WORKING PAPER
BSK14-01

Naar meer inzicht in de politiële netwerkpraktijk in de casus cybercrime, zeehavens en veiligheidshuizen

Ira Helsloot, Jelle Groenendaal




Creating knowledge for society

Institute for Management Research
Radboud University

Naar meer inzicht in de politiële netwerkpraktijk in de casus cybercrime, zeehavens en veiligheidshuizen

Ira Helsloot
Hoogleraar Besturen van Veiligheid
Radboud Universiteit Nijmegen
Faculteit Managementwetenschappen
Thomas van Aquinostraat 5
6500 HK Nijmegen
i.helsloot@fm.ru.nl

Jelle Groenendaal
Promovendus en senior onderzoeker Crisislab
Radboud Universiteit Nijmegen
Faculteit Managementwetenschappen
Thomas van Aquinostraat 5
6500 HK Nijmegen
j.groenendaal@fm.ru.nl

Abstract
De complexer wordende samenleving vraagt, zo stellen beleidsmakers en politieonderzoekers al vele jaren, om een politieorganisatie die als netwerkspeler of regisseur opereert in zich steeds uitbreidende veiligheidsnetwerken om de kernfuncties opsporing en handhaving openbare orde effectief te kunnen vervullen. In dit onderzoek verkennen we deze these door te onderzoeken wat de opbrengst is van het politiële netwerken in de casus cybercrime, zeehavens en veiligheidshuizen voor de kernfuncties van de politie. Daarnaast bekijken we of interne sturing plaatsvindt op de netwerkende taken van politienetwerkers. Op basis van een secundaire analyse van bestaande literatuur en interviews concluderen we dat de politie momenteel geen volwaardige netwerkpartner is, omdat ze alleen maar wil 'nemen' uit - en niet wil 'geven' aan - het netwerk. De opbrengst van het netwerken zoals bedoeld in het formele politiebeleid voor de kerntaken is nihil. Sturing op de netwerkende taken van politienetwerkers lijkt niet plaats te vinden.

1. Inleiding
Sociologen stellen dat onze samenleving verandert in een netwerksamenleving; ze decentraliseert, desintegreert en verticale structuren veranderen in flexibele netwerken van kleine, verspreide eenheden (Boutellier, 2007). De transitie naar een netwerksamenleving heeft volgens onderzoekers gevolgen voor publieke organisaties (De Bruijn & Ten Heuvelhof, 2007). De netwerksamenleving heeft, zo betogen politiebeleidsmakers en politieonderzoekers, ook gevolgen voor de politieorganisatie. Door de komst van de netwerksamenleving, zo luidt de stelling, is het noodzakelijk dat ook de politie zich ontwikkelt als een '*netwerkspeler*.'

In bijvoorbeeld de visienota Politie in Ontwikkeling (PiO) uit 2005 wordt tegen de achtergrond van de netwerksamenleving de politie nadrukkelijk als netwerkspeler neergezet met concepten als programmasturing en 'nodale oriëntatie'. De opstellers beargumenteren dat de politie in toenemende mate dient te kijken naar de fysieke (en virtuele) infrastructuur die lokale gemeenschappen met elkaar verbindt. Het politiewerk heeft in dit licht als nieuwe dimensie het inzicht

verkrijgen in de sociale processen die bepaald worden door stromen van mensen, goederen, geld en vooral informatie (PiO, 2005).

Sommige politieonderzoekers menen dat de netwerksamenleving vraagt om een '*netwerkende*' politie, dat wil zeggen om een intensieve samenwerking tussen politie enerzijds en publieke en private partijen anderzijds. De rationale achter deze benadering is dat een succesvolle aanpak van sociale overlast en criminaliteit in een netwerksamenleving niet meer mogelijk is wanneer het exclusief vanuit de politie wordt benaderd (Terpstra & Kouwenhoven, 2004; Johnston & Shearing, 2003; Van Stokkum & Terpstra, 2006; Wood & Shearing, 2007). Rechtsordehandhaving is in deze optiek niet (langer) het monopolie van de politie, maar een *coproductie* tussen verschillende partijen met gelijksoortige maar zeker ook verschillende belangen. Dit vergt van de politie mogelijk een andere rol dan ze normaliter gewend was: de 'agent 2.0' moet kunnen netwerken, regisseren, partijen bij elkaar brengen, eigen problemen 'integraal' benaderen, participeren in allerhande gremia en verantwoording afleggen aan meerdere partijen, zoals netwerkpartners, burgers, media en niet in de laatste plaats de eigen organisatie.

Andere politieonderzoekers zijn kritischer ten aanzien van de veronderstelde gevolgen van de netwerksamenleving voor de politie. Hoogenboom ziet de 'netwerktaal' vooral als een speeltje van (politie)onderzoekers en meent dat er de facto weinig veranderd is aan de taakuitoefening van de politie (Hoogenboom, 2009). Van Steden meent eveneens dat *"de populariteit van termen als netwerken en governance geenszins betekent dat zich een Copernicaanse wending in beleid en uitvoering heeft voltrokken*." (Van Steden, 2011: 6). Daarnaast maakt bestaand empirisch onderzoek naar de netwerkende politie in Nederland duidelijk dat het netwerken door de politie in de praktijk nog verre van vlekkeloos verloopt (bijvoorbeeld Terpstra & Kouwenhoven, 2004; Terpstra, 2008). Veel van dit empirische onderzoek bestrijkt overigens alleen de gebiedsgebonden politiezorg: de betekenis van het netwerken op andere werkterreinen van de politie is veel minder bestudeerd.

In dit verkennende onderzoek bekijken we daarom wat de betekenis is van het netwerken door de politie in drie nog minder onderzochte casus, namelijk cybercrime, zeehavens en veiligheidshuizen. Meer precies richten we ons ten *eerste* op de vraag wat de opbrengst van het participeren in de door ons onderzochte netwerken is voor de kernpolitiefuncties opsporing en handhaving openbare orde. Ten *tweede* stellen we de vraag wat de participatie in netwerken betekent voor de interne aansturing van politiemensen die in deze netwerken (moeten) opereren.

