Publiek-private samenwerking in tijden van diffuse dreiging

EEN ONDERZOEK NAAR DIVERSITEIT IN WERKWIJZEN EN KANSEN IN DE NEDERLANDSE EN VLAAMSE CONTEXT

Dr. Ronald van Steden
Rozetta Meijer, MSc

Institute for Societal Resilience
VU KENNISWERKPLAATS VEILIGHEID & VEERKRACHT
Verwey-Jonker Instituut

Publiek-private samenwerking in tijden van diffuse dreiging

EEN ONDERZOEK NAAR DIVERSITEIT IN WERKWIJZEN EN KANSEN IN DE NEDERLANDSE EN VLAAMSE CONTEXT

Dr. Ronald van Steden

Rozetta Meijer, MSc

Met medewerking van drs. Jolijn Broekhuizen en dr. Freek de Meere

Utrecht, augustus 2018

Publiek-private samenwerking in tijden van diffuse dreiging

Het onderzoek is in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum uitgevoerd door de Kenniswerkplaats Veiligheid en Veerkracht, een samenwerkingsverband tussen het Institute for Societal Resilience van de Vrije Universiteit Amsterdam (VU) en het Verwey-Jonker Instituut.

Onderzoeksteam:

Dr. Ronald van Steden	Vrije Universiteit Amsterdam
Rozetta Meijer, MSc	Verwey-Jonker Instituut
Drs. Jolijn Broekhuizen	Verwey-Jonker Instituut

Begeleidingscommissie:

Prof. dr. E.H. Klijn (voorzitter)	Erasmus Universiteit Rotterdam
Dr. M. Sanders	Nyenrode Business Universiteit / PPS-Construct
Drs. I.B.M. Egbers	Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), Ministerie van Justitie en Veiligheid
Drs. T.L. van Mullekom	Wetenschappelijk Onderzoek- en Documentatie centrum (WODC)

Woord van dank

Dit rapport had niet tot stand kunnen komen zonder de medewerking van alle respondenten in onze casestudies en de experts die hun input gaven tijdens een reflectiesessie over de uitkomsten van ons onderzoek. Hartelijke dank voor alle medewerking. Tevens gaat onze dank uit naar de begeleidingscommissie – prof. dr. E.H. Klijn, drs. I.B.M. Egbers, dr. M.P.T Sanders en drs. T.L. van Mullekom – die ons in de loop van het project van de nodige suggesties en commentaren voorzag.

Ronald van Steden en Rozetta Meijer

Inhoudsopgave

Samenvatting

Inleiding

Aanleiding

De afgelopen jaren is Europa het toneel geweest van meerdere terroristische aanslagen. Daarbij waren vooral 'soft targets' het doelwit: open plaatsen waar grote groepen mensen komen en die moeilijk te beveiligen zijn. Voorbeelden zijn winkelgebieden, voetbalstadions, evenemententerreinen, openbaar vervoer, luchthavens, horeca, uitgaansgelegenheden, maar ook musea, universiteiten, religieuze instellingen en overheidsgebouwen. De verscheidenheid aan mogelijke doelwitten en de diversiteit aan potentiële daders (organisaties, netwerken of eenlingen), hun motieven (denk bijvoorbeeld aan jihadisme of rechtsextremisme) en modus operandi (onder andere vuurwapengeweld, explosieven, vrachtwagens en steekpartijen) zorgen voor een diffuse dreiging.

Sinds maart 2013 is het dreigingsniveau in Nederland substantieel, wat inhoudt dat de kans op een terroristische aanslag reëel is. Net zoals in andere landen, stelt de (Rijks) overheid in Nederland zich hierbij tot doel aanslagen te voorkomen en maatschappelijke ontwrichting als gevolg van een aanslag te voorkomen of zo kort mogelijk te laten duren. De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) draagt samen met ketenpartners zorg voor de bewaking en beveiliging van personen, objecten, diensten, evenementen en vitale infrastructuur. De capaciteit van de veiligheidsdiensten is echter niet oneindig. Financiële en personele middelen voor het bewaken en beveiligen van doelwitten zijn schaars. De overheid kan deze verantwoordelijkheden en taken niet alleen dragen en zoekt daarom steun bij private partijen. We zien daardoor vormen van publiek-private samenwerking (PPS) op het gebied van veiligheid terug in het openbaar vervoer, bij grote evenementen en rondom 'gevoelige' religieuze instellingen. Dergelijke samenwerkingsverbanden roepen de vraag op hoe de overheid samen met private actoren 'soft targets' op de lange termijn effectief kan bewaken en beveiligen en aldus voor maatschappelijke weerbaarheid kan zorgen.

Probleemstelling

PPS bij het bewaken en beveiligen van 'soft targets' vindt zowel op nationaal als op lokaal niveau plaats. In Nederland en in andere landen zijn er praktijkvoorbeelden (en daarmee ervaringen) voorhanden van samenwerking tussen publieke (overheid) en private (niet-overheid) partijen in het voorkomen van aanslagen en het inperken van de gevolgen daarvan. Het Wetenschappelijke Onderzoek- en Documentatiecentrum (WODC) en de NCTV willen graag weten wat de Nederlandse overheid kan leren van kennis en ervaringen in zowel ons eigen land als in andere West-Europese landen. Daarbij ligt de focus op de koude fase vóór een crisis, dus op PPS in de preventieve sfeer, omdat er zich in ons land nog geen grootschalige aanslag heeft voorgedaan, we tijdens een aanslag waarschijnlijk lastig onderzoek kunnen uitvoeren, en voorkomen altijd beter dan genezen is.

Het doel van dit onderzoek is om inzicht te krijgen in de relevante werkwijzen en ervaringen met betrekking tot PPS bij het bewaken en beveiligen van 'soft targets' in tijden van (toenemende) diffuse dreiging. De ervaringen en percepties van de door ons geïnterviewde respondenten staan daarbij centraal. Deze informatie kan de NCTV ondersteunen bij de afwegingen omtrent het bewaken en beveiligen van potentiële doelwitten ten behoeve van het vergroten van het algehele weerstandsniveau en de aanvullende rol die private actoren daarbij kunnen spelen. We vertrokken daarbij vanuit de volgende hoofdvraag: *welke rol kunnen publieke (overheid) en private (niet-overheid) actoren vervullen binnen samenwerkingsverbanden bij het bewaken en beveiligen van 'soft targets' – en aldus bij het versterken van maatschappelijke weerbaarheid in tijden van diffuse dreiging*?

De bijbehorende deelvragen zijn:

1. Wat zijn volgens de wetenschappelijke literatuur criteria voor succesvolle samenwerking tussen overheidsactoren en private actoren bij het bewaken en beveiligen van 'soft targets' en bij het versterken van maatschappelijke weerbaarheid in tijden van diffuse dreiging?
2. Hoe werken overheden in Nederland en in andere Westerse landen in de praktijk samen met private actoren bij het bewaken en beveiligen van 'soft targets' en bij het versterken van de weerbaarheid van de samenleving?
3. Wat kunnen we leren van praktijkvoorbeelden waarin de overheid met private actoren samenwerkt bij het bewaken en beveiligen van 'soft targets' en bij het versterken van de weerbaarheid van de samenleving?
4. In hoeverre en hoe kan het vergroten van de weerbaarheid van private partijen binnen PPS-constructies een bijdrage leveren aan (a) de maatschappelijke veiligheid, en (b) het maken en accepteren van keuzes van de overheid inzake het bewaken en beveiligen van 'soft targets' in tijden van diffuse dreiging?

Onderzoeksopzet

Het onderzoek bestond uit vier fasen: (1) scan van wetenschappelijke literatuur en opstellen theoretisch kader; (2) verzamelen en analyseren van (inter) nationaal beleid en praktijkvoorbeelden, (3) verdiepende analyse van drie cases en (4) reflectie op de onderzoeksuitkomsten.

Fase 1: Wetenschappelijke literatuur en theoretisch kader

We startten de eerste fase van het onderzoek met een scan van nationale en internationale (wetenschappelijke) literatuur over netwerken, 'governance', PPS, en weerbaarheid in het veiligheidsdomein, specifiek op het gebied van bewaken en beveiligen. Met een analyse van deze literatuur gingen we na wat de mogelijke rol van private actoren is bij het voorkomen van een dreiging of aanslag. Vervolgens hebben we geïnventariseerd welke criteria en voorwaarden PPS op deze thema's succesvol maken en wat juist de aandachtspunten en risico's zijn. Deze criteria en voorwaarden gebruikten we vervolgens om de gevonden cases (zie fase 3) te analyseren.

Fase 2: Verzamelen en analyseren van (inter)nationaal beleid en praktijkvoorbeelden

In de tweede fase verzamelden we verschillende voorbeelden van beleid van nationale overheden en (inter)nationale praktijken van PPS bij het bewaken en beveiligen van 'soft targets'. We maakten gebruik van bestaande contacten van de teamleden van het onderzoeksproject en van het Ministerie van Justitie en Veiligheid en zochten op internet. Het doel van deze fase was om globaal inzicht te krijgen in de diversiteit en variatie aan gevoerde beleidsstrategieën binnen de verschillende landen en een overzicht te krijgen van voorbeelden van PPS in de praktijk. Uit deze inventarisatie is onder andere gebleken dat voorbeelden van hechte, fysieke PPS gericht op het bewaken en beveiligen van 'soft targets' schaars zijn. We vonden zeven cases die veelbelovend leken: RTR-NL, de Johan Cruijff ArenA, de Nijmeegse Vierdaagse, het Diamantkwartier in Antwerpen, Project Argus in Londen, NYPD-Shield en Project-Aware in Denemarken. Project Griffin viel bij voorbaat af, omdat de NCTV hier al onderzoek naar heeft laten uitvoeren. Bij nadere beschouwing bleek dat RTR-NL beperkt bleef tot camerabewaking, het bij Project Argus vooral ging om informatievestrekking vanuit de overheid, project Aware enkel trainingen omvatte en NYPD-Shield praktisch niet haalbaar was. Daarom zijn de vervolgens door ons geselecteerde cases ter verdieping: de Johan Cruijff ArenA, de Nijmeegse Vierdaagse en het Diamantkwartier in Antwerpen.

Fase 3: Verdiepende analyse van drie cases

In de verdiepende fase hebben we de bovenstaande drie cases onderzocht aan de hand van documentanalyse en interviews met respondenten die als beleids- of projectontwikkelaar bij het samenwerkingsverband zijn betrokken en leidinggevenden van uitvoerders van het samenwerkingsverband. Per casus hebben we met vijf tot zeven respondenten gesproken.

Fase 4: Reflectie

Tot slot reflecteerden we op de kennis die we in de eerste drie fasen van het onderzoek hebben opgehaald middels een focusgroep met deelnemers die nauw betrokken zijn bij PPS bij het bewaken en beveiligen van 'soft targets'.

Literatuurstudie

Publiek-private samenwerking

PPS-constructies bestaan uit samenwerkingsverbanden tussen relatief autonome private en publieke partijen vanuit een gedeelde verantwoordelijkheid voor een publiek goed, waaronder veiligheid. Dit type samenwerkingsverbanden binnen het veiligheidsdomein neemt meestal de vorm aan van netwerk-PPS, die ertoe bijdraagt dat private actoren participeren binnen samenwerkingsverbanden in hun eigen belang en in het overheidsbelang. Binnen de wetenschappelijke literatuur over 'netwerken' – en aanpalend over 'governance' – wordt vaak over horizontale samenwerkingsverbanden gesproken. Binnen PPS heeft de overheid echter vaak een sturende of anderszins invloedrijke positie. De overheid blijft immers eindverantwoordelijk voor de openbare orde en veiligheid.

Criteria voor succesvolle PPS

Vanuit de bestuurskundige literatuur en van publicaties over veiligheid en crisismanagement kunnen enkele algemene criteria worden gedestilleerd die het succes van PPS bepalen: 'organisatie en dynamiek', 'culturele kenmerken', 'verdeling van verantwoordelijkheden en sturing' en 'connectie met de overheid'. We bespreken deze elementen één voor één.

De organisatie en dynamiek van het netwerk.

Een netwerk valt of staat met het vermogen van deelnemende partijen om op meer dan ad-hoc basis kennis en informatie met elkaar uit te wisselen. Of het komen tot een daadkrachtige aanpak in informatiedeling lukt, heeft allereerst te maken met de structuur van netwerken (Turrini et al. 2010; Whelan 2011). Een netwerk moet niet te klein zijn, maar ook niet onoverzichtelijk groot. Daarnaast moet de vorm van het netwerk passen bij het probleem dat organisaties gezamenlijk aan willen pakken. Bij voorkeur vormen 'stevige' (formele) afspraken de basis van onderling commitment.

Culturele kenmerken.

Netwerken functioneren binnen historisch gegroeide culturen en subculturen (Johnston & Shearing 2003), die zowel positief als negatief kunnen uitpakken voor PPS. Voor een flink deel bestaan netwerken uit interorganisatorische en interpersoonlijke relaties die gebaseerd zijn op gewoonten, percepties, sympathieën en antipathieën, waarmee vertrouwen in het middelpunt van samenwerking komt te staan. Hoewel vertrouwen niet het enige coördinatiemechanisme binnen netwerken is, blijkt een gebrek aan vertrouwen desastreus voor de samenwerking tussen partijen. Netwerkvorming heeft, kortom, een inherent 'zachte' doelstelling gericht op het verstevigen van wederkerige sociale verhoudingen.

Verdeling van verantwoordelijkheid en sturing.
Machtsstructuren en belangenstrijd over doelen en middelen hangen samen met wie de regels van het spel maakt, wat de inhoud van die regels is, de (financiële) hulpbronnen waarover partijen beschikken en in hoeverre zij hun positie op het speelveld kunnen handhaven of uitbreiden (Johnston & Shearing 2003). Auteurs raden daarom aan dat – 'lichte' – leiders binnen netwerken ervoor moeten zorgen dat andere partijen mede-eigenaar worden van het probleem en vanaf begin af aan bij besluitvormingsprocessen worden betrokken (Beutel & Weinberger 2016; Boutellier 2011; Bures 2013).

Connectie met de overheid.
Tot slot bevindt een netwerk zich in een bepaalde context. Dat vergt flexibiliteit (Beutel & Weinberger 2016). Professionals horen oog te houden voor de samenleving die zij bedienen en van waaruit zij waardevolle informatie over veiligheidsrisico's kunnen destilleren. Een issue dat hierbij moet worden meegenomen, is de evaluatie en daarmee 'accountability' van netwerken richting de buitenwereld.

Maatschappelijke weerbaarheid

Een doel van PPS gericht op het bewaken en beveiligen van 'soft targets' kan zijn dat PPS bijdraagt aan maatschappelijke weerbaarheid (of 'veerkracht'). Binnen deze studie vatten wij 'weerbaarheid' op als onderdeel en uitvloeisel van het functioneren van wederzijds afhankelijke samenwerkingsrelaties tussen publieke en private organisaties die hun kennis en kunde bundelen bij met name de preventie van ingrijpende maatschappelijke gebeurtenissen, zoals terroristische aanslagen. Uit een overzicht van de literatuur over 'resilience' (veerkracht) komt naar voren dat dit begrip vele – soms tegenstrijdige – betekenissen heeft en daarom nauwelijks te operationaliseren valt. Onze eigen veronderstelling is dat PPS leidt tot een zekere mate van maatschappelijke weerbaarheid als deelnemende publieke en private organisaties zinvolle relaties met elkaar aangaan vanuit de beschreven succescriteria' binnen een op preventie gericht veiligheidsnetwerk. Daarbij hoort het besef dat private partijen naast de overheid een eigen verantwoordelijkheid voor veiligheid hebben en dat PPS bijdraagt aan een bewustwording en concrete invulling hiervan.

Operationalisatie

We hebben een theoretisch model opgesteld waarin we naar het verloop van netwerk-PPS kijken en al dan niet aanwezige succesfactoren die daar invloed op hebben. Het *verloop van netwerk-PPS* is de afhankelijke variabele. Omdat het niet eenvoudig is om het verloop van de samenwerking en mogelijke concrete uitkomsten te meten – zeker niet als het om het *voorkomen* van incidenten gaat – vallen we terug op de percepties van betrokkenen: hoe tevreden zijn zij over de praktijk en resultaten van de PPS?

De eerder genoemde criteria voor succes vormen de onafhankelijke variabelen. Bij de *organisatie en dynamiek van het netwerk* gaat het om de aard en inhoud van de PPS, vormgeving van de PPS en de mate van contact tussen deelnemende partijen. Bij *culturele kenmerken* gaat het om de mate van vertrouwen en consensus tussen deelnemende partijen. *Rollen en verantwoordelijkheden* heeft betrekking op de onderlinge rolverdeling, besluitvorming en de aanwezigheid van een 'trekker' of 'verbindend persoon binnen het netwerk. *Connectie met de overheid* gaat tot slot om de invloed van de lokale en landelijke overheid op het netwerk en de mate van verantwoording en evaluatie vanuit het netwerk.

Beknopt (inter)nationaal overzicht

Beleid

Westerse overheden lijken zich in toenemende mate bewust van de noodzaak om met private actoren samen te werken teneinde kwetsbare doelwitten beter te beschermen

tegen aanslagen. Dit blijkt zowel uit beleidsdocumenten als uit gesprekken met verschillende overheidsfunctionarissen en experts in Nederland, België, Duitsland, Denemarken, Frankrijk, Zweden, het Verenigd Koninkrijk, de Verenigde Staten, Canada en Australië. Desondanks is deze wens nog lang niet in alle landen vertaald naar expliciet beleid ten aanzien van PPS bij de bewaking en beveiliging van 'soft targets'. Als er al PPS plaatsvindt dan is dat vaak op lokaal niveau, zonder per se een overkoepelende strategie vanuit de Rijksoverheid. Het Verenigd Koninkrijk, de Verenigde Staten en Australië lijken de langste traditie te hebben in het aangaan van PPS in het veiligheidsdomein. Een mogelijke verklaring hiervoor is de meer open houding van deze overheden ten opzichte van de privatisering van veiligheidstaken. Daarentegen is in bijvoorbeeld Duitsland of Frankrijk het organiseren van veiligheid nog steeds een grotendeels publieke taak. Nederland lijkt zich qua positie in het midden te bevinden door in toenemende mate toenadering tot private partijen te zoeken. De NCTV heeft bijvoorbeeld een 'handleiding drukke plekken' opgesteld en heeft daartoe bijeenkomsten georganiseerd met private stakeholders die een 'soft target' beheren of exploiteren. Ook kent ons land het 'Alerteringssysteem Terrorismebestrijding', dat publieke en private partijen tijdig informeert over terroristische dreiging, zodat de betrokken partijen passende maatregelen kunnen nemen om het risico op een aanslag te verkleinen of de gevolgen ervan te beperken.

Praktijkvoorbeelden

Een brede inventarisatie van PPS bij het bewaken en beveiligen van 'soft targets' leverde 24 voorbeelden op in binnen- en buitenland. Daar zaten de nodige voorbeelden uit het Verenigd Koninkrijk en de Verenigde Staten tussen. Dat is niet verrassend, omdat beide landen een verhoudingsgewijs lange traditie van PPS in het sociale veiligheidsdomein kennen. Verder valt op dat de gevonden praktijkvoorbeelden zich voor een groot deel richten op het uitwisselen van informatie of het geven van trainingen, zonder dat er door publieke en private actoren echt lokaal wordt samengewerkt. Het was opvallend lastig om bruikbare cases van PPS te vinden, waarbij publieke en private actoren daadwerkelijk samenwerken binnen het kader van de bewaking en beveiliging van 'soft targets'. De 24 voorbeelden hebben we teruggebracht tot zeven kansrijke cases, waarvan we er uiteindelijk drie – de Johan Cruijff ArenA, de Nijmeegse Vierdaagse en het Diamantkwartier in Antwerpen – hebben onderzocht. We hebben voor deze drie cases gekozen vanwege PPS op lokaal niveau die verder gaat dan camerabewaking, training en/of geringe informatieoverdracht vanuit de overheid.

Praktijken van PPS

Hieronder geven we eerst een korte beschrijving van de drie onderzochte cases. Voor alle cases geldt dat het gaat om netwerk-PPS die echter minder sterk juridisch gestructureerd is dan in de literatuurstudie werd verondersteld. We zetten per onderzochte casus op een rij in hoeverre geïnventariseerde werkwijzen van PPS voldoen aan de in de literatuur gevonden criteria voor succes. Vervolgens bespreken we aan de hand van de succescriteria voor PPS wat de cases ons leren.

Johan Cruijff ArenA

In het buitengebied van de Johan Cruijff ArenA werken medewerkers van de Johan Cruijff ArenA, de politie, eventorganisatoren zoals MOJO Concerts en de particuliere beveiligingsorganisatie TSC samen om de veiligheid van bezoekers te waarborgen. De samenwerking vindt plaats in de voorbereiding van evenementen en in de commandokamer van het stadion als er een concert of ander (niet-voetbalgerelateerd) evenement plaatsvindt. In de commandokamer komen meldingen van verdachte situaties of gedragingen binnen van serviceteams (koppels van particuliere beveiligers en servicemedewerkers van de ArenA) en van zogenaamde 'event profilers' (geüniformeerde beveiligers), die in een perimeter om het stadion (het 'buitengebied' van de Johan Cruijff

ArenA) patrouilleren. Deze perimeter betreft openbaar terrein, waar de politie primair verantwoordelijk is voor de handhaving van de openbare orde en veiligheid. Over het verloop van de samenwerking en informatie-uitwisseling 'in the heat of the moment' zijn respondenten tevreden. Wel is er sprake van onenigheid tussen partijen over de inrichting van de samenwerking. Dit kan worden verklaard door het feit dat in de literatuur genoemde succescriteria binnen deze samenwerking deels afwezig zijn.

- *Organisatie en dynamiek*: Vooralsnog ontbreekt een formeel convenant die ieders rollen, taken en verantwoordelijkheden vastlegt. Dat zorgt voor enige onduidelijkheid onder de deelnemers. Ook worden de gemeente en aanpalende eventlocaties (Ziggo Dome en AFAS Live) als deelnemers aan deze PPS-constructie gemist. Wel vinden er tussen de deelnemende partijen periodieke overleggen plaats.
- *Culturele kenmerken*: Het vertrouwen in ieders kennis, kunde en toegevoegde waarde voor veiligheid (de private 'event profilers' en de servicemedewerkers) wordt niet door iedereen gedeeld. Ook is er geen consensus over de benodigde inzet van de 'profilers' en servicemedewerkers. Hierbij zij opgemerkt dat de combinatie van veiligheid en service belangrijk lijkt voor het in goede banen leiden van bezoekersstromen, maar er wellicht minder toe doet om aanslagen tegen te gaan.
- *Taken, rollen en verantwoordelijkheden*: Binnen de PPS blijkt de inzet van ongeuniformeerde private 'event profilers' een heikel punt vanwege onduidelijkheid over wat zij doen, c.q. welke informatie zij verzamelen. Er is geen sprake van gelijkwaardigheid tussen de partijen; de regie in het buitengebied is duidelijk in handen van de politie. Tot slot ontbreekt het binnen de PPS aan een formele trekker.
- *Connectie met overheid*: Er bestaat geen duidelijke connectie tussen de overheid en deze netwerk-PPS en het netwerk legt geen verantwoording af aan een democratisch gekozen orgaan. Wel evalueren de partijen onderling het verloop van de samenwerking. Verder zijn vooral respondenten binnen private partijen van mening dat de verstrekking van informatie over diffuse dreigingen vanuit de overheidspartijen beter een explicieter kan, zodat zij hun maatregelen daar beter op kunnen afstemmen.

Nijmeegse Vierdaagse

De PPS met betrekking tot de Nijmeegse Vierdaagse richt zich op informatie-uitwisseling die bijdraagt aan het veiligheidsplan, de vergunningverlening en scenario's en handelingsperspectieven in geval van calamiteiten tijdens de wandelprestatietocht. De kernpartijen binnen dit samenwerkingsverband zijn de privaatrechtelijke Stichting DE 4DAAGSE, de gemeente Nijmegen en de politie. Daarnaast zijn de brandweer, veiligheidsregio Gelderland-Zuid, de Geneeskundige Hulpverleningsorganisatie in de Regio (GHOR) en Stichting Vierdaagsefeesten betrokken bij de samenwerking. Respondenten zijn tevreden over het verloop van samenwerking binnen deze PPS. Zij wisselen in een prettige sfeer voldoende en adequaat informatie uit om de veiligheid tijdens het evenement goed te kunnen organiseren. Ook zorgt de PPS ervoor dat kosten voor de overheid binnen de perken blijven, omdat de private partij (Stichting DE 4DAAGSE) steeds meer verantwoordelijkheid toebedeeld krijgen.

- *Organisatie en dynamiek*: De deelnemende partijen hebben regelmatig contact met elkaar door een vaste overlegstructuur. Voorafgaand aan de Vierdaagse zien zij elkaar maandelijks, en tijdens de Vierdaagse dagelijks. De basis voor de samenwerking is vastgelegd in een schriftelijke raamovereenkomst tussen de gemeente, het ministerie van Defensie en Stichting DE 4DAAGSE. In de samenwerking worden niet zozeer deelnemers gemist, wel is er behoefte aan

intensievere samenwerking met enkele partijen buiten de PPS (zoals Stichting de Vierdaagsefeesten).

- *Culturele kenmerken*: Deelnemers aan de PPS delen grotendeels dezelfde normen, waarden, visies en 'taal' door de langdurige samenwerking, informele contacten en de zitting van voormalige politiefunctionarissen en militairen binnen Stichting DE 4DAAGSE. Wel is er zo nu en dan onenigheid over de te nemen maatregelen tegen diffuse dreigingen, maar dit heeft tot nu toe niet geleid tot een vertrouwensbreuk.
- *Taken, rollen en verantwoordelijkheden*: De verdeling van taken en verantwoordelijkheden is voor de deelnemende partijen duidelijk. Er is een verschuiving zichtbaar van publiek naar privaat, doordat steeds meer veiligheidstaken door de private partij worden opgepakt (bijvoorbeeld verkeersregeling en toezicht en handhaving). Wel leeft bij respondenten de wens om de gemaakte afspraken meer schriftelijk vast te leggen. De verhouding tussen de partijen is niet als horizontaal te definiëren; de gemeente besluit immers over de te verlenen vergunning voor de Vierdaagse en overheidspartijen blijven hoofdverantwoordelijk voor de veiligheid in de publieke ruimte. De samenwerking wordt getrokken door de gemeente.
- *Connectie met overheid*: Er is veel contact met de lokale overheid, de driehoek en soms met de Rijksoverheid. Het netwerk legt verantwoording af over de het verloop van de Nijmeegse Vierdaagse middels jaarlijkse evaluaties. Dit is vastgelegd in de raamovereenkomst.

Diamantkwartier Antwerpen

Het Diamantkwartier in Antwerpen kent een PPS die zich toelegt op constante informatie-uitwisseling tussen de Security Office van het Antwerp World Diamond Centre (AWDC), gebouwbeheerders van diamanthandelaren en diamantbeurzen en particuliere beveiligers (private partijen) enerzijds en de lokale politie en de gemeente (publieke partijen) anderzijds. Naast informatiedeling bestaat de samenwerking uit het gezamenlijk nemen en financieren van beveiligingsmaatregelen. Respondenten zijn unaniem tevreden over deze PPS. Ze delen een gevoel van urgentie om samen te werken en de samenwerking is goed georganiseerd.

- *Organisatie en dynamiek*: De samenwerking tussen het AWDC Security Office, de gemeente en de politie is formeel vastgelegd in een veiligheidsprotocol en in een samenwerkingsovereenkomst. Dit geeft legitimiteit aan de samenwerking. Verder vindt er tussen alle partijen binnen diverse fora geregeld contact plaats.
- *Culturele kenmer*ken: Respondenten ervaren een hoge mate van wederzijds vertrouwen, onder andere omdat er met een vaste ploeg ('Single Points of Contact') wordt gewerkt. Ook is er sprake van consensus over de aanpak van diffuse dreigingen. Alle partijen delen de urgentie om veiligheidsproblemen in de wijk tegen te gaan en zijn bereid om elkaar hierin tegemoet te komen.
- *Taken, rollen en verantwoordelijkheden*: De verdeling van taken, rollen en verantwoordelijkheden is voor iedereen duidelijk. Het helpt dat de afspraken ook schriftelijk zijn vastgelegd. Ondanks dat de overheidspartijen eindverantwoordelijk zijn voor de veiligheid in de openbare ruimte, zien we een mix van 'publiek' en 'privaat' als het gaat om de wijze waarop partijen samenwerken en veiligheidsmaatregelen worden gefinancierd. Er is een duidelijke trekker van de PPS in de vorm van het private AWDC-Security Office, maar in laatste instantie is de burgemeester eindverantwoordelijk voor de openbare orde en veiligheid en kan hij desgewenst knopen doorhakken.
- *Connectie met overheid*: Er is een duidelijke connectie tussen de PPS en overheidspartijen. In de eerste plaats vindt informatie-uitwisseling plaats met een

breed scala aan overheidspartijen. Verder heeft de gemeenteraad invloed op de praktijk van het veiligheidsnetwerk; zo heeft zij de meest recente samenwerkingsovereenkomst (2016-2019) goedgekeurd.

Wat leert dit ons?

Het voorgaande laat zien dat de PPS in het Diamantkwartier van Antwerpen vrijwel aan alle in de literatuur geformuleerde succescriteria voldoet. Ook in Nijmegen zijn veel van de succescriteria aanwezig. Bij de Johan Cruijff ArenA is dit in mindere mate het geval. De uitkomsten bevestigen dat de aan- of afwezigheid van deze criteria een positieve, respectievelijk een negatieve invloed hebben op de tevredenheid van respondenten over het verloop en de resultaten van de PPS. We reflecteren op deze bevindingen door de theoretische bril van in de literatuur gevonden succesfactoren voor netwerk-PPS inzake het bewaken en beveiligen van 'soft targets': wat leren we uit de praktijk over het belang van deze factoren?

- *Organisatie en dynamiek*: Binnen alle drie de cases zien we terug dat het van belang is dat de juiste partijen om tafel zitten en partijen regelmatig contact met elkaar onderhouden (het liefst 'face-to-face' contact middels vaste overlegstructuren). Bij het opzetten van een PPS dienen de overheid en private partijen dus scherp te kijken of het beoogde samenwerkingsverband ook echt compleet is. Daarnaast is gebleken dat schriftelijke (juridische) afspraken, zoals convenanten en protocollen, bijdragen aan duidelijkheid over de rollen en taken van partijen en legitimiteit geven aan de PPS. Bovendien hebben respondenten binnen alle cases opmerkingen gemaakt over beperkende wet- en regelgeving die informatie-uitwisseling tussen publieke en private partijen in de weg staat. De wens tot vrijere informatie-uitwisseling onderstreept het belang van een betere juridische borging van PPS. Vanuit maatschappelijk belang moeten verantwoordelijkheden en bevoegdheden immers goed worden belegd.
- *Culturele kenmerken*: Vertrouwen tussen de partijen, een gezamenlijke urgentie om veiligheid te waarborgen en de wil om eventuele onenigheid te overbruggen blijken belangrijke succesfactoren. We kunnen concluderen dat voor de tevredenheid over het verloop van netwerk-PPS gericht op het bewaken en beveiligen van 'soft targets' de precieze juridische organisatievorm niet doorslaggevend is. De PPS verloopt goed als partijen (redelijk) intensief contact hebben, veel energie in hun samenwerking stoppen en elkaar vertrouwen. Toch is, zoals hierboven al is gesteld, juridische borging vanuit het publieke belang van maatschappelijke veiligheid wel belangrijk met het oog op informatie-uitwisseling en ieders verantwoordelijkheden en bevoegdheden in dezen.
- *Verdeling van taken, rollen en verantwoordelijkheden en sturing van het netwerk*: Binnen netwerken zitten publieke en private partijen met uiteenlopende visies, doelen en belangen. Gelijkwaardigheid tussen de partijen blijkt geen noodzaak, wederkerigheid echter wel. Verder lijkt de aanwezigheid van een verbindend persoon met legitimiteit (en niet per se doorzettingsmacht) die oog heeft voor de verschillende posities cruciaal. Verrassend genoeg werkt die persoon in Antwerpen bij een private partij die zowel het vertrouwen van de overheid als van de commerciële diamantensector geniet. Een belangrijke vaardigheid van een verbindende 'trekker' is dat hij of zij voor wederkerigheid kan zorgen. Aan zowel de publieke als de private kant gaat het om 'geven en te nemen' wat betreft informatiedeling, maar ook de financiering van maatregelen.
- *Connectie tussen de overheid en het netwerk*: De connectie tussen de overheid en het netwerk is niet in alle cases even sterk. Alleen de samenwerkingsverbanden rond het Antwerpse Diamantkwartier en de Nijmeegse Vierdaagse leggen enige vorm van verantwoording af aan een democratisch gekozen orgaan. Uit de onderzochte cases is verder naar voren gekomen dat bestuurlijk draagvlak nodig is voor het succes van de PPS. In zowel Antwerpen als Nijmegen wordt

de PPS gesteund door de burgemeester, de korpschef en bestuurders van de betrokken private partijen, wat het samenwerkingsverband legitimiteit geeft. In Amsterdam ontbreekt dergelijke bestuurlijke betrokkenheid vanuit de gemeente en politie.

Reflectie op maatschappelijke weerbaarheid

Bijdrage PPS aan maatschappelijke weerbaarheid

Het vergroten van de weerbaarheid van private partijen binnen PPS-constructies kan een bijdrage leveren aan de maatschappelijke veiligheid als deze partijen investeren in het nemen van maatregelen – waaronder camerabewaking, de inzet van beveiligers en opschalingsscenario's – en het trainen van het eigen personeel. Door personeel bewuster en alerter te maken, kunnen verdachte gedragingen en voorwerpen eerder worden herkend en gemeld. Dit is de mening van enkele experts die tijdens een focusgroep reflecteerden op de bevindingen van het onderzoek.

Hierbij zij opgemerkt dat de term 'weerbaarheid' een lastig te interpreteren fenomeen wordt gevonden. De term heeft volgens de experts te maken met 'sociale samenhang', 'zelfredzaamheid' en 'alertheid', maar verder is het een 'fluïde' begrip. Dit oordeel van de experts stemt overeen met de kritiek in de literatuur over 'resilience', dat het een zeer ambigu en daarom niet goed te operationaliseren term is. Het valt ook niet te bepalen of er door PPS aanslagen zijn voorkomen. Hoogstens kunnen we volgens een expert de aanname maken dat betere samenwerking en informatie-uitwisseling tussen publieke en private partijen een positief effect heeft, omdat er daardoor meer 'ogen en oren' zijn die afwijkende zaken of personen opmerken.

Deze opmerking is conform onze veronderstelling dat PPS leidt tot maatschappelijke weerbaarheid als deelnemende publieke en private organisaties zinvolle relaties met elkaar aangaan vanuit eerder beschreven criteria: de organisatie en dynamiek van het netwerk, culturele kenmerken, de verdeling van verantwoordelijkheid en sturing en de connectie met de overheid. Tezamen zorgen genoemde elementen voor een goed lopende PPS. In twee cases – de Nijmeegse Vierdaagse en het Antwerpse Diamantkwartier – zijn deze elementen grotendeels aanwezig, wat volgens respondenten inderdaad tot positieve resultaten leidt. In het geval van de Johan Cruijff ArenA ligt er aan de PPS geen convenant ten grondslag en is vertrouwen en consensus onder de deelnemende partijen in mindere mate aanwezig. Dit beïnvloedt de weerbaarheid van deze PPS mogelijkerwijs negatief. Tegelijk moet worden opgemerkt dat, net als in Nijmegen en Antwerpen, respondenten over het algemeen tevreden zijn over hun onderlinge samenwerking.

Het maken en accepteren van keuzes van de overheid

Het vergroten van de weerbaarheid van private partijen binnen PPS-constructies kan een bijdrage leveren aan het maken en accepteren van keuzes van de overheid inzake het meer verantwoordelijk maken van private partijen voor bewaking en beveiliging als er volgens de experts aan ten minste drie randvoorwaarden wordt voldaan. Ten eerste is het noodzakelijk dat de overheid actief investeert in PPS, met aandacht voor hun relaties met, en belangen van, private partijen. Dit wil, ten tweede, zeggen dat private partijen hechter bij PPS kunnen worden betrokken als zij in staat worden gesteld gemaakte kosten in rekening te brengen bij hun klanten of dat kosten eerlijker over deelnemende partijen worden verdeeld. Een derde en laatste randvoorwaarde om private partijen bij PPS te betrekken, is door hen meer informatie te verschaffen over de aard van een diffuse dreiging. Willen private partijen scenario's kunnen preparen en nuttige veiligheidsmaatregelen kunnen nemen, dan moeten zij beter op de hoogte zijn over wat er van hen wordt gevraagd en waarom.

Tot slot

Voortbouwend op de informatie en analyse uit dit onderzoek zijn er drie varianten van netwerk-PPS inzake het bewaken van beveiligen van 'soft targets' in tijden van diffuse dreiging mogelijk. De eerste variant gaat uit van continuering van het bestaande, waarbij hooggespannen verwachtingen over netwerk-PPS moeten worden getemperd. Momenteel bestaan er binnen het veiligheidsdomein geen gelijkwaardige netwerken van publieke en private partijen. De overheid (politie, gemeente, justitie) is vanwege haar geweldsmonopolie onvermijdelijk dominant aanwezig. Daarom kunnen we bij continuering van het bestaande beter spreken over private medeverantwoordelijkheid voor veiligheid dan over netwerk-PPS.

De tweede variant betreft een verdieping van netwerk-PPS en biedt meer ruimte voor wederzijdse informatie-uitwisseling. Dat wil zeggen: de overheid en private partners delen evenveel – ook meer gevoelige – informatie met elkaar. Bekeken vanuit de organisatie en dynamiek van een netwerk betekent dit dat er formelere afspraken moeten worden gemaakt. Bovendien vraagt dit om aanpassing van bestaande wet- en regelgeving omtrent informatie-uitwisseling en privacybescherming. Ook betekent dit dat de connectie tussen de overheid en netwerken moeten worden versterkt door stevigere verantwoordingsmechanismen op te tuigen ten aanzien van de informatie-uitwisseling die plaatsvindt.

In de derde variant verbreedt de overheid de werkzaamheden van private partijen. Dat kan door de onderlinge verdeling van taken, rollen en verantwoordelijkheden grondig te herzien. Omdat de Nederlandse overheid het geweldsmonopolie heeft, zijn veiligheidsnetwerken nooit zo 'horizontaal' als literatuur over netwerksamenwerking soms suggereert, tenzij er verregaande aanpassingen worden doorgevoerd. In het verlengde hiervan is een verbreding van netwerk-PPS mogelijk door naast meer taken ook meer geweldsbevoegdheden aan de particuliere beveiligingsbranche over te dragen. Wederom vraagt dit een andere – 'strakkere' – juridische structurering van netwerk-PPS en de verantwoordingsmechanismen die daarbij horen.

Summary

Introduction

Occasion

In recent years, Europe has been the stage of several terrorist attacks. Mostly soft targets were hit: open locations where large groups of people gather, making it hard to secure them. Examples are shopping areas, football stadiums, event grounds, public transport, airports, the hospitality industry, but also museums, universities, religious institutions and government buildings. The variety of potential targets and the diversity of potential perpetrators (organizations, networks or lone wolfs), their motives (think, for instance, of jihadism or right-wing extremism) and modus operandi (such as gun violence, explosives, trucks and stabbings) generate a diffuse threat.

Since March 2013, the threat level in the Netherlands has been substantial, which means that the chance a terrorist attack will take place is real. Just like in other countries, the Dutch (national) government aims to prevent attacks. It also aims to prevent the social disruption caused by an attack or to shorten its duration as much as possible. In cooperation with chain partners, the National Coordinator for Security and Counter-Terrorism (NCTV) takes care of guarding and securing persons, objects, services, events and vital infrastructure. Yet, the capacity of security services is not endless. The financial and personal means for keeping targets safe are scarce. As it is impossible for the government to carry out these responsibilities and tasks on its own, it looks for support among private parties. In this way, forms of public-private cooperation (PPC) on safety have evolved that can be found in public transport, at large events and around 'sensitive' religious institutions. Such partnerships give rise to the question how the government can work together with private actors to guard and secure soft targets effectively in the long run, which may lead to social resilience.

Problem

PPC, set up for guarding and securing soft targets, takes place both at the national and the international level. In the Netherlands as well as abroad, practical examples can be found for cooperation between public (governmental) and private (non-governmental) parties, focused on the prevention of attacks and the containment of their impact. The Research and Documentation Centre (WODC) of the Ministry of Justice and Security and the NCTV want to know what the Dutch government may learn from knowledge and experiences gained in both our own country and other Western European countries. The focus is on the cold stage before a crisis, that is, PPC in the preventive sphere, since a large-scale terrorist attack has not yet occurred in the Netherlands and it will probably be hard to conduct research during an attack. Moreover, prevention is always better than cure.

The objective of this study is to gain insight into the relevant working methods and experiences regarding PPC for guarding and securing soft targets in times of an (increasing) diffuse threat. Central to us are the experiences and perceptions of the respondents we have interviewed. This information may support the NCTV in their deliberations on guarding and securing potential targets to increase the general level of resilience, and on the ancillary role private actors may play in this. Our main starting point was the following question: Which roles can public (governmental) and private (non-governmental) actors play within forms of cooperation to guard and secure soft targets – thus contributing to strengthening societal resilience in times of diffuse threat?

The accompanying sub-questions are:

1. According to the scientific literature, what are the criteria for a successful partnership between governmental and private actors when guarding and securing soft targets and strengthening social resilience in times of diffuse threat?
2. How do governments in the Netherlands and other western countries cooperate in practice with private actors to guard and secure soft targets and to strengthen the resilience of their society?
3. What can we learn from practical examples of cooperation between the government and private actors in guarding and securing soft targets and strengthening social resilience?
4. To what extent and in what way can increasing the resilience of private parties within PPC constructions contribute to (a) social safety; and (b) choices made by the government with respect to guarding and securing soft targets in times of diffuse threat, and the acceptance of these choices?

Research set-up

The study consisted of four stages: (1) a scan of scientific literature and the development of a theoretical framework; (2) the collection and analysis of (inter)national policies and practical examples; (3) an in-depth analysis of three cases; and (4) reflection on the study's outcomes.

Stage 1: Scientific literature and theoretical framework

We started the first stage of the study with a scan of the national and international (scientific) literature on networks, governance, PPC, and resilience in the security domain, specifically with regard to guarding and securing soft targets. By analysing this literature, we examined the potential role to be played by private actors in preventing a threat or attack. Next, we made an inventory of the criteria and conditions that make PPC successful with respect to these themes and also of the concerns and risks involved. We have then used these criteria and conditions to analyse the cases (see stage 3) we have found.

