing: Co-ordination and control in the management of public services in Britain and Germany.' *International Journal of Public Sector Management, 9(5/6)*: 73-89. DOI:10.1108/09513559610146366

Boutellier, J. C. J. & van Steden, R. (2011). 'Governing nodal governance: The 'anchoring' of local security networks'. In: Crawford, A. (Ed.). *International and comparative criminal justice and urban governance: Convergence and divergence in global, national and local settings*. Cambridge University Press.

Bartol, K.M. & Srivastava, A. (2002). 'Encouraging knowledge sharing: The role of organizational rewards systems.' *Journal of Leadership and Organization Studies 9(1)*: 64-76

Bryson, J.M. (2018). *Strategic Planning for Public and Nonprofit Organizations: A Guide to Strengthening and Sustaining Organizational Achievement, 5th Edition*. Wiley

Bozeman, B. (1987). *All organizations are public: Bridging public and private organization theory.* Jossey-Bass

Cabrera, A., Collins, W.C. & Salgado, J.F. (2006). 'Determinants of individual engagement in knowledge sharing.' *International Journal of Human Resource Management 17(2)*: 245-264

Cachet, A. (1990). *Politie en sociale controle: over het effect van politie-optreden. Een vergelijkend onderzoek naar verkeersdelicten, gezinsgeweld en drugsgebruik*. Gouda Quint

Christensen, T., Lægreid, P. Roness, P. & Røvik, K. (2007). *Organization Theory and the Public Sector*

Instrument, Culture and Myth. Routledge

Cools, M. & Pashley, V. (2018). *Private Veiligheid in een Stedelijke en Gemeentelijke Context.* Gompel & Svacina

De Waard, J. (2020), *Public and private crime control: collaboration on the BENELUX level.* Online: https://www.researchgate.net/publication/346212428_Public_and_private_crime_control_Collaboration_at_the_BENELUX_level

De Waard, J. & Scheepmaker. M. (2012). 'Voorwoord.' *Justitiële Verkenningen 38(8)*: 5-8

Devroe, E. (2015). 'Toekomstige pluralisering van de politiefunctie? De kannibalistische reactie van de Belgische politie.' In: Ponsaers, P.; Bruggeman, W.; Easton, M.; Lemaitre, A. (Eds.). *Toekomstpolitie. Triggers voor een voldragen debat*. Maklu

Eikenaar. T. & van Stokkom, B. (2014). *Van stadswacht naar nieuwe gemeentepolitie? Gemeentelijk toezicht en handhaving in de openbare ruimte*. Politie & Wetenschap

Engberts, B. & Copini, F. (2016). 'Sensing door de politie en publiek-private samenwerking: operationele noodzaak.' *Tijdschrift voor de Politie* 78(7): 18-22

Friperson, R., Bouman, S. & Wilms, P. (2013). *Samen opgespoord? Eindrapport Pilot samenwerking particuliere onderzoeksbureaus met politie en OM*. WODC

Groenendaal, J. & Helsloot, I. (2014). 'De opbrengst van de politiële netwerkfunctie binnen de gebiedsgebonden politiezorg voor de kerntaken handhaving openbare orde en opsporing.' *Bestuurswetenschappen 68(4)*: 34-52

Hagenaars, P.M.M. & Bonnes, J.M. (2015). *De kracht van privaat-publieke samenwerking Succesfactoren in veiligheidsprojecten in het digitale tijdperk*. Boom Juridische Uitgevers

Hood, C. (1991). 'A Public Management for All Seasons?' *Public Administration 69*: 3-19. DOI:10.1111/j.1467-9299.1991.tb00779.x

Hoogenboom, A.B. (2004). 'Over de toekomst van de publiek-private samenwerking in de veiligheidszorg'. In: Muller, E.R. (Ed.). *Veiligheid - studies over inhoud, organisatie en maatregelen*. Kluwer

Huckvale, T. & Ould, M. (1995). `Process modeling: who, what and how: role activity diagramming.' In: Grover, V. & Kettinger, W.J. (Eds.). *Business Process Change: Reengineering Concepts, Methods, and Technologies*. Idea Group Publishing