Deze vragen beantwoorden we in dit onderzoek door het uitvoeren van een secundaire analyse van bestaande literatuur over de participatie van de politie in de netwerken rond cybercrime, zeehavens en veiligheidshuizen. Aanvullend hierop hebben we semigestructureerde interviews afgenomen. Voor de casus zeehavens hebben we gesproken met vier functionarissen van de zeehavenpolitie en andere handhavers in de Rotterdamse haven. Voor de casus cybercrime hebben we twee interviews gehouden met politiemensen direct betrokken bij de opsporing van cybercrime, een interview met een onderzoeker die onderzoek doet op dat terrein en twee interviews met bankmedewerkers met cybercrime in hun portefeuille en regelmatig met de politie te maken hebben. Voor de casus veiligheidshuizen hebben we drie vertegenwoordigers van de politie in de veiligheidshuizen Den Bosch, Amsterdam West en IJsselland geïnterviewd.

2. Theorie

In de bestuurskundige literatuur komen verschillende definities van netwerken voor. Wij volgen in dit onderzoek de meest brede en gangbare definitie en beschouwen een netwerk als een *"min of meer stabiel patroon van sociale relaties tussen verschillende autonome actoren die voor het verwezenlijken van hun doelen in enige mate afhankelijk zijn van elkaar"* (vrij naar De Bruijn & Ten Heuvelhof, 2007 en Kickert et al. 1997).

De netwerktheorie gaat uit van horizontale relaties tussen de actoren in het netwerk. In een netwerk is geen enkele partij de baas. Netwerken worden gekarakteriseerd door een continue interactie tussen actoren gericht op uitwisseling van middelen en onderhandeling over gemeenschappelijke doelen (Rhodes, 2007). Om deze interactieprocessen beter te kunnen begrijpen, zoomen we in op de vier structuurkenmerken van netwerken: pluriformiteit, interdependentie, geslotenheid en dynamiek (De Bruijn & Ten Heuvelhof, 2007).

Een netwerk bestaat vaak uit actoren die op onderdelen raakvlakken vertonen maar ook zekere verschillen kennen, met name met betrekking tot de middelen die ze bezitten (in termen van informatie, kennis, diensten, goederen, financiën etc.). Het feit dat actoren in een netwerk in zekere mate van elkaar verschillen, wordt in de literatuur *pluriformiteit* genoemd. Het principe van pluriformiteit maakt dat partijen door het uitruilen van middelen elkaar kunnen versterken.

Naast de verschillen tussen actoren bestaat er in netwerken ook altijd een zekere mate van *interdependentie*: actoren zijn van elkaar afhankelijk om hun eigen doelen te kunnen verwezenlijken en zullen daarom de (machts)middelen die ze bezitten tegen elkaar uit moeten ruilen. Een elementair principe hierbij is reciprociteit: plichten zijn wederkerig (De Bruijn & Ten Heuvelhof, 2007). Actor A is aan actor B iets verplicht, in de wetenschap dat actor B op een volgend moment iets verplicht is aan actor A. Samen werken in een netwerk vraagt dus om 'geven en nemen'. Wanneer je alleen maar 'neemt' uit het netwerk en niet(s) 'geeft', heb je als netwerkpartner simpelweg geen toegevoegde waarde en zal je uiteindelijk uit het netwerk vallen (Agranoff & McGuire, 1999).

Actoren in netwerken kenmerken zich veelal door *geslotenheid*: ze laten zich niet of nauwelijks sturen door andere actoren in of buiten het netwerk. Deze geslotenheid kan voortkomen uit de behoefte om de onzekerheid en de complexiteit in de omgeving van de organisatie te verminderen. Een andere mogelijke oorzaak van de geslotenheid van actoren is dat de sturing van buiten niet aansluit bij de professionele werkopvattingen en waarden van de actor (De Bruijn & Ten Heuvelhof, 2007).

Het laatste kenmerk van netwerken is dat ze onderhevig zijn aan verandering. Dit wordt ook wel de *dynamiek* van het netwerk genoemd. Het komt er op neer dat de positie van actoren in het netwerk, hun geslotenheid en hun professionele opvattingen voortdurend veranderen. De samenstelling van het netwerk wordt eveneens beïnvloed door nieuwe actoren in het netwerk en andere actoren die het netwerk verlaten. Bovendien kunnen netwerken ook uiteenvallen, zeker wanneer het netwerk sterk leunt op een of twee actoren (De Bruijn & Ten Heuvelhof, 2007). Dit verklaart onder meer waarom het samenwerken in een netwerk nooit vanzelf gaat en veelal met horten en stoten verloopt.

Voor het voortbestaan en de effectiviteit van het netwerk zijn twee netwerkprincipes van groot belang.

In de eerste plaats is het noodzakelijk dat iedere deelnemende actor het idee heeft dat hij of zij er (onder aan de streep) beter van wordt. Het gaat hierbij dus om de gepercipieerde opbrengst van het netwerken. Een partij zal alleen in netwerkverband willen opereren, wanneer het in de perceptie van deze partij bijdraagt aan het verwezenlijken van zijn of haar belangen. In de woorden van Provan & Milward (2001: 420): "*"One clear observation is that sustained collaborative activity, such as that of ongoing networks, must demonstrate worth"*

In de tweede plaats is het voor de effectiviteit en voortbestaan van netwerken cruciaal dat deelnemende actoren bereid zijn om te 'geven en nemen'. Uit de netwerkliteratuur blijkt dat bijna alle problemen bij het samenwerken in netwerken ontstaan wanneer een actor probeert om zoveel mogelijk zijn eigen doelen te verwezenlijken, zonder rekening te houden met de doelen van andere actoren of het 'gezamenlijke' doel (Thompson & Perry, 2006).

Bij de analyse van de drie casus in het volgende hoofdstuk zullen we kijken hoe de politie in de praktijk invulling geeft aan deze twee netwerkprincipes.

3. Resultaten

De resultaten van onze secundaire analyse van bestaande literatuur en interviews presenteren we aan de hand van vier vragen: 1) hoe zien de netwerken in de verschillende casus eruit?; 2) In hoeverre en hoe participeert de politie in deze netwerken?; 3) In hoeverre en hoe sturen politiele leidinggevenden hun medewerkers met een netwerkende taak?; 4) Wat is de aantoonbare opbrengst van het participeren in netwerken door de politie voor de kerntaken opsporing en handhaving openbare orde?