Stage 2: Collection and analysis of (inter)national policies and practical examples

During the second stage, we collected several examples of policies developed by national governments and (inter)national practices of PPC for guarding and securing soft targets. We made use of existing contacts of the research project's team members and of the Ministry of Justice and Security. We also searched the Internet. Goal of this stage was to gain global insight into the diversity of and variation in followed policy strategies in the different countries and to get an overview of practical PPC examples. This inventory has shown, among other things, that examples of a tight-knit PPC aimed at guarding and securing soft targets are scarce. We found seven cases that seemed promising: RTR-NL, the Johan Cruijff ArenA, the Nijmegen Four-Day March [Nijmeegse Vierdaagse], the Diamond Quarter in Antwerp, Project Argus in London, NYPD-Shield and Project-Aware in Denmark. From the outset, Project Griffin was left out, since the NCTV has already commissioned a study on it. On closer inspection, RTR-NL turned out to be limited to camera surveillance, Project Argus turned out to focus mainly on information disseminated by the government, Project Aware just consisted of a training course and NYPD-Shield was unfeasible in practice. For this reason, we then selected the following cases for our in-depth study: the Johan Cruijff ArenA, de Nijmegen Four-Day March and the Antwerp Diamond Quarter.

Stage 3: In-depth analysis of three cases

During the in-depth stage, we have examined the three cases mentioned above by means of a document analysis and interviews with respondents involved in the partnership as policymakers or developers and managers who lead those executing the cooperation. Per case, we have talked to five to seven respondents.

Stage 4: Reflection

Finally, we reflected on the knowledge we had gathered during the first three stages of the study in a focus group, consisting of participants who are closely involved in PPC aimed at guarding and securing soft targets.

Literature study

Public-private partnership

PPC constructs consist of partnerships between relatively autonomous private and public parties, based on shared responsibility for a public good, such as safety. Within the safety domain, this type of partnership most often takes on the form of network PPC, which encourages private actors to participate in their own as well as the government's interest. The scientific literature on networks – and on the neighbouring subject of governance – frequently speaks of horizontal partnerships. Yet, in PPC, the government often holds a steering or otherwise influential position. After all, the government has final responsibility for public order and safety.

Criteria for a successful PPC

We can distil from the public administration literature and publications on safety and crisis management some general criteria determinant for the success of PPC: 'organization and dynamic', 'cultural characteristics', 'distribution of responsibilities and steering' and 'connection to the government'. We will discuss these elements one by one.

The organization and dynamic of the network

A network stands or falls with the ability of the participating parties to exchange knowledge and information on more than just an ad hoc basis. Whether a forceful approach of information sharing succeeds has to do, first of all, with the structure of networks (Turrini et al. 2010; Whelan 2011). A network should not be too small, but not confusingly large either. In addition, the form of the network has to match the problem organizations collectively intend to deal with. Preferably, 'vigorous' (formal) agreements constitute the basis of a mutual commitment.

Cultural characteristics

Networks function within historically grown cultures and subcultures (Johnston & Shearing 2003), which may work out either positively or negatively for PPC. In large part, networks consist of interorganizational ad interpersonal relations, based on habits, perceptions, sympathies and antipathies, putting trust at the centre of cooperation. Although trust is not the only coordination mechanism within networks, a lack of trust proves to be disastrous for the cooperation between parties. In short, creating a network has an inherently 'soft' goal, aimed at strengthening mutual social relations.

Distribution of responsibility and steering

Power structures and conflicts of interest about goals and means are linked to who makes the rules of the game, what the content of those rules is, the (financial) resources at parties' disposal, and the extent to which they are able to maintain or expand their position (Johnston & Shearing 2003). For this reason, authors recommend that 'light' network leaders ensure that other parties become co-owners of the problem and are

involved in decision-making processes from the start (Beutel & Weinberger 2016; Boutellier 2011; Bures 2013).

Connection to the government

To conclude, a network is part of a particular context. This requires flexibility (Beutel & Weinberger 2016). Professionals are supposed to keep an eye on the society they serve and from which they can distil valuable information about safety risks. An issue that needs to be considered is the assessment of networks, which also means their accountability toward the outside world.

Social resilience

One goal of PPC aimed at guarding and securing soft targets can be that PPC contributes to the resilience of society. In this study, we perceive 'resilience' as part and result of the functioning of mutually dependent cooperative relations between public and private organizations; they pool their knowledge and capacity, in particular to prevent major social events such as terrorist attacks. The overview of the literature on resilience shows that this concept has many – sometimes contradictory – meanings, making it almost impossible to operationalize. Our assumption is that PPC results in a certain degree of social resilience when public and private organizations enter into useful relationships with each other, starting from the criteria for success described earlier, within a safety network focused on prevention. Another condition is that private parties realize that, beside the government, they have their own responsibility for safety and that PPC contributes to awareness about this and to a concrete interpretation of it.

Operationalization

We have drawn up a theoretical model to examine the development of network PPC and to look for the presence of success factors that may influence it. The development of network PPC is the dependent variable. Since it is no simple matter to measure the development of the cooperation and potential, concrete outcomes – least of all where the prevention of incidents is involved -, we have fallen back on the perceptions of those involved. How satisfied are they about the practice and results of the PPC?

The aforementioned criteria for success constitute the independent variables. The organization and dynamic of the network is about the nature and substance of the PPC, PPC design and the extent of contact between participating parties. Cultural characteristics deals with the extent of trust and consensus between participating parties. Roles and responsibilities relates to the mutual distribution of roles, decision-making and the presence of a 'driver' or unifying person within the network. Finally, connection to the government deals with the influence of the local and national government on the network, and the accountability and assessment set up from within the network.

Brief (inter)national overview

Policy

Western governments seem increasingly aware of the necessity of cooperating with private actors to improve the protection of vulnerable targets against attacks. This is shown both by policy documents and by interviews with different government officials and experts in the Netherlands, Belgium, Germany, Denmark, France, Sweden, the United Kingdom, the United States, Canada and Australia. Nonetheless, this desire has not yet been translated in all countries into explicit policy regarding PPC for guarding and securing soft targets. If PPC takes place it most often is at the local level, not necessarily based on an overall strategy initiated by the national government. The United Kingdom, the United States and Australia seem to have the longest tradition in engagement in PPC within the safety domain. A possible explanation for this is the more open attitude of these governments with respect to the privatization of safety tasks. The orga-

nization of safety in countries such as Germany and France, on the other hand, is still largely a public task. The position of the Netherlands seems to be in the middle, since it increasingly approaches private parties. The NCTV, for example, has written a 'guide for crowded spots', for which it has set up meetings with private stakeholders who manage or exploit a soft target. The Netherlands also has its 'Alerting System for Counter-terrorism', which warns public and private parties on time about a terrorist threat. This enables the parties involved to take suitable measures to decrease the risk of an attack or limit its impact.

Examples from practice

A broad survey of PPC focused on guarding and securing soft targets yielded 24 examples, both at home and abroad. A lot of these examples were from the United Kingdom and the United States. This is not surprising, since both countries have built up a relatively long tradition of PPC in the social safety domain. We also noticed that the practical examples we found in large part focus on the exchange of information and the provision of training courses, without any real cooperation between public and private actors at the local level. We found it remarkably hard to find useable cases of PPC in which public and private actors actually do cooperate within the framework of guarding and securing soft targets. We have narrowed the 24 examples down to 7 promising cases, 3 of which we have studied: the Johan Cruijff ArenA, the Nijmegen Four-Day March and the Antwerp Diamond Quarter. We have chosen these three cases because these local PPC entail more than camera surveillance, a training course or little information dissemination by the government.

PPC practices

Below, we will first briefly describe the three studied cases. To all cases applies that the network PPC is less soundly structured in a legal sense than is assumed in the literature study. For each case we studied, we will piece together to what extent the surveyed PPC working method meets the criteria for success found in the literature. Next, we will discuss what can be learned from the cases, based on the criteria for the success of PPC.

Johan Cruijff ArenA

In the area surrounding the Johan Cruijff ArenA, its employees cooperate with the police, event organizers such as MOJO Concerts and the private security firm TSC to guarantee the safety of its visitors. The cooperation takes place in preparation of events and in the stadium's command centre whenever there is a concert or other (non-foot-ball-related) event. Reports of suspect situations or behaviours by service teams (couples of private security guards and ArenA service desk employees) and so-called 'event profi-lers' (plain-clothes security guards) who patrol the perimeter around the stadium, come in at the command centre. This perimeter is public space, where the police is primarily responsible for maintaining public order and safety. Respondents are satisfied with the cooperation and exchange of information 'in the heat of the moment'. There is, however, some disagreement between the parties about the organization of this cooperation. This may be explained by the fact that, in this partnership, the criteria for success mentioned in the literature are partly missing.

- *Organization and dynamic:* So far, a formal covenant that establishes everyone's roles, tasks and responsibilities is still lacking. This causes some unclarity among the participants. Furthermore, the municipality and neighbouring event locations (Ziggo Dome and AFAS Live) are missing as participants in this PPC

construction. The participating parties do, however, periodically consult with each other.

- *Cultural characteristics:* Trust in each other's knowledge, capability, and added value with respect to security (concerning the private 'event profilers' and the service desk employees) is not shared by everyone. Nor is there consensus on the necessity of using the 'profilers' and service desk employees. At this, we must note that the combination of security and service may be important for managing the influx of visitors, yet it may be less important when counter-terrorism is involved.
- *Tasks, roles and responsibilities:* Within the PPC, the plain-clothes private 'event profilers' constitute a contentious issue because of unclarity about what they actually do and what sort of information they collect. There is no equality between the parties; in the area surrounding the stadium the police is clearly in control. Finally, the PPC is also missing a formal driver.
- *Connection to the government*: There is no clear connection between the government and this network PPC. The network is not accountable to a democratically chosen body. The parties do, however, mutually assess their cooperation. In addition, respondents from private parties in particular have expressed the view that the dissemination of information about diffuse threats by governmental parties should be improved, be more explicit, which would enable them to adjust their measures more efficiently.

Nijmegen Four-Day March

In case of the Nijmegen Four-Day March, the PPC focuses on the exchange of information that contributes to the safety plan, the granting of licenses and scenarios and action perspectives in case of calamities during the achievement march. Core parties in this partnership are the private-law DE 4DAAGSE Foundation, the municipality of Nijmegen and the police. Other parties involved in this cooperation are the fire department, safety region Gelderland-Zuid, the Regional Medical Emergency Preparedness and Planning Agency (GHOR), and the Four-Day March Celebrations Foundation (Stichting Vierdaagsefeesten). Respondents are satisfied with the way in which the cooperation in this PPC works out. They exchange enough and adequate information in a pleasant atmosphere, which enables them to take good care of safety during the event. The PPC also keeps down costs for the government because the private party (the DE4DAAGSE Foundation) is given more and more responsibility.

- *Organization and dynamic:* The participating parties are in regular contact with each other through an established consultation structure. Prior to the Four-Day March, they see each other monthly and during the March they meet daily. The basis of the partnership has been laid down in a written framework agreement between the municipality, the Ministry of Defence and the DE 4DAAGSE Foundation. Although nobody is missing from this partnership, the need is felt to work together more closely with several parties outside the PPC (such as the Four-Day March Celebrations Foundation).
- *Cultural characteristics*: In majority, PPC participants share the same norms, values, views and 'language' as a result of their long-term cooperation, informal contact and the presence of former police officials and military officials on the board of the DE 4DAAGSE Foundation. Yet, now and then, there is disagreement about the measures to be taken against diffuse threats, but so far, this has not resulted in a breach of trust.
- *Tasks, roles and responsibilities:* For the participating parties, the division of tasks and responsibilities is clear. A shift has become visible from public to private because a growing number of security tasks are taken up by the private party (for

instance traffic control as well as surveillance and enforcement). The respondents did express the wish that commitments made should more often be laid down in writing. The relationship between the parties cannot be defined as being horizontal; after all, the municipality decides on the licence granted for the Four-Day March and governmental parties remain mainly responsible for the safety in public space. The municipality drives the partnership.

- *Connection to the government:* There is frequent contact with the local government, with the triangle (mayor, chief of police and public prosecutor) and sometimes with the national government. The network's accountability for how the Nijmegen Four-Day March has been handled takes form in annual evaluations. This has been set down in the framework agreement.

Antwerp Diamond Quarter

The Diamond Quarter in Antwerp has a PPC focused on a continuous exchange of information between, on the one hand, the Security Office of the Antwerp World Diamond Centre (AWDC), building managers of diamond traders and diamond exchanges and private security firms as the private parties, and the local police and the municipality as the public parties on the other hand. Beside the exchange of information, the partnership revolves around collectively taking and funding security measures. Respondents are unanimously satisfied with this PPC. They share a feeling of urgency to cooperate and the partnership is well organized.

- *Organization and dynamic*: The cooperation between the AWDC Security Office, the municipality and the police has been formally set down in a safety protocol and a cooperation agreement. This lends legitimacy to the partnership. Furthermore, there is regular contact between all parties in several fora.
- *Cultural characteristics:* Respondents experience great mutual trust, in part because they work with an established team and Single Points of Contact within the different organisations. There also is consensus about the approach for dealing with diffuse threats. All parties share a sense of urgency about combating safety issues in the neighbourhood; in this regard, they are willing to meet the others halfway.
- *Tasks, roles and responsibilities:* The division of tasks, roles and responsibilities is clear to everybody. It helps that the agreements have been laid down in writing. Although the governmental parties bear the ultimate responsibility for the safety in public space, we see a mix of public and private with respect to the way in which parties cooperate and safety measures are funded. The PPC has a clear driver in the private AWDC Security Office, yet the mayor is ultimately responsible for public order and safety and he can make crucial decisions, if necessary.
- *Connection to the government*: There is a clear connection between the PPC and governmental parties. Firstly, the exchange of information takes place with a wide range of governmental parties. In addition, the city council exerts influence on the practices of the safety network; it has ratified the most recent cooperation agreement (2016-2019), for instance.

What does this teach us?

The above shows that the PPC in the Antwerp Diamond Quarter answers to almost all criteria for success formulated in the literature. Many of the criteria for success are present in Nijmegen as well. This holds less true for the Johan Cruijff ArenA. The outcomes confirm that the presence or absence of these criteria has a positive or negative influence, respectively, on the satisfaction of respondents with the development and results of the PPC. We will reflect on these findings by looking through the theoretical

glasses of the success factors found in the literature for PPC networks aimed at guarding and securing soft targets. What can we learn from practice about the importance of these factors?

- *Organization and dynamic*: In all three cases, we have found that it is important for the right parties to sit at the table and for parties to keep in regular contact with each other (preferably face-to-face contact by means of consultation structures). For this reason, while setting up a PPC, the government and private parties must be very keen to see to it the intended partnership really is complete. Furthermore, it turns out that written (legal) agreements, such as covenants and protocols, contribute to clarity about the parties' roles and tasks and lend legitimacy to the PPC. In addition, respondents from all cases have made remarks about limiting laws and regulations that stand in the way of the exchange of information between public and private parties. This desired freer exchange of information underlines the importance of an improved legal security of PPC. After all, it is in the public interest to invest responsibilities and powers in a sound manner.
- *Cultural characteristics:* Trust between the parties, a shared sense of urgency to guarantee safety and the will to bridge possible disagreements prove to be important factors for success. We can conclude that the precise legal form of its organization is not decisive for the satisfaction with the development of network PPC aimed at guarding and securing 'soft targets'. A PPC thrives when parties maintain (reasonably) intensive contact, put a lot of energy in their cooperation and trust each other. As stated earlier, however, as seen from the perspective of the public interest of social safety, legal security really is important for the exchange of information and the corresponding responsibilities and powers invested in all parties.
- *Division of tasks,* roles and responsibilities and steering of the network: Networks consist of public and private parties with diverging views, goals and interests. It turns out that equivalence between the parties is not a necessity, yet reciprocity is. Furthermore, the presence of a unifying person in possession of legitimacy (not necessarily the power to persevere) and an eye for the various positions, is crucial. Surprisingly enough, in Antwerp, that person works for a private party that has earned the trust of both the government and the commercial diamond sector. An important skill of a unifying 'driver' is that he or she can make reciprocity happen. At both the private and public side, 'give and take' is central to sharing information and getting the funds for measures.
- *Connection between the government and the network*: The connection between the government and the network is not equally strong in all cases. Only the partnerships for the Antwerp Diamond Quarter and the Nijmegen Four-Day March are in some form or another accountable to a democratically elected body. The studied cases also show that administrative support is needed for PPC success. In both Antwerp and Nijmegen, the PPC is supported by the mayor, the chief of police and board members of the private parties involved, which lends legitimacy to the partnership. In Amsterdam, such administrative involvement from the municipality and the police is missing.

Reflection on social resilience

Contribution of PPC to social resilience

Increasing the resilience of private parties within PPC constructions can contribute to social safety if these parties invest in taking measures, for instance camera surveillance, the use of security guards and up-scaling scenarios, as well as training their own staff. By making employees more aware and alert, suspicious behaviours and objects may be recognised and reported earlier. This is the view of a number of experts who reflected on the findings of this study during a focus group session.

We want to mention here that 'resilience' is generally considered a hard to interpret phenomenon. According to the experts, the term refers to 'social cohesion', 'self-reliance' and 'alertness', but is for the rest a 'fluid' concept. This expert assessment matches the criticism in the literature about 'resilience' that it is a very ambiguous term, making it difficult to operationalise. It is impossible, too, to determine whether PPC has prevented attacks from taking place. According to one expert, we can at best assume that an improved collaboration and exchange of information between public and private parties has a positive effect, because it results in more 'eyes and ears' noticing deviating matters or persons.

This remark is in line with our assumption that PPC results in social resilience when participating public and private organizations enter into useful relationships with each other, based on the criteria described earlier: the network's organization and dynamic, cultural characteristics, the division of responsibilities and steering, and the connection to the government. Together, these elements guarantee a soundly functioning PPC. In two cases – the Nijmegen Four-Day March and the Antwerp Diamond Quarter – most of these elements are present, which does indeed lead to positive results, according to respondents. In the case of the Johan Cruijff ArenA, the PPC is not based on a covenant, and less trust and consensus exists among the participating parties. This may influence the resilience of this PPC in a negative way. At the same time, however, it must be said that the respondents have generally expressed their satisfaction with their mutual cooperation, just as respondents have done in Nijmegen and Antwerp.

Making and accepting governmental choices

According to the experts, increasing the resilience of private parties within PPC constructions may contribute to making and accepting choices by the government on transferring more responsibility for guarding and securing soft targets to private parties, when at least three conditions have been met. Firstly, it is necessary that the government actively invests in PPC and pays attention to the relationships to, and interests of, private parties. Secondly, this means that private parties can be involved more closely in the PPC if they are enabled to charge made costs to their clients, or if costs are divided more fairly among the participating parties. A third and last precondition for involving private parties in PPC is to provide more information to them about the nature of the diffuse threat. For private parties to be able to prepare and take useful measures, they must be better informed about what they are asked to do and why.

Three possible variants of PPC

Building on the information and analysis of this study, there are three possible variants of network PPC aimed at guarding and securing soft targets in times of diffuse threat. The first variant starts from the continuation of what already exists, while high expectations of network PPC must be tempered. At the moment, there are no networks in which public and private parties are equal. The government (the police, the municipality, the judiciary) is present in an unavoidably dominant position because of its monopoly on the use of force. For this reason, it is more accurate to speak about private co-responsibility for safety than about network PPC.

The second variant involves a deepening of network PPC and provides more room for a mutual exchange of information. The governmental and private parties share an equal amount of information with each other, including more sensitive information. From the perspective of a network's organization and dynamic, this means that more formal arrangements should be made. This requires an adaptation of existing laws and regulations on the exchange of information and privacy protection. It also means that the connection between the government and networks should be strengthened by the implementation of more solid accountability mechanisms regarding the exchange of information.

In the third variant, the government broadens the activities of private parties. This can be done by thoroughly reviewing the division of tasks, roles and responsibilities among the participating parties. Since the Dutch government holds the monopoly on the use of violence, safety networks are never as 'horizontal' as sometimes suggested by the literature on network cooperation, unless extensive adjustments are implemented. In line with this, it is possible to broaden network PPC when the government transfers not only more tasks, but also more powers regarding the use of force to the private security branch. Again, this will require a different, 'tighter' legal structuring of network PPC and the mechanisms for accountability that come with it.

1 Inleiding

1.1 Aanleiding

De afgelopen jaren is Europa het toneel geweest van meerdere terroristische aanslagen. Parijs, Brussel en Londen waren enkele keren het doelwit, maar onder andere ook Berlijn, Manchester, Nice en Stockholm werden getroffen. Daarbij maakten aanslagplegers gebruik van vuurwapengeweld, explosieven en vrachtwagens die op groepen flanerende of winkelende burgers inreden. Naast grote aanslagen is er tevens sprake van 'kleinere' – maar desalniettemin zeer ernstige – incidenten zoals schiet- en steekpartijen gericht op burgers en uniformdragers. Deze aanslagen beperken zich niet tot Europa. Wereldwijd vinden grote en kleine incidenten plaats, die tot maatregelen nopen. Nederland is eerder opgeschrikt door de moord op Theo van Gogh door een moslimfundamentalist, maar is tot op heden een grootschalige aanslag bespaard gebleven.

Bij uitstek zijn relatief 'open' plaatsen in de stad kwetsbaar als doelwitten voor (terroristische) aanslagen. In dit verband wordt ook wel gesproken over 'soft targets' die een openbaar of semiopenbaar karakter hebben, waar grote groepen mensen komen en die moeilijk te beveiligen zijn. Neem drukke straten, pleinen, markten en manifestaties. Daarnaast kunnen we denken aan musea, universiteiten, religieuze instellingen of overheidsgebouwen waartoe bezoekers in meer of mindere mate vrij toegang hebben. Tegelijk wordt er in de literatuur gesproken over 'mass private properties' (Shearing & Stenning 1981; Zhang 2017) of 'new communal spaces' (Kempa et al. 2004) die publiek toegankelijk zijn, maar worden beheerd door private partijen. Voorbeelden zijn voetbalstadions, evenemententerreinen, openbaar vervoer, luchthavens, horeca, uitgaansgelegenheden, en winkelgebieden.

Naast de verscheidenheid aan mogelijke doelwitten, zorgt ook de diversiteit aan potentiële daders en hun motieven voor een diffuse dreiging. Aanslagen worden zowel door terroristische organisaties en netwerken als geradicaliseerde eenlingen gepleegd. De meerderheid van de recente aanslagen was geïnspireerd op het jihadistisch gedachtegoed. Door de aanhoudende instabiliteit in het Midden-Oosten en Noord-Afrika, de dreiging die uitgaat van terugkeerders uit oorlogsgebieden en sympathisanten van het jihadisme binnen Europa zal deze dreiging van langdurige aard zijn (NCTV, 2017). Tevens is er sprake van een geweldsdreiging uit rechtsextremistische hoek. Deze dreiging richt zich over het algemeen op minderheden zoals asielzoekers, moslims en joden. Voorbeelden zijn de aanslag met een brandbom op een moskee in Enschede in 2016 en de aanslag op een islamitisch cultureel centrum in Quebec in 2017.[1]

Sinds maart 2013 is het dreigingsniveau in Nederland substantieel, wat inhoudt dat de kans op een terroristische aanslag reëel is. Net zoals in andere landen, stelt de (Rijks) overheid in Nederland zich hierbij tot doel aanslagen te voorkomen en maatschappelijke ontwrichting als gevolg van een aanslag te voorkomen of zo kort mogelijk te laten duren. De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) draagt samen met ketenpartners zorg voor de bewaking en beveiliging van personen, objecten, diensten, evenementen en vitale infrastructuur. Sinds medio 2014 is extra capaciteit vanuit de politie en de Koninklijke Marechaussee ingezet voor de bewaking en beveiliging van een aantal objecten met een hoog risicoprofiel. Daarnaast zijn er zichtbare tekenen van preventief ingrijpen bij de dreiging van een aanslag. Zo controleerde de Koninklijke Marechaussee in juni 2016 extra op en rond Schiphol na een zorgelijk 'signaal'[2], werden er in diezelfde periode extra veiligheidsmaatregelen genomen bij het dansfeest Sensation White[3] en werd besloten beveiligers meer zichtbaar aanwezig te

1 Hoewel er geen sprake was van een aanslag in de zin van terreur laat een incident op 7 april 2018 in Münster ook zien hoe kwetsbaar 'soft targets' zijn. Toen reed een psychisch verwarde man op een terras in met twee doden en twintig gewonden tot gevolg. De man pleegde daarna zelfmoord (https://nos.nl/artikel/2226245-man-die-op-terras-munster-inreed-had-psychische-problemen.html)

2 AT5, 30 juli 2016. 'Marechaussee controleert extra op en rond Schiphol na 'signaal' dreiging'. Geraadpleegd op 3 mei 2018. www.at5.nl/artikelen/158815/enorme_drukte_op_wegen_naar_schiphol_door_controles_marechaussee

3 NOS, 3 mei 2016. 'Extra maatregelen bij dancefeest Sensation na dreiging'. Geraadpleegd juni 2016. Geraadpleegd op 3 mei 2018. http://nos.nl/artikel/2113846-extra-maatregelen-bij-dancefeest-sensation-na-dreiging.html

laten zijn bij de uitvoering van The Passion in Amersfoort, welke daags na de aanslagen in Brussel plaatsvond.[4]

De capaciteit van de veiligheidsdiensten is echter niet oneindig. Financiële en personele middelen voor het bewaken en beveiligen van doelwitten zijn schaars. Er zullen prioriteiten moeten worden gesteld en keuzes worden gemaakt voor de inzet van bewakings- en beveiligingscapaciteit. Een eerste probleem is dat de hoeveelheid potentiële doelwitten – de 'soft targets' – enorm groot is. Hierboven hebben we al een waaier aan voorbeelden gegeven. De overheid kan niet bij alle evenementen, horecagelegenheden, infrastructurele knooppunten en wat dies meer zij massaal aanwezig zijn. Een tweede probleem is dat intensievere beveiliging van enkele doelwitten kan leiden tot nieuwe kwetsbaarheden bij andere doelwitten. Het gevaar bestaat dat aanslagplegers meebewegen en kiezen voor een doelwit met minder intensieve beveiliging. Tot slot zijn sommige 'soft targets' onmogelijk te beveiligen, zonder daarmee het vrije en open karakter van de samenleving aan te tasten (NCTV 2017). Het is bijvoorbeeld problematisch burgers te beschermen tegen aanvallen met voertuigen tenzij hele winkelstraten en boulevards worden afgesloten.

In het evaluatierapport van de nationale contra-terrorismestrategie 2011-2015 wordt gesteld dat de context van terrorismebestrijding de komende jaren complex en onvoorspelbaar blijft (Noordegraaf et al. 2016). De vraag naar veiligheid, bescherming, bewaking en beveiliging blijft dus hoog. De overheid kan deze verantwoordelijkheden en taken niet alleen aan en zoekt daarom steun bij private partijen. Om die reden zien we bijvoorbeeld in het openbaar vervoer, bij grote evenementen en rondom 'gevoelige' religieuze instellingen allerlei vormen van publiek-private samenwerking (PPS) op het gebied van veiligheid terug. Voor de hand ligt samenwerking met particuliere beveiligers (Van Steden 2007), maar we kunnen ook denken aan buitengewoon opsporingsambtenaren (boa's) in dienst van openbaarvervoersbedrijven (Van Steden 2015), evenementenbureaus die 'crowd control' verzorgen en sociale media monitoren (Bennett & Haggerty 2014) of aan joodse en islamitische gemeenschappen die eigen voorzorgsmaatregelen nemen (Flint 2009). Dergelijke samenwerkingsverbanden roepen de vraag op hoe de overheid samen met private actoren 'soft targets' op de lange termijn effectief kan bewaken en beveiligen en aldus voor maatschappelijke weerbaarheid kan zorgen.

Hierbij zij opgemerkt dat maatschappelijke weerbaarheid – oftewel sociale veerkracht ('social resilience') – een ingewikkeld begrip is. Wij vatten dit begrip op als onderdeel en uitvloeisel van het functioneren van wederzijds afhankelijke samenwerkingsrelaties tussen publieke en private organisaties die hun kennis en kunde bundelen bij het bewaken en beveiligen van 'soft targets' in tijden van diffuse dreiging. Onze veronderstelling is dat PPS leidt tot een zekere mate van maatschappelijke weerbaarheid als deelnemende publiek en private organisaties zinvolle relaties met elkaar aangaan binnen een netwerk. Dit moet ook leiden tot betere bewustwording en alertheid bij partijen. De mate waarin partijen binnen PPS in het veiligheidsdomein zinvolle relaties met elkaar aangaan en welke factoren daar een rol bij spelen vormen de insteek van deze studie.

1.2 Gedeelde verantwoordelijkheid voor veiligheid

De Rijksoverheid heeft in de contra-terrorismestrategie 2016-2020 ingestoken op een brede benadering, waar zowel overheidsorganisaties als private actoren onderdeel van uitmaken. Sociale wetenschappers spreken in dit verband over de 'responsabilisering' (Garland 1996) van derden of over 'third-party policing' (Buerger & Mazerolle 1998) om aan te geven dat private partijen – commerciële actoren, non-profit organisaties en burgers incluis – steeds meer verantwoordelijkheid nemen en krijgen in het voorkomen

4 NOS, 22 maart 2016 . 'Extra beveiliging bij The Passion in Amersfoort'. Geraadpleegd op 3 mei 2018. http://nos.nl/artikel/2094563-extra-beveiliging-bij-the-passion-in-amersfoort.html

en tegengaan van onveiligheid. In het geval van diffuse dreiging kunnen private actoren een rol spelen in zowel het voorkomen van een dreiging of aanslag, als het tegengaan van de gevolgen van een aanslag.

In het eerste geval gaat het om het nemen of krijgen van verantwoordelijkheden bij het bewaken en beveiligen van 'soft targets'. Een bijbehorende vorm van preventieve samenwerking in het tegengaan van diffuse dreiging betreft het – binnen de wettelijke mogelijkheden – uitwisselen van signalen en informatie tussen private en publieke partijen. Zo kunnen private actoren de publieke autoriteiten inlichten over mogelijk verdacht gedrag (Unicri 2009). Preventie, pro-actie en risicomanagement zijn hier sleutelwoorden. In het tweede geval gaat het om het voorkomen of beperken van maatschappelijke ontwrichting tijdens en/of na een aanslag. Denk bijvoorbeeld aan private partijen die tijdens een aanslag een bijdrage leveren aan de tijdige evacuatie van burgers (Dempsey 2011). Ook kunnen private partijen na een crisis werken aan herstel. Uit verschillende cases, veelal op het gebied van door natuur veroorzaakte crises, blijkt dat private partijen diensten, mankracht, geld en goederen leveren die bijdragen aan maatschappelijke veerkracht (Busch & Givens 2013). Private actoren kunnen, kortom, zowel tijdens 'warme' (wanneer er sprake is van een crisis) als 'koude' (wanneer er geen crisis is) fasen met de politie en andere publieke partijen op verschillende wijzen een rol spelen in het vergroten van maatschappelijke weerbaarheid bij een diffuse dreiging of daadwerkelijke aanslag. In de praktijk hangen activiteiten in de fasen voor, tijdens en na een aanslag met elkaar samen.

1.3 Focus en doelstelling van dit onderzoek

Publiek-private samenwerking bij het bewaken en beveiligen van 'soft targets' vindt zowel op nationaal als op lokaal niveau plaats. In Nederland en in andere landen zijn er praktijkvoorbeelden (en daarmee ervaringen) voorhanden van samenwerking tussen publieke (overheid) en private (niet-overheid) partijen in het voorkomen van aanslagen en het inperken van de gevolgen daarvan. Het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) en de NCTV willen graag weten wat de Nederlandse overheid kan leren van kennis en ervaringen in zowel ons eigen land als in andere West-Europese landen. Na een inventarisatie van mogelijke cases hebben we besloten ons toe te leggen op twee Nederlandse voorbeelden van PPS bij het bewaken en beveiligen van 'soft targets' (de Johan Cruijff ArenA en de Nijmeegse Vierdaagse) en een in Vlaanderen (het Diamantkwartier in Antwerpen) – zie voor meer details hieronder.

Binnen de cases ligt de focus op de koude fase vóór een crisis, dus op PPS in de preventieve sfeer, omdat er zich in ons land nog geen grootschalige aanslag heeft voorgedaan, we tijdens een aanslag waarschijnlijk lastig onderzoek kunnen uitvoeren, en voorkomen altijd beter dan genezen is. Daarnaast leggen we ons toe op het niveau van beleidsmakers en leidinggevenden van uitvoerenden binnen netwerken, waarbij er sprake is van samenwerking tussen professionals op lokaal niveau. Het doel van dit onderzoek is om inzicht te krijgen in de relevante werkwijzen en ervaringen met betrekking tot PPS bij het bewaken en beveiligen van 'soft targets' in tijden van (toenemende) diffuse dreiging. De ervaringen en percepties van de door ons geïnterviewde respondenten staan hierbij centraal. Deze informatie kan het Ministerie van Justitie en Veiligheid ondersteunen bij de afwegingen omtrent het bewaken en beveiligen van potentiële doelwitten ten behoeve van het vergroten van het algehele weerstandsniveau en de aanvullende rol die private actoren daarbij kunnen spelen.

1.4 Onderzoeksvragen

Dit leidt tot de volgende hoofdvraag:

Welke rol kunnen publieke (overheid) en private (niet-overheid) actoren vervullen binnen samenwerkingsverbanden bij het bewaken en beveiligen van 'soft targets' – en aldus bij het versterken van maatschappelijke weerbaarheid in tijden van diffuse dreiging?

De bijbehorende deelvragen zijn:

1. Wat zijn volgens de wetenschappelijke literatuur criteria voor succesvolle samenwerking tussen overheidsactoren en private actoren bij het bewaken en beveiligen van 'soft targets' en bij het versterken van maatschappelijke weerbaarheid in tijden van diffuse dreiging?
   a. Wat zijn 'soft targets'?
   b. Wat wordt er onder publiek-private samenwerking verstaan?
   c. Wat zijn in theorie criteria voor succesvolle publiek-private samenwerking?
   d. In hoeverre leidt publiek-private samenwerking in theorie tot maatschappelijke weerbaarheid?
2. Hoe werken overheden in Nederland en in andere Westerse landen in de praktijk samen met private actoren bij het bewaken en beveiligen van 'soft targets' en bij het versterken van de weerbaarheid van de samenleving?
   a. Hebben landelijke overheden beleid voor de wijze waarop men publieke en private samenwerking in het bewaken en beveiligen van 'soft targets' en het versterken van de weerbaarheid en zelfredzaamheid van de samenleving vorm wil geven?
   b. Hoe werken overheden samen met private actoren in het bewaken en beveiligen van 'soft targets' en het versterken van de weerbaarheid en zelfredzaamheid van de samenleving, welke partijen zijn hierbij betrokken, en hoe is de samenwerking vormgegeven?
3. Wat kunnen we leren van praktijkvoorbeelden waarin de overheid met private actoren samenwerkt bij het bewaken en beveiligen van 'soft targets' en bij het versterken van de weerbaarheid van de samenleving?
   a. Voldoen de in de praktijk geïnventariseerde werkwijzen van publiek-private samenwerking aan in de literatuur gevonden succescriteria?
   b. Wat zijn ervaringen van de betrokkenen met betrekking tot sterke punten en verbeterpuntenpunten in de samenwerking – welke elementen zijn kansrijk en welke juist niet?
4. In hoeverre en hoe kan het vergroten van de weerbaarheid van private partijen binnen PPS-constructies een bijdrage leveren aan (a) de maatschappelijke veiligheid, en (b) het maken en accepteren van keuzes van de overheid inzake het bewaken en beveiligen van 'soft targets' in tijden van diffuse dreiging?

1.5 Onderzoeksopzet

Het onderzoek bestaat uit vier fasen:

- Fase 1: scan van wetenschappelijke literatuur en het opstellen van een theoretisch kader.
- Fase 2: verzameling en analyse van (inter)nationale praktijkvoorbeelden.
- Fase 3: verdiepende analyse van drie cases: ervaringen met PPS.
- Fase 4: reflectie.

Hieronder lichten we de verschillende fasen nader toe.

Fase 1: Wetenschappelijke literatuur en theoretisch kader

We startten de eerste fase van het onderzoek met een scan van nationale en internationale (wetenschappelijke) literatuur over netwerken, 'governance', PPS, en weerbaarheid in het veiligheidsdomein, specifiek op het gebied van bewaken en beveiligen. Met een

analyse van deze literatuur gingen we na wat de mogelijke rol van private actoren is bij het voorkomen van een dreiging of aanslag. Vervolgens hebben we geïnventariseerd welke criteria en voorwaarden PPS op deze thema's succesvol maken en wat juist de aandachtspunten en risico's zijn.

Bij de analyse van de literatuur richten we ons op informatie die het meest relevant is voor het onderwerp waar deze studie zich op toelegt: de bewaking en beveiliging van 'soft targets' – dat wil zeggen: (semi)openbare ruimten waar veel mensen samenkomen en die moeilijk te beveiligen zijn. Aan de hand van de analyse van de (wetenschappelijke) literatuur stelden we vervolgens een theoretisch kader op. Dit kader bestaat uit elementen die volgens de literatuur een PPS succesvol maken of juist belemmeren. Het kader gebruiken we om de gevonden cases te analyseren.

Fase 2: Verzamelen en analyseren van (inter)nationaal beleid en van praktijkvoorbeelden

In de tweede fase verzamelden we verschillende voorbeelden van beleid van nationale overheden en (inter)nationale praktijken van publiek-private samenwerking bij het bewaken en beveiligen van 'soft targets'. We maakten gebruik van bestaande contacten van de teamleden van het onderzoeksproject en van het Ministerie van Justitie en Veiligheid, waaronder de NCTV, en zochten op Internet.[5] Naast het beleid van de Nederlandse Rijksoverheid en voorbeelden binnen verschillende Nederlandse gemeenten, hebben we gezocht naar beleid ten aanzien van PPS in België, Zweden, Denemarken, Duitsland, Finland, Frankrijk, Italië, Noorwegen, Oostenrijk, Portugal, Spanje, het Verenigd Koninkrijk, de Verenigde Staten, Canada en Australië (een volledige lijst van benaderde contactpersonen is te vinden in bijlage 1). Over Finland, Italië, Noorwegen, Oostenrijk, Portugal en Spanje was onvoldoende informatie beschikbaar of konden we niet de benodigde informatie krijgen. Daarom hebben we deze landen verder buiten beschouwing gelaten. Op basis van de verzamelde beleidsdocumenten hebben we een korte beschrijving gemaakt van het beleid van Westerse landen met betrekking tot PPS bij het bewaken en beveiligen van 'soft targets'. Het doel van deze fase was niet om een volledig en gedetailleerd overzicht te geven, maar om globaal inzicht te krijgen in de diversiteit en variatie aan gevoerde beleidsstrategieën binnen de verschillende landen.

Vervolgens hebben we (inter)nationale praktijkvoorbeelden bij het bewaken en beveiligen van 'soft targets' verzameld. Om zoveel mogelijk voorbeelden te verzamelen, hebben we gekozen voor een brede insteek, waarbij de volgende twee criteria zijn gebruikt:

1. Het project richt zich op bewaken en beveiligen (tegen terrorisme of breder tegen onveiligheid) in het geval van 'soft targets'.
2. Bij het project zijn minstens een publieke en een private partij betrokken.

Op basis van deze criteria hebben we 24 praktijkvoorbeelden gevonden, die we kort hebben samengevat in bijlage 2. Uit deze inventarisatie is gebleken dat voorbeelden van hechte (daadwerkelijke) PPS gericht op het bewaken en beveiligen van 'soft targets' in tijden van diffuse dreiging schaars zijn. Tegen deze achtergrond hebben we onze criteria aangescherpt en uitgebreid om tot een zinnige selectie van cases te komen waarnaar empirisch onderzoek is verricht. De uiteindelijke vijf criteria luiden:

1. Er moet sprake zijn van zichtbare publiek-private samenwerking tussen partijen.
2. Er moet sprake zijn van PPS binnen een (semi)openbaar 'soft target'.

5 Op de websites van Westerse overheden zochten we naar de meest recente beleidsstukken over contraterrorisme en de bewaking en beveiliging van 'soft targets'. Ook zochten we op Google met behulp van de volgende zoektermen (in verschillende talen): counter-terrorism AND strategy AND [naam land]; counter-terrorism AND policy [naam land]; public private partnerships AND terrorism AND [naam land]; public private partnerships AND soft targets AND [naam land]; public private partnerships AND places of mass gathering AND [naam land]; public private partnerships AND crowded places AND [naam land]; private AND terrorism AND [naam land]; private AND soft targets AND [naam land]; private AND places of mass gathering AND [naam land]; private AND crowded places AND [naam land]

3. Samenwerking moet verder gaan dan bijvoorbeeld enkel informatie verstrekken van de overheid aan private partijen of het geven van trainingen.
4. Samenwerking moet gericht zijn op preventie en daarmee op het vergroten van maatschappelijke weerbaarheid.
5. Er moet sprake zijn van praktische haalbaarheid (reistijd, taal, enzovoort) bij het doen van veldwerk.

Hiermee brachten we de 24 gevonden praktijkvoorbeelden terug tot zeven cases die veelbelovend leken: RTR-NL, de Johan Cruijff ArenA, de Nijmeegse Vierdaagse, het Diamantkwartier in Antwerpen, Project Argus in Londen, NYPD-Shield en Project-Aware in Denemarken. Project Griffin viel bij voorbaat af, omdat de NCTV hier al onderzoek naar heeft laten uitvoeren. Bij nadere beschouwing bleek dat RTR-NL beperkt bleef tot camerabewaking, het bij Project Argus vooral ging om informatie-vestrekking vanuit de overheid, project Aware enkel trainingen omvatte en NYPD-Shield praktisch niet haalbaar was. Daarom zijn de vervolgens door ons geselecteerde cases ter verdieping: (1) de Johan Cruijff ArenA, (2) de Nijmeegse Vierdaagse en (3) het Diamantkwartier in Antwerpen.

Fase 3: Verdiepende analyse van drie cases

In de verdiepende fase hebben we de bovenstaande drie cases onderzocht aan de hand van documentanalyse en interviews met respondenten die als beleids- of projectontwikkelaar bij het samenwerkingsverband zijn betrokken en leidinggevenden van uitvoerders van het samenwerkingsverband. Per casus hebben we met vijf tot zeven respondenten gesproken (een overzicht is te vinden in bijlage 3). We hebben met respondenten binnen zoveel mogelijk verschillende bij de PPS betrokken organisaties gesproken. Daarnaast hebben we diversiteit aangebracht op functieniveau: we hebben gesproken met bestuurders, leidinggevenden, beleids- en projectontwikkelaars en uitvoerders die bij de PPS zijn betrokken. De respondenten zijn geworven met behulp van de sneeuwbalmethode: de eerst geïnterviewde respondenten is gevraagd welke andere respondenten van belang zijn om te interviewen. Zij hebben ons vervolgens met andere respondenten in contact gebracht. De interviews zijn semigestructureerd afgenomen; we gebruikten een topiclijst die op basis van de operationalisatie in paragraaf 2.7 is opgesteld. Van de interviews is een gespreksverslag gemaakt, dat ter goedkeuring aan de respondenten is voorgelegd. De interviews duurden ongeveer anderhalf uur.