Immergut, E. (1990). 'Institutions, Veto Points, and Policy Results: A Comparative Analysis of Health Care.' *Journal of Public Policy 10(4)*: 391-416. DOI:10.1017/S0143814X00006061

Johnston, L., & Shearing, C. (2003). *Governing security: Explorations in policing and justice*. Routledge

Kuin, M.C. & Wilms, P.J.M. (2015). *Publiek-private opsporing: vele handen maken licht werk? Eindrapport Evaluatie vervolgpilot samenwerking particuliere onderzoeksbureaus met politie en Openbaar Ministerie*. WODC

Loader, I. (2000), 'Plural Policing and Democratic Governance', *Social & Legal Studies 9(3)*: 323-345.

Loader, I. & Walker, N. (2006). 'Necessary virtues: The legitimate place of the State in the production of security'. In: Wood J. & Dupont, B. (Eds.). *Democracy, Society and the Governance of Security.* Cambridge University Press

Lienert, I. (2009). 'Where Does the Public Sector End and the Private Sector Begin?' *International Monetary Fund Working Paper Series (122)*. DOI:10.5089/9781451872699.001

Linstone, H. A. & Turoff, M. (1975). *The Delphi method: techniques and applications.* Addison-Wesley Pub. Co.

Matthys, J. (2009). *Private Security Companies and Private Military Companies. A comparative and Economical Analysis.* Maklu

Marks, P., van Sluis, A., Vervooren, A & Zeer, M. (2012). *Improving Policing in the Port of Rotterdam, the Netherlands*. Routledge

Mawby, R.I. (1990) *Comparative Policing Issues: The British and American Experience in International Perspective.* Routledge

Mawby, R. I. (2008). 'Models of policing.' In: Newburn, T. (Ed.). *Handbook of policing.* Willan

Meerts, C.A., Huisman, W., Kleemans, E.R. & van Straten, M. (2022). *Living apart together? Publiek-private relaties in de bestrijding van interne ¬financieel-economische criminaliteit.* Politie & Wetenschap

Mehlbaum, S., Van Duijneveldt, I., Holvast, R. & Van Arkel, D. (2014). 'Heterdaadkracht organiseren.' *Tijdschrift voor de Politie 76(1)*: 6-11

Mintzberg, H. (1979). The structuring of organizations: a synthesis of research. Prentice hall

Mulgan, T. (2007). *Understanding utilitarianism*. Routledge

Nokleberg, M. (2020). 'The public-private divide revisited: questioning the middle ground of hybridity in policing.' *Policing and Society (30)6:* 601-617.

Nederlandse Veiligheidsbranche (2014). *Informatie-uitwisseling politie en particuliere beveiliging.* Nederlandse Veiligheidsbranche.

Perry, J. & Hondeghem, A. (2008). *Motivation in Public Management: the Call of Public Service*. Oxford University Press.

Politieacademie (2019). *Strategische Onderzoeksagenda voor de Politie 2019-2022: voor een effectievere politie en een veiligere samenleving*. Politieacademie.

Ponsaers, P. (2005). 'Omtrent de verhouding tussen politie- en inlichtingendiensten. Van "la Police Générale" naar een "Integraal Veiligheidsdispositief"'. In: Cools, M. ,Dassen, K. & Libertz, R. (Eds.). *De Staatsveiligheid: essays over 175 jaar veiligheid van de staat.* Politeia

Raz, J. (1979). *The authority of law: Essays on law and morality*. Oxford

Rachels, J. & Rachels, S. (2012). *The Elements of Moral Philosophy. Seventh Edition.* McGraw-Hill

Sanders, M. (2021). 'Publiek-Private Samenwerking. Succesfactoren voor Operationele Afstemming in PPS.' *Tijdschrift voor de Politie 3*: 38-41

Saxion Hogeschool (2019). *Publiek private samenwerking in het veiligheidsdomein.* Saxion Hogeschool, Safety & Security Lab: Apeldoorn

Schuilenburg, M. & van Steden, R. (2014). 'Praktijken van selectieve uitsluiting: over bescherming door en tegen veiligheidsassemblages'. *Cahiers Politiestudies 30 (1)*, 51-62

Shearing, C. D. (2005). 'Nodal security', *Police Quarterly 8(1)*: 57–63.