3.1 Hoe zien de onderzochte netwerken van de politie eruit?

Cybercrime

Al sinds het begin van de jaren tachtig is cybercrime een probleem. In deze periode zijn computers en andere informatietechnologie voor het eerst ingezet om reguliere vormen van criminaliteit zoals fraude en diefstal te plegen (Furnell, 2003: 8-9). Nadat in de jaren negentig het gebruik van internet snel toenam heeft het probleem zich steeds verder ontwikkeld. Sinds enkele jaren wordt cybercriminaliteit door de politie (maar ook de politiek) gezien als een serieus en complex veiligheidsprobleem dat dringend meer aandacht behoeft (Rustad, 2002).

Sinds het ontstaan van cybercrime aan het begin van de jaren tachtig is in cyberspace een autonoom netwerk ontstaan ter bestrijding van cybercrime (Rustad, 2002). Het netwerk bestaat uit een fluctuerende diversiteit aan vooral publieke en in veel mindere mate private partijen. Midden in het netwerk bevinden zich vooral de grote (internationale) aanbieders van diensten (die zowel 'slachtoffer' als 'handhaver' kunnen zijn) bevinden (Rustad, 2002). Aan de periferie van het netwerk bevindt zich een onoverzichtelijk groot aantal kleinere spelers, waaronder de Nederlandse politie.

Zeehavenpolitie

In de havens van Rotterdam komen verschillende internationale goederen-, mensen-, financiële en informatiestromen samen. Voor het beeld: in 2007 voeren 30.000 zeeschepen, 200.000 binnenschepen en een groot aantal pleziervaartuigen de Rotterdamse Zeehaven binnen. Zo werden in 2007 406 miljoen goederen overgeslagen en 10.8 miljoen containers. De verwachting is dat de

Rotterdamse haven in de komende jaren zal doorgroeien. In 2035 wordt bijvoorbeeld verwacht dat 35 miljoen containers worden omgezet (Hoogenboom, 2010).

In de Rotterdamse Zeehavens zijn behalve de Zeehavenpolitie een groot aantal andere partijen dagelijks betrokken bij het controle en handhaving van deze verschillende stromen. Zo zijn in Rotterdam meer dan twintig bestuurlijke diensten dagelijks bezig met allerlei soorten toezicht, controle, handhaving en opsporing in de havens. Voorbeelden zijn de diensten als de Havenmeester, Rijkswaterstaat en Port Security. Ook bijzondere opsporingsdiensten zoals de FIOD-ECD , SIOD, AID en IOD zijn actief in de havens (Hoogenboom, 2010).

Naast de genoemde bestuurlijke diensten wordt het vervoer over water gecontroleerd door 24 verschillende toezichthouders die 72 verschillende inspecties uitvoeren. In totaal werden er bijvoorbeeld in 2007 in de Rotterdamse Zeehavens 140.500 inspecties uitgevoerd waarvan 26.000 door de Zeehavenpolitie. Ook zijn in de havens verschillende private beveiligingsbedrijven actief. Deze partijen hebben vooral een rol bij het toezicht op industrieterreinen of andersoortige bedrijventerreinen (Hoogenboom, 2010).

Veiligheidshuizen

De Veiligheidshuizen zijn in 2005 ontstaan als opvolger van de vroegere 'Justitie in de Buurt' (JIB) kantoren. JIB kantoren hielden zich bezig met het voorkomen van escalatie van geschillen, het bieden van pre- of buitengerechtelijke oplossingen voor criminaliteitsproblemen en de coordinatie van verschillende justitiediensten op wijkniveau (Luykx & Grapendaal, 1999). Na twee jaar proefdraaien besloot het Kabinet in 2007 dat er een landelijk dekkend systeem van Veiligheidshuizen moest komen 'waarin gemeenten, jeugd- en zorginstellingen, politie en justitie samenwerken in de aanpak van criminaliteit en overlast' (Dammen et al. 2008). Een Veiligheidshuis is meer precies gedefinieerd als een lokaal of regionaal samenwerkingsverband tussen verschillende veiligheidspartners gericht op een integrale probleemgeoriënteerde aanpak van criminaliteit en het bevorderen van de sociale veiligheid (Dammen et al. 2008). Het netwerk van 'het veiligheidshuis' bestaat afhankelijk van de regio uit ten minste de politie, het OM en de gemeente aangevuld met andere justitiële partners en aanbieders van sociale- en medische zorg (ibidem).

3.2 In hoeverre en hoe participeert de politie in netwerken?

Cybercrime

De aandacht voor een groot digitaal kinderpornonetwerk heeft ertoe geleid dat in 1998 vijf rechercheurs zijn vrijgemaakt om het internet af te speuren naar kinderporno. In verloop van tijd is deze kleine groep rechercheurs getransformeerd naar de landelijke groep Digitaal Rechercheren (Stol, 2004: 76). Tegenwoordig opereert de groep Digitaal Rechercheren onder de naam *Team High Tech Crime*. Dit team houdt zich behalve met het bestrijding van kinderporno ook nadrukkelijk bezig met fraudebestrijding op internet. Buiten dit landelijk team aan experts is bij de Nederlandse politie op het gebied van cybercrime momenteel nog weinig expertise aanwezig.

Het aansluiting vinden bij het netwerk ter bestrijding van cybercrime is voor de politie geen gemakkelijke opgave, zo blijkt uit interviews. Een belangrijk reden is dat de politie een zwakke informatiepositie heeft: anders dan op straat heeft de politie niet overal 'oren en ogen'. Ook beschikt de politie nog beperkt over de expertise waarmee op een effectieve manier de cybercriminaliteit kan worden bestreden (Rustad, 2002). In cyberspace is de politie de enige partij die

strafrechtelijk mag handhaven. Om te kunnen handhaven is de politie echter afhankelijk van de informatie en expertise van andere partijen.