Fase 4: Reflectie

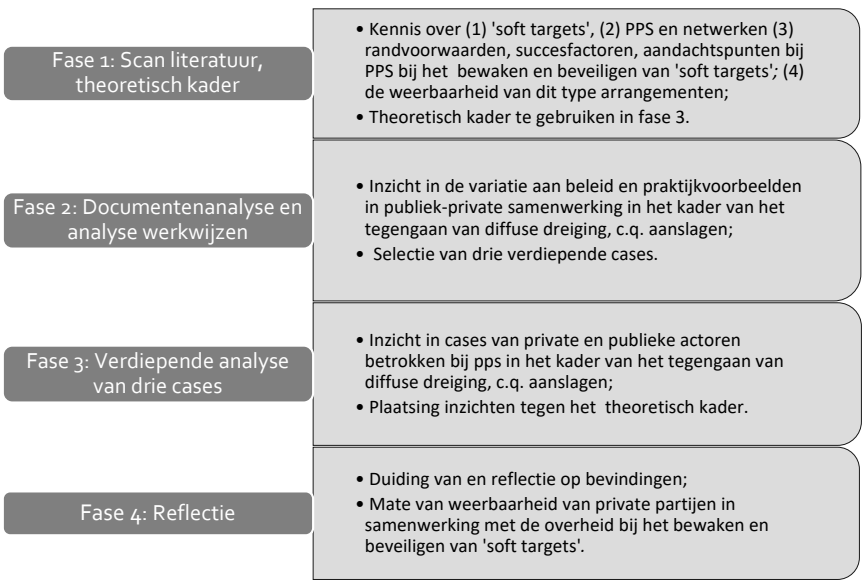
Tot slot reflecteren we op de kennis die we in de eerste drie fasen van het onderzoek hebben opgehaald over:

- De wijze waarop overheden met private actoren samenwerken bij het voorkomen van een (terroristische) aanslag.
- Wat succesvolle elementen zijn van publiek-private samenwerking bij het bewaken en beveiligen van 'soft targets' in tijden van diffuse dreiging.
- Hoe de alertheid en weerbaarheid van private partijen in samenwerking met de overheid een bijdrage kan leveren aan de nationale veiligheid.

Deze reflectie vond plaats middels een focusgroep met deelnemers die nauw betrokken zijn bij publiek-private samenwerking bij het bewaken en beveiligen van 'soft targets'. In bijlage 4 is een overzicht te vinden van de deelnemers aan deze focusgroep.

In figuur 1 vatten we de onderzoekopzet nog eens samen. Per onderzoeksfase benoemen we de opbrengst voor het beantwoorden van de vier onderzoeksvragen.

Figuur 1: Samenvatting onderzoeksopzet



1.6 Wat volgt

Het vervolg van dit rapport bestaat uit zes hoofdstukken. Hoofdstuk 2 bevat een literatuurstudie die uitmondt in het analysekader ten behoeve van onze cases. Daarna bevat hoofdstuk 3 een overzicht van beleid over en praktijkvoorbeelden van publiek-private samenwerking in het kader van het tegengaan van diffuse dreiging, c.q. aanslagen. Vervolgens presenteren en analyseren we in de hoofdstukken 4 tot en met 6 onze drie cases, respectievelijk de Johan Cruijff ArenA, de Nijmeegse Vierdaagse en het Diamantkwartier in Antwerpen. Hoofdstuk 7 sluit af met een conclusie en reflectie.

2 Literatuurstudie

2.1 Introductie

Dit hoofdstuk bevat een overzicht van wetenschappelijke literatuur over 'netwerken' gericht op veiligheid in tijden van diffuse dreiging die de vorm van 'publiek-private samenwerking' aannemen – het hoofdthema van ons onderzoek. Meer in het bijzonder gaat het om gedeelde verantwoordelijkheid bij het bewaken en beveiligen van 'soft targets' in veerkrachtige stedelijke gebieden en het bestrijden van de gevolgen van een eventuele calamiteit. Paragraaf 2.2 biedt een omschrijving van 'soft targets' en presenteert een categorisering van gebieden die relatief kwetsbaar zijn voor een terroristische aanval of een andersoortig incident. Vaak liggen deze gebieden in steden, maar het kan bijvoorbeeld ook om festivalterreinen in rurale omgevingen gaan. Paragraaf 2.3 behandelt bestuurskundige publicaties over netwerken, aangevuld met artikelen die specifieker gaan over de rol van publiek-private samenwerkingsverbanden rondom (de gevolgen van) crises en incidenten. Paragraaf 2.4 zet de 'succescriteria' binnen netwerken en samenwerkingsverbanden op een rij, waarna paragraaf 2.5 ingaat op beperkingen van netwerkbenaderingen. Paragraaf 2.6 geeft een omschrijving van maatschappelijke weerbaarheid in relatie tot netwerkvormen van PPS. We sluiten in paragraaf 2.7 af met een operationalisatie en analysekader ten behoeve van het empirische onderzoek.

2.2 'Soft targets'

Nederland is een open samenleving met veel mobiliteit en publiek toegankelijke plaatsen waar massa's mensen samenkomen. Veel van deze plaatsen zijn kwetsbaar voor een terroristische aanslag of een anderszins grote calamiteit en kunnen vanwege hun toegankelijkheid lastig worden beveiligd. In dit verband spreken auteurs over "*soft insecured targets where large crowds congregate*" (Then & Loosemore 2006: 158). Voorbeelden zijn winkelcentra, pretparken, festivals, pleinen en het openbaar vervoer. 'Soft targets' staan tegenover 'hard targets' die over het algemeen wel goed te beveiligen zijn en dan ook zwaar worden bewaakt. Denk hier aan plaatsen zoals nucleaire installaties, ambassades en militaire bases. Vanwege de grote diversiteit aan stedelijke 'soft targets' waaromheen vraagstukken van bewaking, beveiliging en sociale veerkracht spelen, volgt een categorisering op basis van de literatuur. Een klassieke vierdeling bestaat uit stedelijke gebieden die eigendom zijn van 'publieke' (overheid) dan wel 'private' (niet-overheid) partijen en voor 'algemeen' of 'specifiek' gebruik zijn. Langs deze lijnen biedt tabel 1 een typologie van kwetsbare stedelijke domeinen ('soft targets') waar veel mensen samenkomen en waarvan het eigendom in verschillende handen ligt.

Tabel 1: 'soft targets' naar gebruik getypeerd

	Publiek of semipubliek domein	**Commercieel of ander privaat domein**
Algemeen gebruik	Straten, wegen, pleinen en parken, buurthuizen en bibliotheken	Winkelcentra, festivals, pretparken, sportstadions, treinstations, hotels, luchthavens
Specifiek gebruik	Ministeries, gemeentehuizen, ziekenhuizen en onderwijsinstellingen	Kerken en andere religieuze instellingen

Stedelijke gebieden die publiek of privaat eigendom zijn en waar veel mensen samenkomen, staan in de internationale literatuur bekend als 'communal spaces' (Kempa et al. 2004): plaatsen van gemeenschappelijk belang. Deze aanduiding is echter zeer breed. Datzelfde geldt voor de specificatie van 'soft targets' als vormen van 'mass private property' (Shearing & Stenning 1981): commercieel beheerde, maar openbaar toegankelijke plaatsen. Dit typen plaatsen hebben uiteenlopende fysieke inrichtingen en toegangsregimes (Zhang 2017). Wakefield (2003) definieert toegangsregimes als de mate waarin publieke en/of private beheerders controle over een specifiek gebied uitoefenen. Daarom moeten we bij een verdere classificatie van 'soft targets' naar hun 'mate van toegankelijkheid' (of 'openheid') kijken. Zijn domeinen volledig openbaar of gelden er restricties? In de meest 'harde' variant geldt een restrictie in de vorm van aan te schaffen toegangsbewijzen voor het betreden van commercieel beheerde domeinen.

Tabel 2 bevat een typologie van stedelijke domeinen die als 'soft targets' kunnen worden aangemerkt en uiteenlopende toegangsregimes kennen.

Tabel 2: typen 'soft targets' en hun mate van toegankelijkheid

	Publiek of semipubliek domein	Commercieel of ander privaat domein
Volledig openbaar	Straten, wegen, pleinen en parken, buurthuizen en bibliotheken	Winkelcentra, bedrijventerreinen, treinstations, kerken en andere religieuze instellingen, luchthavens voor de douane, openbare festiviteiten
Met restricties	Ministeries, gemeentehuizen, ziekenhuizen en onderwijsinstellingen	Luchthavens achter de douane, hotels en pretparken, festivals en sportstadions waarvoor een toegangsbewijs nodig is

Deze categorisering biedt een scherper inzicht in de pluriformiteit van 'soft targets' die we op het oog hebben. Bovendien zijn er per gebied verschillende actoren – politie, private veiligheidsdiensten, (in beperkte mate) burgers, enzovoort – (mede)verantwoordelijk voor veiligheidsbeleid (tabel 3). Zij werken dan vaak samen. Hierover gaan de volgende paragrafen.

Tabel 3: de organisatie van veiligheid met betrekking tot 'soft targets'

Domeinen	Organisaties en initiatieven		
	Publieke sector	**Commerciële sector**	**Vrijwillige sector**
Publiek en openbaar toegankelijk	Politie, Koninklijke Marechaussee (KMar), gemeentelijk toezicht	Beveiligingsbedrijven	Buurtwachten, WhatsApp-preventie
Publiek met restricties	Politie, KMar parketpolitie en andere specialistische bewakingsdiensten	Beveiligingsbedrijven	
Privaat en openbaar toegankelijk	Politie, KMar	Beveiligingsbedrijven	
Privaat met restricties	Politie, KMar	Beveiligingsbedrijven, voetbalstewards, evenementenbeveiliging	

2.3 Hybride PPS-praktijken

Veel van de wetenschappelijke literatuur over publiek-private samenwerking (PPS) en netwerken komt uit de Angelsaksische wereld, al hebben ook Nederlandse wetenschappers (o.a. Klijn & Koppenjan 2012; Sanders 2014) hun bijdragen geleverd. Hieronder schetsen we een globaal beeld van thema's die uit de (inter)nationale literatuur naar voren komen en binnen de Nederlandse context relevant zijn. Allereerst gaat het over 'New Public Management' (NPM)-stromingen waarbinnen PPS een centrale plaats inneemt. Daarna gaan we in op typen PPS, waaruit blijkt dat dergelijke samenwerkingsverbanden in toenemende mate binnen netwerken plaatsvinden. We diepen deze constatering uit in een paragraaf over netwerken en netwerk-'governance'. Aansluitend bespreken we de fasen en niveaus, het management, en de praktische opzet van netwerken.

New Public Management

PPS in de veiligheidszorg is niet geheel nieuw. Al sinds de negentiende eeuw helpen bedrijven mee bij de wederopbouw na een grote brand of andere ramp (Busch & Givens 2012). De overheid is niet in staat om zelfstandig soelaas te bieden en zoekt daarom steun bij private – non-profit of commerciële – partijen. Hetzelfde beeld komt naar voren als het gaat om de preventie van criminaliteit, het oplossen van financieel-economische malversaties en het opsporen van misdadigers. Private beveiligingsbedrijven en rechercheburaus in binnen- en buitenland kennen een lange geschiedenis van samenwerking met de overheid (Zedner 2006; Van Steden 2007).

Toch werd binnen het openbaar bestuur en de bestuurskunde het concept PPS eind jaren zeventig, begin jaren tachtig, pas echt populair vanuit de veronderstelling dat de overheid samen met commerciële partijen tot uitvoering van beleid moest komen. PPS-constructies bestaan uit juridisch gestructureerde samenwerkingsverbanden,

waarbij ten minste één publieke partij gezaghebbend is en er één of meerdere private partij(en) betrokken zijn (Sanders 2014). De doelstellingen achter deze constructies waren het introduceren van marktprincipes binnen het overheidsmanagement en het stimuleren van privatisering, opdat de efficiency van publieke diensten kon worden vergroot en de bureaucratie kleiner zou worden (zie ook Dunn-Cavelty & Suter, 2009; Klijn & Koppenjan 2012).

Vooral de centrale metafoor achter NPM-stromingen dat de overheid moet 'sturen' en niet moet 'roeien' (Osborne & Gaebler 1992) kreeg veel invloed. Dit betekende dat de overheid gedetailleerde richtlijnen en contracten ging opstellen, waarbinnen private organisaties publieke diensten moesten leveren. Aldus heeft er een bewuste verschuiving plaatsgevonden van *"the government as the traditional provider of services to the government as the manager of services"* (Beutel & Weinberger 2016: 2) vanuit de aanname dat PPS, mits juist geïmplementeerd, tot lagere kosten en grotere opbrengsten leidt. Als gevolg hiervan werden publieke diensten in toenemende mate 'op afstand' gemanaged (Clarke & Newman 1997); een principe dat nog altijd wordt toegepast binnen bijvoorbeeld het onderwijs, de gezondheidzorg, de wegenbouw, technologische projecten en het gevangeniswezen. PPS groeide uit tot een 'catch-all' concept (Dunn-Cavelty & Suter 2009) of 'containerbegrip' (Sanders 2014) voor allerlei coöperatieve vormen tussen overheid en bedrijfsleven. Daarom zetten we kort drie typen PPS uiteen.

Typen PPS

Binnen NPM-stromingen, waarbij een bedrijfsmatige visie op het organiseren en managen van het openbaar bestuur via PPS-constructies centraal staat, kunnen 'markt-PPS' en 'gezags'-PPS' worden onderscheiden. 'Marktgerichte' PPS is gebaseerd op het 'contract- of concessiemodel', waarbij de regie in handen van de overheid blijft en het realiseren van efficiënte transacties voorop staat. De overheid is dan opdrachtgever met private partijen als opdrachtnemer en uitvoerder van beleid. Daarnaast bestaan er modellen van 'gezags'-PPS, waarbij de overheid bijvoorbeeld (kwaliteits)normen aan de private sector oplegt. De opkomst van netwerk-PPS – een derde vorm van PPS die ertoe bijdraagt dat private actoren in hun eigen en in het overheidsbelang binnen samenwerkingsverbanden participeren (Sanders 2014) – heeft er deels mee te maken dat NPM enigszins uit de gratie is geraakt (Klijn & Koppenjan 2012). Beloften van lagere kosten en hogere opbrengsten bleken niet altijd op waarheid gebaseerd of kunnen niet of nauwelijks adequaat worden vastgesteld (Pollitt & Bouckaert, 2011; Van Steden et al. 2017). Er is empirisch opvallend weinig bekend over de precieze uitkomsten en effecten van PPS en uitbestedingen door de overheid.

Tegelijk vloeien netwerken voort uit het feit dat grote sociale kwesties, waaronder veiligheid, 'wicked problems' (Rittel & Webber 1973) zijn. Dit zijn complexe – of venijnige – vraagstukken die geen definitieve oplossing hebben vanwege onderling strijdige doelen en belangen en waarvoor geen enkele partij, zelfs de overheid niet, alleen verantwoordelijkheid kan dragen. Als gevolg hiervan worden andere – commerciële en non-profit – organisaties 'geresponsabiliseerd' (Garland 1996). Anders gezegd: de verwachting is dat private partijen steeds meer verantwoordelijk voor veiligheid (en voor andere beleidsdomeinen) op zich nemen. De opkomst van netwerken die een gezamenlijke doelstelling hebben of ontwikkelen gericht op het aanpakken van maatschappelijke fenomenen, waaronder diffuse (terroristische) dreigingen, wordt van overheidswege dus actief aangemoedigd. Sanders (2014) spreekt zelfs van een 'reparatiestrategie' voor de behartiging van publieke belangen. Overigens vindt de 'responsabilisering' – en dito 'privatisering' – van veiligheid in Nederland op relatief bescheiden schaal plaats. Weliswaar steken er zo nu en dan 'kerntakendiscussies' de kop op over wat de politie wel, en vooral niet, zou moeten doen, maar het geweldsmonopolie blijft in handen van de overheid (Van Steden 2017). Anders dan in de Verenigde Staten mogen private beveiligers bijvoorbeeld geen vuurwapens dragen.

Netwerken en netwerk-'governance'

Hoewel netwerk-PPS uitgaat van tenminste een gezaghebbende publieke partij, vertrekt veel hedendaagse literatuur over netwerken vanuit het idee dat publieke en partijen op een min of meer gelijkwaardige manier samenwerken, besluitvorming idealiter gezamenlijk plaatsvindt en de eindverantwoordelijkheid bij zowel de publieke als private partners is belegd (o.a. Eversdijk & Korsten, 2007; Klijn & Twist, 2007; Verhees et al., 2015). Om recht te doen aan deze enigszins ambigue situatie spreken auteurs over 'hybride praktijken' (O'Toole 1997; Powell 1990): een ensemble van publieke en private partijen dat sturing geeft aan een beleidsdomein. In een paar zinnen samengevat luidt het uitgangspunt van netwerkbenaderingen dat:

> *"beleid tot stand komt in complexe interactieprocessen tussen een groot aantal actoren. Die actoren zijn wederzijds van elkaar afhankelijk, zodat beleid alleen kan worden gerealiseerd door samenwerking tussen actoren" (Klijn & Koppenjan, 1994: 148).*

Het besef dat de overheid ('government') niet alleen verantwoordelijkheid kan dragen voor grote maatschappelijke kwesties zoals veiligheid heeft binnen de bestuurskunde geleid tot verdere theorievorming over 'governance': sturing of besturing binnen netwerken (Klijn & Twist 2007).

Een waterdichte definitie van 'governance' bestaat niet, maar er kunnen wel verschillende elementen worden onderscheiden (Stoker 1998; Van Steden 2011). Allereerst verwijst 'governance' naar een dynamisch samenstel van actoren binnen en buiten de overheid. Op het terrein van veiligheid en terrorismebestrijding in het kader van 'soft targets' staan vanzelfsprekend de politie en private beveiliging centraal (tabel 3), maar talloze andere actoren – winkelbedrijven, festivalorganisaties, gemeenten, de financiële sector, hotels en horecaondernemingen, facility managers, hulpverleners, enzovoort – zijn eveneens betrokken.

Daarnaast kunnen we denken aan bezoekers van 'soft targets' die spontaan hulp bieden bij calamiteiten of training krijgen om hen weerbaarder te maken en 'burgermoed' (Mehlbaum & Van Steden 2016) te tonen. Voorts overheerst binnen de 'governance'-literatuur het besef dat een strikte afbakening van verantwoordelijkheden tussen 'het publieke' en 'het private' aan het vervagen is. We zien eerder een vloeiend continuüm tussen gradaties van 'publicness' en 'privateness' (Dijkstra & Van der Meer 2003).

Ten derde kunnen publieke en private organisaties niet zonder elkaar om doelen te bereiken. Zo zijn bijvoorbeeld banken belangrijke spelers geworden in het monitoren van internationale geldstromen die terroristische organisaties financieren (Keatinge 2015), dragen bedrijven meer dan de overheid bij aan de bescherming van de vitale infrastructuur, zoals energievoorzieningen, mobiele telefoonnetwerken en het Internet (Busch & Givens 2012; Dunn-Calvelty & Suter 2009) en beschikken uiteenlopende semipublieke ruimten over eigen, commerciële beveiligingsdiensten (Van Steden 2007; Wakefield 2003).

Tot slot bieden hiërarchische machtsrelaties geen oplossing voor de aansturing van netwerken. Johnston en Shearing (2003) typeren de overheid as 'one node among many' binnen grotere hybride verbanden. Genetwerkte publieke en private organisaties leven op een zekere voet van gelijkheid met elkaar.

Niveaus en mate van formaliteit van netwerken

PPS die de vorm van netwerken aanneemt kan op verschillende niveaus gestalte krijgen. Hierbij wordt er vaak onderscheid gemaakt tussen een beleidsnetwerk en een uitvoerend netwerk (Terpstra & Kouwenhoven 2004). Op het beleidsniveau komen managers, bestuurders en andere leidinggevenden bijeen om strategieën en middelen ten behoeve van rampen- en terrorismebestrijding te bepalen. Het uitvoeringsniveau bestaat vervolgens uit professionals op de werkvloer die dagelijks samenwerken en het

beleid uitrollen. Ten tweede kunnen netwerken meer formeel of informeel van aard zijn. We hebben al eerder gezien dat klassieke PPS-constructies meestal zijn ingebed binnen formele contracten en convenanten, maar sociologisch onderzoek naar netwerken benoemt tevens de mogelijkheid van ('sterke' of 'zwakke') informele banden tussen mensen (Granovetter 1973). Tot slot, en samenhangend met het voorgaande, opereren samenwerkende publieke en private professionals niet in een vacuüm. Juist bij crises, rampen en aanslagen is het belangrijk om (formele) organisatienetwerken en (informele) gemeenschappen van burgers aan elkaar te verbinden (Hawkings & Maurer 2010). Veerkracht en weerbaarheid tonen, is iets dat uit de samenleving als geheel moet komen.

Management van netweken

Vanwege de vele publieke en private partijen die betrokken zijn bij de bescherming van 'soft targets' kan de overheid beleid niet simpelweg hiërarchisch implementeren. Het gaat eerder om de creatie van een raamwerk, waarbinnen *"public administration […] becomes a team sport where persuasion, negotiations, and mutual trust are more important than control and regulation*" (Dunn-Calvety & Suster 2009: 183). Beutel & Weinberg (2015) adviseren dan ook om voor heldere 'governance'-structuren te zorgen, waarbinnen (1) de rollen en verantwoordelijkheden (arbeidsdeling) van partijen naar behoren zijn gedefinieerd, (2) de organisatie van het netwerk aansluit op de complexiteit van een probleem en (3) botsende visies of belangen adequaat kunnen worden gekanaliseerd. Provan en Kenis (2007) maken hierbij een veel geciteerd onderscheid tussen geheel zelfsturende netwerken, netwerken waarbinnen een partij een voortrekkersrol heeft en netwerken die binnen een nieuw opgerichte administratieve inbedding opereren.

In de praktijk blijkt dat het managen van netwerken – zelfsturend of niet – een lastige, zelfs onderschatte, taak is (Klijn & Koppenjan 2012). Een zekere mate van hiërarchie blijft meestal noodzakelijk (Hill & Lynn 2005). Weliswaar kunnen publieke autoriteiten binnen netwerken geen 'top-down' beleid voeren, maar een overheid speelt ook geen passieve rol; vooral niet als de (nationale) veiligheid in het geding is. Er wordt derhalve wel gesproken van overheidsprofessionals als innovatieve 'katalysatoren' (Beutel & Weinberg 2016) met een faciliterende en wakende functie binnen netwerken. Concreet zijn netwerkmanagers druk met het activeren en mobiliseren van veelkleurige partijen, het stimuleren van overeenstemming over doelen en middelen, het luisteren naar ieders inbreng, het kweken van wederzijds vertrouwen, het kanaliseren van conflicten en het creëren van interne en externe legitimiteit (Popp et al. 2014). De sturing van netwerken komt derhalve neer op 'improvisatie' in een complexe omgeving (Boutellier 2011).

Praktische opzet

Het zal duidelijk zijn dat de 'governance' – sturing of besturing – van netwerken een ingewikkelde aangelegenheid is. Ten behoeve van een systematische analyse van publiek-private samenwerkingsverbanden gericht op het bewaken en beveiligen van 'soft targets' is het informatief om naar 'governance' te kijken met behulp van de metafoor van een liniemodel, waarin alle partijen kunnen worden beschouwd als de spelers binnen een team (Boutellier & Steden 2011).[6] De vraag is telkens: wat is de aard en zwaarte van de diffuse dreiging (diagnose) en welke actoren zijn vervolgens het best geëquipeerd om actie te ondernemen (behandeling)?[7] Hieruit volgt hoe een netwerk praktisch opgezet kan worden en welke actoren in stelling moeten worden gebracht. Antwoorden hebben ook betrekking op het niveau (strategiebepaling/uitvoering)

6 Vanuit eenzelfde gedachte bieden de Verenigde Naties (VN) een handboek voor het bouwen aan publiek-private samenwerking om 'soft targets' te beschermen, inclusief een vragenlijst die meer inzicht moet geven in de eigen kennis en het eigen handelen van organisaties met betrekking tot veiligheidsvraagstukken. Daarnaast presenteren de VN een stappenplan om PPS-constructies te realiseren. Zie: www.unicri.it/topics/public_private_security_policies/.

7 Een diagnose-behandelplan is bekend uit de geneeskunde. Binnen het veiligheidsveld kunnen we bijvoorbeeld aan een risicoanalyse denken om de diagnose te stellen.

waarop een netwerk opereert en in welke fase (pre-crisis, crisis, post-crisis) een netwerk zich bevindt.

Teneinde het spel zoveel mogelijk voorin te spelen, redeneren we van achteruit naar voren. De partijen op het veiligheidsveld geven elkaar ruggensteun. Dat wil zeggen: de doelman wordt gevormd door justitie bezig met opsporing en sanctioneren, met het strafrecht als 'ultimum remedium'. Vervolgens staan in de verdediging partijen die zich primair bezighouden met toezicht, handhaving en risicomanagement, zoals de politie, particuliere beveiligers en buitengewoon opsporingsambtenaren. Het middenveld wordt gevormd door maatschappelijke organisaties en bedrijven. Zij hebben geen primaire veiligheidstaak, maar zijn in normatieve zin van groot belang voor de opbouw van zelfredzaamheid en weerbaarheid. Dit middenveld bedient tenslotte de voorhoede die wordt gevormd door (verbanden tussen) burgers. Zij vormen het sociale cement van de samenleving.

De coach – regelmatig de lokale of nationale overheid, soms samen met de politie – stelt de kaders (tactiek) vast, betrekt de spelers en is verantwoordelijk voor het bevorderen van 'team play'. Bij het bekijken van PPS kan het voetbalveld helpen om te bepalen welke spelers waar en wanneer aanwezig (moeten) zijn. Welke professionals, organisaties en burgers kunnen bijdragen aan of betrokken worden bij netwerken, coalities en allianties in zowel de 'warme' als de 'koude' fase van een crisis? Verder draagt een probleemdiagnose bij aan het doordenken waar 'de bal' ligt of zou moeten liggen: achterin het veld of juist voorin?

2.4 Criteria voor succes

Is een netwerk eenmaal operationeel dan rijst de vraag wat criteria voor succes zijn. Wat maakt een netwerk effectief? Effectiviteit kan worden opgevat als 'mate van doelbereiking', maar het gaat eveneens om het vermogen van netwerken om zich flexibel en veerkrachtig naar veranderende situaties te voegen en duurzame relaties binnen en buiten het eigen verband aan te gaan (Turrini et al. 2010). Antwoorden op de vraag naar het verloop en de opbrengsten van PPS zullen wederom afhangen van het niveau waarop een netwerk actief is (strategiebepaling/uitvoering) en de fase waarover we spreken (pre-crisis, crisis, post-crisis). Vanuit de bestuurskundige literatuur en van publicaties over veiligheid en crisismanagement kunnen enkele algemene criteria worden gedestilleerd die een nadere uitwerking zijn van de eerder behandelde literatuur over netwerken: 'organisatie en dynamiek', 'culturele kenmerken', 'verdeling van verantwoordelijkheden en sturing' en 'connectie met de overheid'. We bespreken deze elementen één voor één.

Organisatie en dynamiek

Een netwerk valt of staat met het vermogen van deelnemende partijen om op meer dan ad-hoc basis kennis en informatie met elkaar uit te wisselen, gericht op het tegengaan van (urgente) veiligheidsrisco's en/of het versterken van sociale veerkracht. Zoals Popp et al. schrijven:

> *"[…] inter-organizational networks are increasingly seen as mechanisms for improving the spread of new ideas end practices […] and their ability to do so successfully is an indicator of network performance. An ultimate challenge for networks and network managers, then, has to do with both collectively generating new knowledge tailored to address the common problem, and ensuring that this new knowledge is actually used" (2014: 33).*

Nieuwe informatietechnologieën en sociale media nemen hierbij een steeds prominentere plaats in. Aansluitend gaat het om leren van elkaar, zodat een netwerk tot een duurzame, innovatieve en daadkrachtige aanpak van 'wicked problems' komt. Hier stuiten we meteen op een flink dilemma. Juist het faciliteren van informatiedeling en kennisontwikkeling ligt in het veiligheidsdomein erg gevoelig. Wet- en regelgeving, geheimhouding, burgerrechten en privacy zijn – terechte – factoren die het cruciale element 'informatiedeling' binnen veiligheidsnetwerken (ernstig) in de weg kunnen staan.

Of het komen tot een daadkrachtige aanpak in informatiedeling lukt, heeft allereerst te maken met de structuur van netwerken (Turrini et al. 2010; Whelan 2011). Een netwerk moet niet te klein zijn, maar ook niet onoverzichtelijk groot. Voortbouwend op het liniemodel is het dus cruciaal om te weten wie de 'key players' binnen een bepaalde fase (moeten) zijn en wie zich meer in de periferie bevinden. Een netwerkanalyse die de sterkte van relaties en informatiestromen tussen partijen in kaart brengt, kan hierbij helpen (zie voor een voorbeeld: Broekhuizen et al. 2010). Daarnaast kunnen netwerken in meer of mindere mate 'zelfsturend' zijn (Provan & Kenis 2007), waarbij de vorm moet passen bij het probleem dat organisaties gezamenlijk aan willen pakken. Hiermee raken we eveneens aan de wenselijkheid van (in)formaliteit binnen netwerken. Boutellier en Van Marissing suggereren dat bij voorkeur 'stevige' (formele) afspraken – 'op papier' – de basis moeten vormen van onderling commitment:

> *"In de ontwikkeling van het arrangement dient men elkaar goed te leren kennen, maar vervolgens dienen de gemaakte afspraken nadrukkelijk te worden vastgelegd en bestuurlijk te worden gehandhaafd. Indien afspraken niet nagekomen worden, dient te worden gesanctioneerd" (2011: 63).*

Ze voegen hieraan overigens toe dat er idealiter een 'combinatie van controle en vertrouwen' bij samenwerkende partners aanwezig is.

Culturele kenmerken

Daarom zijn, ten tweede, culturele elementen van netwerken het bestuderen waard. Cultuur verwijst naar de overtuigingen, waarden en attitudes die partijen in de loop van de tijd hebben gevormd en hun handelen beïnvloeden (Whelan 2011). Zij volgen een 'network way of working' (Popp et al. 2014) die uniek kan zijn en niet zonder meer overgeplaatst kan worden naar andere plaatsen en omstandigheden. Het heeft daarom zin om naar de geschiedenis van netwerken te kijken:

> *"A history of successful collaboration is likely to build social capital, increasing rapport and trust between parties involved, both of which are highly likely to be conductive towards well-functioning future partnership" (Chen et al. 2013: 140).*

Netwerken en organisaties binnen deze netwerken functioneren binnen historisch gegroeide culturen en subculturen ('mental frameworks'; Johnston & Shearing 2003), die zowel positief als negatief kunnen uitpakken voor publiek-private samenwerking. Voor een flink deel bestaan netwerken uit interorganisatorische en interpersoonlijke relaties die gebaseerd zijn op gewoonten, percepties, sympathieën en antipathieën, waarmee – het woord is al een aantal keer gevallen – vertrouwen in het middelpunt van de genetwerkte samenwerking komt te staan:

> *"Trust is often mentioned as the core coordination mechanism of networks. […] Trust reduces strategic uncertainty, because actors take each other's interest into account. It also reduces the necessity of complex contracts and enhances the possibility that actors will share information and develop innovative solutions" (Klijn en Koppenjan 2012: 593-594).*

Hoewel vertrouwen niet het enige coördinatiemechanisme binnen netwerken is, blijkt een gebrek aan vertrouwen desastreus voor de samenwerking tussen partijen: "*trust is invaluable in fostering effective, mutually beneficial outcomes*" (Busch & Givens 2012: 7). Netwerkvorming heeft, kortom, een inherent 'zachte' doelstelling gericht op het verstevigen van wederkerige sociale verhoudingen.

Verdeling van verantwoordelijkheden en sturing

Dit laat echter onverlet dat netwerken tevens vanuit een meer functionalistisch perspectief kunnen worden benaderd. Machtsstructuren en belangenstrijd over doelen en middelen hangen samen met wie de regels van het spel maakt, wat de inhoud van die regels is, de (financiële) hulpbronnen waarover partijen beschikken en in hoeverre zij hun positie op het speelveld kunnen handhaven of uitbreiden (Johnston & Shearing 2003). Gegeven dat netwerken functioneren op basis van wederzijdse afhankelijkheid,

maar ook van relatieve gelijkheid en autonomie, vergen onderhuidse spanningen en conflicten veel van het management: *"it is difficult to achieve satisfactory outcomes without extensive networking between the actors and managerial activities"* (Klijn en Koppenjan 2012: 592). Commerciële actoren hechten wellicht meer belang aan hun reputatie en aan de beleving van hun klanten dan aan – verstorende – veiligheidsmaatregelen (o.a. Bures 2013; Wakefield 2003). Dit zou tot conflicten kunnen leiden met de doelstellingen van overheidsorganisaties die nationale veiligheid en openbare orde voorop stellen.

Auteurs raden daarom aan dat – 'lichte' – leiders binnen netwerken ervoor moeten zorgen dat andere partijen mede-eigenaar worden van het probleem en vanaf begin af aan bij besluitvormingsprocessen worden betrokken (Beutel & Weinberger 2016; Boutellier 2011; Bures 2013). Zij spreken soms zelfs over de noodzaak van 'kampioenen' (Beutel & Weinberger 2016) of 'schoolvoorbeelden' (Van Hulst et al. 2011) binnen samenwerkingsverbanden: personen die in staat zijn het verschil te maken, kloven tussen 'publieke' en 'private' logica's overbruggen, support organiseren en netwerken laten floreren. Daarbij is het steeds zaak diagnoses uit te voeren – wat is het probleem?; in welke fase zitten we?; wie zijn de spelers?; op welk niveau opereren zij? –, prioriteiten te stellen, tot gezamenlijke (SMART-geformuleerde)[8] doelstellingen te komen en een lange-termijn visie uit te stippelen, met waardering voor wat al is bereikt en waar gevoeligheden liggen (zie ook: Boutellier & Van Marissing 2011). Soms is het nodig om in zo'n proces tot cultuurveranderingen te komen – een punt dat eerder is aangestipt en doorgaans veel tijd en energie vergt.

Connectie met de overheid

Tot slot bevindt een netwerk zich in een bepaalde context. Dat vergt flexibiliteit: *"to meet the needs of their target population(s), public private partnerships need to be able to adapt to changing circumstances and resources"* (Beutel & Weinberger 2016: 18). Professionals horen oog te houden voor de samenleving die zij bedienen en van waaruit zij waardevolle informatie over veiligheidsrisico's kunnen destilleren. Een issue dat hierbij moet worden meegenomen, is de evaluatie en daarmee 'accountability' van netwerken richting de buitenwereld. Het is mogelijk dat betrokken – 'technocratische' – specialisten en experts zich naar binnen keren:

> *"many authors recognise tensions between the idea of representative democracy with a more vertical accountability structure and direct democracy of network governance processes that includes stakeholders in policy-making" (Klijn en Koppenjan 2012: 595).*

Daarbij komt dat de vermenging tussen 'publieke' en 'private' standaarden en codes problemen op kan leveren (Busch & Givens 2012). Overheden die zich te veel mee laten slepen door 'marktwaarden' zouden broeinesten van regelovertredingen of erger kunnen worden, terwijl bedrijven die te veel met overheden meegaan hun informatie en andere middelen wellicht onverantwoord gaan verspillen. Tegelijk zijn netwerken die de nationale veiligheid garanderen en diffuse dreigingen tegengaan vanwege hun karakter niet altijd even transparant, bijvoorbeeld omdat partijen over gevoelige data of technologie beschikken en hun strategieën niet op voorhand openbaar kunnen maken. Net als informatieoverdracht en kennisdeling is 'accountability' – het afleggen van democratische verantwoordelijkheid – dus een potentieel struikelblok voor de legitimiteit van veiligheidsnetwerken. Het is niet altijd duidelijk wat er binnen netwerken gebeurt en hoe resultaten van PPS moeten worden gewaardeerd.

8 SMART (Specific, Measurable, Achievable, Relevant, Time-bound) beoogt als principe het eenvoudig opstellen, controleren en evalueren van doelstellingen die een netwerk wil bereiken.

2.5 Beperkingen

De beschreven netwerken zijn een antwoord op te bureaucratische en centralistische neigingen van overheden aan de ene kant en de tekortkomingen van marktwerking (een te forse focus op eigen belangen) aan de andere kant. Daarentegen sluiten netwerken een groot aantal interdependente, maar autonome, partijen in, die tot collectieve actie moeten komen. Hiermee vormen netwerken geen ei van Columbus (McGuire & Agranoff 2011). Bestuurskundigen hebben de neiging om oplossingen die netwerken bieden te benadrukken, maar zoals eerder gezegd zijn er ook tekortkomingen, spanningen, dilemma's en beperkingen aanwijsbaar. We zetten de belangrijksten op een rij.

Ten eerste kan de grote waarde van vertrouwen binnen, en daarmee een zekere informaliteit van, hybride netwerken botsen met formeel-juridische regelgeving en privacyreglementen (Bures 2013). Tevens maakt vertrouwen kwetsbaar: wederkerigheid in informatiedeling als een van de hoofddoelen binnen netwerkprocessen kan makkelijk worden beschadigd als de vertrouwensbasis onder publiek-private samenwerking wegvalt. Dan is het mogelijk dat een netwerk feitelijk ophoudt te bestaan.

Ten tweede kan de grote nadruk op informatiedeling aanleiding zijn tot 'information-overload', wat de effectiviteit van netwerken in de weg staat: "*the collection and filtering of information represents a daunting and costly challenge*" (Bures 2013: 441). Bovendien zijn niet alle partijen van zins om kostbare data zomaar weg te geven. Bijvoorbeeld banken beschikken over vertrouwelijke informatie die juridisch beschermd wordt en bij deling tot ernstige reputatieschade kan leiden (Keatinge 2015).

Ten derde, schrijft Bures, *"it should be kept in mind that private entities are primarily profit, rather than security maximizers*" (2013: 430). Bedrijven willen eigen schades en verliezen beperken en reputaties beschermen, waarbij het ze er misschien minder aan gelegen is om de maatschappelijke veiligheid te vergroten. De bescherming van 'soft targets' vergt immers hoge investeringen in tastbare maatregelen zoals bewakingscamera's, particulier beveiligingspersoneel en elektronische poortjes, zonder dat meteen duidelijk is wat zoiets oplevert (Busch & Givens 2012). Het voorkomen van aanslagen is lastig meetbaar.

Ten vierde zijn 'management' en 'leiderschap' binnen netwerken problematische begrippen. Popp et al. waarschuwen dat:

> *"although some members of a network, as in other organizational forms, may have more formal power due to position, professional education and training, resources or political clout, this power cannot be wielded unilaterally the way we generally believe it can be in a traditional hierarchy" (2014: 40).*

Daarom moeten leiders en managers zoeken naar andere coördinatiemechanismen, waaronder facilitering, verleiding en consensusvorming. Er wordt daarom wel gesproken van 'dienend leiderschap', maar dat vergt speciale vaardigheden en kan veel tijd kosten, die er tijdens een (dreigende) crisissituatie misschien helemaal niet is.

Tot slot is er het genoemde issue van 'accountability'. Hoe zit het met de democratische verantwoording over, en evaluatie van netwerken; zeker als er iets mis gaat? Dunn-Cavelty en Suter stellen terecht dat "*generating security for citizens is a core task of the state; therefore it is an extremely delicate matter for the government to pass on its responsibility in this area to the private sector*" (2009: 181). Het centrale dilemma van veiligheidsnetwerken is dat overheden, ondanks hun sturende en controlerende taken, afhankelijk zijn van private derden voor het opstellen en uitvoeren van beleid. Dat levert in potentie tegenstrijdige gezichtspunten, belangenconflicten, ambigue waarden en ongewenste uitkomsten op. Het valt te betwijfelen of publieke en private perspectieven op veiligheid eenvoudig kunnen worden verenigd, waarbij zij opgemerkt dat de overheid vanwege haar geweldsmonopolie wel eindverantwoordelijk blijft. Publiek-private samenwerking binnen netwerken stuit dus onmiskenbaar op grenzen met mogelijk onbedoelde negatieve consequenties voor 'good governance'.

2.6 Maatschappelijke weerbaarheid

Publiek-private samenwerkingsverbanden kunnen zich zowel op de 'warme' kant (wanneer er een incident is) als op de 'koude' kant (wanneer er geen incident is) van terrorisme- en crisisbestrijding richten. In de literatuur wordt nog iets preciezer onderscheid gemaakt tussen de 'pre-crisis' (preventie) fase, de 'crisis' (responsie) fase en de 'post-crisis' (herstel) fase (Chen et al. 2013; Then & Loosemore 2006). Binnen de pre-crisis fase ligt het accent vervolgens op het identificeren van mogelijke risico's, preventieve werkzaamheden om (de gevolgen van) dreigingen te beperken en het werken aan strategieën, plannen en procedures voor als er zich een incident voor mocht doen. Tijdens de crisis fase draait het om leiderschap tonen, snelheid betrachten en slagkrachtig zijn binnen onzekere en stressvolle omstandigheden. De post-crisis fase, tot slot, richt zich op herstel en wederopbouw, maar ook op het trekken van langere termijn consequenties door het leren van eventuele fouten, het in gang zetten van veranderingen en het verwerken van een (collectief) trauma. De functie van samenwerking tussen publieke en private partijen verschilt per fase, evenals de kernpartners – politie, beveiliging, burgers, hulpverleners, enzovoort – die binnen elke fase actief zijn. Volgens Bures (2016) zou het hierbij niet zozeer moeten gaan over de eis van efficiency(winst), maar over het bouwen aan 'resilience': de sociale veerkracht en maatschappelijke weerbaarheid van fysieke en sociale infrastructuren en van (lokale) gemeenschappen.

De term 'sociale veerkracht', ook wel aangeduid als 'maatschappelijke weerbaarheid', komt oorspronkelijk uit studies naar complexe ecologische systemen en is inmiddels gemeengoed binnen publicaties over crisismanagement. De precieze betekenis van 'veerkracht' en 'weerbaarheid' blijft echter ambigu: een overzicht van de literatuur laat zien dat *"resilence […] has multiple, and often conflicting meanings"* (Reid & Botterill 2013: 38). Concepten worden binnen uiteenlopende contexten en met verschillende bedoelingen gebruikt, zonder dat er een waterdichte definitie bestaat: de ene auteur verbindt deze termen met instabiliteit, het goed kunnen functioneren onder stress, zich flexibel aan omstandigheden kunnen aanpassen, zelfredzaam zijn en met onzekerheid kunnen omgaan. Daarentegen verwijzen andere auteurs naar het belang van een stabiel evenwicht: het voorkomen en absorberen van schokken en het zelfredzame vermogen van gemeenschappen om weer terug te veren (Duit 2016; Reid & Botterill 2013). Binnen deze studie naar PPS in tijden van diffuse dreiging vatten wij 'maatschappelijke weerbaarheid' op als onderdeel en uitvloeisel van het functioneren van wederzijds afhankelijke samenwerkingsrelaties tussen publieke en private organisaties die hun kennis en kunde bundelen bij de preventie maatschappelijke gebeurtenissen, c.q. diffuse dreigingen zoals terroristische aanslagen.