Simeone, M.J. (2007). *The integration of virtual public-private partnerships into local law enforcement to achieve enhanced intelligence-led policing.* Naval Postgraduate School.

Staats, W., Meerts, C., Kleemans, E. R., & Huisman, W. (2021). *Nieuwe manieren van samenwerken: Een systematische literatuurreview naar de (effectiviteit van) publiek-private samenwerking op het gebied van financieel-economische criminaliteit en cybercrime.* Vrije Universiteit

Talja, S. & Hansen, P. (2006). 'Information Sharing.' In: Spink, A., Cole, C. (Eds.). *New Directions in Human Information Behavior. Information Science and Knowledge Management, vol 8*. Springer. DOI:10.1007/1-4020-3670-1_7

Taylor, F. W. (1911). *The Principles of Scientific Management*. Harper & Brothers.

Terpstra, J. (2008a). 'New security patrols in public places: reassurance, fragmentation, and marketization.' In: Easton, M., Gunther Moor, L., Hoogenboom, B., Ponsaers, P. & Van Stokkom, B. (Eds.). *Reflections on Reassurance Policing in the Low Countries*. BJu Legal Publishers

Terpstra, J. (2008b). *Wijkagenten en hun dagelijks werk een onderzoek naar de uitvoering van gebiedsgebonden politiewerk.* Politie & Wetenschap

Theuns, M. & Wannee, R. (2015). 'Voorkom digitale inbraak met een Security Operations Center.' *Trends in Veiligheid 2015 - digitale dienstverlening in het veiligheidsdomein*: 68-73

Tilley, N. (2008). 'Modern approaches to policing: community, problem-oriented and intelligence-led.' In: Newburn, T. (Ed.). *Handbook of policing*. Willan

TNO (2021), *Verkenning Federatieve Beveiliging – een beveiligingsconcept voor de veilige uitwisseling van informatie tussen publieke en private partijen*. TNO.

Vandenabeele, W. & Schott, C. (2020). 'Public Service Motivation.' *Public Administration. Oxford Research Encyclopedia of Politics.* DOI: 10.1093/acrefore/9780190228637.013.1401

Van den Berg, E., Hermans, C. & Quast, J. (2012). *Politiefunctie in perspectief.* Ministerie van Veiligheid en Justitie / Directie Strategie

Van der Knaap, P., Pattyn, P. & Hanemaayer, D. (2020). *Beleidsevaluatie in theorie en praktijk*. Boom Uitgevers

Van der Meulen, N. & Sanders, M. (2020). 'Vorm volgt functie: adviezen voor publiek-private politiepraktijk.' *Tijdschrift voor de Politie 4*: 42-45

Van Goethem, E. & Easton, E. (2021). 'Public-Private Partnerships for Information Sharing in the Security Sector: What's in It for Me?' *Information & Security: An International Journal 48(1)*: 21-35. DOI:10.11610/isij.4809

Van Hoorn, J., van Dijk, A. & de Leij, J. (2020). *Verkenning van maatschappelijke veiligheid in samenwerking met partijen binnen het WPBR domein.* Nationale Politie

Van Lakerveld, J.A., Gussen, I.W.M. & Van Paridon, Y. (2018). *Visies op de politiefunctie.* WODC

Van Steden, R., Meijer, R. & Broekhuizen, J. (2018). *Publiek-private samenwerking in tijden van diffuse dreiging. Een onderzoek naar diversiteit in werkwijzen en kansen in de Nederlandse en Vlaamse context*. WODC

Van Rooij, A.E. (2017). 'Privacy in het semipublieke domein: De bescherming van privacy bij de publiek-private zorg voor openbare orde en veiligheid.' *De Gemeentestem 167(7460)*: 693-701

Vynckier, G. (2019). 'Eb of vloed? Over informatiestromen over de muur publiek-privaat.' In: Devroe, E., Schmidt, A., Gunther Moor, L. & Ponsaers, P. (eds.). *Cahiers Politiestudies. De essentie van politiewerk*. Gompel & Svacina

Wang, S. & Noe, R.A. (2010). 'Knowledge Sharing: A Review and Directions for Future Research.' *Human Resource Management Review 20*: 115-131. DOI:10.1016/j.hrmr.2009.10.001