In de afgelopen jaren heeft de politie dan ook vooral geïnvesteerd in haar informatiepositie en haar expertise. Ten behoeve van haar informatiepositie heeft de politie vooral afspraken gemaakt over 'informatiedeling' met diverse netwerkpartners in haar directe omgeving. De afspraken zijn feitelijk vooral bedoeld om als politie informatie gemakkelijker te kunnen halen en informatie te krijgen over criminaliteit in cyberspace. Ook heeft de politie actief gezocht naar aanvullingen op haar eigen expertise. Zo zijn in de laatste jaren 'warme contacten' ontstaan met specialistische internetbeveiligingsbedrijven die in opdracht van de politie kunnen werken of meewerken aan strafrechtelijk onderzoek.

Het sluiten van dit soort strategische samenwerkingsverbanden en convenanten betekent feitelijk dat de politie zich niet als netwerker wil opstellen maar de ambitie heeft om een klassieke *alleingang* in de cyberspace mogelijk te maken.

In de dagelijkse praktijk blijkt de mate waarin de politie netwerkt heel persoonlijk te worden ingevuld. Duidelijker gezegd: de mate en manier van netwerken wordt bepaald door het contact op persoonlijk niveau tussen enerzijds politiespecialisten en anderzijds de specialisten van andere (private) partijen. Het gaat daarbij volgens interviews met politiemensen om 'geven en nemen' waarbij de politie vooral haar opsporingsbevoegdheid 'te geven' heeft en heel soms opsporingsinformatie die informeel gedeeld wordt.

Uit interviews met respondenten uit de bancaire sector blijkt echter dat de politie nog lang niet als volwaardig netwerkpartner wordt beschouwd. Een veelgehoorde klacht is dat de politie vaak onvoldoende capaciteit en expertise ter beschikking wil stellen om problemen met cybercrime, al dan niet samen met banken, grondig aan te pakken. Banken daarentegen hebben het gevoel dat zij veel investeren in het netwerk onder andere door het informeel uitwisselen van vertrouwelijke informatie over klanten en opsporingsinformatie uit intern onderzoek. Daarentegen reageert de politie niet of laat op verzoeken vanuit de bank om informatie of worden deze verzoeken afgewezen. Voor private partijen is de politie bovendien een organisatie waarop zij lastig grip kunnen krijgen. Onze respondenten merken een hoop argwaan vanuit de politie tegen banken. Voor banken is het vaak onduidelijk wie aanspreekpunt is en zowel het interne beleid als de organisatie zijn voortdurend aan veranderingen onderhevig. Veranderingen waarover niet of nauwelijks gecommuniceerd wordt. Tot slot vinden banken dat de politie veel te weinig doet aan het voorkomen van cybercrime. Het gevolg is dat banken veel proberen te investeren in goede persoonlijke contacten binnen de politie, bijvoorbeeld door wegkopen van rechercheurs bij de politie voor de eigen fraudeafdeling. Deze oud-politiemensen zijn 'handig' omdat zij in staat zijn om op informele basis informatie te vergaren bij oud collega's. Daarnaast kunnen zij via hun netwerk ervoor zorgen dat er meer politiecapaciteit wordt ingezet op zaken die vanuit de bank worden aangebracht.

Zeehavenpolitie

Na jaren geen contact te hebben gezocht met andere partijen in de Zeehavens zoekt de Zeehavenpolitie tegenwoordig toenadering tot de verschillende organisaties in het handhavingsnetwerk. De ervaring van de Zeehavenpolitie in de afgelopen jaren is dat het netwerken in de Rotterdamse havens niet vanzelf gaat. De politie heeft moeite om aansluiting te krijgen, vooral omdat zich tussen haar en de andere partijen in het netwerk verschillende 'barrières' bevinden die

eerst beslecht moeten worden (Hoogenboom, 2010). Ter toelichting: Hoogenboom (2010) heeft het in zijn onderzoek over zes nodale barrières: bureaucratie, verschillende juridische kaders, tegenstrijdige belangen, verschillende verantwoordelijkheden, diverse handhavingsstijlen en cultuurverschillen. Al deze barrières zorgen ervoor dat de politie niet van nature een rol speelt in het netwerk. De politie moet een *effort* leveren om hierin een rol te vervullen.

De Zeehavenpolitie probeert hoofdzakelijk invulling te geven aan het netwerken door op strategische niveau afspraken te maken over het delen van informatie. De afspraken over het delen van informatie zijn vastgelegd in verschillende convenanten. De convenanten beogen vooral de verkokering in het handhavingsnetwerk te verminderen. De toegenomen aandacht voor informatieprocessen heeft ertoe geleid dat de Zeehavenpolitie in de afgelopen jaren meer zicht heeft gekregen op de activiteiten van de andere partijen in het handhavingsnetwerk (Hoogenboom, 2010).

Het betere zicht op de activiteiten van andere partijen heeft ook ruimte geboden om op operationeel niveau meer invulling te geven aan het netwerken. Op experimentele basis heeft de Zeehavenpolitie al gebruik gemaakt van deze ruimte. Zo heeft de Zeehavenpolitie met de douane afspraken gemaakt over het samen uitvoeren van strafrechtelijke onderzoeken en analyses van trends en ontwikkelingen. Daarbuiten is in 2006 een pilot gestart waarbij de douane, Zeehavenpolitie en de Koninklijke Marechaussee samen controles hebben uitgevoerd (Hoogenboom, 2010).

Of het netwerken op operationeel niveau een 'succes' wordt blijkt vooral afhankelijk te zijn van 'chemie' op persoonlijk niveau. Pas als leidinggevende elkaar in de dagelijkse praktijk weten te vinden bestaat op operationeel niveau ruimte om écht te netwerken. Ook hiervoor geldt dat het gaat om het netwerken afhankelijk is van de mate waarin de betrokken functionarissen bereid zijn om onafhankelijk van welk convenant dan ook te geven en te nemen (Kamerstukken II, 2005-2006, 30 315, 5-6). De Zeehavenpolitie heeft volgens interviews vooral opsporingsinformatie als 'ruilmiddel' die veelal informeel gedeeld wordt omdat een juridische basis nog ontbreekt. Haar wettelijke opsporingsbevoegdheid weegt minder zwaar als ruilmiddel in dit veiligheidsnetwerk van collegahandhavers. De toezichthoudende bevoegdheid van veel van de collegadiensten is op onderdelen zelfs ruimer dan de opsporingsbevoegdheid van de zeehavenpolitie. Voor onderdelen zoals het vervoer van gevaarlijke stoffen zijn de bestuursrechtelijke sancties zelfs veel zwaarder/effectiever dan de sancties vanuit het strafrecht (Helsloot e.a., 2003).