Het kernprobleem met de ambiguïteit van de termen veerkracht en weerbaarheid is dat *"it is also not clear how resilience can be operationalised in either policy or management terms"* (Reid & Botterill 2013: 37). Bovendien bekritiseert Duit (2016) de te deterministische uitgangspunten achter het concept veerkracht: alsof je door het draaien aan de juiste knoppen – door bestuur, sturing en PPS strakker 'in te regelen' – beter bent toegerust om schokken voor te zijn, op te vangen of te verwerken. Volgens haar is de realiteit veel weerbarstiger en gaat veerkracht te veel uit van het idee van een samenleving als mechanisch en maakbaar systeem. Daarom stellen Reid en Botterill (2013: 38) zelfs dat *"avoiding using 'resilience' […] would seem sensible"*. Niettemin gaan wij uit van de veronderstelling dat PPS leidt tot een zekere mate van maatschappelijke weerbaarheid als deelnemende publieke en private organisaties zinvolle relaties met elkaar aangaan vanuit de beschreven 'succescriteria' binnen een op preventie gericht veiligheidsnetwerk. Daarbij hoort het besef dat private partijen naast de overheid een eigen verantwoordelijkheid voor veiligheid hebben en dat PPS bijdraagt aan een bewustwording en concrete invulling hiervan.

2.7 Operationalisatie en analysekader

Onderhavige literatuurstudie biedt conceptuele handvatten voor nader empirisch onderzoek naar nationale en internationale voorbeelden van publiek-private samenwerking binnen netwerken die 'soft targets' beschermen en de veerkracht van een samenleving daarbij willen vergroten. Hierbij wordt er in de literatuur onderscheid gemaakt tussen netwerken die actief zijn voor, tijdens of na een crisis. In het vervolg zullen we ons vooral toeleggen op vormen van netwerk-PPS in de preventieve fase voor een crisis, waarbij we kijken naar het beleids- en uitvoeringsniveau van samenwerkingsverbanden.

We zetten in de analyse van ons empirisch materiaal de volgende stappen: eerst classificeren we de te bestuderen typen 'soft targets': zijn zij publiek of privaat? Gelden er al dan niet restricties bij de toegang van domeinen? Daarna maken we onderscheid tussen een afhankelijke variabele (kenmerken van verloop netwerk-PPS) en vier onafhankelijke variabelen (kenmerken die het verloop van netwerk-PPS beïnvloeden). Hieronder lichten we de operationalisatie van deze variabelen toe.

Kenmerken van verloop netwerk-PPS

De afhankelijke variabele betreft het verloop van netwerk-PPS gericht op het voorkomen van incidenten en aanslagen in tijden van diffuse dreiging. Het gaat hier dus om de ervaringen met PPS vanuit het perspectief van publieke en private partijen. Daarbij kijken we ook naar mogelijke uitkomsten van deze samenwerking (in hoeverre is de samenwerking in de praktijk waardevol gebleken in het voorkomen van terroristische dreigingen of aanslagen?). Omdat het niet eenvoudig is om dergelijke uitkomsten te meten – zeker niet als het om het *voorkomen* van incidenten gaat – vallen we terug op de percepties van betrokkenen. Het verloop van netwerk-PPS wordt langs de volgende dimensies geoperationaliseerd:

- Tevredenheid over de praktijk van PPS:
  - Draagvlak voor samenwerking.
  - Mate van informatiedeling.
- Tevredenheid over de resultaten van de PPS:
  - Concrete uitkomsten.
  - Andere typen resultaten.

Criteria die het verloop van netwerk-PPS beïnvloeden

We bekijken criteria voor succes die – mogelijk – invloed hebben op het verloop van PPS gericht op het voorkomen van incidenten en aanslagen in tijden van diffuse dreiging. Deze criteria zijn langs de volgende vier dimensies geoperationaliseerd:

1. De organisatie en dynamiek van het netwerk:
   - Aard en inhoud PPS:
     - Deelnemers.
     - Aanleiding.
     - Doelstelling.
     - Strategisch, tactisch of operationeel.
     - Eventuele veranderingen door de tijd.
   - Vormgeving van samenwerking tussen organisaties binnen het netwerk:
     - Formeel of informeel (convenanten, afspraken, plannen).
   - Mate van contacten tussen organisaties binnen het netwerk:
     - Hoe vaak contactmomenten.

- Inhoud hiervan.

2. Culturele kenmerken:
   - Onderling vertrouwen binnen het netwerk:
     - Hoe lang al PPS.
     - Routines en teamgeest.
     - Afspraken nakomen ('van elkaar op aankunnen').
   - Mate van consensus over probleemperceptie binnen het netwerk:
     - Gedeeld probleem (of niet).
     - Motivatie tot samenwerken.
3. Verdeling van taken, rollen en verantwoordelijkheden binnen en sturing van het netwerk:
   - Rollen en verantwoordelijkheden van partijen:
     - Wie doet wat.
     - Duidelijkheid voor iedereen (of niet).
     - Gelijkwaardigheid van partijen.
   - Besluitvorming:
     - Verloop hiervan.
     - Consensus of onenigheid.
   - Aanwezigheid van 'trekker' of 'verbindend persoon' binnen het netwerk en tevredenheid hierover:
     - Coördinatie en regie.
     - 'Doorzettingsmacht'.
     - Legitimiteit van persoon.
4. Connectie tussen de overheid en het netwerk:
     - Invloed van lokale en nationale overheid op het netwerk.
     - Samenwerking met partijen buiten de PPS.
   - Verantwoording van gegenereerde resultaten aan democratisch gekozen organen:
     - Evaluaties of audits.
     - Andere vormen van 'accountability'.

De individuele criteria vormen noodzakelijke, maar niet voldoende, voorwaarden voor het succesvol laten verlopen van PPS. Er kunnen bijvoorbeeld veel contactmomenten zijn, maar als deelnemers elkaar niet vertrouwen zullen processen toch moeizaam verlopen (zie ook Raab et al. 2015). Als alle criteria tezamen aanwezig zijn binnen een netwerk zal dit naar verwachting positief bijdragen aan het verloop van de PPS.

Tot slot bieden we een reflectie op de maatschappelijke weerbaarheid van de onderzochte netwerken. Zoals uit de literatuur blijkt, blijft een operationalisatie van dit begrip problematisch vanwege een diversiteit aan – soms tegenstrijdige – betekenissen. Onze eigen veronderstelling is dat PPS leidt tot een zekere mate van maatschappelijke weerbaarheid als deelnemende publieke en private organisaties zinvolle relaties met elkaar aangaan vanuit beschreven 'succescriteria' binnen een netwerk. Dit moet ook leiden tot betere bewustwording en alertheid bij partijen.

3 Een beknopt internationaal beeld

3.1 Introductie

In dit hoofdstuk beschrijven we welk beleid overheden hanteren ten aanzien van PPS bij het bewaken en beveiligen van 'soft targets'. Ook geven we voorbeelden van 'beperkte' PPS in de vorm van training en/of geringe informatie-uitwisseling. Omvangrijker en verdergaande vormen van PPS – daadwerkelijke samenwerking op het lokale niveau van 'soft targets' – worden uitgebreid beschreven en geanalyseerd in hoofdstuk 4 tot en met 6. Onderstaand internationaal beeld is niet uitputtend bedoeld, maar geeft een indruk van wat er binnen 'het Westen' zoal aan beleid en praktische vormen van PPS bestaat.

3.2 Overheidsbeleid

Westerse overheden voeren zonder uitzondering contra-terrorismebeleid of beleid om andere diffuse dreigingen tegen te gaan. Hierbij zijn ze zich in toenemende mate bewust van de noodzaak om met private actoren samen te werken teneinde de weerbaarheid of veerkracht van de samenleving in tijden van diffuse dreiging te vergroten. In nationale beleidsstukken zien we dat daarbij vooral de nadruk wordt gelegd op samenwerking met de private sector als het gaat om het beschermen en bewaken van de vitale infrastructuur (denk aan drinkwatervoorzieningen, nucleaire installaties en cybersecurity). De noodzaak van PPS met betrekking tot 'soft targets', zoals door ons gedefinieerd, komt echter weinig expliciet in deze stukken terug. We zetten in de volgende paragrafen uiteen wat er uit de bestudeerde beleidsdocumenten en gesprekken met experts in Nederland, België, Duitsland, Frankrijk, Denemarken, Zweden, het Verenigd Koninkrijk, de Verenigde Staten, Canada en Australië[9] naar voren is gekomen.

Nederland

In Nederland zoekt de NCTV toenadering tot private actoren. Zij heeft bijvoorbeeld een 'handleiding drukke plekken' opgesteld en heeft daartoe bijeenkomsten georganiseerd met private stakeholders die een 'soft target' beheren of exploiteren.[10] In deze handleiding staan suggesties voor extra maatregelen die ondernemers kunnen helpen bij de voorbereiding op een mogelijke aanslag. De beoogde maatregelen gericht op onder meer toegangs- en ontvangstbeleid, informatiebeveiliging, camerabewaking en de plaatsing van betonblokken zijn aanvullend op die van de lokale en landelijke overheid. Ook kent Nederland het 'Alerteringssysteem Terrorismebestrijding' dat publieke en private partijen tijdig informeert over terroristische dreiging, zodat de betrokken partijen passende maatregelen kunnen nemen om het risico op een aanslag te verkleinen of de gevolgen ervan te beperken (NCTV 2017). Private partijen die deel uitmaken van deze samenwerking zijn te vinden binnen sectoren zoals het openbaar vervoer, zeehavens, luchthavens, grote publieksevenementen, de horeca (grote hotels) en grote winkelcentra. Over het algemeen vindt samenwerking aangaande het bewaken en beveiligen van 'soft targets' vooral op lokale schaal plaats, zonder dat hierover een uniform landelijk beleid wordt gevoerd.

België

De gesproken overheidsfunctionarissen en experts in België zijn niet bekend met een landelijke strategie aangaande PPS bij het bewaken en beveiligen van 'soft targets'. PPS wordt volgens hen belemmerd doordat informatiedeling tussen publieke en private partijen wettelijk maar zeer beperkt is toegestaan. Informeel vindt samenwerking echter wel plaats. Tegelijk is er na de aanslagen in Brussel in maart 2016 sprake van een toenadering tussen publieke en private partijen ten aanzien van de bewaking en beveiliging

9 De verantwoording voor de keuze voor deze landen staat beschreven in hoofdstuk 1, paragraaf 1.5.

10 Zie: www.nctv.nl/drukkeplekken.

van 'soft targets'. In dit verband moet de nieuwe wet op de private veiligheidsbranche, die op 8 juni 2017 door het Belgische parlement werd goedgekeurd, worden genoemd. Deze wet voorziet in een uitbreiding van de bevoegdheden van de sector. Zo zijn private beveiligingsbedrijven nu bevoegd om (on)roerende goederen te beveiligen en te doorzoeken, bijvoorbeeld met technologische middelen zoals drones.[11] Het achterliggende idee is de politie te ontlasten en meer verantwoordelijkheid te geven aan eigenaren of exploitanten van 'soft targets'.

Duitsland

Benaderde overheidsfunctionarissen en experts op het gebied van contra-terrorisme in Duitsland zeggen niet bekend te zijn met beleid op federaal of staatsniveau aangaande de samenwerking tussen publieke en private actoren bij het bewaken en beveiligen van 'soft targets', dan wel het verhogen van de weerbaarheid van de samenleving. Terrorismebestrijding is in Duitsland vooral aan de publieke diensten voorbehouden. Volgens een respondent neemt dit echter niet weg dat private partijen zelfstandig maatregelen nemen om zich beter tegen terroristische aanslagen te beschermen. Zo hebben enkele hotel- en winkelketens voorzorgsmaatregelen getroffen. Tevens financieren en borgen organisatoren in de evenementenbranche maatregelen om hun bezoekers te beschermen. Hiertoe kunnen zij de politie en private beveiliging inhuren.

Frankrijk

Frankrijk heeft, kort na de aanslagen in Parijs in november 2015, een strategie opgesteld ('Faire Face Ensemble'), waarin wordt gesproken over een gezamenlijke aanpak van terrorisme door publieke en private partijen. De Franse overheid stelt in het beleidsdocument dat eigenaren en exploitanten van 'soft targets' verantwoordelijk zijn voor het nemen van adequate veiligheidsmaatregelen. Zij dienen hun eigen veiligheid en dat van de mensen die zij bedienen te waarborgen (SGDSN 2016). Publieke partijen ondersteunen hen daarin door het bieden van kennis. Zo heeft de overheid handleidingen uitgebracht voor managers en personeel werkzaam in sectoren die als 'soft targets' zijn aan te merken: de medische sector, winkelcentra, bedrijventerreinen, de culturele sector (onder andere erfgoed, concerthallen, festivals en bioscopen) en scholen. In deze handleidingen staan per sector maatregelen beschreven die bijdragen aan het voorkomen van aanslagen, dan wel aan het verminderen van de impact hiervan. Uit de strategie komt naar voren dat de private partijen in principe aan zet zijn: zij dienen contact te leggen met lokale autoriteiten om tot een gezamenlijke risicoanalyse te komen en moeten met publieke veiligheidsdiensten afstemmen bij het nemen van maatregelen.

Denemarken

In 2015 publiceerde Denemarken haar contra-terrorismebeleid, getiteld: 'Een sterke verdediging tegen terrorisme' (Regeringen Denemarken 2015). Het beleidsplan gaat voornamelijk in op het versterken van de publieke veiligheids- en inlichtingendiensten, maar spreekt niet over samenwerking met private actoren in het bestrijden van terrorisme. Ook uit gesprekken met Deense overheidsfunctionarissen blijkt dat een dergelijk beleid ontbreekt. Wel vindt er in de praktijk samenwerking plaats tussen de inlichtingendienst en privaat personeel, met name particuliere beveiligers en winkeleigenaren, werkzaam op locaties die als 'soft target' zijn aan te duiden (PET 2011). Deze samenwerking bestaat voornamelijk uit het geven van trainingen aan private partijen over het herkennen van signalen van verdacht gedrag en hoe te handelen tijdens een aanslag. In paragraaf 3.3 komen we hier nader op terug.

11 Meer informatie over deze wet is te vinden op: www.besafe.be

Zweden

De Zweedse overheid benadrukt in haar nationale contra-terrorismestrategie dat meer samenwerking tussen publieke en private partijen noodzakelijk is om tot gezamenlijke risicoanalyses te komen voor het beter bewaken en beveiligen van 'soft targets', waaronder de culturele sector, sportactiviteiten en winkelcentra (Zweeds Ministerie van Justitie 2015). Een uitgewerkte beleidsstrategie over hoe deze samenwerking in de praktijk vorm moet krijgen ontbreekt echter. De Zweedse overheid geeft vooral aan dat er nog onvoldoende sprake is van samenwerking tussen de publieke en private sector. In hoeverre en op welke manier er inmiddels PPS-arrangementen zijn, blijft onduidelijk. Verscheidene benaderde overheidsfunctionarissen uit Zweden konden geen concrete voorbeelden noemen van PPS gericht op het bewaken en beveiligen van 'soft targets' en het verhogen van de weerbaarheid van de samenleving.

Verenigd Koninkrijk

Het Verenigd Koninkrijk kent een nationaal contra-terrorismebeleid, waarin de noodzaak tot samenwerking met private actoren in het bewaken en beveiligen van 'soft targets' expliciet wordt benoemd. Daarnaast heeft de Britse regering in juni 2017 de 'Crowded Places Guidance' uitgebracht met richtlijnen en adviezen voor sectoren die als 'soft targets' kunnen worden aangemerkt (NaCTSO 2017). Deze handleiding is gericht op de particuliere veiligheidsbranche en de – meestal private – eigenaren en exploitanten van 'soft targets'. De Britse overheid ziet het implementeren en financieren van veiligheidsmaatregelen tegen aanslagen als verantwoordelijkheid van de eigenaren en exploitanten. Daarbij worden deze partijen wel vanuit de overheid ondersteund. Door het hele land zijn politieagenten (zogeheten 'counter-terrorism security advisors') getraind, die als taak hebben aandacht te hebben voor kwetsbare locaties. Het is hun taak om met de betrokken private actoren informatie te delen over het dreigingsniveau en een gezamenlijk veiligheidsplan op te stellen.

Verenigde Staten

De Verenigde Staten benadrukken in diverse beleidsstukken dat terrorismebestrijding alleen kan slagen door effectieve samenwerkingsverbanden met de private sector (onder andere Department of Homeland Security 2017). Na de aanslagen op de Twin Towers in 2001 heeft de Amerikaanse overheid de samenwerking met private actoren geïntensiveerd. Deze partijen worden onder andere betrokken bij het opstellen van dreigingsanalyses, het delen van informatie en het leveren van technologische oplossingen. Zo wordt op regionaal niveau in 'Fusion Centers' informatie verzameld, geanalyseerd en gedeeld tussen publieke en private partijen – denk hierbij vooral aan partijen binnen de kritische infrastructuur en aan particuliere beveiligers. Ook kunnen private partijen van overheidswege training krijgen over het beter beveiligen van hun bedrijfszaken en hoe te handelen tijdens een aanslag.

Canada

Canada benadrukt in haar nationale contra-terrorismestrategie dat deze strategie alleen kan slagen door effectieve samenwerkingsverbanden tussen de overheid, de private sector, non-gouvernementele organisaties en de bredere gemeenschap (Government of Canada 2013). In dit beleidsdocument staat opgenomen dat de overheid samenwerkt door het delen van informatie en door het gezamenlijk vergroten van de veerkracht van gemeenschappen. De concrete invulling hiervan ontbreekt niettemin. Ondanks dat de Canadese overheid het belang van samenwerking met niet-overheidsactoren in haar contra-terrorismestrategie dus benadrukt, stelt een benaderde expert dat dergelijke vormen van PPS in Canada minder ontwikkeld zijn dan in sommige Europese landen.

Australië

Australië heeft sinds 2011 een beleidsstrategie gericht op het bewaken en beveiligen van 'soft targets' tegen terroristische aanslagen: de 'National Guidelines for the Protec-

tion of Places of Mass Gathering from Terrorism'. De meest recente versie stamt uit augustus 2017. PPS staat hierbij centraal. Daarbij hanteert de Australische overheid het uitgangspunt dat eigenaren en exploitanten van 'soft targets' primair verantwoordelijk zijn voor het nemen van adequate veiligheidsmaatregelen om aanslagen te voorkomen, dan wel de gevolgen te beperken. PPS bestaat uit samenwerking binnen 'crowded places forums': samenwerkingsverbanden tussen regionale overheidsvertegenwoordigers, de politie en eigenaren en exploitanten van 'soft targets' (Commonwealth of Australia, 2017). Binnen deze fora is het de bedoeling dat publieke partijen informatie delen met private actoren over het dreigingsniveau en dat zij private actoren ondersteunen bij het nemen van gepaste veiligheidsmaatregelen door kennis, 'tools', waaronder risicoanalyses, en adviezen aan te bieden. Naast het nemen van adequate veiligheidsmaatregelen wordt van private actoren verwacht dat zij vroegtijdig informatie delen met de publieke actoren over verdachte situaties en geleerde lessen.

Wat leert dit ons?

Binnen de hierboven genoemde overheden lijkt in toenemende mate een bewustwording te ontstaan van de noodzaak om met private actoren samen te werken teneinde kwetsbare doelwitten beter te beschermen tegen aanslagen. Dit blijkt zowel uit beleidsdocumenten als uit gesprekken met verschillende overheidsfunctionarissen en experts. Desondanks is deze wens nog niet in alle landen vertaald naar expliciet beleid ten aanzien van PPS rondom het bewaken en beveiligen van 'soft targets'. Diverse overheden zijn wel bezig met het beschikbaar stellen van een handleiding ter bevordering van te nemen veiligheidsmaatregelen door private partijen. Daarbij ondersteunen overheden door advisering, het overdragen van kennis en informatie en het beschikbaar stellen van tools, zoals risicoanalyse-instrumenten. Het Verenigd Koninkrijk, de Verenigde Staten en Australië lijken de langste traditie te hebben in het aangaan van PPS in het veiligheidsdomein. Een mogelijke verklaring hiervoor is de meer open houding van deze overheden ten opzichte van de privatisering van veiligheidstaken. Daarentegen is in bijvoorbeeld Duitsland of Frankrijk het organiseren van veiligheid nog steeds een grotendeels publieke taak. Nederland lijkt zich qua positie in het midden te bevinden.

3.3 Voorbeelden van PPS

Bij de inventarisatie van praktijkvoorbeelden van PPS bij het bewaken en beveiligen van 'soft targets' en het verhogen van de maatschappelijke weerbaarheid kwamen we tot 24 voorbeelden in binnen- en buitenland (zie bijlage 2). Deze brede inventarisatie leverde de nodige voorbeelden op uit het Verenigd Koninkrijk en de Verenigde Staten. Dat is niet erg verrassend, omdat beide landen een verhoudingsgewijs lange traditie van PPS in het sociale veiligheidsdomein kennen. Verder valt op dat de gevonden praktijkvoorbeelden zich voor een groot deel richten op het uitwisselen van informatie of het geven van trainingen, zonder dat er door publieke en private actoren echt lokaal wordt samengewerkt. Voorbeelden van daadwerkelijke PPS gericht op het bewaken en beveiligen van 'soft targets' in tijden van diffuse dreiging blijken schaars. De 24 voorbeelden hebben we teruggebracht tot zeven kansrijke cases, waarvan we er uiteindelijk drie – de Johan Cruijff ArenA, de Nijmeegse Vierdaagse en het Diamantkwartier in Antwerpen – in de volgende hoofdstukken uitdiepen. We hebben voor deze drie cases gekozen vanwege PPS op lokaal niveau die verder gaat dan camerabewaking, training en/of geringe informatieoverdracht vanuit de overheid (zie hoofdstuk 1 voor een gedetailleerde verantwoording). De vier cases die we niet gekozen hebben voor de verdiepende fase – Project Argus (Londen), NYPD-Shield (New York), Project Aware (Denemarken) en RTR-NL (Nederland) – staan hieronder kort beschreven. Binnen deze praktijkvoorbeelden gaat het om 'beperkte' PPS in de vorm van camerabewaking, training en/of informatie-uitwisseling.

Project Argus – Londen

Het project Argus biedt medewerkers binnen het bedrijfsleven, detailhandel, horeca, hotels, onderwijs en gezondheidszorg een drie uur durende simulatie aan over het voorkomen van aanslagen en over handelingsrichtingen tijdens en na aanslagen. Het doel van de samenwerking is om bewustzijn onder medewerkers van de hierboven genoemde sectoren te creëren over wat te doen voor, tijdens en na een aanslag. Er worden ook sessies gehouden met personen die in 'crowded places' werken, waarin informatie gedeeld wordt over 'best practices'. Deelnemende partijen zijn de Londense politiediensten en bedrijven uit (de omgeving van) Londen. De samenwerking lijkt niet verder te gaan dan een eenzijdige informatieverstrekking vanuit de overheid richting de private sector. Zowel tijdens trainingen als tijdens werkgroepen ontvangen deelnemers door 'Counter Terrorism Security Advisers' van de politie aangeleverde kennis en ervaringen.[12]

NYPD-Shield – New York

NYPD-Shield – 'Countering terrorism through information-sharing' – is een paraplu voor verschillende projecten waarbinnen de politiediensten in New York samenwerken met private partijen en burgers om aanslagen te voorkomen. Geïnteresseerde private organisaties melden zich aan om lid te worden. Ze worden dan bezocht door een rechercheur van de NYPD-Shield, die met hen bespreekt welke sectoren kwetsbaar zijn voor terroristische activiteiten en op welke indicatoren de specifieke organisatie (gezien hun sector) alert zou kunnen of moeten zijn. Vervolgens geeft de New York Police Department (NYPD) (contraterrorisme) trainingen aan veiligheidsmanagers van private partijen en houdt deze partijen op de hoogte over mogelijke dreigingen in de stad. De private partijen fungeren op hun beurt als 'ogen en oren' van de NYPD, en melden verdachte situaties zo vroeg mogelijk. Het kan hier bijvoorbeeld gaan om verdachte zakelijke transacties of om verdacht en ongewoon gedrag bij 'soft targets'. Wanneer we naar de activiteiten van dit project kijken, ligt de focus op informatie-uitwisseling en training in de preventieve fase. Daarnaast richt NYPD-Shield zich op het dempen van het effect van een aanslag, het onderzoeken van terroristische activiteiten, en het opsporen van daders.[13]

Project Aware – Denemarken

Personen die in 'crowded places' werken, waaronder winkeleigenaren en beveiligingsmedewerkers, kunnen een bewustzijnstraining volgen van de Deense Inlichtingendienst PET. Deelnemers leren verdacht gedrag herkennen (voorkomen van een aanslag) en hoe ze moeten handelen tijdens een aanslag. Zij volgen een vier uur durende cursus, gevolgd door een additionele online-trainingsmodule waarin enkele belangrijke punten worden herhaald.[14]

RTR-NL – Nederland

RTR-NL richt zich op het handhaven van de openbare orde en het beschermen van goederen, personen, diensten en objecten door proactief cameratoezicht in het publieke domein. In twee operationele toezichtruimten in Eindhoven en Nijmegen komen informatiestromen van publieke en private camerabewaking samen. Deze camera's staan gericht op bedrijventerreinen, winkelcentra, binnensteden, (probleem)wijken, evenementen, personen, objecten en diensten. De kern van de samenwerking bestaat uit de stichting RTR-NL, particuliere beveiligingsbedrijven en de politie. In verschil-

12 E-mailcontact en via: www.cityoflondon.police.uk/advice-and-support/countering-terrorism/Pages/project-argus.aspx

13 Zie: http://www.nypdshield.org/public/default.aspx www.nypdshield.org/public/default.aspx

14 Telefonisch interview inlichtingenofficier PET (9 november 2017); zie ook: www.pet.dk/English/The%20Preventive%20Security%20Department/~/media/Forebyggende%20Afdeling/AFS_publikationer/2014/Safetyagainsttheterrorthreatpdf.ashx

lende steden werkt men ook samen met andere partijen, zoals de gemeente, brandweer en de organisatoren van evenementen zoals de Vierdaagse in Nijmegen (zie verder in hoofdstuk 5). RTR-NL werkt specifiek met particuliere beveiligingsorganisaties samen voor het uitlezen van de camera's en het opvolgen van alarmeringssystemen. De politie houdt in alle gevallen de regie over het cameratoezicht. Deze vorm van PPS is preventief bedoeld, gericht op het voorkomen van een mogelijke aanslag, al kunnen camerabeelden mogelijk ook gebruikt worden voor opsporing nadat een aanslag heeft plaatsgevonden.[15]

Wat leert dit ons?

In onze brede zoektocht naar voorbeelden van samenwerking tussen publieke en private partijen kwamen we in binnen- en buitenland 24 praktijkvoorbeelden tegen (zie bijlage 2 voor een overzicht). Deze brede inventarisatie leverde veelal voorbeelden op uit het Verenigd Koninkrijk en de Verenigde Staten, gezien de lange traditie van deze landen van PPS in het veiligheidsdomein. Hierboven hebben we vier projecten beschreven die veelbelovend leken, maar toch zijn afgevallen omdat de PPS beperkt van aard blijkt. Het gaat veelal om kennis en informatieverstrekking vanuit de overheid aan private partijen (bijvoorbeeld door middel van een training) of om camerabewaking door publieke en private partijen samen. Het was opvallend lastig om bruikbare cases van PPS te vinden, waarbij publieke en private actoren daadwerkelijk samenwerken ten behoeve van de bewaking en beveiliging van 'soft targets'. Dit is des te opmerkelijker gelet op de politieke, economische en maatschappelijke urgentie van diffuse (terroristische) dreiging en de gewenste aanpak daarvan. De volgende drie hoofdstukken bevatten niettemin cases waarbinnen van verregaande PPS gericht op het bewaken en beveiligen van 'soft targets' sprake is.

15 Telefonisch interview directeur RTR-NL (4 oktober 2017); zie ook: http://rtr-nl.nl/index.php

4 Johan Cruijff ArenA

4.1 Introductie

Dit hoofdstuk gaat over de publiek-private samenwerking bij het bewaken en beveiligen van het buitengebied van de Johan Cruijff ArenA tijdens concerten. In paragraaf 4.2 geven we een beschrijving van PPS rondom de Johan Cruijff ArenA als 'soft target'. Vervolgens bespreken we in paragraaf 4.3 het verloop van deze PPS. We gaan hierbij in op de tevredenheid van respondenten met het verloop van hun samenwerking en op de concrete uitkomsten van hun samenwerking. Paragraaf 4.4 tot en met 4.7 gaan over onze vooraf opgestelde succesfactoren van PPS: de organisatie en dynamiek van het netwerk; culturele kenmerken; verdeling van taken en verantwoordelijkheden binnen en sturing van het netwerk; connectie tussen de overheid en het netwerk. Paragraaf 4.8 bevat tot slot een overzicht van succesfactoren en verbeterpunten die bijdragen of afdoen aan de weerbaarheid van het netwerk.

4.2 PPS rondom een 'soft target'

In Amsterdam Zuidoost werken de Johan Cruijff ArenA, de politie-eenheid Amsterdam, eventorganisatoren (zoals MOJO Concerts) en een particuliere beveiligingsorganisatie (voornamelijk evenementenbeveiliger The Security Company, afgekort TSC) sinds 2016 in de openbare ruimte rond de Johan Cruijff ArenA samen om de veiligheid van bezoekers aan concerten en evenementen in de ArenA te waarborgen. De samenwerking in het buitengebied van de ArenA borduurt voort op de reeds lange samenwerking tussen deze partijen binnen de Johan Cruijff ArenA. De partijen hebben expliciet aandacht voor de diffuse dreiging met betrekking tot (terroristische) aanslagen. Deze vorm van samenwerking vindt alleen plaats bij de organisatie van concerten en andere evenementen, niet tijdens voetbalwedstrijden. Jaarlijks vinden er veel grootschalige concerten en evenementen plaats in de ArenA, waar rond de 55.000 bezoekers in kunnen. Het gaat dan bijvoorbeeld om Toppers in Concert, optredens van Rihanna, Beyonce, U2 en de Rolling Stones, het Amsterdam Music Festival (AMF) en, tot en met 2017, het dance-event Sensation White.

De samenwerking bestaat allereerst uit onderlinge afstemming tussen de partijen in de voorbereiding van een evenement of concert. Op de dag van het evenement/concert zelf werken de partijen samen in de private commandokamer van de Johan Cruijff ArenA. Daar komen meldingen binnen van serviceteams (koppels van particuliere beveiligers en servicemedewerkers van de ArenA) en van zogenaamde 'event profilers' (ongeüniformeerde beveiligers), die in een perimeter om het stadion (het 'buitengebied' van de Johan Cruijff ArenA) patrouilleren. De meldingen gaan over verdachte situaties of afwijkend gedrag van personen. In de commandokamer wordt vervolgens in gezamenlijkheid besloten over de opvolging van deze meldingen.

Het 'buitengebied' direct rond het Johan Cruijff ArenA-stadion is een openbaar en voor iedereen toegankelijk terrein waar bezoekers, maar ook anderen (winkelend publiek, forensen) zich begeven voorafgaand aan evenementen die in de ArenA plaatsvinden. Om de samenwerking op openbaar terrein mogelijk te maken, wordt het buitengebied enkele uren voor en tijdens concerten en andere festiviteiten als evenemententerrein aangemerkt. Anders dan bij andere stadions heeft de ArenA geen perimeter rond het stadion waar de eerste bezoekerscontrole plaatsvindt. Een respondent binnen de ArenA stelt: *"Dat is ook wel wat we een beetje missen. Dat is waar in Parijs die eerste bomgordels zijn tegengehouden."* Bezoekerscontroles vinden plaats bij de ingangen die direct tot de ArenA leiden.

Het buitengebied van de ArenA kan als 'soft target' worden aangemerkt. Er komen immers grote groepen mensen samen in een openbare ruimte die moeilijk volledig te bewaken en te beveiligen is. Jaarlijks komen er voor concerten en evenementen 3,5 miljoen bezoekers die niet alleen naar de ArenA gaan, maar ook naar de Ziggo Dome en AFAS Live die binnen hetzelfde gebied zijn gesitueerd. Daarnaast grenzen er een

winkelgebied met megastores en een bioscoop aan de ArenA en maken 65.000 reizigers dagelijks gebruik van het trein- en metrostation Amsterdam-Bijlmer dat schuin tegenover het stadion ligt. Opgeteld komen er volgens schattingen van de politie jaarlijks rond de 6 tot 16 miljoen bezoekers het buitengebied van de ArenA binnen.

Ondanks dat private partijen rondom de ArenA actief zijn, blijft de politie in dit buitengebied primair verantwoordelijk voor de handhaving van de openbare orde en veiligheid. Het betreft immers een openbaar toegankelijk plein met toegangsstraten. Daarentegen is de verantwoordelijkheid voor de openbare orde en veiligheid binnen de ArenA zelf primair in handen van de Johan Cruijff ArenA en eventorganisaties die beide gebruik maken van private beveiligers. Het stadion is in iets beperktere mate dan het buitengebied een 'soft target', omdat er sprake is van een semipubliek domein waar een privaat toegangsregime geldt: om binnen te komen, heb je een kaartje nodig en er kan gevisiteerd worden. Daarmee is er een ring van bewaken en beveiligen gecreëerd.

4.3 Verloop en opbrengsten van de PPS

In deze paragraaf bespreken we in hoeverre respondenten tevreden zijn over het verloop van de samenwerking en in hoeverre de PPS in de praktijk waardevol is gebleken voor het voorkomen van terroristische dreigingen en aanslagen. Omdat het niet eenvoudig is om dergelijke uitkomsten te meten – zeker niet als het om het *voorkomen* van incidenten gaat – vallen we terug op de percepties van respondenten.

Wisselende tevredenheid over PPS

Respondenten zijn tevreden over de operationele samenwerking in de commandokamer van de Johan Cruijff ArenA. Er is daar volgens hen daadwerkelijk sprake van PPS. Op de dag van het evenement of concert komen alle informatiestromen in de commandokamer samen. Een vertegenwoordiger van elk van de publieke en private partijen is daar aanwezig. Respondenten zijn vooral te spreken over de samenwerking tussen de private partijen enerzijds en de politie anderzijds. De politie[16] is positief over de extra informatie waarover zij door de private ogen en oren in het buitengebied beschikken. De private partijen zijn positief over de opvolging van de meldingen door de politie en de terugkoppeling die zij op de ontvangen meldingen geven. Een servicemedewerker die in het buitengebied werkt, vertelt:

> *"Er kwamen mensen naar ons toe: 'die gast daar, die zat voor de Pathé en is een drugsdealer'. Toen hebben we daar een melding van gemaakt. De commandokamer staat in contact met de politie, zo konden ze via cameratoezicht die drugsdealer oppakken toen hij langs mij liep."*

Respondenten zijn minder tevreden over de samenwerking tussen 'event profilers' van TSC en de politie. MOJO Concerts huurt via TSC al langere tijd 'event profilers' in die getraind zijn in het herkennen van afwijkend gedrag met het oog op de diffuse dreiging. Deze 'event profilers' begeven zich ongeüniformeerd in de openbare ruimte. Hun inzet zorgt daarbij voor spanningen tussen de publieke en private partijen. Een respondent binnen MOJO Concerts:

> *"Eigenlijk is dat een bijzonder frustrerende reis geweest om dat voor elkaar te krijgen. Wij willen als organisatie onze verantwoordelijkheid nemen, maar dit wordt niet met open armen ontvangen aan de publieke kant. De publiek-private samenwerking is rondom deze 'spotters' [synoniem voor 'profilers'] heel erg lastig gebleken."*

De politie is terughoudend bij de samenwerking, omdat voor hen onvoldoende duidelijk is waar 'event profilers' op letten en hoe zij met de door hen verzamelde informatie omgaan. Een respondent binnen de politie vertelt: *"Het levert ons niks op, alleen maar ongemak. We krijgen alleen maar meldingen waarvan we niet weten hoe we dat moeten*

16 Dit betreft de geïnterviewde respondent binnen de politie. Waar in het vervolg wordt gesproken op organisatieniveau (de politie, de Johan Cruijff ArenA), bedoelen we de respondent binnen deze organisaties.

duiden en hoe we daarop moeten inzetten." MOJO Concerts en TSC stellen daartegenover dat 'event profilers' zich niet bezig houden met opsporing, maar enkel met het signaleren en bij de politie rapporteren van verdacht gedrag. 'Event profilers' kunnen hun meldingen echter onvoldoende bij de politie kwijt.

Voorts blijkt de wetgeving een barrière op te werpen voor de inzet van 'event profilers'. In de huidige wetgeving op particuliere beveiliging kunnen alleen persoonsbeveiligers en winkelsurveillanten ontheffing krijgen van de uniformplicht,[17] maar politie-eenheden blijken landelijk verschillend om te gaan met de invulling van deze regeling. Een respondent van MOJO Concerts stelt:

> *"Het is afhankelijk van hoe een politie-eenheid ermee omgaat. In Rotterdam Ahoy wordt die samenwerking bijvoorbeeld enorm opgezocht. Daar zetten we bijvoorbeeld een bomhond in en de politie zegt 'mooi'. Die pakken die samenwerking op. In het Arenagebied is dat nog wel eens lastig. In Amsterdam zijn ze strenger op de regels."*

Desondanks hebben de politie en de private partijen betrokken bij de PPS in het buitengebied van de Johan Cruijff ArenA gezocht naar een oplossing om de inzet van 'event profilers' mogelijk te maken. Er is sprake van een gedoogconstructie: TSC kan nu ontheffing van de uniformplicht aanvragen voor 'event profilers'. Ook zijn de partijen op het moment van schrijven aan het verkennen of het mogelijk is een convenant op te stellen, dat afspraken over de inzet van 'event profilers' formaliseert. Alle respondenten juichen dat toe.

Beperkte informatiedeling in de voorbereidingsfase

Partijen delen informatie met elkaar in de voorbereiding van en tijdens een evenement/concert. In de voorbereiding van een evenement blijkt deze informatiedeling beperkt. Men deelt vooral informatie over bezoekersprofielen en daaraan gerelateerde risico's. Over de aard van de diffuse dreiging wordt weinig of niet gesproken. Illustrerend is de opmerking van een respondent binnen de politie dat terrorisme een zaak van de overheid is en dat het dus de taak van de politie is om informatie te verzamelen en niet zozeer om informatie met private partijen te delen. Respondenten binnen de ArenA beamen dit: zij vertellen dat de politie weinig informatie over dreigingen aan hen doorgeeft, maar dat dit ook niet per se noodzakelijk is. Tot nog toe is er volgens hen geen sprake geweest van een concrete dreiging bij een van de concerten van MOJO in de Johan Cruijff ArenA.

Tegelijk klinken er binnen MOJO Concerts en TSC andere geluiden. Zij vinden dat publieke partijen, in het bijzonder de NCTV, de gemeente Amsterdam en de politie, te weinig informatie met hen delen over de diffuse dreiging om adequaat maatregelen te kunnen nemen. Iemand binnen TSC: "*Wij snappen dat we niet alle informatie hoeven te hebben, maar we hebben wel behoefte aan een kapstok waar we onze gemitigeerde maatregelen aan kunnen ophangen.*" Deze respondenten zouden graag meer informatie en ondersteuning ontvangen om beter af te kunnen wegen welke maatregelen passend zijn met het oog op diffuse dreigingen.

Veel informatiedeling tijdens evenementen/concerten

Anders dan tijdens de voorbereidingsfase vindt er tijdens evenementen en concerten wel veel informatiedeling tussen de publieke en private partijen plaats. Zoals we al hebben geschetst, komen meldingen van de serviceteams en 'event profilers' in de commandokamer binnen en worden deze meldingen (indien relevant) met elkaar gedeeld. Dergelijke meldingen hebben voornamelijk betrekking op operationele informatie, zoals bezoekersstromen, verdachte of vervelende personen en onbeheerde tassen. Respondenten zijn tevreden over de informatiedeling tussen de serviceteams en de politie: meldingen worden opgevolgd en er vindt terugkoppeling plaats aan de

17 Zie voor meer informatie: www.justis.nl/producten/particuliere-beveiliging-en-recherche/opleidingseisen/index.aspx

melder. Vanwege de hierboven beschreven ontevredenheid over de samenwerking tussen politie en private, ongeüniformeerde 'event profilers' zal het niet verbazen dat de informatiedeling tussen hen momenteel stroef verloopt. Al met al heeft de inzet van beveiligers en servicemedewerkers geleid tot meer meldingen. Dit leidt soms tot een 'information overload' met als gevolg dat er niet altijd actie wordt ondernomen. Zo kwamen er bijvoorbeeld meldingen binnen van illegale kaarthandel, terwijl de inzet van de politie te beperkt is om dergelijke zaken aan te pakken. Er moeten in zo'n geval prioriteiten worden gesteld.

Concrete uitkomsten PPS

De inzet van geüniformeerde beveiligers en servicemedewerkers heeft bijgedragen aan meer 'ogen en oren' voor de politie in het openbare gebied rondom de ArenA. Daardoor worden er meer verdachte personen of situaties opgemerkt. Een respondent van MOJO Concerts vertelt: "*We hebben niet iemand aangehouden, maar wel een aantal zaken gezien die we anders minder zagen. Een tas die ergens werd achtergelaten; dat zie je nu sneller.*" Bovendien is de reactiesnelheid verhoogd door de samenwerking in de commandokamer. Een servicemedewerker vertelt:

> *"Met de Toppers had ik een situatie dat ik iemand aansprak met een hele rits kogels om zijn nek. Ik sprak hem aan en hij deed net alsof hij niet Nederlands was. Dus toen heb ik de ArenA contactpersonen in de commandokamer ingeschakeld. En 30 seconden later zag ik dat hij door een politieagent werd aangehouden. Dat vind ik heel erg boeiend, dat het zo snel gaat."*

De PPS leidt er ook toe dat de politie zich kan richten op de zaken die er voor hen toe doen. Voorheen werd de politie vaak naar de weg gevraagd; zoiets wordt nu ondervangen door servicemedewerkers die buiten staan. De politie is tevreden over deze extra 'ogen en oren', omdat zij voor ontlasting zorgen en de politie meer focus kan aanbrengen in haar werk. Van haar kant is de ArenA tevreden over de toename van gastvrijheid richting het publiek: serviceverlening en de weg wijzen, dat kunnen private partijen beter doen volgens hen. Tegelijk ziet TSC, als private beveiligingsorganisatie, liever samenwerking met de politie dan met servicemedewerkers van de ArenA in het buitengebied van het stadion: "*Het samenwerken met de politie is goed. Het samenwerken met de servicemedewerkers hoeft van mij niet.*" De gemiddelde servicemedewerker is niet opgeleid tot beveiliger; zijn of haar enige meerwaarde is kennis van het gebied. Daarom zijn respondenten bij TSC en bij MOJO Concerts van mening dat de inzet van servicemedewerkers niet direct bijdraagt aan het voorkomen van aanslagen.