ANNEX I: VRAGENLIJST VOOR SLEUTELPERSONEN

1. Wordt er binnen de eigen organisatie al gewerkt rond informatie-uitwisseling tussen jullie en publieke actoren (en specifiek de politie of Openbaar Ministerie)?
2. Is er materiaal beschikbaar, extern of intern, waar deze ideeën werden uitgewerkt? Of is er materiaal beschikbaar dat tot inspiratie heeft geleid om hierover te discussiëren binnen de eigen organisatie?
3. Indien u zelf een aantal kansen rond informatie-uitwisseling zou schetsen, wat zouden de belangrijkste zijn? En welke randvoorwaarden ziet u zelf die hiervoor noodzakelijk zijn?
4. Mogelijke suggesties (op basis) van literatuur en/of interne documenten.

ANNEX II: SLEUTELPERSONEN LIJST

Manager particulier recherchebureau en beveiligingsbedrijf: interview dinsdag 19 april 2022 (Respondent 1).

Directeur gespecialiseerd en regionaal beveiligingsbedrijf: interview woensdag 20 april 2022 (Respondent 2).

Directeur waardetransportbedrijf: interview 27 april 2022 (Respondent 3).

Directeur en medewerker particulier recherchebureau: interview 4 mei 2022 (Respondent 4).

Directeur regionaal beveiligingsbedrijf: interview dinsdag 10 mei 2022 (Respondent 5).

Operationeel Specialist Sensing Politie: interview 17 mei (Respondent 6).

Directeur landelijk beveiligingsbedrijf: interview 17 mei 2022 (Respondent 7).

Programmadirecteur en regionaal sectorhoofd bij de politie recherche : interview 1 juni 2022 (Respondent 8).

Strateeg ondermijning Nationale Politie: interview 13 juni 2022 (Respondent 9).

ANNEX III: PROJECTEN VOORGELEGD IN DE SURVEY

1. Aangiftesysteem voor personen met high level clearance

Het aantal aangiften vanuit de particuliere beveiligingssector naar de politie is niet optimaal. Een digitaal centraal meldpunt verkleint deze stap. De aangifte wordt gedaan door een geverifieerd persoon in naam van de klant of van het particulier bedrijf zelf, en de geverifieerde persoon wordt, binnen de perken van de wettelijke mogelijkheden, op de hoogte gehouden van de follow-up van de aangifte aan de politie. De politie kan de mogelijkheid worden gegeven om via het systeem verduidelijking of bijkomende informatie op te vragen over de aangifte.

2. Klantendossiers doorgeven aan een centraal meldpunt.

Particuliere bedrijven beschikken vaak over openbare informatie die interessant is voor de politie, maar voor intern gebruik is verzameld. Er wordt in veel zaken echter geen aangifte of zelfs een melding gedaan. Voor de politie kan een dossier wel waarde hebben. Tegelijkertijd kan het verstrekken van deze informatie ook meer veiligheid opleveren voor hun klanten. En indien gemeld door personen met een high level clearance via een digitaal centraal meldpunt, kan door de politie ook meer waarde worden toebedeeld aan de verkregen informatie.

3. Vermoedens van criminele activiteiten melden (gedeeltelijk anoniem)

De medewerkers van particuliere bedrijven hebben vaak vermoedens van criminele activiteiten. Dit wordt echter niet gemeld aan de politie wegens gebrek aan echt concrete bewijzen. Particuliere beveiligingsbedrijven (of hun klanten) kunnen nu reeds meldingen maken via Meld Misdaad Anoniem (MMA), maar indien er via MMA duidelijk kan gemaakt worden dat de melding gemaakt wordt door een medewerker van een particulier beveiligingsbedrijf (met pasnummer), kan deze informatie mogelijk met meer aandacht door de politie opgevolgd worden.

4. Real-time uitwisselen van informatie in het kader van een specifiek evenement

Bij (openbare) evenementen zijn vaak zowel politie als particuliere bedrijven betrokken. Zij zijn soms elk apart wel bekend met een aantal potentiële dreigingen of bedreigende personen, maar deze informatie wordt niet (steeds) uitgewisseld. Dit kan wel wanneer leidinggevenden langs beide kanten informatie filteren en aan elkaar doorgeven via een landelijk aangeboden, snel en eenvoudig te gebruiken software systeem.