Veiligheidshuizen

In de praktijk, zo onderkennen ook de voor dit onderzoek geïnterviewde respondenten, bestaan (grote) verschillen in organisatie, werkwijze, doelstellingen en doelgroepen van de Veiligheidshuizen. Dit komt omdat niet 'van bovenaf' in detail is voorgeschreven hoe ze ingericht dienen te worden (Rovers, 2011). Uit de bestudeerde literatuur blijkt dat de basis van de Veiligheidshuizen gevormd wordt door het openbaar ministerie, de politie, Raad voor Kinderbescherming, reclassering en de gemeente (Dammen et al. 2008). Afhankelijk van de problematiek kunnen ook andere organisaties deelnemen (zoals Bureau Jeugdzorg, verslavingszorg, jongerenwerk, HALT, etc.). Ieder van deze organisaties levert één of meerdere medewerkers aan het Veiligheidshuis. Elke vertegenwoordiger neemt vanuit zijn of haar eigen rol, taken en bevoegdheden zitting in het Veiligheidshuis. Al naar gelang de aard en omvang van de lokale problematiek nemen partijen (structureel) deel aan de overleggen binnen het Veiligheidshuis. Sommige vertegenwoordigers voeren al hun dagelijkse werkzaamheden uit vanaf hun vaste werkplek in het Veiligheids-

huis, anderen zijn er alleen op bepaalde (vaste) dagen, weer anderen nemen alleen deel aan het (voor hen relevante) casusoverleg (Dammen et al. 2008; Van Vianen et al. 2008).

Hoewel de precieze doelstelling per Veiligheidshuis (kunnen) verschillen, is het Veiligheidshuis volgens beleid en onderzoek vooral een poging om middels betere samenwerking te komen tot oplossingen voor een maatschappelijk en een organisatorisch probleem. Het maatschappelijk probleem is de structurele criminaliteit en overlast door jongeren en veelplegers. De gedachte is dat het probleem dat de daders hebben met justitie voorkomt uit diverse andere problemen zoals bijvoorbeeld werkloosheid, verslaving, gebrek aan inkomen en huisvestingsproblemen. Het organisatorisch probleem is dat er veel diensten zijn die bezighouden met het bieden van zorg op al deze aspecten maar dat samenhang moeizaam te bereiken is (waarbij de achterliggende, doch onbewezen gedachte is dat meer samenhang tot betere resultaten zal leiden) (Dammen et al. 2008.).

De dominante motivatie voor het ontstaan van de veiligheidshuizen is de wens van het openbaar ministerie om de instroom van zaken te verminderen door pre- en nietgerechterlijke interventies te promoten en daartoe andere partijen preventieve maatregelen te laten nemen. De aanwezigheid van de politie in de veiligheidshuizen geeft het OM de mogelijkheid om als 'ruilmiddel' gericht specifieke individuele gevallen door opsporing en vervolging gedurende langere tijd op te sluiten (bijvoorbeeld veelplegers) en daarmee overlast door deze individuen te verminderen. Momenteel lijken het vooral de gemeenten te zijn die energie steken in het in stand houden en 'doorontwikkelen' van de veiligheidshuizen vanuit een onderkenning dat alleen een justitiële aanpak niet werkt om sociale onveiligheid(sgevoelens) in de gemeente te beheersen.

3.3 In hoeverre en hoe sturen politiële leidinggevenden hun medewerkers met een netwerkende taak?

Cybercrime

De Nederlandse politie heeft op *strategisch* niveau veel tijd en energie geïnvesteerd in het organisatorisch versterken van haar informatiepositie binnen cyberspace. Verder maakt de politie waar nodig (en mogelijk) gebruik van de (inhuur van) expertise van andere (vooral private) partijen. Deze afspraken en initiatieven zijn het kader waarbinnen de politie wil komen tot een eigen capaciteit ten behoeve van het opsporen en handhaven van cybercrime.

Of en hoe in de praktijk invulling wordt gegeven aan het netwerken is echter bovenal afhankelijk van het persoonlijk contact tussen functionarissen. Volgens respondenten ontbreekt het momenteel aan gerichte en structurele sturing op de uitvoerders van de politiële netwerktaak in het domein cyberspace.

Zeehavenpolitie

Door strategisch manoeuvreren en het sluiten van convenanten beoogt de Zeehavenpolitie zichzelf centraler te positioneren in het complexe handhavingsnetwerk in de havens. Het gaat ook hier om een versterking van de eigen kracht, niet die van het netwerk.

Ook hier geldt echter dat het afhankelijk is van de betrokken operationeel leidinggevende of en hoe vervolgens het netwerken in de praktijk invulling wordt gegeven (Hoogenboom, 2010). Dit duidt er in onze analyse op dat het in de huidige praktijk ontbreekt aan structurele sturing op het uitvoeren van de netwerktaak.

Veiligheidshuizen

De structurele deelname van de politie aan de Veiligheidshuizen wordt 'bestuurd' door middel van formele afspraken, vaak in de vorm van samenwerkingsconvenanten (Van Vianen et al. 2008). In het convenant staan afspraken beschreven over de structurele inbreng en aansturing van de politie in het Veiligheidshuis.

In de praktijk werken de meeste Veiligheidshuizen met een stuurgroep, waarin leidinggevenden van Justitie, gemeente en de politie zijn vertegenwoordigd. De stuurgroep informeert en wordt aangestuurd door de driehoek (burgemeester, (hoofd)officier van justitie en korpschef). De operationele aansturing van (de afstemming binnen het) Veiligheidshuis vindt plaats door een ketenmanager of de coördinator Veiligheidshuis.