Vooral de politie en private beveiligers letten bewust op afwijkend gedrag dat met een diffuse dreiging, zoals een aanslag, te maken kan hebben. TSC benadrukt daarbij het belang van 'event profilers': *"De beveiligingsmethodiek rondom 'predictive profiling' is op dit moment één van de weinige methodieken die afwijkend gedrag zou kunnen detecteren."* Doordat particuliere beveiligers mensen proactief aanspreken, halen ze hen uit de anonimiteit. Dat schrikt wellicht af om over te gaan tot het plegen van een aanslag. Ook stelt de aanwezigheid van particuliere beveiliging bezoekers gerust:

> *"De 50.000 die wel voor het feestje komen, geef je het gevoel dat je als ArenA je best hebt gedaan om stressgebieden weg te nemen. Je merkt wel een omslag bij het publiek; in het verleden kregen we nog weleens een klacht als je gefouilleerd werd, nu krijgen we een klacht als je niet gefouilleerd wordt."*

Respondenten geven aan dat de daadwerkelijke bijdrage van beveiligers en politie aan het voorkomen van aanslagen lastig vast te stellen is. Ook wijzen zowel respondenten binnen de ArenA als van TSC erop, dat het gaat om een geheel van zichtbare en onzichtbare maatregelen die een bijdrage leveren – deze maatregelen rijken verder dan alleen PPS.

Wat leert dit ons?

PPS rondom de Johan Cruijff ArenA vindt plaats in de voorbereiding van evenementen en in de commandokamer van het stadion als er een concert of ander (niet-voetbalgerelateerd) evenement plaatsvindt. Over de samenwerking en informatie-uitwisseling 'in the heat of the moment' zijn respondenten unaniem tevreden. Ook heeft de politie dankzij de PPS meer 'ogen en oren' ter beschikking, waardoor er meer zaken worden opgemerkt. Wel klinken er binnen de ArenA, MOJO Concerts en TSC geluiden dat publieke organisaties, zoals de politie en de NCTV, vooraf aan evenementen best meer informatie over diffuse dreigingen zou kunnen delen, zodat zij als private organisaties hier hun maatregelen beter op af zouden kunnen stemmen. Verder blijkt de inzet van ongeüniformeerde private 'event profilers' een heikel punt. Volgens TSC zijn zij bij uitstek geschikt om afwijkend gedrag te herkennen, terwijl de politie liever niet met hen samenwerkt vanwege een ontbrekende wettelijke basis onder het optreden van deze 'event profilers' en onduidelijkheid over wat zij doen, c.q. welke informatie zij verzamelen. Verder zien TSC en MOJO Concerts weinig meerwaarde in de samenwerking tussen hun eigen private beveiligers en de servicemedewerkers van de ArenA, omdat de laatste groep niet getraind is in bewaken en beveiligen. De ArenA vindt deze medewerkers echter wel belangrijk vanwege hun publieksvriendelijkheid en serviceverlening richting bezoekers.

4.4 Organisatie en dynamiek

In deze paragraaf bespreken we hoe de organisatie en de dynamiek van de PPS eruit ziet. We beschrijven welke partijen bij de samenwerking betrokken zijn, de aanleiding en het doel van de samenwerking, hoe de samenwerking is vormgegeven en tot slot, de mate van contact tussen de betrokken actoren.

Betrokken partijen

De PPS in het buitengebied van de Johan Cruijff ArenA vindt zowel op beleids- als op uitvoerend niveau plaats. De betrokken private partijen zijn de Johan Cruijff ArenA, eventorganisatoren, zoals MOJO Concerts (wij beperken ons hier tot de samenwerking met MOJO Concerts) en de particuliere beveiligingsorganisatie The Security Company (TSC). De betrokken publieke partijen zijn de politie Amsterdam-Zuidoost en, meer op afstand, de gemeente Amsterdam (in het bijzonder de dienst Toezicht & Handhaving, afdeling openbare orde en veiligheid en stadsdeel Amsterdam-Zuidoost).

Hoewel de kernpartners, met de geplaatste kanttekeningen, tevreden zijn over de PPS, vinden zij dat de samenwerking breder zou moeten worden getrokken. Zo mist de politie een hechte samenwerking met de gemeente. Vanuit de gemeente worden er vergunningen verleend voor evenementen en vindt er over andere zaken contact met de ArenA plaats. Maar operationeel is de gemeente niet, of erg op afstand, betrokken bij de veiligheid rondom het stadion. Daarnaast is de rol van de handhavers van de gemeente die zich ook in het buitengebied van de Arena bevinden onvoldoende duidelijk. Behalve de politie hebben de andere (private) partijen geen contacten met deze medewerkers. Tot slot is er behoefte aan meer samenwerking tussen de ArenA en de andere eventlocaties in het gebied, zoals AFAS Live en Ziggo Dome.

Aanleiding voor en doelstelling van de samenwerking

De directe aanleiding voor de huidige vorm van PPS was het thema van de Toppers in Concert in 2017: 'Wild West Thuis Best' (dit concert werd overigens niet door MOJO Concerts, maar door een andere eventorganisatie georganiseerd). De wens tot PPS bestond al langer, maar de urgentie ontstond door bezorgdheid dat bovengenoemd thema ertoe zou bijdragen dat bezoekers nepwapens gingen meenemen. Serviceteams bestaande uit een particuliere beveiliger en een servicemedewerker van de ArenA werden in het buitengebied van de ArenA ingezet om bezoekers te wijzen op het verbod

op nepwapens. Soortgelijke PPS-constructies zijn in het vervolg ook ingezet tijdens concerten en evenementen georganiseerd door andere eventorganisaties, zoals MOJO Concerts.

Hoewel het tegengaan van terrorisme niet de primaire aanleiding was voor de PPS, maakt dat intussen wel een onderdeel uit van de samenwerking. Het doel van de PPS is tweeledig. Ten eerste gaat het om het signaleren van afwijkend gedrag of verdachte situaties (specifiek ook met het oog op terrorisme). Een servicemedewerker verwoordt het als volgt: "*extra 'ogen en oren' in het gebied. Private beveiliging en serviceverlening zijn een soort eerstelijnsdefensie. Mocht er iets gebeuren dan kunnen we dat gelijk doorgeven aan de controlekamer*". Ten tweede heeft de PPS tot doel een extra service te verlenen aan het publiek. Door de zichtbare aanwezigheid van particuliere beveiligers en servicemedewerkers in de openbare ruimte moeten bezoekers zich veilig en welkom voelen. Daarnaast worden bezoekers proactief geïnformeerd over attributen die het stadion niet in mogen, zoals tassen groter dan A4 (MOJO Concerts hanteert deze specifieke regel om oponthoud bij fouillering te voorkomen). Door bezoekers tijdig te informeren, wordt teleurstelling bij de ingangscontrole zoveel mogelijk voorkomen.

Vormgeving van de samenwerking

Onder de PPS rondom de ArenA ligt geen convenant. De samenwerking is dus niet geborgd en er zijn geen formele afspraken gemaakt over informatiedeling. Wel is de werkwijze omschreven in de veiligheidsplannen die voorafgaand aan een evenement worden opgesteld. Gezien de behoefte van partijen aan een convenant, is men op het moment van schrijven bezig met het verkennen van mogelijkheden om tot een convenant te komen. Dat zo'n convenant tot nu toe niet bestaat is opmerkelijk, omdat de PPS gevoelig ligt. Een respondent van de ArenA zegt:

> *"De wet werkt beperkend. Wat wij nu doen, de samenwerking in het buitengebied mag eigenlijk nog niet. Het wordt nu wel gedoogd door politie en door bijzondere wetten. Wij mogen eigenlijk alleen handelen binnen het stadion."*

Volgens respondenten wordt voor de PPS in de publieke ruimte rondom het stadion 'ruimte' gezocht door van dit buitengebied een evenemententerrein te maken, waar onder regie van de politie private beveiligers hun werkzaamheden kunnen uitvoeren.

Mate van contact

De bij de PPS betrokken partijen hebben zowel in de voorbereiding van als tijdens een evenement/concert contact. Alle voorbereiding die bij een evenement hoort, vindt plaats binnen twee verschillende overlegstructuren. De eerste is het wekelijkse operationeel evenementenoverleg waar de ArenA en de politie om tafel zitten met de gemeente, de brandweer, de GGD, de beheerders van parkeergebouwen, Stadstoezicht en openbaar vervoerders (NS en het GVB). Eventorganisatoren en TSC nemen geen deel aan dit overleg. Tijdens het overleg worden de evenementen die op de planning staan doorgesproken en wordt informatie gedeeld over mogelijke risico's. Daarnaast vinden er per evenement twee tot drie overleggen plaats tussen de ArenA, MOJO Concerts, TSC en de politie. In deze overleggen wordt afstemming gezocht over het op te stellen veiligheidsplan. Respondenten zijn van mening dat er voldoende contact plaatsvindt in de voorbereidingsfase.

Op de dag van het evenement of concert vindt het contact plaats tussen de verschillende partijen in de private commandokamer van de ArenA. Van elke partij neemt een vertegenwoordiger zitting in de commandokamer: onder andere de operationeel politiecommandant, een coördinator Crowd Services van de ArenA, een vertegenwoordiger vanuit MOJO Concerts en een liaison van TSC. De serviceteams (particuliere beveiliger en servicemedewerker ArenA), politie en 'event profilers' op straat hebben geen rechtstreeks contact met elkaar. Al het contact tussen de partijen verloopt via de commando-

kamer. Wel krijgen de serviceteams en 'event profilers' voorafgaand aan hun inzet een gezamenlijke briefing, waarbij de politie aanwezig is. Tijdens de briefing krijgen de aanwezigen informatie over het aantal bezoekers, zaken waar in het bijzonder op gelet moet worden en de werkwijze (verdachte situaties melden aan de commandokamer).

Wat leert dit ons?

Veiligheid (waaronder het letten op verdachte gedragingen die te maken kunnen hebben met terreur) en service zijn twee kernpijlers onder de PPS rondom de ArenA. Deze PPS is niet in een convenant vastgelegd, al wordt hier wel aan gewerkt. Contact tussen de politie, de ArenA, particuliere beveiliging en evenementorganisatoren vindt vooraf ter voorbereiding van een evenement plaats. Tijdens een evenement zitten de partijen in de commandokamer van het stadion. Vertegenwoordigers van de politie, private partijen (ArenA, TSC en MOJO Concerts) werken daar 'real-time' samen bij het aansturen van koppels beveiligers en servicemedewerkers, 'event profilers' en van politiefunctionarissen in het buitengebied rond de ArenA. Hierbij delen zij informatie over verdachte personen en situaties. Een specifiek punt van aandacht dat respondenten naar voren brengen, is dat de samenwerking omvattender zou kunnen, omdat de gemeente Amsterdam, Ziggo Dome en AFAS Live niet nauw zijn betrokken bij de PPS in het buitengebied van de ArenA.

4.5 Culturele kenmerken

In deze paragraaf bespreken we in hoeverre de betrokken actoren normen, waarden en visies delen. Dit doen we aan de hand van de mate van onderling vertrouwen binnen het netwerk en de mate van consensus over de probleemperceptie.

Onderling vertrouwen binnen het netwerk

Respondenten menen dat de verschillende partijen begrip hebben voor elkaars positie, elkaar waarderen en respecteren. Vooral tussen vertegenwoordigers van de politie en de ArenA is er sprake van een vertrouwensrelatie: zij werken al lang met elkaar samen en kennen elkaar goed. Zoals aangestipt, zit er in de relatie tussen TSC, MOJO Concerts en de politie enige spanning vanwege het werk en de positie van de 'event profilers'. Niettemin heerst er volgens respondenten bij de ArenA op zowel tactisch als operationeel niveau een gevoel van gemeenschappelijkheid: 'we doen het met z'n allen'.

Mate van consensus over probleemperceptie binnen de PPS

Zoals opgemerkt is de PPS rondom de ArenA gericht op een combinatie van service en veiligheid. Binnen de PPS verschillen de meningen over hoe de samenwerking het beste in te richten om diffuse dreigingen en andere veiligheidsproblemen het hoofd te bieden. De inzet van geüniformeerde private beveiligers in combinatie met servicemedewerkers is een idee van de politie: "*Mijn ervaring met servicemedewerkers is dat die vriendelijk zijn. Beveiligersmedewerkers kijken toch meer naar de veiligheid. Die combi maakt dat je hospitality en veiligheid combineert*" (respondent politie). De ArenA is hier ook enthousiast over, maar respondenten binnen MOJO Concerts en TSC zien het belang hier minder van in. De inzet van servicemedewerkers heeft volgens hen weinig toegevoegde waarde met het oog op het voorkomen van aanslagen.

Wat leert dit ons?

Binnen de PPS is er sprake van respect en begrip voor elkaars positie. Tussen sommige partijen (politie en ArenA) is er sprake van een vertrouwensband. Tegelijk bestaan er binnen de PPS meningsverschillen over de nut en noodzaak van zowel 'event profilers' en servicemedewerkers. Vertrouwen in hun kennis en kunde wordt niet door iedereen gedeeld.

4.6 Verdeling van verantwoordelijkheden en sturing

In deze paragraaf bespreken we hoe de verdeling van rollen en verantwoordelijkheden en de sturing van het netwerk eruit ziet. Dit doen we door de verdeling van rollen en verantwoordelijkheden tussen publieke en private actoren, de sturing van het netwerk en het verloop van de besluitvorming te bespreken.

Rollen en verantwoordelijkheden

In de openbare ruimte hebben de publieke en private partijen verschillende rollen en verantwoordelijkheden. De politie is verantwoordelijk voor de handhaving van de openbare orde en veiligheid in het buitengebied van de ArenA. In hun optiek werken private beveiligers daar onder hun regie. MOJO Concerts en TSC zien dit anders: zij spreken liever niet over regie van de politie, maar over samenwerking met de politie. De relatie tussen politie en beveiliging wordt aldus als 'meer horizontaal' voorgesteld. Toch beamen deze partijen dat zij in het buitengebied geen bijzondere bevoegdheden hebben en enkel verdachte situaties bij de politie kunnen melden of hen hierover kunnen adviseren. Binnen het stadion is de ArenA als vergunninghouder verantwoordelijk. De ArenA faciliteert de PPS in de commandokamer door deze aan alle partijen beschikbaar te stellen. Servicemedewerkers van de ArenA krijgen de opdracht mee om als gastheer/gastvrouw op te treden – dat wil zeggen: een praatje te maken met mensen en hen de weg te wijzen. Geüniformeerde en ongeüniformeerde beveiligers letten op verdacht gedrag en op verachte situaties.

De rolafbakening tussen de partijen is helder. De politie is hoofverantwoordelijkheid in de openbare ruimte, beveiligers hebben daar formeel geen bevoegdheid om in te grijpen. Dat kunnen zij wel binnen het stadion vanwege de private regels en het bijbehorende toegangsregime die binnen de ArenA gelden. Overtreedt iemand die regels dan kan hij of zij door de beveiligers uit het stadion worden verwijderd. Het is duidelijk dat servicemedewerkers zoiets niet kunnen doen; zij kunnen overlast of en verdachte situatie wel aan de politie of aan een beveiliger melden. Het wringt bij de 'event profilers', omdat een respondent binnen de politie van mening is dat zij ongeoorloofd met opsporing bezig zijn, terwijl MOJO Concerts en TSC erop wijzen dat zij slechts afwijkend gedrag signaleren en dit aan de politie melden, zodat deze vervolgens passend actie kan ondernemen. Tegen deze achtergrond vindt een respondent van de ArenA dat de politie iets meer verantwoordelijkheid aan private partijen mag geven:

> *"De politie kan nog wel iets meer meewerken met de inzet in het buitengebied – dat de private partijen daar meer verantwoordelijkheden krijgen. De politie is erg gericht op het handhaven van wet- en regelgeving en op de bescherming van de eigen taak."*

Sturing en besluitvorming

Er is geen formele trekker binnen de PPS. Informeel is ArenA de trekker van het samenwerkingsverband: zij brengt de partijen bij elkaar en faciliteert onderlinge samenwerking binnen de eigen commandokamer. De ArenA heeft goed contact met de afzonderlijke partijen, maar heeft geen doorzettingsmacht. Dat heeft de politie met betrekking tot het buitengebied wel: zij kan private beveiligers aansturen. Als er besluiten worden genomen, gebeurt dat echter meestal op basis van consensus. Bij onenigheid gaan partijen om de tafel om tot een oplossing te komen, maar de politie heeft het laatste woord als er opgetreden moet worden. Het samenwerkingsverband kan daarom niet als geheel gelijkwaardig worden gedefinieerd. Een respondent binnen de ArenA verwoordt het als volgt: "*Uiteindelijk heeft de politie wel heel veel te bepalen en te zeggen. Als de politie het er niet mee eens is, dan gebeurt het ook niet.*"

Wat leert dit ons?

De rollen en verantwoordelijkheden van partijen zijn helder. In het gebied direct om de ArenA is de politie primair verantwoordelijk voor de openbare orde en veiligheid, zij

het in samenwerking met private beveiligers en servicemedewerkers. Binnen de ArenA zijn beveiligers als eerste voor de veiligheid verantwoordelijk, al is het mogelijk dat de politie ook hier de regie overneemt bij calamiteiten. Hoewel de private partijen het liefst over gelijkwaardige PPS spreken, is de samenwerking niet geheel horizontaal. Weliswaar werkt de PPS op basis van overleg en collegialiteit, toch is het de overheid – in de gedaante van de politie – die een leidinggevende rol op zich kan nemen als dat nodig blijkt.

4.7 Connectie met de overheid

In deze paragraaf bespreken we of er een connectie is tussen de lokale PPS in het buitengebied van de Johan Cruijff ArenA en de overheid. Dit doen we door te kijken naar de invloed van externe actoren op het samenwerkingsverband. Ook is het de vraag hoe partijen verantwoording afleggen over de resultaten van de PPS.

Invloed van externe publieke actoren

Naast contacten met de gemeente, is er ook contact tussen afzonderlijke bij de PPS betrokken partijen en de NCTV. MOJO Concerts en TSC zijn bijvoorbeeld betrokken bij het alerteringssyteem terrorismebestrijding van de NCTV. Dit houdt in dat partijen informatie krijgen over de terroristische dreiging wanneer dit noodzakelijk wordt geacht. Van hun kant vinden private partijen dat de NCTV (geen onderdeel van de PPS) meer informatie zou mogen delen en zich explicieter zou mogen uitspreken over welke maatregelen eventueel getroffen dienen te worden. Een respondent van MOJO Concerts stelt:

> *"In de huidige situatie doen MOJO en TSC naar eer en geweten eigenlijk maar wat, zonder daar een mening over te krijgen van de NCTV. Voorbeelden van dit soort initiatieven zijn bomhonden, het compleet afsluiten van de backstage, metaaldetectoren en de eerder besproken 'profilers'."*

Publieke verantwoording

Er vindt geen rechtstreekse verantwoording van de PPS naar de gemeente of naar ander overheden plaats. Wel wordt de samenwerking bij concerten van MOJO Concerts (en ook bij de Toppers) door alle partijen zelf geëvalueerd. Uit deze evaluaties is naar voren gekomen dat partijen tevreden zijn over de resultaten van de samenwerking: meer 'ogen en oren', 'welkom gevoel' bij bezoekers. Genoemde verbeterpunten zijn bijvoorbeeld meer duidelijkheid over het type meldingen waar de politie behoefte aan heeft (voorkomen 'information-overload') en een betere bekendheid van particuliere beveiligers en 'event profilers' met de locatie, omdat ze daar niet altijd vast werken.

Wat leert dit ons?

Er bestaat geen duidelijke connectie tussen de overheid en de lokale PPS rondom de Johan Cruijff ArenA. Wel evalueren de partijen de samenwerking intern. Daar zijn enkele succes- en verbeterpunten uit naar voren gekomen. Verder heeft het netwerk contact met de NCTV over eventuele dreigingen, maar respondenten wensen dat de informatieverstrekking over wat zich voordoet en welke maatregelen dan te treffen duidelijker is.

4.8 Succesfactoren en verbeterpunten

Tijdens de interviews hebben respondenten succespunten, maar ook enkele verbeterpunten genoemd die van invloed zijn op de weerbaarheid van hun netwerk. Volgens respondenten zijn de voornaamste succesfactoren: (1) feedbackloops, (2) bereidheid om onenigheid te overbruggen, en (3) een goede balans tussen veiligheid en service. Tezamen kunnen zij de weerbaarheid van de PPS versterken. De genoemde voornaamste verbeterpunten zijn: (1) gebrekkige borging van de PPS, (2) afwezigheid formele trekker, (3) beperkte omvang van PPS, en (4) de positie van ongeüniformeerde

'event profilers'. Tezamen kunnen zij de weerbaarheid van de PPS verzwakken. We zetten alle punten op een rij.

Succesfactor 1: Feedbackloops

De operationele samenwerking in de commandokamer verloopt tijdens concerten goed: meldingen worden door politie, beveiligers en servicemedewerkers doorgegeven, de commandokamer zet deze meldingen uit bij de juiste partijen en de politie volgt meldingen als dat nodig is adequaat op. De melder ontvangt vervolgens een terugkoppeling over de opvolging van de melding. Hierdoor kan worden bijgestuurd op het type meldingen dat relevant is. Bovendien motiveert dit de uitvoerders om meldingen door te blijven geven. Voorts brengen interne evaluaties verbeterpunten aan het licht die de PPS ten goede kunnen komen, zoals betere bekendheid van particuliere beveiligers met de locatie.

Succesfactor 2: Onenigheid overbruggen

Er is een wil om samen te werken en begrip voor elkaars positie. Op de punten waar onenigheid is (bijvoorbeeld over de inzet van 'event profilers') wordt naar oplossingen gezocht om de PPS te continueren of te verbeteren. Hoewel de ArenA de PPS praktisch faciliteert, heeft de politie de meest stevige positie in de besluitvorming.

Succesfactor 3: Veiligheid en service

Naast het vergroten van de veiligheid, draagt de PPS ook bij aan serviceverlening richting het publiek. Hiermee wordt aan de belangen van alle deelnemers tegemoetgekomen. Net zoals de politie wil de ArenA veilige en leuke evenementen organiseren. Daarom moet de focus op veiligheid niet ten koste gaan van de sfeer en gezelligheid die belangrijk is om bezoekers te trekken. Door de inzet van politie, private beveiligers en servicemedewerkers lijkt een optimale balans gevonden.

Verbeterpunt 1: Gebrekkige borging

Alle partijen benoemen de structurele borging van de PPS als verbeterpunt. Momenteel ligt er geen convenant onder de samenwerking waarin afspraken, verantwoordelijkheden, rollen en taken formeel zijn vastgelegd. Op het moment van schrijven wordt er wel aan zo'n convenant gewerkt.

Verbeterpunt 2: Afwezigheid formele trekker

Op het moment van schrijven ontbreekt het aan een formele trekker van het samenwerkingsverband. Partijen zouden graag zien dat de gemeente de rol van trekker van de PPS op zich neemt.

Verbeterpunt 3: Beperkte omvang van PPS

Het derde verbeterpunt dat wordt genoemd, is de beperkte omvang van de PPS. Gelet op het feit dat de ArenA grenst aan andere evenementenlocaties, zoals AFAS Live en Ziggo Dome, is het opmerkelijk dat de samenwerking hiermee gering is. Ook de gemeente Amsterdam (Toezicht & Handhaving) staat op enige afstand van de PPS. Respondenten zouden dus graag een bredere PPS zien.

Verbeterpunt 4: Positie van ongeüniformeerde 'event profilers'

Ze zijn verschillende keren voorbij gekomen: ongeüniformeerde 'event profilers'. MOJO Concerts en TSC zien hen als onmisbaar om verdacht gedrag te detecteren. De politie interpreteert hun werk als een ongeoorloofde manier van opsporing, waarbij het onduidelijk is wat er met de verkregen informatie gebeurt. In het te ontwikkelen convenant moet hun positie eenduidig worden vastgelegd.

5 Nijmeegse Vierdaagse

5.1 Introductie

Dit hoofdstuk gaat over de publiek-private samenwerking bij het bewaken en beveiligen van de Nijmeegse Vierdaagse. In paragraaf 5.2 geven we een beschrijving van PPS rondom de Vierdaagse als 'soft target'. Vervolgens bespreken we in paragraaf 5.3 het verloop van deze PPS, onze afhankelijke variabele. We gaan hierbij in op de tevredenheid van respondenten met het verloop van hun samenwerking en op de concrete uitkomsten van hun samenwerking. Paragraaf 5.4 tot en met 5.7 gaan over onze vooraf opgestelde succesfactoren van PPS: de organisatie en dynamiek van het netwerk; culturele kenmerken; verdeling van taken en verantwoordelijkheden binnen en sturing van het netwerk; connectie tussen de overheid en het netwerk. Paragraaf 5.8 bevat tot slot een overzicht van succesfactoren en verbeterpunten die bijdragen of afdoen aan de weerbaarheid van het netwerk.

5.2 PPS rondom een 'soft target'

De Vierdaagse is een meerdaagse wandelprestatietocht in de omgeving van Nijmegen waar jaarlijks meer dan 42.000 Nederlandse en buitenlandse wandelaars aan deelnemen. Deelnemers lopen vier dagen lang routes van dertig tot vijftig kilometer per dag. Aan de wandeltochten nemen zowel burgers als zesduizend militairen deel. Tegelijk met de wandelvierdaagse vinden de Vierdaagsefeesten plaats, waar muziek, theater, dans en lezingen op het programma staan. De Nijmeegse Vierdaagse was in 2016 het op één na grootste vrij toegankelijke evenement van Nederland.[18] De feesten trekken jaarlijks rond de anderhalf miljoen bezoekers.

De Nijmeegse Vierdaagse is bij uitstek een *soft target*: er komen grote groepen mensen samen in de openbare ruimte die moeilijk volledig te beveiligen is. Voor deelname aan de wandelprestatietocht dient men zich in te schrijven, maar de wandeltochten zelf zijn vanwege hun uitgestrektheid – het gaat om tweehonderd kilometer aan wandelroutes door drie regio's – niet geheel af te sluiten. Het evenement vindt immers plaats op straten en pleinen die veelal publiek eigendom, openbaar toegankelijk en voor algemeen gebruik zijn. Ook de Vierdaagsefeesten zijn voor iedereen vrij toegankelijk.

Om de veiligheid van alle bezoekers en wandelaars te waarborgen, werken publieke en private partijen in de voorbereiding van en tijdens de Vierdaagse nauw samen. We beschrijven de samenwerking die plaatsvindt tussen Stichting DE 4DAAGSE (de organisator van de wandelprestatietocht) en de gemeente Nijmegen, politie, brandweer, veiligheidsregio Gelderland-Zuid en de Geneeskundige Hulpverleningsorganisatie in de Regio (GHOR) bij het organiseren van veiligheid. Daarbij hebben partijen expliciet aandacht voor de diffuse dreiging met betrekking tot (terroristische) aanslagen.

Vanwege praktische redenen van tijd en een anders te grote omvang van respondenten hebben we ons tot de samenwerking rondom de wandelprestatietocht beperkt. De samenwerking met het Ministerie van Defensie in het bewaken en beveiligen van militairen die aan de Vierdaagse deelnemen, valt daarom buiten de scope van ons onderzoek. Dit geldt eveneens voor de samenwerking tussen publieke partijen en de organisator van de Vierdaagsefeesten, Stichting Vierdaagsefeesten. Daar waar relevant voor de PPS omtrent de wandelprestatietocht, zal de samenwerking met de organisator van de Vierdaagsefeesten wel aan bod komen.

5.3 Verloop en opbrengsten van de PPS

In deze paragraaf bespreken we in hoeverre respondenten tevreden zijn over het verloop van de samenwerking en in hoeverre de PPS in de praktijk waardevol is gebleken in het

18 https://www.clcvecta.nl/ledenportal/kennis-onderzoek/top100-evenementen-monitor-2017 (9 juli 2018)

voorkomen van terroristische dreigingen en aanslagen. Omdat het niet eenvoudig is om dergelijke uitkomsten te meten – zeker niet als het om het *voorkomen* van incidenten gaat – vallen we terug op de percepties van respondenten.

Tevredenheid over verloop PPS

Alle geïnterviewde respondenten lijken zeer tevreden te zijn over het verloop van de PPS; er is volgens hen voldoende draagvlak voor de samenwerking. Meerdere respondenten stellen dat doordat private partijen steeds meer taken, zoals toezicht, handhaving en verkeersregeling, hebben opgepakt, er tijdens de Nijmeegse Vierdaagse relatief weinig politie-inzet nodig is. Volgens een respondent van de politie zijn er gemiddeld rond de honderd agenten actief. Dit bespaart veel kosten voor de overheid. Bovendien maakt de PPS het überhaupt mogelijk dat het evenement doorgang kan vinden. Een respondent van Stichting DE 4DAAGSE noemt dan ook als belangrijke uitkomst van de samenwerking:

> *"Het feit dat wij, als private organisatie, dankzij deze samenwerking het aandurven anno 2018 een dergelijk grootschalig evenement te organiseren. Ik denk dat het grootste risico dat wij als samenleving lopen, is dat wij ten onder gaan aan een te groot wordende subjectieve veiligheidsbeleving. Dat mensen te bang worden gemaakt om nog naar buiten te treden bij dit soort grote evenementen."*

Tevredenheid over informatiedeling

Respondenten geven aan dat er informatie wordt gedeeld om de veiligheid van de Vierdaagse te waarborgen. Een centraal doel van de informatiedeling is het komen tot een advies voor de vergunningsverlening, waarbij alle veiligheidsaspecten worden besproken die van belang kunnen zijn. Partijen bespreken het door de Stichting DE 4DAAGSE opgestelde veiligheidsplan en maken afspraken over de inrichting van de openbare ruimte, de route van de wandeltochten en mogelijke vluchtroutes. Een respondent van Stichting DE 4DAAGSE zegt:

> *"Er zijn in samenspraak met de politie binnen het veiligheidsoverleg analyses gemaakt van te verwachten dingen die in een Vierdaagseweek zouden kunnen gebeuren. Op basis van deze analyses zijn passende afspraken gemaakt over hoe te handelen. Deze zijn te vinden in het draaiboek en hierop worden de verschillende vrijwilligers getraind."*

Het delen van informatie ligt wel gevoelig vanwege juridische beperkingen. Een respondent binnen de politie vertelt:

> *"Wij delen geen operationele informatie, maar we delen wel algemene beelden waar we rekening mee moeten houden."*

Respondenten binnen de politie en de gemeente erkennen dat de gedeelde informatie hierdoor selectief is. Desondanks zijn alle respondenten van mening dat er voldoende informatie wordt gedeeld om hun werk naar behoren te kunnen uitvoeren. Dat geldt ook voor de informatiedeling van de private partij (Stichting DE 4DAAGSE) naar de publieke partijen. Respondenten van de gemeente en de politie geloven niet dat de Stichting belangrijke informatie voor hen achterhoudt.

Concrete uitkomsten

Respondenten zijn van mening dat de PPS ertoe heeft bijgedragen dat deelnemende partijen beter zijn toegerust om te reageren op een mogelijke aanslag en om de gevolgen van een aanslag te beperken. Een respondent binnen de politie stelt:

> *"Het voorkomen van [een aanslag] zou ik niet durven te beweren, maar we prepareren ons er beter op en we zijn beter in staat om op een aanslag te reageren door de samenwerking."*

Een onderdeel van de organisatie van de beveiliging van grote evenementen is het doornemen van scenario's, en het vaststellen met welke maatregelen de risico's van deze scenario's gemitigeerd kunnen worden. Een belangrijke opbrengst van de PPS die respondenten noemen, is dat hun samenwerking ertoe leidt dat deze scenario's en bijbehorende maatregelen tegen diffuse dreiging daadwerkelijk gezamenlijk worden voorbe-

reid. Hierbij denken de partijen hun taken en verantwoordelijkheden per scenario uit. Een respondent bij de politie geeft de volgende illustratie:

> *"De scenario's worden op verschillende faseringen toegepast. Je hebt bijvoorbeeld het scenario dat we worden geïnformeerd over een vrachtwagen die richting Nijmegen rijdt die wel eens op de stad zou kunnen inrijden. Dan wordt het ANPR[19] geactiveerd op de wegen naar Nijmegen en worden er roadblocks neergezet. Maar als je een scenario hebt dat er per direct een vrachtwagen op het publiek inrijdt, dan wordt ernaar gehandeld en wordt de DSI[20] opgeroepen."*

Dankzij deze scenario's ontstaat er een handelingsperspectief: men weet wat in een bepaalde situatie moet gebeuren en met wie moet worden samengewerkt. Een respondent binnen de gemeente geeft aan:

> *"De laatste jaren hebben we ons geprepareerd op dat we sneller dingen, zoals roadblocks, kunnen neerzetten. Op het moment dat er een specifieke dreiging is, hebben we nu een handelingsperspectief zodat we niet alles stil hoeven te leggen".*

Wat leert dit ons?

De respondenten die deelnemen aan de PPS met betrekking tot het organiseren van veiligheid tijdens de Nijmeegse Vierdaagse zijn positief over hun samenwerking. In de praktijk bestaat hun samenwerking uit informatie-uitwisseling die bijdraagt aan het veiligheidsplan, de vergunningverlening en scenario's en handelingsperspectieven in geval van calamiteiten. Dankzij de PPS kan het evenement daadwerkelijk plaatsvinden. Ook zorgt de PPS ervoor dat kosten voor de overheid binnen de perken blijven, omdat de private partij (Stichting DE 4DAAGSE) steeds meer verantwoordelijkheid toebedeeld krijgen.

5.4 Organisatie en dynamiek

In deze paragraaf bespreken we hoe de organisatie en de dynamiek van de PPS eruit ziet. We beschrijven welke partijen bij de samenwerking betrokken zijn, de aanleiding en het doel van de samenwerking, hoe de samenwerking is vormgegeven en tot slot, de mate van contact tussen de betrokken actoren.

Betrokken partijen

Bij het organiseren van veiligheid tijdens de wandelvierdaagse wordt zowel op beleids- als op uitvoerend niveau samengewerkt. De samenwerking vindt plaats op strategisch, tactisch en operationeel niveau. Hier richten we ons met name op de samenwerking op tactisch niveau, omdat de samenwerking tussen publieke en private partijen daar het meest tot uiting komt. Op sommige punten komen de strategische, tactische en operationele niveaus samen. Daar waar relevant zullen we de samenwerking op strategisch en operationeel niveau dan ook kort aanstippen.

De publieke kernpartijen binnen de PPS gericht op veiligheid zijn de gemeente Nijmegen en de politie-eenheid Oost-Nederland. De private kernpartij is de privaatrechtelijke Stichting DE 4DAAGSE. Daarnaast zijn de volgende partijen nauw betrokken bij de samenwerking: Brandweer Gelderland-Zuid, de GHOR, het veiligheidsbureau Gelderland-Zuid (publieke partijen) en Stichting Vierdaagsefeesten (private partij). Volgens alle respondenten zijn hiermee de belangrijkste actoren betrokken bij de PPS. Ook vinden zij dat de juiste personen aan tafel zitten. Deze personen hebben voldoende draagvlak binnen hun eigen organisaties en zijn gemandateerd om besluiten te nemen.

19 ANPR staat voor: Automatic Number Plate Recognition

20 DSI staat voor Dienst Speciale Interventies. De DSI bestaat uit speciale eenheden van de politie en Defensie en kan bijvoorbeeld als arrestatieteam worden ingezet in (mogelijk) gewelddadige situaties.

Aanleiding voor en doelstelling van de samenwerking

Meer samenwerking tussen publieke en private partijen in het organiseren van de Nijmeegse Vierdaagse ontstond rond het jaar 2000. In heel Nederland, en zo ook in Nijmegen, kwam er rond die tijd meer aandacht voor meer 'integraal' en 'multidisciplinair' samenwerken binnen het veiligheidsdomein. Het belang van een multidisciplinaire benadering vanuit gemeente, politie, brandweer, de GHOR, Stichting DE 4DAAGSE en anderen stond in het vormgeven van de Nijmeegse PPS voorop. De samenwerking heeft nader vorm gekregen na de afgelasting van de Vierdaagse in 2006. In dat jaar kon de Vierdaagse geen doorgang vinden door aanhoudende medische problemen wegens hitte; er overleed zelfs een aantal wandelaars. Dit incident heeft geleid tot een professionaliseringslag bij alle partijen om tot duidelijkere afspraken te komen over de invulling van de PPS. Concreet is er sprake van een 'verzakelijking', waarbij er meer afspraken formeel worden vastgelegd en private partijen meer verantwoordelijkheid krijgen. We komen hier later nog op terug.

Het doel van de PPS is om de veiligheid van het evenement te waarborgen. In de afgelopen jaren is daarbij in toenemende mate het voorkomen en bestrijden van terroristische aanslagen op de agenda komen te staan. Andere onderwerpen zijn bijvoorbeeld de gevolgen van extreme weersomstandigheden of het uitbreken van een epidemie.

Vormgeving van de samenwerking

Aan de PPS ligt een raamovereenkomst ten grondslag die is getekend door de gemeente Nijmegen, het Ministerie van Defensie[21] en Stichting DE 4DAAGSE. Met de andere bij de PPS betrokken partijen is geen convenant getekend. In de raamovereenkomst zijn met betrekking tot openbare orde en veiligheid de volgende afspraken vastgelegd voor de jaren 2018 tot 2022:

- Het is de verantwoordelijkheid van de gemeente en Stichting DE 4DAAGSE om de veiligheid van de wandelaars optimaal te waarborgen.
- Stichting DE 4DAAGSE neemt deel aan het gezamenlijke veiligheidsoverleg.
- Stichting DE 4DAAGSE handhaaft de vergunningsvoorwaarden.
- Stichting DE 4DAAGSE maakt een mobiliteitsplan.
- De organisatie van de Nijmeegse Vierdaagse wordt jaarlijks geëvalueerd.
- Er vindt afstemming plaat tussen Stichting DE 4DAAGSE en Stichting Vierdaagsefeesten.

In de overeenkomst zijn geen afspraken vastgelegd over informatiedeling. Ook buiten de overeenkomst zijn geen formele afspraken gemaakt over informatiedeling tussen de betrokken publieke en private partijen. Informatiedeling gebeurt op informele basis en binnen de kaders van de Wet Politiegegevens (WPG). Op de vraag of formele afspraken over informatiedeling nodig zijn, antwoordt een respondent binnen Stichting DE 4DAAGSE:

> *"Afspraken maken doe je niet met papier, afspraken maken doe je met mensen. Je werkt samen omdat je elkaar vertrouwt, omdat je elkaars verantwoordelijkheden kent en omdat je begrip hebt voor deze verantwoordelijkheden."*

Aanvullende afspraken over informatiedeling zijn ook volgens de overige respondenten niet noodzakelijk.

Mate van contact

De inhoud en vorm van de samenwerking verschilt wanneer er wel of geen sprake is van een concrete dreiging. We bespreken eerst de elementen van PPS op tactisch niveau

21 Het Ministerie van Defensie is nauw betrokken bij de organisatie van de Vierdaagse vanwege de militairen die aan de wandelprestatietocht deelnemen. Dit onderzoek beperkt zich echter tot de burgers die aan de tochten deelnemen. Over de rol van het Ministerie van Defensie wordt daarom niet verder uitgeweid.

in het geval er géén sprake is van een concrete dreiging. Vervolgens gaan we in op de inhoud en vorm van de PPS bij een concrete dreiging.

Tijdens een 'normale' situatie (als er geen sprake is van specifieke omstandigheden) vindt er in de periode van februari tot september een maandelijks veiligheidsoverleg plaats.[22] Dit overleg wordt voorgezeten door de gemeente Nijmegen. Aan deze overleggen nemen de volgende partijen en personen deel:

- Gemeente Nijmegen: beleidsambtenaren van de afdelingen Openbare Orde en Veiligheid, Mobiliteit en Economische Zaken.
- Politie: agenten betrokken bij crisis- en conflictbeheersing (CCB), staf grootschalig en bijzonder optreden (SGBO) en de teamchef van Nijmegen-Noord.
- Stichting DE 4DAAGSE: bestuursleden belast met veiligheid.
- Brandweer: adviseur evenementen en calamiteitenroutes.
- GHOR: adviseur evenementen en calamiteitenroutes.
- Veiligheidsbureau: coördinator advies.

De gemeente vervult in deze overleggen meerdere rollen: zij is zowel voorzitter, vergunningsverlener als samenwerkingspartner binnen de PPS.

Naast het maandelijkse veiligheidsoverleg, hebben betrokken partijen ook bilaterale contacten. Er is vooral veel bilateraal contact tussen de gemeente en Stichting DE 4DAAGSE en tussen de politie en de Stichting, bijvoorbeeld over mobiliteitsvraagstukken, zoals verkeersstromen. Deze overleggen nemen toe met het naderen van de Vierdaagse.

Drie keer per jaar vindt er een intergemeentelijk overleg plaats over veiligheid en gezondheid onder leiding van de veiligheidsregio Gelderland-Zuid. Dit is een overleg tussen alle gemeenten waar de routes van de wandelvierdaagse doorheen loopt. Naast vertegenwoordigers van deze gemeenten, nemen dezelfde partijen (politie, brandweer, GHOR en veiligheidsbureau) en grotendeels dezelfde personen deel aan deze overleggen als bij de reguliere, maandelijkse veiligheidsoverleggen.

Tijdens de Nijmeegse Vierdaagse zelf is er een dagelijks veiligheidsoverleg over de wandeltochten.[23] Ook hieraan nemen dezelfde partijen en personen deel als aan de veiligheidsoverleggen voorafgaand aan de Vierdaagse. Tijdens de dagelijkse overleggen komen urgente zaken aan de orde. Hierover schetst een respondent van de gemeente Nijmegen het volgende beeld:

> *"Op het gebied van veiligheid gaan de overleggen over hoe het weer is, of er geen bacterie is uitgebroken, hoe het zit met het vuurwerk 's avonds, of we nog tegen knelpunten aanlopen qua mobiliteit, of er incidenten zijn en hoe het gaat met de wandelaars. Deze overleggen zijn heel operationeel. Er wordt afgestemd wat er speelt en welke maatregelen genomen moeten worden."*

Indien er sprake is van een concrete dreiging, komen hoofdzakelijk de publieke partijen in stelling. Dan wordt de Vierdaagse 'een driehoeks-zaak' – dat wil zeggen: de burgemeester van Nijmegen, de hoofdofficier van justitie en de districtschef van Gelderland-Zuid nemen alle beslissingen op het gebied van openbare orde en veiligheid. Private partijen, zoals Stichting DE 4DAAGSE, vervullen alleen een adviseursfunctie, denken mee over maatregelen en nemen, waar nodig, zelf de benodigde maatregelen.

22 Een soortgelijk veiligheidsoverleg is in het leven geroepen voor de Vierdaagsefeesten. Daarbij zitten dezelfde partijen om tafel, met uitzondering van Stichting DE 4DAAGSE, die vervangen wordt door Stichting Vierdaagsefeesten

23 Een soortgelijke constructie bestaat ook voor de Vierdaagsefeesten

Wat leert dit ons?

De PPS tijdens de Vierdaagse wandeltochten is geprofessionaliseerd nadat er in 2006 doden waren te betreuren vanwege aanhoudende hitte. Deze PPS bestaat allereerst uit voorbereidende veiligheidsoverleggen tussen de gemeente Nijmegen, de politie, Stichting DE 4DAAGSE, de brandweer, de GHOR en het veiligheidsbureau. Tijdens de Vierdaagse zelf komen dezelfde partijen en personen samen om (mogelijke) dreigingen en incidenten in 'real-time' te bespreken en maatregelen af te stemmen. De samenwerking tussen de gemeente, het Ministerie van Defensie en Stichting DE 4DAAGSE is formeel vastgelegd in een raamovereenkomst.