5. Doorgeven gevaarsindicatie aan particuliere beveiligingsbedrijven

Particuliere bedrijven hebben in hun zaken een goed idee waar dreiging van uitgaat (persoon of organisatie), maar beschikken vaak niet over informatie over die dreiging waar de politie wel over beschikt (bijvoorbeeld: beschikt de persoon over een wapen). Daardoor ontstaat een niet-optimale threat assessment. Indien de politie een algemene gevaarsindicatie kan geven wanneer dit wordt gevraagd door een particulier bedrijf, is dit zeer gewenst. Ook de politie kan hierbij gebaat zijn, omdat ze dan op het juiste moment kan worden ingeschakeld.

6. Doorgeven informatie uit omgevingssensoren bij alarm- en heterdaad-situaties

Binnen de huidige wetgeving is het mogelijk dat informatie uit hoger (op daken) geplaatste camera's en andere sensoren aan de politie wordt gegeven bij alarm- en heterdaad-situaties, zelfs indien het gaat om opnames van straten/publieke omgeving van de woning of gebouw waar deze situatie zich voordoet. Deze systemen worden echter zelden aangelegd door particuliere beveiligingsbedrijven of hun klanten. Er kan gestimuleerd worden om dit wel te doen, en om deze informatie ook daadwerkelijk door te geven aan de politie.

7. Gebruik informatie vanuit mobiele sensing platforms

Particuliere bedrijven hebben vaak een groot wagenpark dat heel veel in Nederland rondrijdt. Er kunnen contracten afgesloten worden tussen een aantal particuliere bedrijven en de politie (en/of andere overheidsdiensten) om sensoren op deze wagens te plaatsen om controles uit te voeren. Te denken valt aan illegale radiozenders, verlopen APK-status, kwaliteit van wegen/asfalt (niet aan de politie), etc. De sensoren zijn eigendom van de publieke sector, worden door hen ook onderhouden, en informatie kan niet uitgelezen worden door de private partner.

8. Opsporingsindicatie

Particuliere beveiligingsbedrijven hebben er belang bij om te weten of er binnen nieuwe of bestaande klanten opsporingsonderzoeken lopen. Het is minder belangrijk om te weten tegen wie die gericht zijn, enkel of ze lopen. De politie kan op aanvraag die informatie geven

aan (vertrouwde) particuliere beveiligingsbedrijven. Met dat ' signaal' kunnen de bedrijven bij hun klant aandringen meer maatregelen tegen criminaliteit te nemen.

9. Publiek-Private Recherche samenwerking

In het verleden hebben reeds een aantal proeftuin PPS-trajecten plaats gevonden, waarbij afspraken gemaakt werden wat de taken zijn van de particuliere recherchebedrijven, en waar de politie het voortouw neemt. Deze proeftuinen werden echter niet voortgezet. Er zijn echter wel documenten beschikbaar die de redenen hiervoor aangeven, en die ook mogelijke remedies voorstellen. Deze PPS-constructies kunnen, eventueel opnieuw in proefopzet, opnieuw opgestart worden.

10. Stimuleren Privaat-Private informatie-uitwisseling

De politie heeft niet enkel belang bij informatie-uitwisseling met private actoren, maar tevens tussen private actoren. Een voorbeeld is hoe verzekeringsbedrijven kentekennummers van gestolen auto's aan particuliere beveiligingsbedrijven kunnen doorgeven, die zij kunnen zoeken, en als er één wordt gevonden de politie inschakelen. De politie zou met particuliere beveiligingsbedrijven en andere commerciële actoren een onderzoek kunnen doen welke van dit soort privaat-private informatie-uitwisselingen er al bestaan, welke ook nuttig zouden zijn, en hoe die kunnen worden gepromoot.