Volgens de in het kader van dit onderzoek geïnterviewde respondenten vindt er weinig politiële sturing plaats op de werkzaamheden die zij verrichten in het veiligheidshuis. Zo hoeven zij in het algemeen weinig verantwoording af te leggen aan de eigen organisatie over dat wat ze in het veiligheidshuis doen en afspreken met andere partijen. Wel geven de respondenten aan dat ketenpartners nog wel eens boven-over willen gaan als ze hun zin niet krijgen. Dit heeft volgens de geïnterviewde respondenten echter nooit geleid tot bijsturing of een interventie vanuit de leiding.

Een andere respondent gaf aan dat hij weliswaar weinig sturing krijgt vanuit de eigen organisatie, maar vindt wel dat er vanuit de korpsleiding voldoende interesse is voor het werk in het veiligheidshuis. Deze respondent geeft aan dat hij tweewekelijks overleg heeft met een lid van de korpsleiding om de lopende zaken door te spreken. Support vanuit de politieleiding wordt als essentieel ervaren. Een respondent: *"Ik informeer mijn chef regelmatig over wat ik doe. Niet omdat ik verantwoording wil of moet afleggen en ook niet omdat ik dan tips en adviezen krijg. Ik doe het omdat ik zo back-up kan organiseren wanneer ik er met een bepaalde partij in het veiligheidshuis niet uitkom. Soms helpt het als een lid van de korpsleiding zijn contacten bij de gemeente kan aanspreken op de problemen waar wij in het veiligheidshuis tegenaan lopen. Gemeenten werken bijvoorbeeld soms best bureaucratisch. Een telefoontje van de baas van mijn baas werkt dan als smeermiddel."*

Daarmee lijken politiële leidinggevenden weinig invloed te hebben op het dagelijkse werk van de politiële vertegenwoordiging in de Veiligheidshuizen. Relevant is de kanttekening dat we ons hier baseren op slechts drie respondenten en dat er in de literatuur niet bijzonder veel geschreven is over de sturing van politiële functionarissen in het veiligheidshuis.

3.4 Wat is de aantoonbare opbrengst van het participeren in netwerken voor de kerntaken opsporing en handhaving van de openbare orde?

Cybercrime

Bij het bestrijden van cybercrime is gebleken dat de politie maar beperkt de mogelijkheden heeft om cybercrime effectief te bestrijden. Vooral het tekort aan capaciteit en expertise maken het uitvoeren van haar rol als opsporingsinstantie en handhaver moeilijk. De politie geeft te kennen dat zij haar rol alleen kan vervullen als andere partijen haar hierbij actief ondersteunen, niet alleen omdat de capaciteit en expertise van de politie beperkt zijn maar vooral ook omdat de informatiepositie van andere partijen (banken, internetproviders, etc.) beter is. Of andere partijen ook bereid zijn om capaciteit en informatie te leveren hangt volgens respondenten weer

af van de vraag of de netwerkpartijen ook betrokken zijn bij de cybercrime. Indien het geval is, zo geven respondenten aan, dan is de bereidheid van netwerkpartijen om mee te helpen bij de opsporing vele malen groter dan wanneer netwerkpartijen zelf geen slachtoffer zijn. In alle gevallen geldt wel dat de politie hiervoor 'iets' terug moet doen zoals het delen van opsporingsinformatie.

De politie heeft in de laatste jaren vooral geïnvesteerd in haar eigen informatiepositie en expertise. Ondertussen is het aantal meldingen van de cybercrime in de afgelopen jaren alleen maar toegenomen. De eerste publicatie van het Nationaal Trendrapport Cybercrime en Digitale veiligheid bevestigt dat de pakkans in cyberspace nog altijd onveranderd klein is.

Zeehavenpolitie

De Zeehavenpolitie bevindt zich in een omgeving waarin dagelijks vele stromen aan goederen, personen en financiën op hoog tempo voorbij trekken. De politie heeft zelf maar een heel beperkt beeld van wat er gebeurt in de Rotterdamse havens. De politie heeft vooral informatie beschikbaar uit de strafrechtelijke onderzoeken, zo stellen ook respondenten. Het is onmogelijk om alleen op basis van deze informatie gericht te kunnen opsporen en handhaven in de Rotterdamse Zeehavens (Hoogenboom, 2010).

De strategische inzet op netwerken via convenanten etc. heeft dan ook vooral bijgedragen aan de algemene informatiepositie van de politie in het netwerk. Veel meer dan vroeger heeft de politie de beschikking over algemene informatie van andere inspecties en toezichthouders. Deze informatie helpt de Zeehavenpolitie volgens Hoogenboom om gerichter haar capaciteit in te zetten, waar wenselijk in samenwerking met enkele andere diensten (Hoogenboom, 2010). Of de informatie ook aantoonbaar leidt tot meer effectiviteit van de kernpolitietaken opsporing en handhaving van de openbare orde blijft onduidelijk uit de beschikbare informatie en ook onze respondenten durven hier geen uitspraken over te doen.

Veiligheidshuizen

De opbrengst van het participeren in veiligheidshuizen voor de kerntaken opsporing en handhaving openbare orde lijkt op basis van de bestudeerde literatuur minimaal te zijn. Ook de respondenten kunnen geen cijfers geven van opbrengst van het werken in het veiligheidshuis voor deze kerntaken. Een respondent: *"Als ik eerlijk ben denk ik dat de politie best zonder veiligheidshuis zou kunnen. Het is denk ik niet zo dat de politie het opeens veel drukker gaat krijgen als de veiligheidshuizen opgedoekt worden. Het is in de eerste plaats vooral de crimineel of de ex-delinquent die er voordeel bij hebben dat wij bestaan, omdat we echt proberen om te zorgen dat zij weer een redelijk normaal leven kunnen leiden. Veiligheidshuizen dienen hoofdzakelijk het maatschappelijk belang."*

Zelfs wanneer we de respondenten vragen naar hun onderbuik gevoel, dan durven ze geen uitspraak te doen over de opbrengst van het werken in het veiligheidshuis voor de kerntaken van politie, zoals bijvoorbeeld minder recidieven en daarmee minder opsporing en handhaving openbare orde. Wel noemen alle respondenten dat het werken in het veiligheidshuis heeft geleid tot meer kennis over het werk van ketenpartners en daarmee betere samenwerking.