5.5 Culturele kenmerken

In deze paragraaf bespreken we in hoeverre de betrokken actoren normen, waarden en visies delen. Dit doen we aan de hand van de mate van onderling vertrouwen binnen het netwerk en de mate van consensus over de probleemperceptie.

Onderling vertrouwen binnen het netwerk

Volgens de respondenten is het vertrouwen tussen de partijen groot. Dit is volgens hen in de eerste plaats te danken aan de langdurige samenwerking in veelal dezelfde constellatie en met dezelfde personen. Het onderlinge vertrouwen heeft zich dus door de jaren heen kunnen opbouwen. Een respondent binnen de gemeente Nijmegen vertelt:

> *"Als je helemaal opnieuw zou moeten beginnen met de Vierdaagse lukt het niet. Het vergt heel veel overleg, afstemming, vertrouwen, zoeken naar oplossingen en niet alleen op je strepen gaan staan [..] We hebben hier nu al decennia ervaring mee. Dit zou je niet zomaar in een andere stad kunnen doen. We hoeven sommige dingen niet te formaliseren omdat we weten 'dit zijn de 'drills'. In Nederland geloven we in formele plannen, maar hier hebben we er niet zoveel. Het gaat hier meer om kennen en gekend worden."*

In de tweede plaats dragen de vele (informele) contacten tussen de partijen – ook buiten het organiseren van veiligheid om – bij aan het onderlinge vertrouwen. Mensen kennen elkaar persoonlijk. Hier wordt door de burgemeester bewust in geïnvesteerd. Zo organiseert hij jaarlijks voorafgaand aan de Vierdaagse een diner voor de betrokkenen. Ook tijdens de Vierdaagse blijkt er veel ruimte voor informeel contact: "*Het is informeel ook gewoon gezellig tussen de partijen.*" Wel zijn respondenten zich bewust van het risico dat de samenwerking te informeel wordt en te veel uitgaat van onderling vertrouwen, waardoor zaken onvoldoende worden vastgelegd of aangekaart. Het gevolg hiervan kan zijn dat men te weinig kritisch is op de kwaliteit van elkaars bijdrage. Dit probleem wordt ondervangen door een scherpe, jaarlijkse evaluatie van de Vierdaagse (zie hieronder meer).

Tot slot stellen alle respondenten dat de zitting van voormalige politiefunctionarissen en militairen binnen Stichting DE 4DAAGSE bijdraagt aan het vertrouwen tussen de partijen. De oudgedienden spreken immers dezelfde taal en begrijpen de organisatiestructuren en werkwijzen van de publieke partijen goed. Een respondent binnen de politie zegt: "*We hebben maar een half woord nodig om te begrijpen wat we bedoelen en wat we willen.*" Zijn observatie geldt overigens niet voor Stichting Vierdaagsefeesten. Vooral het vertrouwen tussen Stichting DE 4DAAGSE en Stichting Vierdaagsefeesten wordt door enkele respondenten binnen de politie en de gemeente als onvoldoende getypeerd. Dat is volgens hen onder andere te wijten aan de verschillen in het type mensen dat er werkt, het type evenement dat zij organiseren en het verschillende publiek dat zij dienen.

Mate van consensus over probleemperceptie binnen de PPS

Respondenten geven aan dat alle partijen de urgentie van de aanpak van een diffuse dreiging delen. Wel blijken er binnen de PPS verschillen van mening te bestaan over de benodigde aanpak. Een respondent binnen de gemeente: "*Er zit wel spanning tussen*

wat de een veilig vindt en de ander niet". De diffuse dreiging leidt er bijvoorbeeld toe dat sommige partijen, zoals de politie en Stichting DE 4DAAGSE, meer veiligheidsmaatregelen willen inzetten dan nu het geval is. Onze respondent binnen de gemeente is het hier niet altijd mee eens, omdat maatregelen ook binnen proporties moeten worden gehouden, wil de Nijmeegse Vierdaagse een open en gezellig evenement blijven.

Naar buiten toe presenteren de partijen een gedeeld beeld van hun gezamenlijke aanpak. Een respondent van Stichting DE 4DAAGSE:

> *"Wanneer er aan de verschillende partijen afzonderlijk van elkaar vragen worden gesteld, bijvoorbeeld omtrent terroristische dreigingen, zal geen enkele partij een ander antwoord geven."*

Deze aanpak bestaat uit terughoudendheid bij het nemen van aanvullende maatregelen, zolang er geen sprake is van een concrete (terroristische) dreiging.

Wat leert dit ons?

Deelnemers aan de PPS rondom de Nijmeegse Vierdaagse delen grotendeels dezelfde normen, waarden en visies door de langdurige samenwerking, informele contacten en de zitting van voormalige politiefunctionarissen en militairen binnen Stichting DE 4DAAGSE. Hierdoor spreken publieke en private partijen dezelfde taal. Wel bestaan er soms meningsverschillen over de te nemen maatregelen in het kader van een diffuse dreiging. Desondanks scharen alle partijen zich uiteindelijk achter de lijn die de gemeente naar buiten toe communiceert: zolang er geen sprake is van een concrete dreiging worden er geen aanvullende maatregelen genomen.

5.6 Verdeling van verantwoordelijkheden en sturing

In deze paragraaf bespreken we hoe de verdeling van rollen en verantwoordelijkheden en de sturing van het netwerk eruit ziet. Dit doen we door de verdeling van rollen en verantwoordelijkheden tussen publieke en private actoren, de sturing van het netwerk en het verloop van de besluitvorming te bespreken.

Rollen en verantwoordelijkheden

Stichting DE 4DAAGSE, de private organisator van de wandelprestatietocht tijdens de Nijmeegse Vierdaagse, is hoofdverantwoordelijk voor het treffen van maatregelen om de veiligheid en gezondheid te waarborgen van de wandelaars binnen gebieden die als evenemententerrein zijn aangemerkt. Binnen de grenzen van de gemeente Nijmegen betreffen die gebieden de start en finish van de wandeltochten. De stichting heeft een team dat zich toelegt op toezicht en handhaving dat samen met een particuliere beveiligingsorganisatie over de evenemententerreinen surveilleert. Ook buiten deze specifieke gebieden draagt de hoofdorganisator verantwoordelijkheid voor het welzijn van de wandelaars. Zo heeft de stichting een eigen medisch team en zet zij, onder regie van de politie, verkeersregelaars in langs de route. Tot slot heeft de stichting een eigen meldkamer waar alle meldingen van vrijwilligers en posten langs de weg binnenkomen en camera's worden uitgekeken.

Respondenten van de publieke partijen (politie, gemeente) merken op dat Stichting DE 4DAAGSE zich door de jaren heen steeds meer bezig is gaan houden met de veiligheid van de bezoekers. Daardoor zijn volgens hen 'publiek' en 'privaat' naar elkaar toegegroeid. Dit heeft er onder andere toe geleid dat er minder politie wordt ingezet voor toezicht, handhaving en verkeersregeling. Desondanks geven de publieke partijen aan dat waar het gaat om de diffuse dreiging het primaat bij de overheid blijft liggen. De publieke partijen zijn immers wettelijk verantwoordelijk voor het handhaven van de openbare orde en veiligheid in de openbare ruimte. Bovendien worden de rollen van

de publieke partijen groter wanneer er sprake is van een incident. Bij GRIP-situaties[24] (rampen, crises en calamiteiten) zijn primair de publieke partijen aan zet en vervullen vertegenwoordigers van Stichting DE 4DAAGSE enkel een liaisonrol tussen het gemeentelijk beleidsteam en de eigen organisatie.

Formeel is de PPS dus niet gelijkwaardig. De gemeente heeft een leidende en beslissende rol: zij is de vergunningverlener van de Nijmeegse Vierdaagse en neemt samen met politie en justitie besluiten in geval van nood (het zogeheten 'driehoeksoverleg'). Toch zorgt het onderlinge vertrouwen en de langdurige samenwerking ervoor dat respondenten hun samenwerking wel als gelijkwaardig beleven en typeren.

Heldere definitie van rollen en verantwoordelijkheden

Respondenten binnen de gemeente en de politie geven aan dat de rollen en verantwoordelijkheden in toenemende mate helder worden gedefinieerd en belegd. Dit blijkt uit het optreden van een 'verzakelijking', waarbij men een scherper onderscheid maakt tussen de rol en verantwoordelijkheden van de opdrachtgever (gemeente) enerzijds en de opdrachtnemer (Stichting DE 4DAAGSE) anderzijds. In het verleden namen de gemeente en politie meer verantwoordelijkheden op zich bij het organiseren van de Vierdaagse, maar die worden in toenemende mate privaat belegd. Een eerder genoemd voorbeeld hiervan is de afwikkeling van verkeersstromen. Voorheen nam de politie deze taak op zich, nu huurt Stichting DE 4DAAGSE private verkeersregelaars in. Volgens een respondent binnen de gemeente worden deze taken overgedragen met een aanpak die zich laat omschrijven als *"honing en azijn"*. Daarmee bedoelt hij dat er ruimte en begrip is om te groeien in het privaat oppakken van dergelijke taken (honing); tegelijkertijd heeft de gemeente van het opstellen van een beter mobiliteitsplan een harde voorwaarde gemaakt voor de vergunningsverlening (azijn). Deze verzakelijking draagt bij aan de wens van de gemeente om afspraken meer te formaliseren. Een respondent binnen de gemeente:

24 GRIP staat voor Gecoördineerde Regionale Incidentbestrijdingsprocedure. Het is een werkwijze waardoor de verschillende hulpverleningsdiensten (brandweer, politie, geneeskundige zorg en bevolkingszorg) gecoördineerd met elkaar kunnen samenwerken bij incident- en rampbestrijding

"We moeten kunnen aantonen wat we hebben gedaan. We moeten de verantwoordelijkheden beter beleggen en minder afgaan op vertrouwen en persoonlijke klik. We kunnen nog wel een professionaliseringsslag maken. Dan kunnen we beter duidelijk maken wat we hebben gedaan als er een incident zou zijn."

Andere partijen hebben deze wens overigens niet geuit.

Sturing en besluitvorming

De voorzitter van de 'normale' (niet-crisis) veiligheidsoverleggen voorafgaand en tijdens de Vierdaagse is een ambtenaar van de afdeling Openbare Orde en Veiligheid van de gemeente Nijmegen. Deze ambtenaar heeft zowel een trekkende als verbindende rol. Zij roept de partijen bijeen, faciliteert de overleggen en zorgt ervoor dat alle inhoudelijke punten ter tafel komen. Hierbij geeft zij aan:

"Ik heb een procesrol. Ik neem geen besluit, maar zorg ervoor dat we integraal een besluit nemen. De burgemeester beslist over de vergunningsverlening. Ik faciliteer dat de juiste punten die nodig zijn voor de beslissing, waarin alle partijen worden meegenomen, aanwezig zijn."

De trekker van de PPS heeft dus geen doorzettingsmacht, maar stimuleert en adviseert. Haar legitimiteit wordt door geen van de respondenten in twijfel getrokken.

Alle besluiten over veiligheid worden in principe gezamenlijk genomen in het maandelijkse veiligheidsoverleg. Als men geen overeenstemming bereikt, hakt het college van burgemeester en wethouders de knoop door.

Wat leert dit ons?

De afgelopen jaren heeft Stichting DE 4DAAGSE in toenemende mate veiligheidstaken op zich genomen. Deze ontwikkeling heeft er onder andere toe geleid dat minder politiecapaciteit (bijvoorbeeld verkeersregelaars) ingezet hoeft te worden tijdens de Vierdaagse. Dat is een ontwikkeling die de publieke partijen toejuichen. Respondenten spreken van een verzakelijking die ingezet is, waarbij de formele rollen tussen opdrachtgever (de gemeente) en opdrachtnemer (Stichting DE 4DAAGSE) duidelijker uit elkaar zijn getrokken en schriftelijk zijn vastgelegd. Een deel van de samenwerking, zoals het contact tussen publieke en private partijen tijdens een incident, is echter nog gestoeld op informele afspraken. Bij de gemeente leeft daarom de wens meer afspraken te formaliseren en vast te leggen. De gemeente kan deze rol ook op zich nemen, aangezien zij een sturende rol inneemt in het samenwerkingsverband en het besluit neemt over de te verlenen vergunning voor de Vierdaagse. PPS binnen de context van de Nijmeegse Vierdaagse is dus allerminst volledig horizontaal. Dit komt ook terug in het feit dat de politie, samen met justitie, hoofdverantwoordelijk blijft voor de veiligheid in de publieke ruimte en als zodanig ook het voortouw kan nemen.

5.7 Connectie met de overheid

In deze paragraaf bespreken we of er een connectie is tussen de lokale PPS in Nijmegen en de overheid. Dit doen we door te kijken naar de invloed van externe actoren op het samenwerkingsverband. Ook is het de vraag hoe partijen verantwoording afleggen over de resultaten van de PPS.

Invloed van externe publieke actoren

Vanuit de nationale overheid is er contact tussen de NCTV en de lokale gezagsdriehoek (burgemeester van Nijmegen, districtschef Gelderland-Zuid en hoofofficier van justitie). Dit contact is ontstaan naar aanleiding van een verhoogde terroristische dreiging en de komst van de koning tijdens de honderdste Nijmeegse Vierdaagse in 2016. Het contact met de NCTV heeft volgens respondenten geen invloed op de vormgeving of inhoud van de PPS zelf. Wel zorgt de NCTV ervoor dat het samenwerkingsverband een extra impuls krijgt. Een respondent binnen de politie zegt hierover:

"Wat de NCTV bijdraagt, is dat we met z'n allen weer even iets scherper zijn. De aanwezigheid van de NCTV zorgt ervoor dat je binnen je organisatie geen fouten wilt maken."

Publieke verantwoording

In de raamovereenkomst tussen de gemeente Nijmegen, het Ministerie van Defensie en Stichting DE 4DAAGSE is opgenomen dat alle partijen het verloop van de Vierdaagse jaarlijks evalueren. Respondenten zijn van mening dat leerpunten uit de evaluaties voldoende worden geïmplementeerd. Genoemde leerpunten gaan bijvoorbeeld over de inrichting van het evenemententerrein en de omlegging van een route. De meeste leerpunten hebben betrekking op verbeteringen in *crowd management*: het in goede banen leiden van het publiek.

Wat leert dit ons?

Er is duidelijk een connectie tussen de overheid en de lokale PPS in Nijmegen. In de eerste plaats omdat er contact is tussen de NCTV en het netwerk. In de tweede plaats omdat er in de raamovereenkomst tussen de gemeente, het Ministerie van Defensie en Stichting DE 4DAAGSE is vastgelegd dat het verloop van de Vierdaagse jaarlijks wordt geëvalueerd.

5.8 Succesfactoren en verbeterpunten

Tijdens de interviews hebben respondenten succespunten, maar ook enkele verbeterpunten genoemd die van invloed zijn op de weerbaarheid van hun netwerk. Volgens respondenten zijn de voornaamste succesfactoren: (1) een langdurige, continue samenwerking met een duidelijke feedbackloop; (2) een 'persoonlijke klik' tussen de betrokkenen en (3) een inzet voor het gezamenlijke belang. Tezamen kunnen zij de weerbaarheid van de PPS versterken. De genoemde voornaamste verbeterpunten zijn: (1) de samenwerking tussen de organisaties van de wandelprestatietochten en de feesten, (2) de informaliteit van PPS, en (3) de beperkte politie-inzet. Tezamen kunnen zij de weerbaarheid van de PPS verzwakken. We zetten alle punten op een rij.

Succesfactor 1: Continue samenwerking en feedbackloop

Doordat de Nijmeegse Vierdaagse een jaarlijks terugkerend evenement is, werken de publiek en private actoren al lange tijd, op structurele basis en in grotendeels dezelfde samenstelling met elkaar samen. Een maand na de afronding van de Vierdaagse wordt er geëvalueerd en starten de voorbereidingen voor de volgende editie. Hierdoor is er gedurende het gehele jaar nauw contact tussen alle betrokken partijen en kan de opgedane kennis en ervaring niet wegzakken. Een cyclus van evalueren stimuleert bovendien dat men alert blijft op verbeterpunten.

Succesfactor 2: Een 'persoonlijke klik'

Bij de samenwerking betrokken personen vormen met elkaar een hecht netwerk. Door de jarenlange samenwerking is er een vertrouwensband ontstaan. Het helpt daarbij dat een aantal personen betrokken bij Stichting DE 4DAAGSE in het verleden voor politie of defensie heeft gewerkt en dus de taal van de publieke partijen spreekt. Respondenten omschrijven hun PPS als collegiaal: men weet elkaar te vinden, er is ruimte voor humor en er is sprake van een 'persoonlijke klik'.

Succesfactor 3: Inzet voor een gezamenlijk belang

Respondenten benoemen dat alle partijen met veel professionaliteit en inzet werken aan het organiseren van veiligheid (en daarmee het tegengaan van een diffuse dreiging) tijdens de Vierdaagse. In de optiek van onze respondenten pakt elke partij hierbij zijn rol, wordt er voldoende informatie gedeeld en is er, ondanks de jarenlange samenwerking, nog altijd ruimte voor discussie en een kritische blik.

Verbeterpunt 1: Samenwerking tussen de organisaties van de wandelprestatietocht en de feesten

Het eerste verbeterpunt dat respondenten benoemen, heeft betrekking op de samenwerking tussen Stichting DE 4DAAGSE (de organisator van de wandelprestatietocht) en Stichting Vierdaagsefeesten (de organisator van de Vierdaagsefeesten). Tussen beide partijen vindt jaarlijks afstemming plaats, maar er kan niet gesproken worden van een innige samenwerking. Dit komt volgens respondenten binnen de gemeente en politie door het verschil in de aard van de evenementen en het type mensen dat werkzaam is bij beide organisaties.

Verbeterpunt 2: De informaliteit van PPS

Ondanks dat een 'persoonlijke klik' als grote succesfactor naar voren komt, betreft het derde verbeterpunt de informaliteit van het netwerk. De schaduwzijden van informaliteit binnen een PPS, aldus een respondent binnen de gemeente, is dat de samenwerking door een lange betrokkenheid van mensen te persoonsafhankelijk kan worden en er 'blinde vlekken' kunnen ontstaan.

Verbeterpunt 3: Beperkte politie-inzet

Een respondent van de politie waarschuwt dat een te groot beroep op de eigen verantwoordelijkheid van private partijen risico's met zich meeneemt. Weliswaar kan door hun werk de inzet van politieambtenaren worden teruggebracht tot het minimaal benodigde, maar het is de vraag of er voldoende politiecapaciteit aanwezig blijft in het geval er echt een aanslag plaatsvindt.

6 Diamantkwartier Antwerpen

6.1 Introductie

Dit hoofdstuk gaat over de publiek-private samenwerking bij het bewaken en beveiligen van het Diamantkwartier in Antwerpen. In paragraaf 6.2 beschrijven we kort de PPS en waarom dit kwartier als 'soft target' is aan te merken. Vervolgens bespreken we in paragraaf 6.3 het verloop van deze PPS, onze afhankelijke variabele. We gaan hierbij in op de tevredenheid van respondenten met het verloop van hun samenwerking en op de concrete uitkomsten van hun samenwerking. Paragraaf 6.4 tot en met 6.7 gaan over onze vooraf opgestelde succesfactoren van PPS: de organisatie en dynamiek van het netwerk; culturele kenmerken; verdeling van taken en verantwoordelijkheden binnen en sturing van het netwerk; connectie tussen de overheid en netwerk. Paragraaf 6.8 bevat tot slot een overzicht van succesfactoren en verbeterpunten die bijdragen of afdoen aan de weerbaarheid van het netwerk.

6.2 PPS rondom een 'soft target'

In het Diamantkwartier werken de private stichting Antwerp World Diamond Centre (AWDC) Security Office[25], de Lokale Politie Antwerpen (LPA), in het bijzonder het team DIA-ISRA en het team GOUDI[26], de gemeente Antwerpen, gebouwbeheerders van gebouwen waar diamantairs en diamantbeurzen in zijn gevestigd en particuliere beveiligingsorganisaties (waarvan Securitas de grootste is) samen om het Diamantkwartier te bewaken en beveiligen tegen diffuse dreigingen. De PPS bestaat uit het delen van informatie, het afstemmen van veiligheidsmaatregelen en het gezamenlijk nemen en financieren van deze maatregelen. Het Diamantkwartier in Antwerpen is vanuit terroristisch oogpunt zowel een symbolisch als een economisch doelwit. Respondenten spreken van een "*target rich environment*" gezien de fysieke ligging, de aard van de activiteiten, de personen en bedrijven gevestigd in de wijk en het internationale profiel van de diamantsector. Het Diamantkwartier ligt in het hart van de Joodse wijk, naast het Centraal Station van Antwerpen en is omgeven door winkelcentra, hotels en woningen. Daarnaast staat Antwerpen bekend als het grootste diamantcentrum wereldwijd. In het Diamantkwartier zijn rond de 6.600 personen werkzaam met 72 verschillende nationaliteiten en met verschillende culturele en religieuze achtergronden. De grootste gemeenschappen actief in het Diamantkwartier zijn de Joodse en de Indische gemeenschap.

Het Diamantkwartier bestaat uit een Secure Antwerp Diamond Area (S-ADA) die wordt gevormd door drie straten (de Schupstraat, Hoveniersstraat en Rijfstraat) en enkele straten daaromheen die een buffer vormen rond de 'secure area'. Deze buffer is openbaar publiek terrein. De 37 gebouwen binnen de S-ADA, waarbinnen de 1.600 bedrijven verbonden aan de diamantsector zijn gevestigd, gelden als privaat terrein. De S-ADA zelf is semiopenbaar toegankelijk: voetgangers en fietsers kunnen het gebied vrij betreden, maar voor voertuigen geldt een beperking. Bij de toegangswegen tot de S-ADA staan dan ook beveiligingsslagbomen. Voertuigen mogen alleen het gebied in als zij zijn aangemeld en als bestuurders zijn gescreend door de politie.

De S-ADA en de aanpalende straten (voortaan: het Diamantkwartier) kunnen als 'soft target' worden aangemerkt vanwege het, ondanks de genomen beveiligingsmaatregelen, grotendeels openbare karakter van de wijk: het gebied is niet volledig af te sluiten en/of te beveiligen. Daarnaast is het een plek waar veel mensen samenkomen. Zoals gezegd zijn er duizenden mensen werkzaam en begeeft zich een veelvoud daarvan als klant door het handelscentrum.

25 Het AWDC is de sector- en belangenfederatie van de diamanthandel. Bij de federatie zijn 1.600 bedrijven in de diamantsector aangesloten. Het Security Office van het AWDC houdt zich bezig met het bevorderen van de veiligheid van het Diamantkwartier en de gemeenschappen en diamantairs die daarbinnen actief zijn

26 De afkorting DIA staat voor Diamant en ISRA staat voor Israël vanwege de grote joodse gemeenschap woonachtig in het Diamantkwartier. ISRA- patrouilles staan in voor de bescherming van de Joodse gemeenschap en instellingen (te voet en per auto); DIA- patrouilles staan in voor de beveiliging van het diamantkwartier (te voet en per auto). GOUDI is de rechercheafdeling die verdachte handelingen onderzoekt en misdaad in de diamant- en juwelensector opspoort

6.3 Verloop en opbrengsten van de PPS

In deze paragraaf bespreken we de tevredenheid van de respondenten met het verloop van de PPS en in hoeverre de samenwerking in de praktijk waardevol is gebleken in het voorkomen van terroristische dreigingen en aanslagen. Omdat het niet eenvoudig is om dergelijke uitkomsten te meten – zeker niet als het om het *voorkomen* van incidenten gaat – vallen we terug op de percepties van respondenten.

Tevredenheid over verloop PPS

De gesproken respondenten zijn tevreden over het verloop van de PPS. Hun oordeel is in de eerste plaats te danken aan een wil bij alle partijen om samen te werken en een gedeelde urgentie van het probleem. Iedereen is het erover eens dat er in het Antwerpse Diamantkwartier sprake is van een diffuse (terroristische) dreiging en is bereid om in gezamenlijkheid maatregelen te nemen (en te financieren) die bijdragen aan het bewaken en beveiligen van de wijken. In de tweede plaats benoemen respondenten het onderlinge vertrouwen en respect voor elkaars verantwoordelijkheden en bijdragen. Dit vertrouwen blijkt uit de welwillende onderlinge informatiedeling, al is men kritisch over de wettelijke kaders hieromtrent (zie hieronder voor meer details). In de derde plaats stellen respondenten dat het succes van de PPS te danken is aan een duidelijke trekker in de vorm van één organisatie – het private AWDC-Security Office – en een persoon daarbinnen die de partijen weet te verbinden en draagvlak heeft onder alle betrokkenen. De trekker fungeert als een spil in de informatiedeling tussen de partijen. In de vierde plaats wordt het permanente contact tussen de verschillende partijen als belangrijk aangemerkt: "*de lijnen staan open*", aldus een respondent binnen de gemeente. In de vijfde plaats zorgt de aangebrachte structuur van vaste overlegmomenten voor tevredenheid onder respondenten over de PPS. Tot slot dragen formeel vastgelegde afspraken tussen de gemeente, de politie en het AWDC-Security Office bij aan de legitimiteit van de samenwerking en daarmee aan de tevredenheid over het verloop van de PPS.

Tevredenheid over informatiedeling

Het AWDC-Security Office fungeert als informatiemakelaar tussen alle partijen. Het AWDC krijgt informatie binnen van zowel private als publieke partijen, analyseert deze informatie en zet deze vervolgens, al dan niet geanonimiseerd, door aan de partijen waarvoor de informatie relevant is. Een gebouwbeheerder stelt ter illustratie: *"Het AWDC-Security Office krijgt 'inside information' van overheden en diensten waarmee zij in verbinding staan, ook wereldwijd. Zij beslissen wie welke informatie moet weten."* Het AWDC-Security Office informeert gebouwbeheerders bijvoorbeeld over verdachte personen of veiligheidsincidenten in de wijk. Andersom delen de gebouwbeheerders, en andere private partijen, informatie met het AWDC-Security Office over verdachte personen, handelingen of incidenten. Volgens een respondent van het AWDC delen deze partijen gemakkelijker informatie met een private partij als het AWDC dan met een publieke partij als de politie:

> *"De opstap om naar mij te komen is veel kleiner. De barrière van privaat naar publiek is groter. Er kleeft namelijk een negatief effect aan het delen van informatie met publieke instanties; alles wordt door hen officieel geregistreerd. Private partijen hebben er dan geen controle over. Nu komt informatie bij de politie via ons."*

De informatiedeling tussen de private en publieke partijen vindt hoofdzakelijk tussen het AWDC-Security Office en het team DIA-ISRA van de Lokale Politie Antwerpen plaats. Het type informatie dat het AWDC met de politie deelt, betreft: (1) dreigingsbeelden, trends en modus operandi aangaande terrorisme en andere vormen van criminaliteit; (2) geopolitieke ontwikkelingen die mogelijk van invloed zijn op de veiligheid van de wijk; (3) verdachte handelingen of situaties; en (4) camerabeelden als de politie hierom vraagt. De politie deelt op haar beurt ook informatie over het dreigingsbeeld,

trends en modus operandi op het gebied van terrorisme met het AWDC-Security Office. Daarnaast levert de politie informatie aan het AWDC-Security Office over verdachte bedrijven en personen die potentieel een risico vormen voor de diamanthandel en die toegang tot de gebouwen dus beter ontzegd kan worden.

Tussen de politie en particuliere beveiligers vindt, zij het in beperktere mate, eveneens informatie-uitwisseling plaats. Particuliere beveiligers geven meldingen van verdachte situaties of handelingen aan de politie door. De politie levert vervolgens feedback op de ontvangen meldingen door aan te geven of de melding nuttig was en geeft, indien mogelijk, informatie over de opvolging van de melding. Een respondent binnen Securitas geeft het volgende voorbeeld:

> *"Een mobiele bewaker zag iemand met een antenne lopen en maakte daar melding van bij de politie. De politie checkt dit. Het bleek te gaan om een ontsnapte roofvogel uit de dierentuin die werd gezocht. Vanuit de politie wordt dan teruggekoppeld dat het gecheckt is en dat het dus onschuldig was. Maar er wordt ook feedback gegeven dat de bewaker het sneller had kunnen melden, toen de persoon nog in het gebied was. Dan hadden ze het geval sneller kunnen onderzoeken. Nu waren ze er drie uur aan kwijt."*

De geïnterviewde respondenten zijn tevreden over de kwaliteit van informatiedeling binnen de PPS, maar blijken kritisch over juridische obstakels. Respondenten binnen de politie en het AWDC-Security Office stellen dat het delen van informatie operationeel werkbaar is. Dit is volgens hen in de eerste plaats te danken aan het aanstellen van 'Single Points Of Contact' (SPOC's) binnen de organisaties waartussen een vertrouwensrelatie bestaat. In de tweede plaats hebben de partijen een pragmatische manier gevonden om de vertrouwelijkheid van informatie aan te duiden. Om te voorkomen dat gevoelige informatie bij de verkeerde partijen terechtkomt, werken de politie en het AWDC-Security Office met een zogenaamd 'traffic light protocol' (TLP): groen heeft het laagste vertrouwelijkheidsgehalte, rood betekent dat informatie enkel gedeeld kan worden nadat daar toestemming voor is verleend. Tot slot verloopt het delen van informatie volgens een respondent binnen de politie soepel, omdat de korpschef achter de PPS staat en de partijen een formeel 'veiligheidsprotocol' hebben ondertekend (meer details over dit protocol volgen hieronder). Dit protocol geeft de nodige legitimiteit aan de samenwerking.

Ondanks de tevredenheid over de kwaliteit van de informatiedeling, geven respondenten van de politie en het AWDC-Security Office aan dat de huidige wetgeving beperkend en op sommige punten zelfs ambigu is. Een respondent binnen het AWDC-Security Office stelt: *"De wetgeving is totaal onvoldoende om op een correcte manier met elkaar samen te werken. Veel regels, wat het praktisch onmogelijk maakt."* Zowel het AWDC-Security Office als de politie hebben behoefte aan de instelling van een beroepsgeheim voor private partijen, met bijbehorende screening en sancties bij de schending van de geheimhoudingsplicht.

Concrete uitkomsten PPS

Respondenten zijn over het algemeen tevreden over de uitkomsten van de PPS. Voor de politie heeft de samenwerking geleid tot beter zicht op wat er speelt in de wijk; zij krijgt meer meldingen binnen sinds het ontstaan van de PPS in vergelijking met de situatie daarvoor. Vooral in de opsporing van criminele activiteiten heeft de samenwerking zijn meerwaarde bewezen. Inmiddels heeft de PPS geleid tot de opsporing van misdrijven en de arrestatie van verdachten. Op de vraag in hoeverre de samenwerking bijdraagt aan het voorkomen van aanslagen is echter lastig antwoord te geven. Diverse respondenten zijn van mening dat de PPS een bijdrage levert aan het voorkomen van aanslagen, maar kunnen dit niet uitdrukken in concrete resultaten (ofwel omdat deze er niet zijn, ofwel vanwege de vertrouwelijke aard van dergelijke voorbeelden). Een respondent binnen de politie vertelt: "*Ik ga ervan uit dat er een aantal incidenten voorkomen is door alertheid*". De PPS heeft er in ieder geval concreet toe geleid dat er meer veiligheidsmaatregelen zijn genomen die een bijdrage moeten leveren aan het voorkomen van aanslagen. Zo

zijn er beveiligingsslagbomen geplaatst bij de in- en uitgangen van het Diamantkwartier en is het cameranetwerk uitgebreid en uitgerust met 'Automatic NumberPlate Recognition' (ANPR). Daarnaast houden particuliere beveiligers zich op openbaar terrein bezig met de detectie van afwijkend gedrag door middel van methodieken als 'predictive profiling' en 'security questioning'. Tot slot kan onnodige evacuatie van het gebied – en daarmee bedrijfsonderbreking en financieel verlies – worden voorkomen door de inzet van een zogeheten 'sniffer': een mobiele explosievenscanner die verdachte pakketjes of achtergelaten tassen controleert op explosieven.

Wat leert dit ons?

De PPS in het Diamantkwartier in Antwerpen wordt door alle partijen als positief beoordeeld. Zij ervaren een gedeeld gevoel van urgentie: het Diamantkwartier is symbolisch en economisch een aantrekkelijk doelwit voor aanslagen en andere diffuse dreigingen. Tussen alle partijen vindt informatiedeling plaats die operationeel werkbaar is en de samenwerking zelf is goed georganiseerd. Verschillende respondenten vinden echter dat de duidelijkheid van wetgeving over wat 'kan' en 'mag' voor verbetering vatbaar is. Meest concrete resultaten van de PPS zijn meer meldingen bij de politie, het opsporen van criminaliteit en het treffen van zichtbare (en onzichtbare) veiligheidsmaatregelen binnen het Diamantkwartier.

6.4 Organisatie en dynamiek

In deze paragraaf bespreken we hoe de organisatie en de dynamiek van de PPS eruit ziet. We beschrijven welke partijen bij de samenwerking betrokken zijn, de aanleiding en het doel van de samenwerking, hoe de samenwerking is vormgegeven en tot slot, de mate van contact tussen de betrokken actoren.

Betrokken partijen

De PPS binnen het Diamantkwartier vindt zowel op beleids- als op uitvoerend niveau plaats. De betrokken personen zijn werkzaam op strategisch, tactisch of operationeel niveau. Wij beperken ons hier zoveel mogelijk tot de samenwerking op het tactische niveau, omdat dit gezien de onderzoeksvraag de meest relevante informatie oplevert. Daar waar relevant benoemen we ook de samenwerking op strategisch en operationeel niveau. Bij de samenwerking is een groot netwerk aan publieke en private stakeholders betrokken. De private kernspelers binnen de PPS zijn:

- Het Security Office van de private stichting Antwerp World Diamond Centre (AWDC). Het AWDC is de sector- en belangenfederatie van de diamanthandel. Bij de federatie zijn 1.600 bedrijven uit de diamantsector aangesloten. Het Security Office van het AWDC houdt zich bezig met het bevorderen van de veiligheid van het Diamantkwartier en de gemeenschappen en diamantairs die daarbinnen actief zijn.
- Gebouwbeheerders van de 37 gebouwen waar diamantairs en diamantbeurzen in het Diamantkwartier in zijn gevestigd.
- Particuliere beveiligingsorganisaties die door het AWDC en de gebouwbeheerders worden ingehuurd voor de bewaking en beveiliging van de gebouwen in het Diamantkwartier (het gaat hier hoofdzakelijk om beveiligers in dienst van Securitas).

Andere private spelers die meer op de achtergrond van de PPS meespelen, zijn waardentransporteurs, verzekeringsmaatschappijen en de diamantairs actief in de wijk.

De publieke kernspelers binnen de PPS zijn:

- Het team DIA-ISRA van de Lokale Politie Antwerpen (LPA). LPA DIA-ISRA is gevestigd in de 'secure area', in hetzelfde gebouw als de AWDC-Security Office.
- De gemeente Antwerpen, in het bijzonder de burgemeester en de schepen (in Nederland: wethouder) belast met de diamantsector en hun kabinetten.

Andere publieke spelers die meer op de achtergrond van de PPS meespelen, zijn de federale politie, de Veiligheid van de Staat (de burgerlijke inlichtingen- en veiligheidsdienst), de Militaire inlichtingendienst, de Provinciale overheid, het Ministerie van Defensie (onder andere over de inzet van militairen ter bewaking en beveiliging van het Diamantkwartier), de Federale Overheidsdienst Economie en de Federale overheidsdienst Binnenlandse Zaken.

Aanleiding voor de samenwerking

Het eerste zaadje voor meer samenwerking tussen publieke en private partijen om de weerbaarheid tegen een diffuse dreiging in het Diamantkwartier te verhogen, werd reeds geplant in 1981. Toen ontplofte een autobom voor de ingang van de Portugese synagoge in de wijk. De PPS in de huidige vorm bestaat echter pas sinds 2013. Toen ontstond op strategisch niveau bij de burgemeester van Antwerpen, de korpschef van de Lokale Politie Antwerpen en de CEO van het AWDC de behoefte om de PPS op tactisch en operationeel niveau beter vorm te geven. Tot dan toe bestond de samenwerking uit een jaarlijkse bijeenkomst tussen bovengenoemde personen. Redenen waren de steeds voller wordende agenda van de bestuurlijke overleggen, het veranderende dreigingsbeeld en de behoefte van de politie aan meer informatie uit de wijk. De urgentie voor meer samenwerking om aanslagen te voorkomen, werd vervolgens onderstreept door een schietpartij in het Joodse Museum in Brussel in 2014 en door een bomexplosie op de luchthaven Zaventem in 2016.

Doelstelling van de samenwerking

Het doel van de samenwerking is het waarborgen van de fysieke en economische veiligheid van de personen werkzaam en woonachtig in het Diamantkwartier, de diamantsector en de gebouwen in het gebied. De samenwerking richt zich op de volgende veiligheidsthema's: terrorisme, criminaliteit (waaronder fraude en kidnappings), demonstraties en cybercrime. Het voorkomen van aanslagen is een expliciet doel van de PPS. Een respondent van het AWDC-Security Office vertelt:

> *"Wij zetten daar [op het voorkomen van aanslagen, red.] zeer streng op in. De modus operandi worden duidelijk uitgelegd aan de mensen. Als je het proces kent, de dynamieken, de indicatoren, dan verhoogt dat de kans om te detecteren, rapporteren, registreren en analyseren – en dan kijken of er gehandeld moet worden."*

Andere respondenten beamen dat het AWDC-Security Office deze boodschap uitdraagt.

Vormgeving van de samenwerking

De samenwerking tussen de gemeente Antwerpen, de Lokale Politie Antwerpen (LPA) en het Antwerp World Diamond Centre (AWDC) is vastgelegd in twee documenten: het 'Veiligheidsprotocol Antwerpse Diamantsector' en de 'Samenwerkingsovereenkomst 2016-2019 tussen de stad Antwerpen, Antwerp World Diamond Centre en de provincie Antwerpen'. Met de gebouwbeheerders zijn geen formele afspraken gemaakt over de PPS. Een gebouwbeheerder stelt: *"Hier gaat veel op woord, weinig formeel. Als diamanten worden verkocht, wordt dit ook mondeling gedaan. Zonder iets op papier. Dat is hier gewoon de cultuur."* Ook de samenwerking tussen particuliere beveiligers en de politie is niet opgetekend in een convenant. Dit is volgens een respondent binnen Securitas ook niet nodig, omdat de samenwerking plaatsvindt binnen de reeds geldende kaders van de Wet op Particuliere Beveiliging.

In het 'Veiligheidsprotocol Antwerpse Diamantsector' staan de taken en verantwoordelijkheden van de gemeente, het AWDC en de LPA omschreven. Zo meldt het veiligheidsprotocol dat de gemeente periodieke overleggen organiseert op zowel strategisch als tactisch niveau. Het protocol legt verder vast dat een specifiek team van de LPA (de DIA-ISRA) zich bezighoudt met de handhaving van de openbare orde en veiligheid in de Secure Antwerp Diamond Area (S-ADA) en de directe omgeving daarvan middels permanente camerabewaking, patrouilles op het terrein en de afhande-

ling van misdrijven. Het protocol stelt daarnaast dat er periodiek overleg plaatsvindt tussen dit politieteam en het AWDC-Security Office over relevante aangelegenheden, zoals verschillende criminele fenomenen. Tot slot is in het protocol afgesproken dat het AWDC een gespecialiseerd en professioneel Security Office biedt dat fungeert als centraal aanspreekpunt voor alle veiligheidsgerelateerde onderwerpen in het Diamantkwartier. Het AWDC fungeert als een spil tussen enerzijds de gemeente en politie en anderzijds de gemeenschappen werkzaam in het Diamantkwartier. Het protocol regelt ook dat het AWDC een locatie ter beschikking stelt aan de LPA DIA-ISRA en beveiligingsvoorzieningen financiert voor de toegang tot de S-ADA area.

De 'Samenwerkingsovereenkomst 2016-2019' is een overeenkomst tussen de gemeente Antwerpen, het AWDC en de Provinciale overheid. We beperken ons hier tot de opgetekende afspraken tussen de gemeente en het AWDC, omdat de rol van de Provinciale overheid in de samenwerking omtrent het voorkomen van aanslagen beperkt is. De Provinciale overheid speelt daarentegen wel een belangrijke rol tijdens een crisis, voornamelijk in de coördinatie van de hulpdiensten. Omtrent de veiligheid van het Diamantkwartier zijn in de overeenkomst een aantal afspraken opgenomen die hoofdzakelijk betrekking hebben op de financiering van beveiligingsmaatregelen. Zo is opgetekend dat het AWDC de plaatsing van beveiligingsslagbomen financiert die de toegang tot de 'secure area' beperken, terwijl de gemeente Antwerpen de financiële kosten van de bestrating en straatmeubilair voor de plaatsing van deze slagbomen draagt. Ook is in de overeenkomst opgenomen dat de gemeente Antwerpen de investerings- en operationele kosten van het uitgebreide camera- en ANPR netwerk rond de 'secure area' op zich neemt. Het AWDC-Security Office draagt zorg voor de investerings- en operationele kosten van een CCTV-systeem (een gesloten cameracircuit) binnen de 'secure area', dat door de politie in operationeel gebruik is genomen.

Mate van contact

Zoals uit bovenstaande is gebleken, vormt het AWDC-Security Office de spil tussen de verschillende partijen. Zij hebben dan ook veelvuldig bilateraal contact met partijen. Daarnaast zijn er drie overlegfora. Het eerste betreft de overleggen tussen de gemeente, de LPA en het AWDC-Security Office. Het tweede betreft de overleggen tussen het AWDC-Security Office en de gebouwbeheerders. Het derde bestaat uit overleggen tussen het AWDC-Security Office, gebouwbeheerders, LPA DIA-ISRA en Securitas. We bespreken de drie fora hieronder afzonderlijk.

Binnen het eerste forum – Gemeente Antwerpen, Lokale Politie Antwerpen, AWDC-Security Office – vindt op *strategisch niveau* overleg plaats tussen vertegenwoordigers van de Provinciale overheid, de burgemeester, de schepen belast met de diamantensector, de korpschef van de LPA en het AWDC-Security Office. Dit overleg vindt eens per jaar plaats. Partijen delen dan informatie en bespreken de te nemen veiligheidsmaatregelen. Op *tactisch niveau* vindt er overleg plaats tussen het kabinet van de schepen belast met de diamantsector, een veiligheidsadviseur van de burgemeester, een commissaris van de politie (binnen de Nederlandse politie iemand met de rang van hoofdinspecteur) en het AWDC-Security Office. In dit overleg worden de details van de te nemen veiligheidsmaatregelen besproken. Sinds de samenwerkingsovereenkomst van kracht is geworden, is de frequentie van dit overleg gedaald. De partijen komen bijeen wanneer daartoe behoefte is bij een van de betrokken partijen. Bij de overleggen zijn over het algemeen dezelfde personen betrokken. Afhankelijk van de onderwerpen op de agenda kunnen ook andere afdelingen van de gemeente aansluiten.