11. Sensing aanvraagpunt voor camera's

De politie beschikt over mobiele sensor (ANPR-)camera's, en heeft ook software om informatie te krijgen van privé-camera's, maar deze worden slechts zelden gebruikt op particuliere terreinen. Particuliere beveiligingsbedrijven hebben soms klanten waar zij aanwijzingen hebben dat (veel) criminaliteit plaatsvindt of dat er hoge (maatschappelijke) veiligheidsrisico's zijn. Zij kunnen dan een aanvraag indienen bij de politie of het OM om camera's te installeren of om bestaande camera's beelden te laten doorsturen naar de politie.

12. Delen van Trends

De politie kan aan particuliere beveiligingsbedrijven analyses en notities over criminele trends sturen. De organisaties kunnen ook samen analyses opstellen voor intern gebruik, zoals over nieuwe modus operandi, nieuwe soorten incidenten, nieuwe daderprofielen etc. Zowel politie als bedrijven kunnen dan binnen hun werkzaamheden hier (beter) op gaan letten en daartegen optreden. De politie kan op deze manier uiteraard ook leren van en reageren op trends die het eerst door bedrijven worden opgemerkt. Voor deze trend informatie-uitwisseling kan een aparte samenwerkingsvorm worden georganiseerd.

13. Samenwerking met beveiligingssoftware leveranciers

Particuliere bedrijven gebruiken bepaalde softwarepakketten om informatie over hun klanten, locaties en incidenten in te registeren en deze informatie intern (en met hun klanten) te delen. Een aantal van deze pakketten wordt door veel particuliere bedrijven gebruikt, alsook door een aantal Nederlandse gemeenten. De politie zou met de (Nederlandse) leveranciers van deze pakketten kunnen uitzoeken hoe via deze software interessante informatie van de politie naar beveiligers en andersom kan worden gestuurd, binnen de wettelijke mogelijkheden hiertoe.

14. Veiligheidsofficier

Een particulier beveiligingsbedrijf kan verplicht worden om een vaste, op hoog niveau door de overheid gescreende voor veiligheid verantwoordelijke functionaris te hebben. De politie kan specifiek met deze persoon informatie delen wanneer gevraagd. Het is de taak van de veiligheidsofficier om op basis van deze informatie te handelen, zonder dat andere personen binnen de organisatie weten wat de inhoud is van deze informatie.

15. Verstrekkingsregime informatie verruimen

Particuliere recherchebureaus zijn vaak gebaat bij informatie die enkel verkregen kan worden bij de politie. Voor gecertificeerde particuliere recherchebureaus zou het beleid om informatie te geven kunnen worden verruimd. Nu gebeurt het al informeel dat bepaalde bureaus die worden vertrouwd, concrete vragen kunnen stellen aan contactpersonen bij de politie. Dit systeem kan men een wettelijke basis geven, en door te certificeren kan met een objectieve basis bepaald worden of een bureau al dan niet "te vertrouwen" is.

16. Voorvallenregistratie

Er werd in het verleden door particuliere recherchebureaus een lijst met antecedenten bijgehouden, zodat er kon worden vastgesteld of een persoon (of organisatie) reeds in het verleden het voorwerp van een onderzoek was geweest. Bij de implementatie van AVG werd dit pad verlaten, maar dit soort systeem kan mogelijk wel in overeenstemming gebracht worden met de AVG en weer ingevoerd. Een dergelijk registratiesysteem zou ongemerkt door de politie moeten kunnen geraadpleegd worden.

17. Quid pro quo samenwerking

Een commerciële private actor kan informatie krijgen van de politie indien op het einde van een onderzoek/project alle informatie verzameld binnen het kader van dit onderzoek/project geleverd wordt aan de politie. De politie kan daarna zelf beslissen of er verder wordt gewerkt op de resultaten van het dossier. Dit betekent dat de commerciële actor steeds een keuze heeft: een contract uitvoeren zonder input vanuit de politie, of input krijgen van de politie en op het einde van het contract informatie delen.

ANNEX IV: VRAGEN VOORGELEGD IN DE SURVEY

Alle vragen voorgelegd in de survey werden getoetst op een vijfpunts Likert-schaal, met een extra categorie "ik weet het niet/niet van toepassing"

Vragen over efficiëntie/effectiviteit

1. In hoeverre gelooft u dat deze informatie-uitwisseling een rechtstreekse waarde heeft voor de betrokken partijen? 1 is daarbij lage toegevoegde waarde en 5 hoge toegevoegde waarde.
2. In hoeverre ziet u een toegevoegde waarde voor maatschappelijke veiligheid bij deze informatie-uitwisseling? 1 is daarbij lage toegevoegde waarde en 5 een hoge toegevoegde waarde.