Het empirisch onderzoek naar Veiligheidshuizen heeft zich tot nu hoofdzakelijk gericht op het intern functioneren en de maatschappelijke opbrengsten. In een zeer beperkt aantal onderzoeken wordt ook gekeken naar de (door politiemensen veronderstelde) opbrengst van het Veiligheidshuis voor de politie. In deze onderzoeken wordt gesteld dat de meerwaarde is dat de poli-

tie vaste aanspreekpunten heeft bij ketenpartners, de informatiepositie van de wijkagent verbeterd kan worden en de doorlooptijd van strafzaken wordt versneld (Van Haaf et al. 2010.).

Ook hier geldt daarmee dat de directe betekenis van het netwerk veiligheidshuizen voor de kerntaak opsporing van de politie zeer beperkt is, maar de maatschappelijke veiligheid hiermee theoretisch zeer gediend zou kunnen zijn.

In een recente literatuursynthese uit 2011 worden echer methodologische kanttekeningen gezet bij de (veronderstelde) maatschappelijke effecten van Veiligheidshuizen: *"Wat ook moeilijk uit de beschikbare studies kan worden afgeleid zijn algemene conclusies over 'waar' of 'door wie of wat' precies de resultaten worden geboekt. Zijn dit de veiligheidshuizen? De casusoverleggen die in het veiligheidshuis zijn ondergebracht (en die ook zonder veiligheidshuis kunnen functioneren)? De moederorganisatie waar het uitvoerende deel van de werkzaamheden voor het belangrijkste deel ligt? Of zijn het de toegepaste methodieken?" (*Rovers, 2011: 81).

In de literatuursynthese wordt geconcludeerd dat er alleen aanwijzingen zijn dat de Veiligheidshuizen leiden tot verbeteringen op het vlak van de uitvoering van interventies en dat er (in beperkte mate) sprake is van maatschappelijke opbrengsten op het vlak van veiligheid en het welzijn van cliënten. Dit effect wordt echter alleen bereikt wanneer veel obstakels overwonnen worden. Uit de literatuursynthese blijkt dat niet alle Veiligheidshuizen hierin slagen (Roovers, 2011). Het aantal niet succesvolle Veiligheidshuizen is echter op basis van de bestaande literatuur niet vast te stellen.

Volgens Rovers is in een deel van het onderzoek naar de effecten van Veiligheidshuizen sprake van een *sympathy bias* van de kant van onderzoekers. Volgens Rovers kan deze bias onder meer afgeleid worden uit de neiging van onderzoekers een positieve draai te geven aan negatieve uitkomsten, het benadrukken van de (nog niet gerealiseerde) potentie of het simpelweg pleiten voor de goede zaak: het Veiligheidshuis. De sympathie van onderzoekers ten aanzien van enthousiaste professionals die in een vaak ingewikkelde situatie er het beste van proberen te maken, is in een aantal onderzoeken duidelijk merkbaar aldus Rovers (2011: 82).

4. Analyse

In dit verkennende onderzoek hebben we door middel van secundaire literatuuranalyse en enkele interviews bestudeerd wat de opbrengst en betekenis is van het netwerken door de politie in de casus cybercrime, zeehavens en veiligheidsdiensten voor de kerntaken opsporing en handhaving openbare orde. Daarnaast zijn we nagegaan wat het netwerken in deze drie casus betekent voor de organisatie van de politie en dan met name de aansturing van politiële netwerkers.

Een bestudering van de netwerktheorie laat zien dat het effectief kunnen vervullen van een netwerkfunctie 'geven en nemen' betekent. Dit heeft betekenis voor de politie. Een politieorganisatie die een rol ambieert in veiligheidsnetwerken zal zich moeten openstellen voor en committeren aan de prioriteiten die vanuit deze netwerken komen. Dit betekent dat de politie niet alleen kan participeren in netwerken om haar eigen informatie- en kennispositie te verstevigen, maar ook zal moeten investeren in de noden van netwerkpartners. Dit gaat verder dan het ongestructureerd delen van informatie of het 'bijwonen' van netwerkoverleggen.

Kijkend naar de aard van de onderzochte netwerken dan valt op dat binnen het domein zeeha-

vens het netwerk vooral bestaat uit 'collega overheidshandhavers' en dat er nauwelijks sprake is van samenwerking met private partijen. Binnen cyberspace bestaat het netwerk van de politie uit grote aanbieders van diensten via internet (die zowel 'slachtoffer' kunnen zijn van cybercrime als 'opspoorder' vanwege hun bijzondere kennis en zelfs 'handhaver' door het niet meer ter beschikking stellen van die diensten). De beleidsmatige keuze lijkt in beide gevallen te zijn om netwerkpartners te kiezen die beoogd (vooral) de (informatie)positie van de politie versterken als *zelfstandige* handhaver. Het netwerk 'Veiligheidshuis' bestaat uit ten minste de politie, het OM en de gemeente aangevuld met andere justitiële partners en aanbieders van sociale- en medische zorg.

Binnen de netwerken zeehavens en cyberspace is zichtbaar dat de politie vooral haar eigen belang probeert te waarborgen en zich nadrukkelijk niet lijkt bezig te houden met de belangen van andere netwerkpartners, laat staan het gedeelde belang.

- Op strategisch niveau worden daartoe convenanten gesloten over informatiedeling (door andere organisaties naar de politie toe). Fraai zichtbaar is dat in cyberspace waar de politie niet inzet op het zo effectief mogelijk organiseren van de capaciteiten van netwerkpartners maar de 'concurrentie' aangaat door het oprichten van een eigen 'hightech crime unit'.
- Op operationeel niveau wordt het netwerken vooral ingevuld afhankelijk van individuele politiefunctionarissen die tegen het formele politienetwerkbeleid in 'geven en nemen' in hun eigen netwerk. In beide casus is het informeel delen van opsporingsinformatie een belangrijk onderdeel van het 'geven'. Voor de cyberspace geldt aanvullend dat (gepercipieerde) 'opsporingsbevoegdheden' soms een aanvullend ruilmiddel zijn.