Binnen het tweede forum – AWDC-Security Office en gebouwbeheerders – organiseert het AWDC-Security Office een maandelijks overleg met de gebouwbeheerders van de 37 gebouwen in het Diamantkwartier. Tijdens deze overleggen wordt gesproken over incidenten, zorgen en trends omtrent de veiligheid van de wijk en de te nemen (of

genomen) veiligheidsmaatregelen. Onderwerpen die worden besproken, zijn bijvoorbeeld de screening van koeriersdiensten en het bewerkstellingen van een uniforme beveiliging van de gebouwen.

Binnen het derde forum vindt eens in de drie maanden overleg plaats tussen het AWDC-Security Office, gebouwbeheerders, LPA DIA-ISRA en Securitas. In dit overleg delen partijen informatie over zorgen, trends en incidenten. Ook geeft de politie tijdens deze overleggen feedback aan Securitas over de gemaakte meldingen door particuliere beveiligers. In hoeverre waren deze nuttig? Aan wat voor type meldingen heeft de politie behoefte?

Naast genoemde drie formele overlegfora, onderhoudt het AWDC-Security Office ook structureel contact met verschillende afdelingen binnen de politie en andere overheidsdiensten. Een respondent binnen het AWDC-Security Office geeft aan dat bilateraal contact met deze partijen de voorkeur geniet, vanwege de verschillende belangen en de beperkingen voor publieke partijen bij het delen van informatie met private partijen. Het AWDC-Security Office overlegt onder andere eens per maand met de commissaris van LPA DIA-ISRA; eens in de vier maanden met de hoofdcommissaris van de directie Operaties en Intel van de LPA en eens in de drie maanden met een contactpersoon binnen de Veiligheid van de Staat.

Tot slot vindt er naast de periodieke overlegmomenten veelvuldig informeel contact tussen de partijen plaats. Vooral tussen het AWDC-Security Office en de LPA DIA-ISRA en het AWDC-Security Office en de gebouwbeheerders vindt dagelijks persoonlijk of via e-mail en telefoon contact plaats. Alle respondenten zijn van mening dat er voldoende contact plaatsvindt tussen de partijen.

Wat leert dit ons?

De PPS in het Diamantkwartier bestaat uit een groot aantal partijen, waarvan Security Office van private stichting Antwerp World Diamond Centre, gebouwbeheerders en Securitas (een privaat beveiligingsbedrijf), de Lokale Politie Antwerpen en de gemeente Antwerpen hoofdrolspelers zijn. Sinds 2013 heeft een professionalisering van deze PPS plaatsgevonden vanwege een veranderd dreigingsbeeld en twee concrete aanslagen in Brussel: op het Joods Museum in 2014 en op luchthaven Zaventem in 2016. Een belangrijke doelstelling van de samenwerking is dan ook het tegengaan van terreur. De PPS is formeel vastgelegd in een veiligheidsprotocol en in een samenwerkingsovereenkomst. Er vindt tussen alle partijen binnen diverse fora geregeld contact plaats. Al met al kunnen we concluderen dat PPS in het Diamantkwartier strak is georganiseerd en gestructureerd.

6.5 Culturele kenmerken

In deze paragraaf bespreken we in hoeverre de betrokken actoren normen, waarden en visies delen. Dit doen we aan de hand van de mate van onderling vertrouwen binnen het netwerk en de mate van consensus over de probleemperceptie.

Onderling vertrouwen binnen het netwerk

Er is volgens respondenten sprake van groot onderling vertrouwen; vooral tussen de politie, het AWDC-Security Office en de gemeente Antwerpen. Deze partijen weten elkaar goed te vinden, komen hun afspraken na, en delen informatie met elkaar. Dat de mate van vertrouwen groot is, is volgens een respondent binnen de politie te danken aan de professionaliteit en discretie van de 'Single Points Of Contact' (SPOC). Dat maakt de samenwerking echter ook persoonsafhankelijkheid en daarmee de vertrouwensrelatie ook kwetsbaar.

Dezelfde respondent bij de politie stelt: "*Het zou niet persoonsafhankelijk mogen zijn, maar zit hier morgen iemand anders dan zou de samenwerking niet zo goed zijn.*"

Mate van consensus over probleemperceptie binnen de PPS

Alle partijen zijn het volgens respondenten met elkaar eens dat PPS noodzakelijk is om de veiligheid van het Diamantkwartier te waarborgen. Zij wijzen daarbij op problemen van criminaliteit, maar ook van terreurdreiging. Respondenten ervaren dat op het onderwerp 'veiligheid' alle partijen elkaar gemakkelijk vinden – het komt ook zelden voor dat iemand niet wil meegaan met de veiligheidswensen van een van de partijen. Er is volgens respondenten sprake van een gevoel van gezamenlijkheid. Een gebouwbeheerder verwoordt dit als volgt:

> *"Het gevoel dat we allemaal voor hetzelfde gaan. Niemand zit hier voor eigen eer en glorie in de samenwerking. Gezamenlijk doel is voorkomen dat er iets gebeurt en dat iedereen die hier komt een veilig gevoel heeft."*

En een respondent binnen de gemeente Antwerpen benadrukt:

> *"Er is wederzijdse bekommernis. De diamantsector is begaan met de eigen veiligheid en wil daarin investeren, maar kan dat niet altijd vanwege beperkingen op het openbaar terrein en de privacywetgeving. Dus moet dat via de overheid gebeuren. Wij zijn geïnteresseerd dat er geen calamiteiten gebeuren. Dat is niet goed voor ons imago en niet voor de sector an sich."*

Bij politieagenten in de operatie was er in het begin wel enige scepsis over de samenwerking met private partijen. Zo was er weerstand bij de agenten tegen het ontvangen van trainingen door het AWDC-Security Office en tegen de samenwerking met particuliere beveiligers. Verschillende respondenten hebben echter de indruk dat politieagenten in toenemende mate de meerwaarde van de samenwerking met private partijen inzien. Een respondent van de politie stelt dat dankzij de meldingen van private beveiligers de politie bijvoorbeeld meer informatie over criminaliteit en verdachte personen tot haar beschikking heeft. Private beveiligers merken ook op dat de samenwerking wordt gewaardeerd, omdat de politie navolging geeft aan hun meldingen; dat motiveert hen om informatie te blijven verschaffen.

Wat leert dit ons?

Binnen de PPS in het Antwerpse Diamantkwartier heerst een hoge mate van vertrouwen en gezamenlijkheid. Dat komt enerzijds door de persoonsgebonden insteek van de samenwerking: er wordt met 'Single Points Of Contact' gewerkt. Anderzijds is er consensus over urgentie van veiligheidsproblemen die moeten worden tegengegaan (criminaliteit, terrorisme), zeker in een wijk die internationaal de aandacht trekt en in een land dat al meerdere aanslagen te verwerken heeft gehad.

6.6 Verdeling van verantwoordelijkheden en sturing

In deze paragraaf bespreken we hoe de verdeling van rollen en verantwoordelijkheden en de sturing van het netwerk eruit ziet. Dit doen we door de verdeling van rollen en verantwoordelijkheden tussen publieke en private actoren, de sturing van het netwerk en het verloop van de besluitvorming te bespreken.

Rollen en verantwoordelijkheden

Het private AWDC-Security Office is de spil binnen de PPS en draagt verantwoordelijkheid voor:

- Het bieden van een centraal aanspreekpunt met betrekking tot veiligheidsvraagstukken voor alle betrokken partijen.
- Het onderhouden van contact en voeling met de diamantsector en communicatie richting die sector.
- Het nemen en financieren van beveiligingsmaatregelen.

- Het vergroten van de 'security awareness' van private partijen door deze partijen te voorzien van trainingen, informatie (bijvoorbeeld middels posters en e-mails) en advies.
- Het informeren van publieke partners over criminele fenomenen.
- Het opstellen en delen van een dreigingsbeeld.
- Het organiseren van jaarlijkse evacuatieoefeningen.

De lokale politie Antwerpen, dienst DIA-ISRA, is verantwoordelijk voor de handhaving van de openbare orde en veiligheid in het Diamantkwartier. Zij houdt zich bezig met camerabewaking op het openbare terrein en patrouilleren door het Diamantkwartier. Ook de gemeente Antwerpen is verantwoordelijk voor het nemen van adequate veiligheidsmaatregelen op openbaar terrein. Zij heeft bijvoorbeeld het cameranetwerk binnen en rond het Diamantkwartier uitgebreid. Verder is de gemeente initiator van de veiligheidsoverleggen tussen de gemeente zelf, het AWDC-Security Office en de politie. Gebouwenbeheerders zijn verantwoordelijk voor het waarborgen van de veiligheid van hun eigen gebouwen, waarbij particuliere beveiligers voor de bewaking en beveiliging daarvan zorgen. Daarbij detecteren particuliere beveiligers afwijkend gedrag in de openbare ruimte en melden dit aan de politie.

Heldere definitie van rollen en verantwoordelijkheden

Alle respondenten zijn van mening dat de rollen en verantwoordelijkheden van de verschillende partijen voldoende helder zijn gedefinieerd. De afbakening van deze rollen en verantwoordelijkheden is deels wettelijk bepaald en deels vastgelegd in het beschreven veiligheidsprotocol en de samenwerkingsovereenkomst tussen de gemeente, de politie en het AWDC. Zo zijn de bevoegdheden van particuliere beveiligers wettelijk bepaald en staan de taken en verantwoordelijkheden van het AWDC-Security Office zwart-op-wit in het veiligheidsprotocol. Ondanks de afbakening van taken en bevoegdheden geven verschillende respondenten aan dat er bij alle partijen bereidheid bestaat om de scheiding tussen publieke en private taken niet al te strak af te bakenen. Een respondent binnen de politie stelt: *"Voor een deel komen wij op hun terrein en voor een deel komen zij op ons terrein. Wij in hun gebouwen, zij op de openbare weg."* Zo heeft de politie toegang tot alle gebouwen als dat nodig is, houden particuliere beveiligers een oogje op het publieke domein van de straat, schakelt de politie beveiligers in bij een verdacht pakketje (de laatste beschikt over een mobiele explosievenscanner) en heeft het AWDC-Security Office beveiligingsmaatregelen zoals beveiligingsslagbomen en de uitbreiding van het cameranetwerk medegefinancierd. De bediening van de slagbomen en het cameranetwerk is wel weer in publieke handen.

Sturing

Het AWDC-Security Office is de trekker van het samenwerkingsverband vanuit de private kant. Volgens een respondent is het noodzakelijk dat het AWDC deze rol op zich neemt, omdat de afstand van diamantairs en gebouwbeheerders tot de publieke partijen anders te groot is. Alle respondenten zijn van mening dat de huidige trekker draagvlak geniet bij alle bij de PPS betrokken partijen. Binnen de gemeente is er ook een persoon aangewezen die de PPS coördineert. De persoon in kwestie initieert overleggen en zorgt voor de benodigde contacten met private partijen.

Besluitvorming

De besluitvorming binnen het netwerk vindt plaats binnen de beschreven overlegfora. In het overleg tussen de gebouwbeheerders, het AWDC-Security Office, Securitas en de politie worden besluiten zoveel mogelijk met consensus genomen. Voorbeelden van zaken waarover wordt gediscussieerd, zijn uniforme toegangscontroles van de verschillende gebouwen en een gezamenlijke werkwijze voor de screening van koeriersdiensten. In het overleg tussen de gemeente, het AWDC-Security Office en de politie worden

besluiten eveneens zoveel mogelijk met consensus genomen. Een respondent binnen de gemeente zegt: *"We debatteren, koppelen terug en koppelen nog eens terug. Dan landen we meestal ergens tussenin"*. Als de partijen er niet uitkomen, wordt een besluit in het bestuurlijk overleg genomen of wordt het op dit niveau informeel opgelost (de burgemeester of schepen belt dan de CEO van het AWDC). De uiteindelijke verantwoordelijkheid voor veiligheidsmaatregelen in het (semi-)publieke domein van het Diamantkwartier ligt bij de burgemeester; hij hakt dan ook de knoop door als dit noodzakelijk is. Volgens een respondent binnen de gemeente komt het echter zelden voor dat partijen over veiligheidsthema's geen overeenstemming bereiken.

Wat leert dit ons?

Binnen de Antwerpse PPS in het Diamantkwartier zijn rollen en verantwoordelijkheden van publieke en private partijen schriftelijk vastgelegd en afgebakend. Dat schept veel helderheid. Desondanks zien we een mix van 'publiek' en 'privaat' als het gaat om de wijze waarop partijen samenwerken en veiligheidsmaatregelen worden gefinancierd. Er is een duidelijke trekker van de PPS in de vorm van het private AWDC-Security Office. PPS vindt voornamelijk via 'horizontale' consensus plaats, maar in laatste instantie is de burgemeester eindverantwoordelijk voor de openbare veiligheid en kan hij desgewenst knopen doorhakken.

6.7 Connectie met de overheid

In deze paragraaf bespreken we of er een connectie is tussen de PPS in het Diamantkwartier en de overheid. Dit doen we door te kijken naar de invloed van externe actoren op het samenwerkingsverband. Ook is het de vraag hoe partijen verantwoording afleggen over de resultaten van de PPS.

Invloed van externe publieke actoren

Zoals al is besproken, onderhoudt het AWDC-Security Office naast contacten met de kernpartijen binnen de PPS, ook contact met een groter netwerk dat voornamelijk bestaat uit publieke stakeholders, waaronder veiligheidsdiensten. Het doel van deze contacten is om informatie en kennis uit te wisselen. Externe publieke partijen hebben qua informatiedeling dus aanzienlijke invloed op de lokale PPS binnen het Antwerpse Diamantkwartier.

Publieke verantwoording

Over de resultaten van de PPS als geheel wordt geen rechtstreekse verantwoording afgelegd aan een publieke partij. Wel leggen de afzonderlijke partijen verantwoording af binnen hun eigen organisaties. Zo leggen de private partijen verantwoording af aan hun raden van bestuur, legt de dienst DIA-ISRA van de Antwerpse politie verantwoording af aan de korpschef en doet het college van burgemeester en schepenen dit aan de gemeenteraad. De gemeenteraad heeft bijvoorbeeld de 'Samenwerkingsovereenkomst 2016-2019' goedgekeurd. Ook kan de gemeenteraad vragen stellen over besluiten die zijn genomen door het college. Zodoende is er indirect wel sprake van publieke verantwoording over de PPS.

Evaluatie

De PPS wordt niet formeel geëvalueerd. Wel worden kritiek en verbeterpunten informeel besproken. Op basis van een dergelijke informele evaluatie hebben de gemeente, het AWDC-Security Office en de politie bijvoorbeeld besloten om de veiligheidsoverleggen niet langer maandelijks te laten plaatsvinden, maar alleen wanneer daar bij een van de partijen behoefte aan is.

Wat leert dit ons?

Er vindt geen formele evaluatie van de PPS binnen het Diamantkwartier plaats. Toch hebben publieke partijen – met aan het hoofd de burgemeester, gecontroleerd door de gemeenteraad – de nodige kijk en invloed op het reilen en zeilen van het samenwerkingsverband. Daarnaast deelt een breder netwerk van publieke partijen, waaronder veiligheidsdiensten, informatie met het private AWDC-Security Office.

6.8 Succesfactoren en verbeterpunten

Tijdens de interviews hebben respondenten succespunten, maar ook enkele verbeterpunten genoemd die van invloed zijn op de weerbaarheid van hun netwerk. Volgens respondenten zijn de voornaamste succesfactoren: (1) de aanwezigheid van een trekker met draagvlak, (2) een gedeelde urgentie en motivatie om samen te werken en (3) organisatie van de PPS. Tezamen kunnen zij de weerbaarheid van de PPS versterken. De genoemde voornaamste verbeterpunten zijn: (1) persoonsafhankelijkheid van de PPS en (2) verruiming van de mogelijkheden voor informatiedeling. Tezamen kunnen zij de weerbaarheid van de PPS verzwakken. We zetten alle punten op een rij.

Succesfactor 1: Trekker

De PPS in het Diamantkwartier laat zich kenmerken door de aanwezigheid van een private trekker – een medewerker van het AWDC-Security Office – die draagvlak geniet onder de bij de PPS betrokken partijen. De trekker onderhoudt contact met alle afzonderlijke partijen, initieert overleggen en verzamelt en deelt informatie.

Succesfactor 2: Gedeelde urgentie en motivatie

De kernpartijen delen de urgentie dat samenwerking nodig is om de weerbaarheid tegen een diffuse dreiging te vergroten. Het onderlinge vertrouwen, een persoonlijke klik tussen de SPOC's, de vele (informele) contactmomenten en de feedback die de politie geeft op de ontvangen meldingen dragen bij aan de motivatie om samen te werken en informatie te blijven delen.

Succesfactor 3: Organisatie van de PPS

Het aanstellen van SPOC's, vaste overlegmomenten en de formeel vastgelegde afspraken tussen de gemeente Antwerpen, de politie en het AWDC-Security Office dragen bij aan een soepel verloop van de PPS. Het feit dat de PPS in een protocol en overeenkomst is vastgelegd, draagt hier ook aan bij.

Verbeterpunt 1: Persoonsafhankelijkheid

Het enthousiasme van respondenten over de trekker van het samenwerkingsverband is tegelijkertijd ook een kwetsbaarheid van de PPS. Het is onvoldoende duidelijk hoe de samenwerking voortgezet zal worden mocht de trekker wegvallen. Persoonsafhankelijke relaties zijn cruciaal.

Verbeterpunt 2: Verruiming mogelijkheden informatiedeling

De huidige wetgeving werkt voor publieke en private partijen beperkend om de nodige informatie te kunnen delen en is op sommige punten ambigu. Er is behoefte aan een verruiming van de wettelijke mogelijkheden om informatie te delen, bijvoorbeeld door het instellen van een beroepsgeheim voor private partijen, met bijbehorende screening en sancties bij schending van het beroepsgeheim.

7 Samenvattende conclusies en reflectie

7.1 Inleiding

Dit rapport gaat over publiek-private samenwerking (PPS) rondom het bewaken van beveiligen van 'soft targets' in tijden van diffuse dreiging. We vertrokken vanuit de volgende hoofdvraag: *welke rol kunnen publieke (overheid) en private (niet-overheid) actoren vervullen binnen samenwerkingsverbanden bij het bewaken en beveiligen van 'soft targets' – en aldus bij het versterken van maatschappelijke weerbaarheid in tijden van diffuse dreiging?* Hieronder geven we puntsgewijs antwoord aan de hand van vier deelvragen. Eerst vatten we samen wat de wetenschappelijke literatuur zegt over 'soft targets', PPS, criteria voor succesvolle samenwerking en maatschappelijke weerbaarheid (deelvraag 1). Daarna geven we een beknopt overzicht van hoe Nederland en andere landen PPS aangaan, gericht op het bewaken en beveiligen van 'soft targets' (deelvraag 2). Voorts bespreken we wat we kunnen leren van de drie onderzochte cases: de Johan Cruijff ArenA, de Nijmeegse Vierdaagse en het Diamantkwartier in Antwerpen (deelvraag 3). Vervolgens reflecteren we op het belang van weerbare private partijen binnen PPS-constructies (deelvraag 4). Tot slot beschrijven we drie varianten van netwerk-PPS die mogelijk zijn voor de toekomst van PPS inzake het bewaken van beveiligen van 'soft targets' in tijden van diffuse dreiging.

7.2 De wetenschappelijke literatuur

Deelvraag 1: *Wat zijn volgens de wetenschappelijke literatuur criteria voor succesvolle samenwerking tussen overheidsactoren en private actoren bij het bewaken en beveiligen van 'soft targets' en het versterken van maatschappelijke weerbaarheid in tijden van diffuse dreiging?*

'Soft targets'

Zogeheten 'soft targets' zijn kwetsbare doelwitten in de stad en soms ook op het platteland, omdat daar veel mensen samenkomen en de betreffende plekken door hun (relatieve) openheid lastig geheel te bewaken en beveiligen zijn. Denk hierbij aan grote evenementen, winkelstraten of openbaar vervoer-knooppunten. Hoewel politie, justitie, gemeenten en het Rijk verantwoordelijk zijn voor veiligheid in het publieke domein, delen private partijen, zoals organisatoren van evenementen of beheerders van gebieden met een commerciële doelstelling ook deze verantwoordelijkheid. Derhalve ontstaat er publiek-private samenwerking (PPS) gericht op lokale (on)veiligheid, meer in het bijzonder diffuse dreigingen, waaronder terreuraanslagen.

Publiek-private samenwerking

PPS-constructies bestaan uit samenwerkingsverbanden tussen relatief autonome private en publieke partijen vanuit een gedeelde verantwoordelijkheid voor een publiek goed, waaronder veiligheid. Dit type samenwerkingsverbanden binnen het veiligheidsdomein neemt meestal de vorm aan van netwerk-PPS, die ertoe bijdraagt dat private actoren participeren binnen samenwerkingsverbanden in hun eigen belang en in het overheidsbelang. Binnen de wetenschappelijke literatuur over 'netwerken' – en aanpalend over 'governance' – wordt vaak over horizontale samenwerkingsverbanden gesproken. Binnen PPS heeft de overheid echter vaak een sturende of anderszins invloedrijke positie. De overheid blijft immers eindverantwoordelijk voor de openbare orde en veiligheid. Tegelijk gaat het bij de onderzochte cases van netwerk-PPS niet altijd om formeel-juridische constructies, waarbij ten minste één publieke partij gezaghebbend is, maar zien we ook 'lossere' of 'informelere' vormen van samenwerking functioneren. We komen daar hieronder op terug.

Literatuur over PPS in het kader van diffuse dreigingen richt zich op de fasen 'voor', 'tijdens' en 'na' een crisis. Onze focus ligt op de 'koude fase' vóór een crisis, dus op PPS

in de preventieve sfeer, omdat er zich in ons land nog geen grootschalige aanslag heeft voorgedaan, we tijdens een aanslag waarschijnlijk lastig onderzoek kunnen uitvoeren, en voorkomen altijd beter dan genezen is. We hebben een theoretisch model opgesteld waarin we naar het verloop van netwerk-PPS kijken en al dan niet aanwezige succesfactoren die daar invloed op hebben. Het *verloop van netwerk-PPS* gericht op het voorkomen van incidenten en aanslagen in tijden van diffuse dreiging is onze afhankelijke variabele. Omdat het niet eenvoudig is om dergelijke uitkomsten te meten – zeker niet als het om het voorkomen van incidenten gaat – vallen we terug op de percepties van betrokkenen: hoe tevreden zijn zij over de praktijk en resultaten van de PPS?

Criteria voor succesvolle PPS

Naast de afhankelijke variabele onderscheiden we vier onafhankelijke variabelen die invloed hebben op het *verloop van de netwerk-PPS*:

- De organisatie en dynamiek van het netwerk: aard en inhoud van de PPS, vormgeving PPS en mate van contact tussen deelnemende partijen.
- Culturele kenmerken: mate van vertrouwen en consensus tussen deelnemende partijen.
- Verdeling van verantwoordelijkheid en sturing: rollen en verantwoordelijkheden, besluitvorming en de aanwezigheid van een 'trekker' of 'verbindend persoon'.
- Connectie met de overheid: invloed van de lokale en landelijke overheid op het netwerk, en mate van verantwoording en evaluatie vanuit het netwerk.

Maatschappelijke weerbaarheid

Een doel van PPS gericht op het bewaken en beveiligen van 'soft targets' kan zijn dat de PPS bijdraagt aan maatschappelijke weerbaarheid (of 'veerkracht'). Binnen deze studie vatten wij 'weerbaarheid' op als onderdeel en uitvloeisel van het functioneren van wederzijds afhankelijke samenwerkingsrelaties tussen publieke en private organisaties die hun kennis en kunde bundelen bij met name de preventie van ingrijpende maatschappelijke gebeurtenissen, zoals terroristische aanslagen. Uit een overzicht van de literatuur over 'resilience' (veerkracht) komt naar voren dat dit begrip vele – soms tegenstrijdige – betekenissen heeft en daarom nauwelijks te operationaliseren valt.

Onze eigen veronderstelling is dat PPS leidt tot een zekere mate van maatschappelijke weerbaarheid als deelnemende publieke en private organisaties zinvolle relaties met elkaar aangaan (verloop van PPS als afhankelijke variabele) vanuit de beschreven criteria voor succes (de organisatie en dynamiek van het netwerk; culturele kenmerken; verdeling van taken en verantwoordelijkheden binnen en sturing van het netwerk; en de connectie tussen de overheid en netwerk als onafhankelijke variabelen) binnen een netwerk.

7.3 Beknopt (inter)nationaal overzicht

Deelvraag 2: *Hoe werken overheden in Nederland en in andere Westerse landen samen met private actoren bij het bewaken en beveiligen van 'soft targets' en bij het versterken van de weerbaarheid van de samenleving?*

Beleid

Westerse overheden lijken zich in toenemende mate bewust van de noodzaak om met private actoren samen te werken teneinde kwetsbare doelwitten beter te beschermen tegen aanslagen. Dit blijkt zowel uit beleidsdocumenten als uit gesprekken met verschillende overheidsfunctionarissen en experts in Nederland, België, Duitsland, Denemarken, Frankrijk, Zweden, het Verenigd Koninkrijk, de Verenigde Staten, Canada en Australië. Desondanks is deze wens nog lang niet in alle landen vertaald naar expliciet

beleid ten aanzien van PPS rondom de bewaking en beveiliging van 'soft targets'. Als er al PPS plaatsvindt dan is dat vaak op lokaal niveau, zonder per se een overkoepelende strategie vanuit de Rijksoverheid. Het Verenigd Koninkrijk, de Verenigde Staten en Australië lijken de langste traditie te hebben in het aangaan van PPS in het veiligheidsdomein (zie ook de voorbeelden hieronder). Een mogelijke verklaring hiervoor is de meer open houding van deze overheden ten opzichte van de privatisering van veiligheidstaken. Daarentegen is in bijvoorbeeld Duitsland of Frankrijk het organiseren van veiligheid nog steeds een grotendeels publieke taak. Nederland lijkt zich qua positie in het midden te bevinden door in toenemende mate toenadering tot private partijen te zoeken. De NCTV heeft bijvoorbeeld een 'handleiding drukke plekken' opgesteld en heeft daartoe bijeenkomsten georganiseerd met private stakeholders die een 'soft target' beheren of exploiteren. Ook kent ons land het 'Alerteringssysteem Terrorismebestrijding', dat publieke en private partijen tijdig informeert over terroristische dreiging, zodat de betrokken partijen passende maatregelen kunnen nemen om het risico op een aanslag te verkleinen of de gevolgen ervan te beperken.

Voorbeelden

Voorbeelden van netwerk-PPS gericht op het tegengaan van diffuse dreigingen binnen het kader van 'soft targets' zijn in binnen- en buitenland schaars. Bovendien gaat het bij veel van de gevonden voorbeelden om een beperkte vorm van PPS (in tegenstelling tot diepgaander vormen van PPS). Voorbeelden van gevonden beperkte varianten zijn de volgende:

1. Het project Argus in Londen biedt medewerkers binnen het bedrijfsleven, detailhandel, horeca, hotels, onderwijs en gezondheidszorg een drie uur durende simulatie aan over het voorkomen van aanslagen en over handelingsrichtingen tijdens en na aanslagen. Deelnemende partijen zijn de Londense politiediensten en bedrijven uit (de omgeving van) Londen. De samenwerking lijkt echter niet verder te gaan dan een eenzijdige informatieverstrekking vanuit de overheid richting de private sector.
2. NYPD-Shield is een paraplu voor verschillende projecten waarbinnen de politiediensten in New York (NYPD) samenwerken met private partijen en burgers om aanslagen te voorkomen. De private partijen fungeren als 'ogen en oren' van de NYPD, en melden verdachte situaties zo vroeg mogelijk. Het kan hier bijvoorbeeld gaan om verdachte zakelijke transacties of om verdacht en ongewoon gedrag bij 'soft targets'. Wanneer we naar de activiteiten van dit project kijken, lijkt de focus zich te beperken tot informatie-uitwisseling en training in de preventieve fase. Het was praktisch niet haalbaar om deze casus nader te onderzoeken.
3. Binnen het project Aware in Denemarken kunnen personen die in 'crowded places' werken, waaronder winkeleigenaren en beveiligingsmedewerkers, een bewustzijntraining volgen van de Deense Inlichtingendienst PET. Deelnemers leren verdacht gedrag herkennen (voorkomen van een aanslag) en hoe ze moeten handelen tijdens een aanslag. Zij volgen een vier uur durende cursus. Het gaat hier om een eenzijdige informatieverstrekking vanuit de overheid richting private partners. Er lijkt daarmee geen sprake te zijn van een daadwerkelijke PPS.
4. RTR-NL in Nederland richt zich op het handhaven van de openbare orde en het beschermen van goederen, personen, diensten en objecten door proactief cameratoezicht in het publieke domein. De kernpartijen binnen de samenwerking zijn de stichting RTR-NL, particuliere beveiligingsbedrijven en de politie. De PPS gaat in de praktijk niet verder dan het uitlezen van de camera's en het opvolgen van alarmeringssystemen. De politie houdt in alle gevallen de regie over het cameratoezicht. Deze vorm van PPS is preventief bedoeld, gericht op het voorkomen van een mogelijke aanslag, al kunnen camerabeelden mogelijk ook gebruikt worden voor opsporing nadat een aanslag heeft plaatsgevonden.

Voor onderhavig onderzoek waren we geïnteresseerd in diepgaandere vormen van netwerk-PPS. We hebben daarom verdiepend onderzoek uitgevoerd naar de volgende drie cases: de Johan Cruijff ArenA, de Nijmeegse Vierdaagse en het Diamantkwartier in Antwerpen. We gaan hier in de volgende paragraaf op in.

7.4 Praktijken van PPS

Deelvraag 3: *Wat kunnen we leren van voorbeelden waarin de overheid met private actoren samenwerkt bij het bewaken en beveiligen van 'soft targets' en bij het versterken van de weerbaarheid van de samenleving?*

Hieronder geven we eerst een korte beschrijving van de drie onderzochte cases. Voor alle cases geldt dat het gaat om netwerk-PPS die echter minder sterk juridisch gestructureerd is dan in de literatuurstudie werd verondersteld. We zetten per onderzochte casus op een rij in hoeverre geïnventariseerde werkwijzen van PPS voldoen aan de in de literatuur gevonden criteria voor succes. Tabel 4 bevat een samenvattend overzicht van de bevindingen. Vervolgens bespreken we aan de hand van de succescriteria voor PPS wat de cases ons leren.

Tabel 4: Samenvatting van bevindingen

	Johan Cruijff ArenA	Nijmeegse Vierdaagse	Diamantkwartier Antwerpen
Type PPS	Netwerk-PPS	Netwerk-PPS	Netwerk-PPS
Tevredenheid over verloop PPS	Tevredenheid over samenwerking en informatie-uitwisseling in commandokamer Ontevredenheid over samenwerking tussen politie en 'event profilers' Wisselende tevredenheid over informatie-uitwisseling voorafgaand aan evenement	Tevredenheid over samenwerking en informatie-uitwisseling voorafgaand en tijdens evenement	Tevredenheid over samenwerking en informatie-uitwisseling binnen het kwartier, wel kritisch over juridische obstakels in informatie-deling
Tevredenheid over resultaat van PPS	Tevredenheid over extra 'ogen en oren', waardoor meer zicht is gekomen op verdachte situaties en politie zich kan richten op kerntaken Wisselende tevredenheid over combinatie van service en veiligheid	Tevredenheid over betere toerusting van partijen om te reageren op mogelijke aanslagen of incidenten Tevredenheid over veiligheidstaken die private partij in toenemende mate op zich neemt Wisselende tevredenheid over beperkte politie-inzet	Tevredenheid over toegenomen zicht op verdachte situaties of personen in de wijk Tevredenheid over de gezamenlijk genomen veiligheidsmaatregelen
Organisatie en dynamiek	Geen convenant Missende partijen Regelmatig contact	Raamovereenkomst Geen missende partijen Regelmatig contact	Veiligheidsprotocol en samenwerkingsovereenkomst Geen missende partijen Regelmatig contact
Culturele kenmerken	Wantrouwen omtrent inzet van 'event profilers' Geen consensus over inzet service & veiligheid	Gevoel van vertrouwen door dezelfde 'taal' tussen publieke en private partijen Soms onenigheid over aanpak diffuse dreiging	Gevoel van vertrouwen door een vaste ploeg: 'Single Points of Contact' Consensus over aanpak diffuse dreigingen
Taken, rollen en verantwoordelijkheden	Onduidelijkheid over rol 'event profilers' Geen gelijkwaardigheid, regie bij politie Geen formele trekker van de PPS	Heldere rolverdeling Geen gelijkwaardigheid, sturende rol van de gemeente Nijmegen, maar besluitvorming zoveel mogelijk in consensus Publieke trekker vanuit gemeente Nijmegen met legitimiteit, maar geen (directe) doorzettingsmacht.	Heldere rolverdeling Lichte vorm van gelijkwaardigheid (mix van publiek en privaat in uitvoering), besluitvorming zoveel mogelijk in consensus, maar eindverantwoordelijkheid bij gemeente Private trekker in de vorm van het AWDC-office met legitimiteit en doorzettingsmacht aan private zijde.
Connectie met de overheid	Weinig contact en informatie-uitwisseling met gemeente en Rijk Er wordt geen verantwoording afgelegd, wel vindt interne evaluatie plaats.	Veel contact met lokale overheid en driehoek, soms met NCTV. Verantwoording afleggen middels jaarlijkse evaluatie	Veel contact met overheidspartijen Lichte democratische controle op de samenwerkingsovereenkomst vanuit de gemeenteraad

Johan Cruijff ArenA

Netwerk-PPS rondom de Johan Cruijff ArenA vindt plaats in de voorbereiding van evenementen en in de commandokamer van het stadion als er een concert of ander (niet-voetbalgerelateerd) evenement plaatsvindt. De volgende partijen zijn bij de samenwerking betrokken: de Johan Cruijff ArenA, politie, eventorganisatoren zoals MOJO Concerts en de particuliere beveiligingsorganisatie TSC. Over het verloop van de samenwerking en informatie-uitwisseling 'in the heat of the moment' zijn respondenten tevreden. Wel is er sprake van onenigheid tussen partijen over de inrichting van de samenwerking. Dit kan worden verklaard door het feit dat in de literatuur genoemde succescriteria binnen deze samenwerking deels afwezig zijn.

- *Organisatie en dynamiek*: Vooralsnog ontbreekt een formeel convenant die ieders rollen, taken en verantwoordelijkheden vastlegt. Dat zorgt voor enige onduidelijkheid onder de deelnemers. Ook worden de gemeente en aanpalende eventlocaties (Ziggo Dome en AFAS Live) als deelnemers aan deze PPS-constructie gemist. Wel vinden er tussen de deelnemende partijen periodieke overleggen plaats.
- *Culturele kenmerken*: Het vertrouwen in ieders kennis, kunde en toegevoegde waarde voor veiligheid (de private 'event profilers' en de servicemedewerkers) wordt niet door iedereen gedeeld. Ook is er geen consensus over de benodigde inzet van de 'profilers' en servicemedewerkers. Hierbij zij opgemerkt dat de combinatie van veiligheid en service belangrijk lijkt voor het in goede banen leiden van bezoekersstromen, maar er wellicht minder toe doet om aanslagen tegen te gaan.
- *Taken, rollen en verantwoordelijkheden*: Binnen de PPS blijkt de inzet van ongeuniformeerde private 'event profilers' een heikel punt vanwege onduidelijkheid over wat zij doen, c.q. welke informatie zij verzamelen. Er is geen sprake van gelijkwaardigheid tussen de partijen; de regie in het buitengebied is duidelijk in handen van de politie. Tot slot ontbreekt het binnen de PPS aan een formele trekker.
- *Connectie met overheid*: Er bestaat geen duidelijke connectie tussen de overheid en deze netwerk-PPS en het netwerk legt geen verantwoording af aan een democratisch gekozen orgaan. Wel evalueren de partijen onderling het verloop van de samenwerking. Verder zijn vooral respondenten binnen private partijen van mening dat de verstrekking van informatie over diffuse dreigingen vanuit de overheidspartijen beter een explicieter kan, zodat zij hun maatregelen daar beter op kunnen afstemmen.

Nijmeegse Vierdaagse

De PPS met betrekking tot de Nijmeegse Vierdaagse richt zich op informatie-uitwisseling die bijdraagt aan het veiligheidsplan, de vergunningverlening en scenario's en handelingsperspectieven in geval van calamiteiten tijdens de wandelprestatietocht. De kernpartijen binnen dit samenwerkingsverband zijn de privaatrechtelijke stichting DE 4DAAGSE, de gemeente Nijmegen en de politie. Respondenten zijn tevreden over het verloop van samenwerking binnen deze PPS. Zij wisselen in een prettige sfeer voldoende en adequaat informatie uit om de veiligheid tijdens het evenement goed te kunnen organiseren.

- *Organisatie en dynamiek*: De deelnemende partijen hebben regelmatig contact met elkaar door een vaste overlegstructuur. Voorafgaand aan de Vierdaagse zien zij elkaar maandelijks, en tijdens de Vierdaagse dagelijks. De basis voor de samenwerking is vastgelegd in een schriftelijke raamovereenkomst tussen de gemeente, het ministerie van Defensie en Stichting DE 4DAAGSE. In de samenwerking worden niet zozeer deelnemers gemist, wel is er behoefte aan

intensievere samenwerking met enkele partijen buiten de PPS (zoals Stichting de Vierdaagsefeesten).

- *Culturele kenmerken*: Deelnemers aan de PPS delen grotendeels dezelfde normen, waarden, visies en 'taal' door de langdurige samenwerking, informele contacten en de zitting van voormalige politiefunctionarissen en militairen binnen Stichting DE 4DAAGSE. Wel is er zo nu en dan onenigheid over de te nemen maatregelen tegen diffuse dreigingen, maar dit heeft tot nu toe niet geleid tot een vertrouwensbreuk.
- *Taken, rollen en verantwoordelijkheden*: De verdeling van taken en verantwoordelijkheden is voor de deelnemende partijen duidelijk. Er is een verschuiving zichtbaar van publiek naar privaat, doordat steeds meer veiligheidstaken door de private partij worden opgepakt (bijvoorbeeld verkeersregeling en toezicht en handhaving). Wel leeft bij respondenten de wens om de gemaakte afspraken meer schriftelijk vast te leggen. De verhouding tussen de partijen is niet als horizontaal te definiëren; de gemeente besluit immers over de te verlenen vergunning voor de Vierdaagse en overheidspartijen blijven hoofdverantwoordelijk voor de veiligheid in de publieke ruimte. De samenwerking wordt getrokken door de gemeente.
- *Connectie met overheid*: Er is veel contact met de lokale overheid, de driehoek en soms met de Rijksoverheid. Het netwerk legt verantwoording af over de het verloop van de Nijmeegse Vierdaagse middels jaarlijkse evaluaties. Dit is vastgelegd in de raamovereenkomst.

Diamantkwartier Antwerpen

Het Diamantkwartier in Antwerpen kent een PPS die zich toelegt op constante informatie-uitwisseling tussen de Security Office van het Antwerp World Diamond Centre (AWDC), gebouwbeheerders van diamanthandelaren en diamantbeurzen en particuliere beveiligers (private partijen) enerzijds en de lokale politie en de gemeente (publieke partijen) anderzijds. Naast informatiedeling bestaat de samenwerking uit het gezamenlijk nemen en financieren van beveiligingsmaatregelen. Respondenten zijn unaniem tevreden over deze PPS. Ze delen een gevoel van urgentie om samen te werken en de samenwerking is goed georganiseerd.

- *Organisatie en dynamiek*: De samenwerking tussen het AWDC Security Office, de gemeente en de politie is formeel vastgelegd in een veiligheidsprotocol en in een samenwerkingsovereenkomst. Dit geeft legitimiteit aan de samenwerking. Verder vindt er tussen alle partijen binnen diverse fora geregeld contact plaats.
- *Culturele kenmer*ken: Respondenten ervaren een hoge mate van wederzijds vertrouwen, onder andere omdat er met een vaste ploeg ('Single Points of Contact') wordt gewerkt. Ook is er sprake van consensus over de aanpak van diffuse dreigingen. Alle partijen delen de urgentie om veiligheidsproblemen in de wijk tegen te gaan en zijn bereid om elkaar hierin tegemoet te komen.
- *Taken, rollen en verantwoordelijkheden*: De verdeling van taken, rollen en verantwoordelijkheden is voor iedereen duidelijk. Het helpt dat de afspraken ook schriftelijk zijn vastgelegd. Ondanks dat de overheidspartijen eindverantwoordelijk zijn voor de veiligheid in de openbare ruimte, zien we een mix van 'publiek' en 'privaat' als het gaat om de wijze waarop partijen samenwerken en veiligheidsmaatregelen worden gefinancierd. Er is een duidelijke trekker van de PPS in de vorm van het private AWDC-Security Office, maar in laatste instantie is de burgemeester eindverantwoordelijk voor de openbare orde en veiligheid en kan hij desgewenst knopen doorhakken.
- *Connectie met overheid*: Er is een duidelijke connectie tussen de PPS en overheidspartijen. In de eerste plaats vindt informatie-uitwisseling plaats met een

breed scala aan overheidspartijen. Verder heeft de gemeenteraad invloed op de praktijk van het veiligheidsnetwerk; zo heeft zij de meest recente samenwerkingsovereenkomst (2016-2019) goedgekeurd.

Wat leert dit ons?

De voorgaande paragraaf en tabel laten zien dat de PPS in het Diamantkwartier van Antwerpen vrijwel aan alle in de literatuur geformuleerde succescriteria voldoet. Ook in Nijmegen zijn veel van de succescriteria aanwezig. Bij de Johan Cruijff ArenA is dit in mindere mate het geval. De uitkomsten bevestigen dat de aan- of afwezigheid van deze criteria een positieve, respectievelijk een negatieve invloed hebben op de tevredenheid van respondenten over het verloop en de resultaten van de PPS. We reflecteren op deze bevindingen door de theoretische bril van in de literatuur gevonden succesfactoren voor netwerk-PPS inzake het bewaken en beveiligen van 'soft targets': wat leren we uit de praktijk over het belang van deze factoren?