Vragen over technische haalbaarheid

1. Zijn er weinig of veel partijen betrokken wat betreft het invoeren van het voorstel? 1 is daarbij een beperkt aantal actoren, 5 een groot aantal.
2. In hoeverre past deze vorm van informatie-uitwisseling in het huidige wettelijke kader? Zijn er wettelijke of regulatieve wijzigingen nodig? 1 betekent dat er geen wijzigingen nodig zijn, 5 betekent dat het huidige wettelijke kader significant zou moeten aangepast worden.

Vragen over maatschappelijke wenselijkheid

1. In hoeverre vergroot het voorstel de hoeveelheid data die verzameld wordt? 1 betekent dat enkel gebruik gemaakt wordt van reeds verzamelde data, 5 betekent dat er voor het voorstel nieuwe informatie moet verzameld worden.

Vragen over relevantie voor het onderzoek

1. In welke mate ziet u de noodzaak om een aantal randvoorwaarden te vervullen vooraleer dit voorstel kan uitgevoerd worden? 1 betekent dat er geen enkele verdere randvoorwaarde is (uitvoering kan onmiddellijk starten), 5 betekent dat er een groot aantal randvoorwaarden moeten vervuld worden.
2. Hoe noodzakelijk is het voor partijen om hun eigen werking/processen te wijzigen om het voorstel mogelijk te maken? 1 betekent dat er geen enkele aanpassing nodig is, 5 betekent dat een volledig nieuwe procedure moet uitgewerkt worden.

ANNEX V: VERGELIJKING SCORES PROJECTEN

Gezamenlijke scores projecten:

VOORSTEL	EFFICIENTIE/ EFFECTIVITEIT	TECHNISCHE HAALBAARHEID	MAATSCHAPPELIJKE WENSELIJKHEID	INHOUDELIJKE CRITERIA	COMPLEXITEIT
01 - Aangiftesysteem	3,443181818	2	2,5	2,647727273	3,458333333
02 - Bedreigingsdossiers	3,25	1,898989899	1,545454545	2,231481481	3,59469697
03 - Beveiligingssoftware leveranciers	3,3	1,522727273	2,090909091	2,304545455	3,809090909
07 - Meld Misdaad Anoniem	3,727272727	2,2	1,75	2,559090909	2,958333333
04 - Evenementen systeem	4,041666667	1,647727273	2,090909091	2,593434343	3,708333333
05 - Gevaarsindicatie	4	1,988636364	2,166666667	2,718434343	3,958333333
06 - Heterdaad omgevingssensoren	3,733333333	1,7	1,5	2,311111111	3,411111111
08 - Mobiele sensing-Platforms	3,222222222	1,85	0,7	1,924074074	3,8
09 - Opsporingsindicatie	3,355555556	1,35	2,2	2,301851852	3,65
10 - Proeftuin PPS	3,819444444	2,03030303	2,1	2,649915825	3,465909091
11 - Sensing aanvraagpunt	3,7	1,85	1,111111111	2,22037037	3,222222222
12 - Stimuleren privaat-private samenwerking	3,818181818	1,717171717	1,9	2,478451178	3,095454545
13 - Delen van Trends	4,136363636	2,545454545	2,636363636	3,106060606	1,904545455
14 - Veiligheidsofficier	3,916666667	2,125	2,083333333	2,708333333	3,541666667
15 - Verstrekkingsregime verruimen	3,793650794	2,178571429	2,25	2,740740741	2,944444444
16 - Voorvallenregistratie	3,2	2,340277778	2,625	2,721759259	2,883333333
17 - Quid pro quo samenwerking	3,255555556	2,238888889	1,888888889	2,461111111	2,95

Top gezamenlijk

Top inhoudelijk

Top complexiteit

Scores projecten vanuit de politie:

VOORSTEL	EFFICIENTIE/ EFFECTIVITEIT	TECHNISCHE HAALBAARHEID	MAATSCHAPPELIJKE WENSELIJKHEID	INHOUDELIJKE CRITERIA	COMPLEXITEIT
01 - Aangiftesysteem	3,166666667	1,75	3,5	2,805555556	4,166666667
02 - Bedreigingsdossiers	3,666666667	1,833333333	1,5	2,333333333	4,75
03 - Beveiligingssoftware leveranciers	1,75	0,666666667	3	1,805555556	4,083333333
04 - Evenementen systeem	3,666666667	1,333333333	3	2,666666667	4
05 - Gevaarsindicatie	1,916666667	2	3,333333333	2,416666667	4,666666667
06 - Heterdaad omgevingssensoren	3,916666667	1,333333333	1,333333333	2,194444444	4,416666667
07 - Meld Misdaad Anoniem	3,5	1,083333333	1	1,861111111	3
08 - Mobiele sensing-Platforms	2,75	1,333333333	0,333333333	1,472222222	3,833333333
09 - Opsporingsindicatie	1,5	0,833333333	2	1,444444444	4
10 - Proeftuin PPS	2,833333333	1,666666667	3	2,5	4,583333333
11 - Sensing aanvraagpunt	3,666666667	1,666666667	0,333333333	1,888888889	4
12 - Stimuleren privaat-private samenwerking	3,333333333	1,583333333	2,333333333	2,416666667	3,916666667
13 - Delen van Trends	3,666666667	2,333333333	4	3,333333333	2
14 - Veiligheidsofficier	2,166666667	1,666666667	3	2,277777778	4,5
15 - Verstrekkingsregime verruimen	3,25	0,5	2,5	2,083333333	5
16 - Voorvallenregistratie	3,75	0,5	3	2,416666667	4,25
17 - Quid pro quo samenwerking	2,5	3,75	2	2,75	3,5

Top gezamenlijk

Top inhoudelijk

Top complexiteit

Scores projecten vanuit de particuliere veiligheidsactoren:

VOORSTEL	EFFICIENTIE/ EFFECTIVITEIT	TECHNISCHE HAALBAARHEID	MAATSCHAPPELIJKE WENSELIJKHEID	INHOUDELIJKE CRITERIA	COMPLEXITEIT
01 - Aangiftesysteem	3,534722222	2,0625	2,25	2,615740741	3,222222222
02 - Bedreigingsdossiers	3,111111111	1,9375	1,555555556	2,201388889	3,277777778
03 - Beveiligingssoftware leveranciers	3,6875	1,669642857	1,75	2,369047619	3,75
04 - Evenementen systeem	4,166666667	1,770833333	1,75	2,5625	3,611111111
05 - Gevaarsindicatie	4,555555556	1,986111111	1,777777778	2,773148148	3,722222222
06 - Heterdaad omgevingssensoren	3,642857143	1,857142857	1,571428571	2,357142857	3,071428571
07 - Meld Misdaad Anoniem	3,777777778	2,513888889	2	2,763888889	2,944444444
08 - Mobiele sensing-Platforms	3,357142857	2,083333333	0,857142857	2,099206349	3,785714286
09 - Opsporingsindicatie	3,848214286	1,5625	2,25	2,553571429	3,5625
10 - Proeftuin PPS	4,125	2,166666667	1,875	2,722222222	3,166666667
11 - Sensing aanvraagpunt	3,714285714	1,928571429	1,5	2,380952381	2,845238095
12 - Stimuleren privaat-private samenwerking	4	1,794642857	1,714285714	2,50297619	2,875
13 - Delen van Trends	4,3125	2,625	2,125	3,020833333	1,866071429
14 - Veiligheidsofficier	4,5	2,277777778	1,777777778	2,851851852	3,222222222
15 - Verstrekkingsregime verruimen	3,94047619	2,44047619	2,166666667	2,849206349	2,357142857
16 - Voorvallenregistratie	3,142857143	2,589285714	2,571428571	2,767857143	2,625
17 - Quid pro quo samenwerking	3,375	2	1,857142857	2,410714286	2,8125

Top gezamenlijk

Top inhoudelijk

Top complexiteit

Universiteit
Leiden
Institute of Security
and Global Affairs

Discover the world at Leiden University