In de casus veiligheidshuizen is zichtbaar dat mede door de afwezigheid van landelijk geldende voorschriften de politie per Veiligheidshuis bepaalt in welke mate en op welke wijze zij participeert in de verschillende netwerken. Binnen de veiligheidshuizen wordt de politie vooral 'ingezet' door het openbaar ministerie dat de veiligheidshuizen als een middel ziet om de instroom van zaken op het terrein van veelplegers en jeugdcriminaliteit te verminderen. Deze inzet past overigens goed bij de 'klassieke' opvatting van de 'maatschappelijke' politie dat preventie loont. Het belang van de politie om in deze netwerken te opereren is onduidelijk en lijkt nog weinig specifiek te zijn onderzocht.

5. Conclusie

In de casus cybercrime en zeehavens trekken wij uit de literatuur en de interviews de conclusie dat het netwerken leidt tot persoonlijke relaties die de politie (soms) voorzien van noodzakelijke informatie op basis waarvan opsporing kan worden ingezet. In ruil hiervoor wordt opsporingsinformatie gedeeld.

Dit is niet conform het officiële politiebeleid dat vooral gericht is op 'nemen uit' het netwerk en niet wil 'geven aan' het netwerk. Binnen de politie lijkt een sterke voorkeur te bestaan om te netwerken met publieke organisaties. De politie lijkt terughoudend in het netwerken met private partijen. De politie is daarmee momenteel geen volwaardige netwerkspeler.

In de casus van de veiligheidshuizen is er volgens de literatuur nog geen enkel maatschappelijk effect aangetoond. Wij zien geen reden om anders te veronderstellen voor het effect voor de kerntaken opsporing en handhaving openbare orde van de politie.

De analyse van de aansturing van de politienetwerkers op operationeel niveau met betrekking tot hun netwerkende taken kan kort zijn: een dergelijke aansturing lijkt niet aanwezig te zijn. In alle drie de behandelde casusdomeinen is de centrale observatie dat 'alles afhangt van de betrokken politiemedewerker'.

Literatuur

Agranoff, R., en McGuire, M. (1999). Managing in network settings. Policy studies Review. 16 (1), pp. 19-40.

Boutellier, J.C.J. (2007) Nodale orde. Veiligheid en burgerschap in een netwerksamenleving. Vrije Universiteit: Amsterdam.

Dammen, R., Van der Varst, L.P., Bervoets, E., Dobbelaar, J., Van Bolhuis, V.J., Luiten, T. (2008). Quick scan veiligheidshuizen. COT Instituut voor Veiligheids- en Crisismanagement, Den Haag.

De Bruijn, H. en Ten Heuvelhof, E. (2007). Management in netwerken. Over veranderen in een multi-actorcontext. Lemma, Den Haag.

Furnell, S. (2003). Cybercrime: vandalizing the information society. Web Engineering. 2722, pp. 333-365.

Helsloot, I., Muller, E., Pieterman, R., en Voermans, W.J. (red)(2003). Vervoer gevaarlijke stoffen in perspectief. Evaluatie van de Wet vervoer gevaarlijke stoffen 1996-2002. Boom Juridische Uitgevers, Den Haag.

Hoogenboom, A.B. (2009). Dingen veranderen en blijven gelijk. Justitiële Verkenningen. 35 (februari), 63-77.

Hoogenboom, A.B. (2010). Politie in de netwerksamenleving. De havens in Rotterdam. Stichting Maatschappij, Veiligheid en Politie, Dordrecht.

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

Kickert, W., Klein, E.H., en Koppenjan, J.F.M. (red.) (1997). Managing complex networks: Strategies for the public sector. Londen: Sage.

Luykx, F. Grapendaal, M. (1999). Justitie in de buurt: Een evaluatie van vier experimenten. Den Haag: WODC.

Projectgroep Visie op de politiefunctie (2005) Politie in Ontwikkeling. Visie op de politiefunctie. Den Haag: NPI.

Provan, K.G., en Milward, B.H. (2001). Do networks really work? A framework for evaluating public-sector organizational networks. Public Administration Review. 61 (4), 414-423.

Rhodes, R.A.W. (2007). Understanding Governance: Ten Years On. Organization Studies. 28, pp. 1243-1264.

Rovers, B. (2011). Resultaten van veiligheidshuizen. Een inventarisatie en evaluatie van beschikbaar onderzoek. BTVO – Bureau voor toegepast veiligheidsonderzoek, 's-Hertogenbosch (in opdracht van het WODC).

Rustad, M.L. (2002). Private enforcement of cybercrime on the electronic frontier. Southern California Interdisciplinary Law Journal. 11, pp. 63-116.

Stol, W.Ph. (2004). Trends in cybercrime. Justitiele Verkenningen. 30 (8), 76-94.

Terpstra, J. (2008). Wijkagenten en hun dagelijks werk: Een onderzoek naar de uitvoering van gebiedsgebonden politiewerk. Commissie Politie en Wetenschap, Apeldoorn.

Terpstra, J. & Kouwenhoven, R. (2004) Samenwerken en netwerken in de lokale veiligheidszorg. Enschede, IPIT.

Thomson, A.M., en Perry, J.L. (2006). Collaboration Processes: Inside the Black Box. Public Administration Review. 66(s1), pp. 20-32.

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

Van Stokkom, B., en Terpstra, J. (2006). Probleemgericht werken in lokale veiligheidsnetwerken. In: P.L. Meurs, E.K. Schrijvers, G. De Vries. (red). Leren van de praktijk. Gebruik van lokale kennis en ervaring voor beleid. Amsterdam University Press, Amsterdam.

Van Vianen, R.T. Hoogeveen, C. Slump, G.J., Maaskant, G.M, Persoon, A.M. (2008). Evaluatie Justitie in de Buurt Nieuwe Stijl: Verbindende netwerken in de veiligheidshuizen. Woerden/Den Haag. Van Montfoort/WODC.

Wood, J. & Shearing, C. (2007). Imagining security. Cullompton: Willan.

Contact details

Ira Helsloot
Nijmegen School of Management
P.O. Box 9108
6500 HK Nijmegen
The Netherlands
Tel. +31 24 361 2891
E-mail: i.helsloot@fm.ru.nl

More information about the working paper series is available at the website of the Institute for Management Research: **www.ru.nl/imr**