- *Organisatie en dynamiek*: Binnen alle drie de cases zien we terug dat het van belang is dat de juiste partijen om tafel zitten en partijen regelmatig contact met elkaar onderhouden (het liefst 'face-to-face' contact middels vaste overlegstructuren). Bij het opzetten van een PPS dienen de overheid en private partijen dus scherp te kijken of het beoogde samenwerkingsverband ook echt compleet is. Daarnaast is gebleken dat schriftelijke (juridische) afspraken, zoals convenanten en protocollen, bijdragen aan duidelijkheid over de rollen en taken van partijen en legitimiteit geven aan de PPS. Bovendien hebben respondenten binnen alle cases opmerkingen gemaakt over beperkende wet- en regelgeving die informatie-uitwisseling tussen publieke en private partijen in de weg staat. De wens tot vrijere informatie-uitwisseling onderstreept het belang van een betere juridische borging van PPS. Vanuit maatschappelijk belang moeten verantwoordelijkheden en bevoegdheden immers goed worden belegd.
- *Culturele kenmerken*: Vertrouwen tussen de partijen, een gezamenlijke urgentie om veiligheid te waarborgen en de wil om eventuele onenigheid te overbruggen blijken belangrijke succesfactoren. We kunnen concluderen dat voor de tevredenheid over het verloop van netwerk-PPS gericht op het bewaken en beveiligen van 'soft targets' de precieze juridische organisatievorm niet doorslaggevend is. De PPS verloopt goed als partijen (redelijk) intensief contact hebben, veel energie in hun samenwerking stoppen en elkaar vertrouwen. Toch is, zoals hierboven al is gesteld, juridische borging vanuit het publieke belang van maatschappelijke veiligheid wel belangrijk met het oog op informatie-uitwisseling en ieders verantwoordelijkheden en bevoegdheden in dezen.
- *Verdeling van taken, rollen en verantwoordelijkheden en sturing van het netwerk*: Binnen netwerken zitten publieke en private partijen met uiteenlopende visies, doelen en belangen. Gelijkwaardigheid tussen de partijen blijkt geen noodzaak, wederkerigheid echter wel. Verder lijkt de aanwezigheid van een verbindend persoon met legitimiteit (en niet per se doorzettingsmacht) die oog heeft voor de verschillende posities cruciaal. Verrassend genoeg werkt die persoon in Antwerpen bij een private partij die zowel het vertrouwen van de overheid als van de commerciële diamantensector geniet. Een belangrijke vaardigheid van een verbindende 'trekker' is dat hij of zij voor wederkerigheid kan zorgen. Aan zowel de publieke als de private kant gaat het om 'geven en te nemen' wat betreft informatiedeling, maar ook de financiering van maatregelen.
- *Connectie tussen de overheid en het netwerk*: De connectie tussen de overheid en het netwerk is niet in alle cases even sterk. Alleen de samenwerkingsverbanden rond het Antwerpse Diamantkwartier en de Nijmeegse Vierdaagse leggen enige vorm van verantwoording af aan een democratisch gekozen orgaan. Uit de onderzochte cases is verder naar voren gekomen dat bestuurlijk draagvlak nodig is voor het succes van de PPS. In zowel Antwerpen als Nijmegen wordt

de PPS gesteund door de burgemeester, de korpschef en bestuurders van de betrokken private partijen, wat het samenwerkingsverband legitimiteit geeft. In Amsterdam ontbreekt dergelijke bestuurlijke betrokkenheid vanuit de gemeente en politie.

7.5 Reflectie op maatschappelijke weerbaarheid

Deelvraag 4: *In hoeverre en hoe kan het vergroten van de weerbaarheid van private partijen binnen PPS-constructies een bijdrage leveren aan (a) de maatschappelijke veiligheid, en (b) het maken en accepteren van keuzes van de overheid inzake het bewaken en beveiligen van 'soft targets' in tijden van diffuse dreiging?*

We beantwoorden deze vragen aan de hand van onze onderzoeksuitkomsten en een focusgroep met experts (zie bijlage 4), waarmee we op 5 juni 2018 over deze bevindingen hebben gesproken.

Bijdrage PPS aan maatschappelijke weerbaarheid

Het vergroten van de weerbaarheid van private partijen binnen PPS-constructies kan volgens de gesproken experts een bijdrage leveren aan de maatschappelijke veiligheid als deze partijen investeren in het nemen van maatregelen – waaronder camerabewaking, de inzet van beveiligers en opschalingsscenario's – en het trainen van het eigen personeel. Door personeel bewuster en alerter te maken, kunnen verdachte gedragingen en voorwerpen eerder worden herkend en gemeld.

Private partijen worstelen volgens de experts met de vraag of en hoe burgers hierbij te betrekken. Ze noemen onder andere de mogelijkheid om een telefonische meldlijn of Twitter-account te openen, waar burgers melding kunnen maken van verdachte personen of situaties. De private partijen vrezen echter dat ze onvoldoende in staat zijn om deze meldingen vervolgens allemaal op te volgen. Tevens vragen zij zich af of burgers wel de juiste inschatting kunnen maken van wat 'verdacht' is. Daarnaast speelt mee dat het nemen van meer veiligheidsmaatregelen juist kan leiden tot verhoogde onveiligheidsgevoelens onder de bevolking. Bovendien zijn bij winkelcentra, het openbaar vervoer en andere eigenaren van 'soft targets' burgers ook klanten die een plezierige belevenis mee naar huis willen nemen en niet te veel met veiligheid moeten worden belast.

Hierbij zij opgemerkt dat de term 'weerbaarheid' een lastig te interpreteren fenomeen wordt gevonden. De term heeft volgens de experts te maken met 'sociale samenhang', 'zelfredzaamheid' en 'alertheid', maar verder is het een 'fluïde' begrip. Dit oordeel van de experts stemt overeen met de kritiek in de literatuur over 'resilience', dat het een zeer ambigu en daarom niet goed te operationaliseren term is. Het valt ook niet te bepalen of er door PPS-aanslagen zijn voorkomen. Hoogstens kunnen we volgens een expert de aanname maken dat betere samenwerking en informatie-uitwisseling tussen publieke en private partijen een positief effect heeft, omdat er daardoor meer 'ogen en oren' zijn die afwijkende zaken of personen opmerken.

Deze opmerking is conform onze eerder in hoofdstuk twee geformuleerde veronderstelling dat PPS leidt tot maatschappelijke weerbaarheid als deelnemende publieke en private organisaties zinvolle relaties met elkaar aangaan vanuit eerder beschreven criteria: de organisatie en dynamiek van het netwerk, culturele kenmerken, de verdeling van verantwoordelijkheid en sturing en de connectie met de overheid. Tezamen zorgen genoemde elementen voor een goed lopende PPS. In twee cases – de Nijmeegse Vierdaagse en het Antwerpse Diamantkwartier – zijn deze elementen grotendeels aanwezig, wat volgens respondenten inderdaad tot positieve resultaten leidt. In het geval van de Johan Cruijff ArenA ligt er aan de PPS geen convenant ten grondslag en is vertrouwen en consensus onder de deelnemende partijen in mindere mate aanwezig. Dit beïnvloedt de weerbaarheid van deze PPS mogelijkerwijs negatief. Tegelijk moet worden opgemerkt

dat, net als in Nijmegen en Antwerpen, respondenten over het algemeen tevreden zijn over hun onderlinge samenwerking.

Een expert stelt dat het hem niet verbaast dat de PPS rondom de Johan Cruijff ArenA relatief lastig verloopt, omdat er juist van publieke zijde minder urgentie tot samenwerking bestaat. In zijn optiek gaat het hier om grote commerciële belangen van een evenementenorganisatie die daarom veel middelen voor bewaking en beveiliging wil uittrekken, en door een vergunningenstelsel dat ook moet doen. De overheid heeft minder behoefte aan investeren of opschalen, tenzij zich een urgente dreiging voordoet. Daarentegen zijn in Nijmegen en Antwerpen de gezamenlijke – publiek/private – belangen groter, omdat het daar om activiteiten gaat die meer op de steden zelf uitstralen. Kortom, niet alleen door private organisaties, maar ook vanuit overheidswege, worden er soms kanttekeningen geplaatst bij de noodzaak van hechte PPS ter bewaking en beveiliging van 'soft targets'.

Het maken en accepteren van keuzes van de overheid

Onze bevinding dat voorbeelden van netwerk-PPS gericht op het tegengaan van diffuse dreigingen binnen het kader van 'soft targets' schaars zijn, wordt in de focusgroep herkend. Een belangrijke reden die experts aanvoeren, is dat niemand tegen meer samenwerking is, maar dat onvoldoende rekening wordt gehouden met hoe moeilijk diepgaande vormen van publiek-private samenwerking te realiseren zijn. Samenwerken is immers niet gratis. Private partijen moeten de kosten van het participeren in een PPS en van het nemen van veiligheidsmaatregelen kunnen doorberekenen aan hun klanten (afhankelijk van het type organisatie zijn dit bijvoorbeeld reizigers, dagjesmensen, huurders van winkels of de overheid zelf). Daarom zijn private partijen momenteel vaak terughoudend in het doen van extra investeringen.

Deze terughoudendheid komt ook door het feit dat er sprake is van een 'diffuse' in tegenstelling tot een 'concrete' dreiging. Private partijen weten niet goed wat een 'voldoende investering' precies inhoudt, want waar wapen je je eigenlijk tegen? Bij evenementen of (risico)voetbalwedstrijden gelden er vergunningenstelsels die voorschrijven voor hoeveel particuliere beveiligers en andere maatregelen een organisator moet zorgen. Dat is meestal niet zo duidelijk wanneer er geen sprake is van een evenement. Daarom nemen eigenaren van 'soft targets' vanuit hun eigen belangen en naar eigen inzicht veiligheidsmaatregelen en hebben zij, indien nodig, contact met de politie, zonder dat er een hechte publiek-private samenwerking van de grond komt.

Het vergroten van de weerbaarheid van private partijen binnen PPS-constructies kan een bijdrage leveren aan het maken en accepteren van keuzes van de overheid inzake het meer verantwoordelijk maken van private partijen voor bewaking en beveiliging als er volgens de experts aan ten minste drie randvoorwaarden wordt voldaan. Ten eerste is het noodzakelijk dat de overheid actief investeert in PPS, met aandacht voor hun relaties met, en belangen van, private partijen. Dit wil, ten tweede, zeggen dat private partijen hechter bij PPS kunnen worden betrokken als zij in staat worden gesteld gemaakte kosten in rekening te brengen bij hun klanten of dat kosten eerlijker over deelnemende partijen worden verdeeld. Een derde en laatste randvoorwaarde om private partijen bij PPS te betrekken, is door hen meer informatie te verschaffen over de aard van een diffuse dreiging. Willen private partijen scenario's kunnen preparen en nuttige veiligheidsmaatregelen kunnen nemen, dan moeten zij beter op de hoogte zijn over wat er van hen wordt gevraagd en waarom.

7.6 Drie varianten van netwerk-PPS

Voortbouwend op de informatie en analyse uit dit onderzoek zijn er drie varianten van netwerk-PPS inzake het bewaken van beveiligen van 'soft targets' in tijden van diffuse dreiging mogelijk. De eerste variant gaat uit van continuering van het bestaande, waarbij hooggespannen verwachtingen over netwerk-PPS moeten worden getemperd. De tweede variant biedt meer ruimte voor wederzijdse informatie-uitwisseling. In de derde

variant draagt de overheid ook bevoegdheden aan private partijen over. We lichten alle drie de varianten toe.

1. *Continuering van het bestaande,* met tempering van verwachtingen over netwerk-PPS De drie onderzochte cases – de Johan Cruijff ArenA, de Nijmeegse Vierdaagse en het Diamantkwartier in Antwerpen – laten zien dat de netwerk-PPS over het algemeen naar tevredenheid van alle deelnemers verloopt. De meeste spanning zit op de netwerk-PPS rondom de Johan Cruijff ArenA, wat te maken heeft met een ontbrekend convenant waarin ieders rollen, verantwoordelijkheden en toegevoegde waarde staat geëxpliciteerd. Wordt aan deze voorwaarde voldaan, dan lijkt de precieze organisatievorm van samenwerking tussen publieke en private partijen niet van doorslaggevend belang. Het gaat in de praktijk vooral om intensief contact en voldoende vertrouwen – afspraken nakomen, dezelfde 'taal' spreken, met een vast team werken – tussen deelnemers binnen een PPS. Als we deze variant blijven volgen, moeten verwachtingen ten aanzien van netwerk-PPS worden bijgesteld of getemperd. Momenteel bestaan er binnen het veiligheidsdomein geen gelijkwaardige netwerken van publieke en private partijen. De overheid (politie, gemeente, justitie) is vanwege haar geweldsmonopolie onvermijdelijk dominant aanwezig. Daarom kunnen we bij continuering van het bestaande beter spreken over private medeverantwoordelijkheid voor veiligheid dan over netwerk-PPS.
2. *Verdieping van netwerk-PPS:* Een verdieping van netwerk-PPS is mogelijk door de mate van informatiedeling tussen partijen te vergroten – dat wil zeggen: de overheid en private partners delen evenveel – ook meer gevoelige – informatie met elkaar. Bekeken vanuit de organisatie en dynamiek van een netwerk betekent dit dat er formelere afspraken moeten worden gemaakt. Dan wordt netwerk-PPS binnen het veiligheidsdomein een 'strakker' juridisch gestructureerd samenwerkingsverband gericht op informatie-uitwisseling. Voor de overheid brengt deze verdieping van netwerk-PPS het doorbreken van bestaande juridische grenzen tussen publieke en private domeinen met zich mee. Dat vraagt om aanpassing van bestaande wet- en regelgeving omtrent informatie-uitwisseling en privacybescherming. Ook betekent dit dat de connectie tussen de overheid en netwerken moeten worden versterkt door stevigere verantwoordingsmechanismen op te tuigen ten aanzien van de informatie-uitwisseling die plaatsvindt. Niettemin blijven vertrouwen en consensus cruciaal om binnen een netwerk-PPS goed samen te kunnen werken. Hierbij kan tevens verdieping van netwerk-PPS worden gezocht door niet een publieke, maar private trekker aan te stellen (de Antwerpse casus laat zien dat zoiets mogelijk is). Het is niet per se noodzakelijk dat de overheid enthousiasmeert, belangentegenstellingen gladstrijkt en voor wederkerigheid binnen het netwerk zorgt.
3. *Verbreden van netwerk-PPS:* In deze variant verdiepen partijen de PPS niet alleen door vrijer wederzijds informatie uit te wisselen en/of een private trekker aan te stellen. De overheid verbreedt ook de werkzaamheden van private partijen. Dat kan door de onderlinge verdeling van taken, rollen en verantwoordelijkheden grondig te herzien. Omdat de Nederlandse overheid het geweldsmonopolie heeft, zijn veiligheidsnetwerken nooit zo 'horizontaal' als literatuur over netwerksamenwerking soms suggereert, tenzij er verregaande aanpassingen worden doorgevoerd. In het verlengde hiervan is een verbreding van netwerk-PPS mogelijk door naast meer taken ook meer geweldsbevoegdheden aan de particuliere beveiligingsbranche over te dragen. Daardoor kunnen private beveiligers zelf optreden bij verstoringen van de openbare orde en hoeven zij niet op de politie wachten. Denk hierbij concreet aan het bewapenen van particuliere beveiligers. Wederom vraagt dit een andere – 'strakkere' – juridische structurering van netwerk-PPS en de verantwoordingsmechanismen die daarbij horen. In principe kan verbreding van netwerk-PPS onder de eindverantwoordelijkheid van de overheid plaatsvinden, waardoor er toch een verticale verankering van samenwerking blijft bestaan. Niettemin zijn er dan ingrijpende wijzigingen noodzakelijk in onder meer de Politiewet en de Wet particuliere beveiligingsorganisaties en recherchebureaus. Vanzelfsprekend is het dan ook nodig om de praktische samenwerking tussen politie en private beveiliging te herstructureren.

Literatuur

Wetenschappelijke publicaties

Bennett, C.J. & Haggerty, K.D. (red.) (2011). *Security games: surveillance and control at mega-events*. Milton Park: Routledge.

Beutel, A. & Weinberger, P. (2016). *Public-private partnerships to counter violent extremism: field principles for action: final Report to the U.S. Department of State*. College Park: University of Maryland.

Boutellier, H. (2011). *De improvisatiemaatschappij: over de sociale ordening van een onbegrensde wereld*. Den Haag: Boom Lemma uitgevers.

Boutellier, H. & Marissing, E. (2011). 'Veiligheidsarrangementen in IJburg: over de praktijk van de besturing van veiligheid'. *Tijdschrift voor Veiligheid*, 10 (1), 59-68.

Boutellier, H. & Steden, R. van (2011). 'Governing nodal governance: the "anchoring" of local security networks', in: A. Crawford (red.), *International and comparative criminal justice and urban governance: convergences and divergences in global, national and local settings*. Cambridge: Cambridge University Press, 461-482.

Broekhuizen, J., Steden, R. van & Boutellier, H. (2010). 'Versnipperde regie: de positie van de gemeente in een lokaal veiligheidsnetwerk'. *Tijdschrift voor Veiligheid*, 9 (3), 21-33.

Buerger, M. and Mazerolle, L., (1998). 'Third-party policing: a theoretical analysis of an emerging trend'. *Justice Quarterly*, 15 (2), 301-327.

Bures, O. (2013). 'Public-private partnerships in the fight against terrorism?'. *Crime, Law and Social Change*, 60 (4), 429-455.

Bures, O. (2016). 'Contributions of private businesses to the provision of security in the EU: beyond public-private partnerships'. *Crime, Law and Social Change*, 67 (3), 289-312.

Busch, N.E. & Givens, A.D. (2012). 'Public-private partnerships in homeland security: opportunities and challenges'. *Homeland Security Affairs*, 8 (1), 1-23.

Chen, J., Chen, T. H. Y., Vertinsky, I., Yumagulova, L., & Park, C. (2013). 'Public-private partnerships for the development of disaster resilient communities'. *Journal of Contingencies and Crisis Management*, 21 (3), 130-143.

Clarke, J. & Newman, J. (1997). *The managerial state: power, politics and ideology in the remaking of social welfare*. Londen: Sage.

Dempsey, J.S. (2011). *Introduction to private security.* Belmont, CA: Wadsworth.

Dijkstra, G. & Van der Meer, F. (2003). 'Disentangling blurring boundaries: the public/private dichotomy from an organizational perspective', in: M. Rutgers (red.), *Retracing public administration*. Oxford: Elsevier Science, 89-106.

Duit, A. (2016). 'Resilience thinking: lessons for public administration'. *Public Administration*, 94 (2), 364-380.

Dunn-Cavelty, M., & Suter, M. (2009). 'Public-private partnerships are no silver bullet: an expanded governance model for Critical Infrastructure Protection'. *International Journal of Critical Infrastructure Protection*, 2 (4), 179-187.

Flint, J. (2009). 'Cultures, ghettos and camps: sites of exception and antagonism in the city'. *Housing Studies*, 24 (4), 417-431.

Garland, D. (1996). 'The limits of the sovereign state: strategies of crime control in contemporary society'. *British Journal of Criminology*, 36(4), 445-71.

Granovetter, M. (1973). 'The strength of weak ties'. *The American Journal of Sociology*, 78 (6), 1360-1380.

Hawkings, R. & Maurer, K. (2010). 'Bonding, bridging en linking: how social capital operated in New Orleans following Hurricane Katrina'. *British Journal of Social Work*, 40 (6), 1777-1793.

Hill, J. & Lynn, L. (2005). 'Is hierarchical governance in decline? Evidence from empirical research'. *Journal of Public Administration Research and Theory*, 15 (2), 173-95.

Hulst, M. van, Graaf, L. de en Brink, G. van den (2011). 'Exemplary practitioners'. *Administrative Theory & Praxis*, 33 (1), 120-143.

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

Keatinge, T. (2015). *Identifying foreign terrorist fighters: the role of public-private partnership, information sharing and financial intelligence*. Leiden/Londen; The International Centre for Counter-Terrorism/RUSI.

Kempa, M., Stenning, P. & Wood, J. (2004). 'Policing communal spaces: a reconfiguration of the "mass private property" hypothesis. *The British Journal of Criminology*, 44 (4), 562-581.

Klijn, E.H. & Koppejan, J. (1994). 'Beleidsnetwerken als theoretische benadering: een tussenbalans'. *Beleidswetenschap*, 11 (2), 143-167.

Klijn, E.H. & Koppenjan, J. (2012). 'Governance network theory: past, present and future'. *Policy & Politics*, 40 (4), 587-606.

Klijn, E.H. & Twist, M. van (2007). 'Publiek-private samenwerking in Nederland: overzicht van theorie en praktijk'. *Management & Organisatie,* 3/4, 156-170.

Mehlbaum, S. & Steden, R. van (2016). *Tussen 112 bellen en een rotschop geven: burgermoed vanuit maatschappelijk, politiek en juridisch perspectief*. Den Haag/Amsterdam: SMV/Vrije Universiteit.

McGuire, M. & Agranoff, R. (2011). 'The limitations of public management networks'. *Public Administration*, 89 (2), 265-281.

Noordegraaf, M., Douglas S., Bos, A. & Klem, W. (2016). *Gericht, gedragen en geborgd interventievermogen? Evaluatie van de nationale contraterrorisme-strategie 2011-2015.* Utrecht: Universiteit Utrecht.

Osborne, D. & Gaebler, T. (1992). *Reinventing government: how the entrepreneurial spirit is transforming the public sector*. Reading: Addison-Wesley.

O'Toole, L. (1997). 'Treating networks seriously: practical and research-based agendas in public administration'. *Public Administration Review*, 57 (1), 45-52.

Pollitt, C. & Bouckaert, G. (2011). *Public management reform: a comparative analysis – New Public Management, governance and the Neo-Weberian state*. Oxford: Oxford University Press.

Popp, J.K, Brinton Milward, H., MacKean, G., Casebeer, A. & Lindstrom, R. (2014). *Inter-organizational networks: a review from the literature to inform practice*. Washington, D.C.: IBM Centre for the Business of Government.

Powell, W. (1990). 'Neither market nor hierarchy: network forms of organization'. *Research in Organizational Behavior*, 12, 295-336.

Provan, K. & Kenis, P. (2007). 'Modes of network governance: structure, management, and effectiveness'. *Journal of Public Administration Research and Management*, 18 (2), 229-252.

Raab, J., Mannak, R. & Cambré, B. (2015). 'Combining structure, governance, and context: a configurational approach to network effectiveness'. *Journal of Public Administration Research and Theory*, 25 (2), 479-511.

Reid, R .& Botterill, L.C. (2013). 'The multiple meanings of "resilience": an overview of the literature'. *Australian Journal of Public Administration*, 72 (1), 31-40.

Rittel, H. & Webber, M. (1973). 'Dilemmas in a general theory of planning'. *Policy Sciences*, 4, 155-169.

Sanders, M. (2014). 'Publiek-private samenwerking: een reparatiestrategie voor falende ordeningsvormen'. *Bestuurskunde*, 23 (3), 69-77.

Steden, R. van (2007). *Privatizing policing: describing and explaining the growth of private security*. Den Haag: Boom Juridische Uitgevers.

Steden, R. van (red.) (2011). *Strategieën van lokale veiligheid: een achtergrondstudie en drie reflecties.* Amsterdam: Amsterdam University Press.

Steden, R. van (2015). 'Van Spoorwegpolitie naar Service & Veiligheidsteams: tussen publieke en private orde op de trein'. *Cahiers Politiestudies*, 36 (3), 177-189.

Steden, R. van (2017). *De opsporings- en handhavingstaak van de Nederlandse politie: een kritische reflectie en lessen uit het buitenland*. Den Haag/Amsterdam: SMV/Vrije Universiteit.

Steden, R. van, Stougie, L. & Veldhoven, D. van (2017). 'Particuliere uitbesteding van gemeentelijke handhavingstaken: wat levert het de lokale overheid op?' *Bestuurskunde*, 26 (2), 51-60.

Stoker, G. (1999). 'Governance as theory: five propositions'. *International Social Science Journal*, 155, 17-28.

Terpstra, J. & Kouwenhoven, R. (2004). *Samenwerking en netwerken in de lokale veiligheidszorg*. Zeist: Kerckebosch (Commissie Politie en Wetenschap).

Then, S.K. & Loosemore (2006). 'Terrorism prevention, preparedness, and response in built facilities'. *Facilities*, 24 (5/6), 157-176.

Turrini, A., Cristofoli, D., Frosini, F. & Nasi, G. (2010). 'Networking literature about determinants of network effectiveness'. *Public Administration*, 88 (2), 528-550.

Unicri. (2009). *Public-Private partnership (PPPs) fort the protection of vulnerable targets against terrorist attacks: review of activities and findings* (www.un.org).

Wakefield, A. (2003). *Selling security: the private policing of public space*. Cullompton: Willan.

Whelan, C. (2011). 'Network dynamics and network effectiveness: a methodological framework for public sector networks in the field of national security'. *The Australian Journal of Public Administration*, 70 (3), 275-286.

Zedner, L. (2006). 'Policing before and after the police: the historical antecedents of contemporary crime control'. *The British Journal of Criminology*, 46 (1), 78-96.

Zhang, X. (2017). 'Identifying consumerist privately owned public spaces : the ideal type of mass private property'. *Urban Studies*, 54 (15), 3464-3479.

Beleidsdocumenten en andere literatuur

Commonwealth of Australia (2017). *Australia's Strategy for Protecting Crowded Places from Terrorism*. Geraadpleegd op: www.nationalsecurity.gov.au/Media-and-publications/Publications/ Documents/Australias-Strategy-Protecting-Crowded-Places-Terrorism.pdf (september 2017).

Department of Homeland Security (DHS) (2017). *State and Major Urban Area Fusion Centers*.

Geraadpleegd op: www.dhs.gov/state-and-major-urban-area-fusion-centers (september 2017).

Government of Canada (2013). *Building Resilience Against Terrorism. Canada's Counter-Terrorism*

Strategy. Geraadpleegd op: www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/index-en.aspx (september 2017).

National Counter Terrorism Security Office (NaCTSO) (2017). *Crowded Places Guidance*. Geraadpleegd op: www.gov.uk/government/uploads/system/uploads/attachment_data/file/619411/170614_crowded-places-guidance_v1.pdf (september 2017).

Nationale Coördinator Terrorismebestrijding en Veiligheid (NCTV) (2017). *Dreigingsbeeld terrorisme Nederland 44*. Den Haag: Ministerie van Veiligheid en Justitie.

Nationale Coördinator Terrorismebestrijding en Veiligheid (NCTV) (2017). *Alteringssysteem Terrorismebestrijding*. Geraadpleegd op: www.nctv.nl/organisatie/ct/atb/index.aspx (september 2017).

PET (Politiets Efterretningstjeneste) (2011). *Safety from the terror threat*. Geraadpleegd op: www.pet.dk/English/The%20Preventive%20Security%20Department/~/media/Forebyggende%20Afdeling/AFS_publikationer/2014/Safetyagainsttheterrorthreatpdf.ashx (september 2017).

Regeringen Denemarken (2015). *Et stærkt værn mod terror. 12 nye tiltag mod terror [Een sterke verdediging tegen terreur. 12 nieuwe maatregelen tegen terrorisme]*. Geraadpleegd op: www.fmn.dk/nyheder/Documents/Et-staerkt-vaern-mod-terror-2015.pdf (september 2017).

Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN) (2016). *Tackling Terrorism Together. Vigiliance, Prevention mand Protection against the Terrorist Threat.* Geraadpleegd op: www.sgdsn.gouv.fr/vigipirate/tackling-terrorism-together-vigilance-prevention-and-protection-against-the-terrorist-threat/ (september 2017).

Zweeds Ministerie van Justitie (2015). *Prevent, Preempt, Protect. The Swedish counter-terrorism strategy.* Geraadpleegd op: www.government.se/4a80d6/contentassets/b56cad17b4434118b16cf449dbdc973d/en_strategi-slutlig-eng.pdf (september 2017).

Bijlage 1: Lijst van benaderde contactpersonen

Land	Organisatie	Functie	E-mail / Telefonisch
Australië	Perpetuity Research	Wetenschapper	E-mail
	University of Sunshine Coast	Wetenschapper	E-mail
	University of South Australia	Wetenschapper	E-mail
België	Federale overheidsdienst binnenlandse zaken - directie veiligheid en preventie	Adjunct directeur-generaal en projectmanager	E-mail
	Antwerp World Diamond Center	Hoofd Security Office	Telefonisch interview
	European Corporate Security Association (ECSA)	Secretaris-generaal	Telefonisch interview
Canada	University of Winnipeg	Wetenschapper	E-mail
Denemarken	Ministerie van Immigratie en Integratie – Deens centrum voor preventie van extremisme	Beleidsmedewerker	E-mail
	Politie en lokale overheid	Coördinator exitprogramma's	E-mail
	Deense veiligheids- en inlichtingendienst (PET)	Inlichtingenofficier	Telefonisch interview
Duitsland	Federale dienst voor migratie en vluchtelingen	Onderzoeker	E-mail
	The modern security consulting group	Beleidsadviseur contra-terrorisme	Telefonisch interview
	Violence Prevention Network	Onderzoeker	E-mail
	ASW Bundesverband	Voorzitter	Telefonisch interview
	Universiteit van Münster	Wetenschapper	E-mail
Frankrijk	Foundation pour la Recherche	Onderzoeker	E-mail
	Operational general staff of terrorism prevention	Luitenant-kolonel	E-mail
	Université de Versailles-Saint-Quentin	Wetenschapper	E-mail
Finland	The criminal sanctions agency	Projectmanager	E-mail
Italië	CEVAS	Directeur	E-mail

Land	Organisatie	Functie	E-mail / Telefonisch
Nederland	Gemeente Almere	Projectleider veiligheid	E-mail
	Gemeente Amersfoort	Onderzoeker preventie radicalisering, beleidsregisseur diversiteit en preventie radicalisering	E-mail
	Gemeente Amsterdam	Beleidsadviseur burgerschap en diversiteit, bestuursadviseur openbare orde en veiligheid	Telefonisch interview
	Gemeente Den Haag	Beleidsmedewerkers integratie en openbare orde en veiligheid	E-mail
	Gemeente Deventer	Adjunct directeur	E-mail
	Gemeente Gouda	Beleidsmedewerker openbare orde en veiligheid	E-mail
	Gemeente Nijmegen	Adviseur veiligheid	E-mail
	Gemeente Rotterdam	Programmamanager aanpak radicalisering	E-mail
	Gemeente Tilburg	Adviseur veiligheid	E-mail
	Gemeente Utrecht	Beleidsadviseur veiligheid	E-mail
	Gemeente Zoetermeer	Beleidsadviseur veiligheid	E-mail
	Gemeente Zwolle	Adviseur veiligheid	E-mail
	SDR	CEO	Telefonisch interview
	RTR-NL	Directeur	Telefonisch interview
Noorwegen	Hogeschool van Ostfold	Wetenschapper	E-mail
Oostenrijk	Adviescentrum extremisme	Adviseur	E-mail
Spanje	Gemeente Malaga	Loco-burgemeester	E-mail
	Intelligence center against terrorism and organized crime	Overheidsfunctionaris	E-mail
Verenigd Koninkrijk	RAND	3 onderzoekers	E-mail
	Home Office – office for security and counter-terrorism – prevent research team	Beleidsmedewerker / Onderzoeker	E-mail
	Politie Londen	Prevent programmamanager	E-mail
	National Counter Terrorism Security Office	Politie	E-mail
	University of Portsmouth	Wetenschapper	E-mail
Verenigde Staten	University of Michigan	Wetenschapper	E-mail
	NYPD Shield	Politie	E-mail
Zweden	Swedish Defence University	Directeur onderzoek	E-mail
	Universiteit van Lund	Wetenschapper	E-mail
	Swedish civil contingencies agency	Onderzoeker	E-mail
	Nationaal coördinator voor de bescherming van de democratie tegen gewelddadig extremisme	Vice-secretaris	E-mail

Bijlage 2: Praktijkvoorbeelden PPS

Naam praktijkvoorbeeld	Locatie	Korte beschrijving	Bron
Australië			
Crowded Places Forum	Australië	Samenwerkingsverbanden tussen regionale overheden, politie en eigenaren en exploitanten van soft targets. De overheid ondersteunt private partijen bij het vergroten van de weerbaarheid van 'soft targets' door het delen van informatie over het dreigingsniveau en het aanbieden van kennis, tools en adviezen. Eigenaren en exploitanten van soft targets delen informatie over verdachte situaties en geleerde lessen.	https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-places-mass-gatherings.pdf
TISN	Australië	Overheid en bedrijven uit de vitale sector werken samen in het vergroten van de weerbaarheid van de vitale infrastructuur middels informatiedeling en initiatieven die bijdragen aan het vergroten van de weerbaarheid.	https://www.tisn.gov.au/Pages/default.aspx
België			
Samenwerking in het Diamantkwartier	Antwerpen	Het Antwerpen World Diamond Center werkt samen met o.a. de politie en gemeente in het voorkomen van aanslagen en om een gecoördineerde respons te kunnen geven tijdens en na aanslagen.	telefonische informatie
Canada			
Protect	Canada	Financial Transactions and Reports Analysis Centre of Canada (FinTRAC), banken, politie en justitie delen informatie. Hierdoor komt er zicht op de aanwezigheid van (een cumulatie) van verdachte indicatoren op bepaalde rekeningen. Door controle kan financiering van terrorisme worden tegengegaan.	https://www.canada.ca/en/financial-transactions-reports-analysis/news/2016/11/results-fight-against-money-laundering-terrorism-financing.html?=undefined&wb-disable=true
Denemarken			
Project Aware	Denemarken	Personeel werkzaam op locaties die als soft target zijn aan te duiden kunnen training krijgen van de Deense inlichtingendienst over het herkennen van signalen van verdacht gedrag en hoe te handelen tijdens een aanslag.	https://www.pet.dk/English/The%20Preventive%20Security%20Department/~/media/Forebyggende%20Afdeling/AFS_publikationer/2014/Safetyagainsttheterrorthreatpdf.ashx
The Alliance	Denemarken	Een opleiding voor private organisaties, met name beveiligingsorganisaties (bijvoorbeeld in winkelcentra of in conflictzones), waarin zij geïnformeerd worden over hoe zij kunnen acteren of reageren in het geval van een crisis, zoals een aanslag.	informatie per e-mail
Frankrijk			
The Plan Vigipirate	Frankrijk	Terrorisme alarm systeem vanuit overheid naar burgers: beschermen populatie, infrastructuur en instituties en meer voorbereid zijn als er een aanslag plaatsvindt.	http://www.osce.org/atu/111438?download=true

Naam praktijkvoorbeeld	Locatie	Korte beschrijving	Bron
Nederland			
Johan Cruijff ArenA	Amsterdam	Samenwerking tussen ArenA, politie, evenementorganisaties en particuliere beveiliging in het bewaken en beveiligen van bezoekers die zich in het buitengebied van de ArenA bevinden voorafgaand aan een concert of evenement.	Telefonsiche informatie
Alerterings-systeem terrorismebestrijding	Nederland	Informatie-uitwisseling en afstemming van te nemen maatregelen tussen NCTV en relevante publieke en private partijen (gemeenten, politie en vitale sector) bij terroristische dreiging.	https://www.nctv.nl/organisatie/ct/atb/index.aspx
Bondgenoten	Utrecht	Samenwerking en informatie-uitwisseling tussen overheid (politie en gemeente) en (private) partijen en individuen (zogenaamde sleutelfiguren): preventie van spanningen en behouden sociale stabiliteit na een incident.	https://www.kis.nl/artikel/politie-interventie-bondgenoten-investeert-vredestijd
Continuïteit samenleving	Vier veiligheids-regio's in Nederland	Verbeteren informatie-uitwisseling en crisiscommunicatie vier veiligheidsregio's, partners vitale sector en rijksoverheid: voor, tijdens en na een ramp/incident.	http://www.strategische-agenda.nl/project/continuiteit-van-de-samenleving/
Nijmeegse Vierdaagse	Nijmegen	Samenwerking tussen de organisator van de Vierdaagse (private stichting), de gemeente, politie en andere hulpdiensten in het waarborgen van de veiligheid van de wandelaars.	Telefonsiche informatie
Oog en Oor	Rotterdam	Politie en particuliere beveiligingsbedrijven delen informatie om Rotterdamse haven te beschermen.	http://www.veiligheidsbranche.nl/media/publicaties_nwe_site/brochure_projecten_informatie_uitwisseling_nvb_versie_web.pdf
RTR-NL	Nederland	RTR-NL levert pro-actief cameratoezicht aan politie, gemeente, ambulancezorg: handhaving openbare orde, beschermen goederen/personen/objecten.	http://rtr-nl.nl/index.php
Search Detect React trainingen	o.a. Hilversum, Breda, Oosterhout, Amsterdam, Schiphol	Trainingen om aanslagen te voorkomen. Vaak in gezamenlijkheid publiek-privaat. Trainingen worden verzorgd aan publieke partijen door private partij.	Telefonische informatie
Weuro	Utrecht	Extra maatregelen zijn genomen na de oproep van IS om een aanslag te plegen tijdens de WEURO in Utrecht, waarbij in ieder geval gemeente, politie, OM, stadion Galgenwaard en FC Utrecht betrokken waren.	Telefonische informatie
Portugal			
Parcerias	Portugal	Publieke partijen en private bedrijven met een verhoogde blootstelling aan de dreiging van terrorisme, zoals hotels en winkelcentra, vervoer, energie en postbedrijven komen regelmatig bij elkaar om te praten en ontwikkelen persoonlijke relaties gebaseerd op onderling begrip en vertrouwen. De Portugese inlichtingendienst is de trekker van het initiatief.	http://www.un.org/en/terrorism/ctitf/pdfs/web_protecting_human_rights.pdf
Spanje			
PPS zeehavens	Spanje	Publieke en private beveiligers werken samen in het bewaken en beveiligen van zeehavens.	http://www.un.org/en/terrorism/ctitf/pdfs/web_protecting_human_rights.pdf
Verenigd Koninkrijk			
Project Argus	London	Politie Londen en bedrijven worden getraind: bewustzijn dreiging terrorisme, adviezen over voorkomen en handelen tijdens en na een eventuele aanval.	https://www.cityoflondon.police.uk/advice-and-support/countering-terrorism/Pages/project-argus.aspx
Project Griffin	Verenigd Koninkrijk	Preventie en adequate respons door informatiedeling tussen politie en private partijen en door training van private partijen.	https://www.gov.uk/government/publications/project-griffin/project-griffin

Naam praktijkvoorbeeld	Locatie	Korte beschrijving	Bron
Verenigde Staten			
Chicago PP Taskforce	Chicago	Samenwerking stad Chicago en bedrijven; gericht op veerkrachtige infrastructuur en economie voor als ramp/aanslag plaatsvindt.	http://sisokagroup.com/chicagofirst/wp-content/uploads/2017/03/cpptf_fact_sheet_nov_2013.pdf http://www.chicagofirst.org/wp-content/uploads/2017/05/2016_ChicagoFIRST_Annual_Report.pdf
NYPD Shield	New York	New York politiedepartement (NYPD) geeft training aan private organisaties en houdt hen op de hoogte van ontwikkelingen. Organisaties geven relevante signalen door aan de politie.	http://www.nypdshield.org/public/about.aspx https://www.hsaj.org/articles/233
OSAC	Verenigde Staten	Op een forum worden 'best practices' uitgewisseld en informatie gedeeld tussen bedrijven en de overheid onder andere m.b.t. terrorisme.	http://www.un.org/en/terrorism/ctitf/pdfs/web_protecting_human_rights.pdf
Overig			
PPS op vliegvelden	Bijv. België, Nederland, Spanje	Op veel vliegvelden vindt samenwerking plaats tussen publieke en private partijen in het bewaken en beveiligen van airports en het controleren van personen en goederen.	Telefonische informatie

Bijlage 3: Overzicht van geïnterviewde respondenten per casus

Casus	Organisatie	Typering respondent
Johan Cruijff ArenA	Johan Cruijff ArenA	Belast met veiligheid bezoekers
	Johan Cruijff ArenA	Belast met veiligheid bezoekers
	Johan Cruijff ArenA	Servicemedewerker
	MOJO Concerts	Belast met vergunningen en veiligheid
	MOJO Concerts	Verantwoordelijk voor operationele veiligheid
	The Security Company	Verantwoordelijk voor operationele veiligheid
	Politie-eenheid Amsterdam	Politie ArenA-gebied
Nijmeegse Vierdaagse	Stichting DE 4DAAGSE	Bestuurslid
	Stichting DE 4DAAGSE	Bestuurslid
	Gemeente Nijmegen	Bestuurder
	Gemeente Nijmegen	Ambtelijk verantwoordelijk voor veiligheid
	Gemeente Nijmegen	Ambtelijk verantwoordelijk voor veiligheid
	Politie-eenheid Oost Nederland	Teamchef
Diamantkwartier Antwerpen	Antwerpen World Diamond Center	Security Office
	Lokale Politie Antwerpen	Hoofdinspecteur
	Securitas	Management
	ADC-gebouw	Facilitair management
	Gemeente Antwerpen	Ondersteuning schepen Diamantkwartier

Bijlage 4: Overzicht deelnemers reflectiesessie

Organisatie	Typering respondent
NCTV, directie Bewaking, Beveiliging, Burgerluchtvaart	Beleidsmedewerker
NCTV, directie Contraterrorisme	Beleidsmedewerker
Politie, expertgroep bewaken en beveiligen	Teamchef
G4S	Directeur
GVB	Stafbureau sociale veiligheid
Kleppiere	Facility Manager
Vrije Universiteit Amsterdam	Facility Manager / Beveiliging

Colofon

Opdrachtgever: WODC

Auteurs:
Dr. R. van Steden
R.T. Meijer, MSc

Met medewerking van
Drs. J. Broekhuizen en dr. F. de Meere

Omslag: Ontwerppartners, Breda

Foto: Hollandse Hoogte

Uitgave Verwey-Jonker Instituut
Kromme Nieuwegracht 6
3512 HG Utrecht
T (030) 230 07 99
E secr@verwey-jonker.nl
I www.verwey-jonker.nl

De publicatie kan gedownload worden via onze website:
http://www.verwey-jonker.nl.

ISBN 978-90-5830-900-6

De afgelopen jaren is Europa het toneel geweest van meerdere terroristische aanslagen. Daarbij waren vooral ‘soft targets’ het doelwit: open plaatsen die moeilijk te beveiligen zijn en waar grote groepen mensen komen. De verscheidenheid aan mogelijke doelwitten en de diversiteit aan potentiële daders (organisaties, netwerken of eenlingen), hun motieven (denk bijvoorbeeld aan jihadisme of rechtsextremisme) en modus operandi (onder andere vuurwapengeweld, explosieven, vrachtwagens en steekpartijen) zorgen voor een diffuse dreiging.

De capaciteit van de veiligheidsdiensten om soft targets te beveiligen heeft zijn beperkingen. Financiële en personele middelen voor het bewaken en beveiligen van doelwitten zijn schaars. De overheid zoekt daarom steun bij private partijen, zoals organisatoren van evenementen. We zien vormen van deze publiek-private samenwerking (PPS) op het gebied van veiligheid terug in het openbaar vervoer, bij grote evenementen en rondom ‘gevoelige’ religieuze instellingen.

De Kenniswerkplaats Veiligheid en Veerkracht (een samenwerking tussen de VU en het Verwey-Jonker Instituut) onderzocht hoe de overheid samen met private actoren soft targets op de lange termijn effectief kan bewaken en beveiligen en aldus voor maatschappelijke weerbaarheid kan zorgen. We brachten in kaart wat hier relevante werkwijzen voor zijn. De ervaringen en percepties van de door ons geïnterviewde respondenten stonden daarbij centraal. De informatie uit dit onderzoek kan de Nationaal Coördinator Terrorismebestrijding en Veiligheid ondersteunen bij afwegingen omtrent het bewaken en beveiligen van potentiële doelwitten en de aanvullende rol die private actoren daarbij kunnen spelen.

Verwey-Jonker Instituut

VERWEY-JONKER INSTITUUT
Kromme Nieuwegracht 6
3512 HG Utrecht

T 030 230 07 99
E secr@verwey-jonker.nl
I www.verwey-jonker.nl