DE NODALE ORIËNTATIE VAN DE NEDERLANDSE POLITIE:
OVER CRIMINALITEITSBESTRIJDING IN DE NETWERKSAMENLEVING

BOUWSTENEN VOOR EEN BELEIDSTHEORIE

Victor Bekkers
Arie van Sluis
Peter Siep

ERASMUS UNIVERSITEIT ROTTERDAM
CENTER FOR PUBLIC INNOVATION
BURGEMEESTER OUDLAAN 50
ROTTERDAM, DECEMBER 2006

INHOUDSOPGAVE

1 INLEIDING

1.1 Aanleiding

Het regiokorps Amsterdam-Amstelland heeft in de afgelopen twee jaren vergevorderde plannen ontwikkeld die zich richten op het instellen van een 'controlepolitie'. Deze politie gaat zich vooral bezighouden met het systematisch scannen van de (verkeers)infrastructuur op de aanwezigheid van wetsovertredingen en wetsovertreders. Deze nieuwe functie wordt ook wel de nodale politie genoemd. Het stelselmatig monitoren en controleren van stromen van mensen en goederen op uiteenlopende locaties en niveaus neemt daarbij een centrale plaats in. Een cruciale rol is daarbij weggelegd voor 'intelligente' surveillance op basis van software die gevoed moet worden met informatie uit politie- en andere systemen over onder meer relevante daders en dadergroepen.

Inmiddels heeft ook de Raad van Hoofdcommissarissen in haar Visiedocument 'Politie in ontwikkeling' deze gedachte overgenomen en tot een van haar speerpunten gemaakt. Zij spreekt in dit verband over de nodale oriëntatie van de politie die echter verder gaat dan het controleren van de personen en goederenstroom die gebruikt maken van de verkeersinfrastructuur. De nodale oriëntatie van de politie richt zich in deze visie vooral op het uitoefenen van controles die gericht zijn op het ontanonimiseren en het identificeren van kwaad op de knooppunten van de infrastructuur. Het bijzondere aan het visiedocument is dat de politie haar positie nadrukkelijk tracht te bepalen in het licht van een aantal kenmerken van de netwerksamenleving, die vanuit het oogpunt van de politie bedreigingen maar ook kansen kan bieden.

Op voorhand kan worden gesteld dat deze invulling van de 'nodale oriëntatie' uniek is. Wie mocht denken dat het begrip nodale politie een keurige vertaling is van het internationaal klinkende 'nodal policing' komt bedrogen uit. Beiden hebben weinig met elkaar te maken. Een zoektocht op internet, daarbij gebruik makende van de zoekmachine Google, levert bij het begrip 'nodal policing' 14.000 hits op. Veel daarvan verwijzen naar 'nodal police stations' (bijvoorbeeld in Tokio) of 'nodal police officers'. Hiermee wordt doorgaans verwezen naar de politie als een soort buurtregisseur, een politieagent met een netwerkfunctie, of doorverwijsfunctie. In meer wetenschappelijke bronnen wordt 'nodal policing' in verband gebracht met begrippen als 'police governance', 'security networks' en 'the hollowing of the state'. Daarbij wordt deze politie vooral gezien als een van de vele knooppunten binnen veiligheidsnetwerken, waarbij politietaken door ook andere organisaties dan de politie ter hand worden

genomen. Een voorbeeld is Clifford Shearing, een bekend politieonderzoeker, die in dit verband doelt op de toenemende pluralisering en ontstatelijking van de politie en daarmee samenhangende de opkomst van allerlei vormen van private politie, hetgeen allerlei sturings- en legitimiteitsvraagstukken oproept. De Nederlandse uitwerking van het begrip gaat echter een heel andere kant op.

1.2 Doel- en probleemstelling

Doelstelling van het onderzoek is het uitwerken van het concept 'nodale oriëntatie' van de politie om vervolgens beter in kaart te kunnen brengen wat de potentiële meerwaarde van dit concept is, alsmede inzicht te krijgen in de te verwachten condities waaronder deze meerwaarde kan worden gerealiseerd. Belangrijk is om aandacht te vragen voor de verschillende soorten van veronderstellingen die aan dit concept ten grondslag liggen (de zogenaamde beleidstheorie). Veronderstellingen die verwijzen naar de volgende vragen.
Voor welke problemen is de nodale oriëntatie van politie een oplossing? Welke soort van instrumenten cq. interventiestrategieën zijn nodig om deze nodale oriëntatie daadwerkelijk te kunnen ondersteunen? En, tenslotte, welke normatieve vraagstukken roept de nodale oriëntatie op? Beantwoording van de laatste twee vragen maakt het mogelijk om tevens inzicht te krijgen in de soort van implementatieagenda die de nodale oriëntatie oproept en de onderwerpen die geadresseerd moeten worden. Op grond hiervan kan de volgende vraagstelling worden geformuleerd:

Wat zijn de aannames ('de beleidstheorie') achter het concept van de nodale oriëntatie van de politie, wat zijn relevante toepassingsmogelijkheden en onder welke te verwachten condities zou deze nodale oriëntatie gerealiseerd kunnen worden?

Dit leidt tot de volgende relevante deelvragen:

a) *Waarop berust het concept van de nodale oriëntatie van de politie, wat zijn achterliggende aannames en wat is de relatie of verwantschap met andere concepten zoals tegenhouden?*
b) *Welke toepassingen van deze nodale oriëntatie zijn denkbaar en waarop hebben deze betrekking?*
c) *Wat zijn de te verwachten condities (bijv. menskracht, expertise, ICT, bevoegdheden) waaronder deze toepassingen gerealiseerd kunnen worden, wat zijn mogelijke effecten en mogelijke kritische succes- en faalfactoren?*

Alvorens deze vragen te beantwoorden is het zinvol om preciezer in kaart te brengen wat de nodale oriëntatie van de politie precies inhoudt. Een eerste bron van inspiratie is het visiedocument ' Politie in Ontwikkeling', waarin deze notie uitgebreider voor het

voetlicht is gebracht. Wat is de beleidstheorie die volgens de opstellers van het visiedocument ten grondslag ligt aan de nodale oriëntatie?

1.3 Nodale oriëntatie van de politie als handelingstheorie

In veel gevallen kan beleid of kunnen beleidsmatige concepten worden gezien als een poging om een bepaald probleem op te lossen. Volgens bestuurskundigen neemt de kans hierop toe, indien aan een beleid een zogenaamde beleidstheorie ten grondslag ligt (Hoogerwerf, 1987).

1.3.1 Veronderstellingen achter beleid

De ontwikkeling van een beleidstheorie kan daarom worden gezien als een poging om via een ex-ante evaluatie zicht te krijgen op de vraag of het te voeren beleid tot succes zal leiden. Volgens Hoogerwerf (1987) speelt daarin een, min of meer samenhangend, stelsel van veronderstellingen of aannames een rol. Daarbij gaat het om drie typen van veronderstellingen:

- causale veronderstellingen, die verwijzen naar de relatie tussen de in het geding zijnde oorzaken van een probleem en de gevolgen die dit probleem oproept. In dit onderzoek gaat het om de vraag welke oorzaken ten grondslag liggen aan het probleem waarop de nodale politie een antwoord is. Bijvoorbeeld, wat is de aard van de netwerksamenleving en de stromen en knooppunten in deze netwerksamenleving en op welke wijze maakt de criminaliteit hiervan gebruik?

- finale veronderstellingen verwijzen naar de mate waarin de inzet van bepaalde middelen daadwerkelijk zal leiden tot de realisatie van de gestelde doelstellingen. In dit onderzoek gaat het dan primair om twee vragen. Ten eerste gaat het om de vraag of, en onder welke condities, de nodale politie als instrument een effectieve en efficiënte bijdrage kan leveren aan de doelstellingen die de politie zich heeft gesteld en de functies die zij wil uitoefenen; en in het verlengde daarvan ook aan de oplossing van bepaalde maatschappelijke problemen, in dit geval criminaliteit. Ten tweede gaat het om de vraag of de instrumenten die de nodale politie wil inzetten daadwerkelijk bijdragen aan de doelstelling van de nodale politie: het uitoefenen van controles die gericht zijn op het ontanonimiseren en het identificeren van kwaad op de knooppunten van de infrastructuur. Zo wordt in het visiedocument vooral vertrouwd op de zegeningen van de technologie, bijvoorbeeld daar waar het gaat om 'catch-ken' technieken. Ook wordt veel

belang gehecht aan samenwerking. Belangrijk is tevens de vraag naar de condities waaronder deze instrumenten effectief en efficiënt kunnen worden ingezet.

- normatieve veronderstellingen, die verwijzen naar relevante politieke waarden die in het geding zijn en de afweging ('trade offs') tussen deze waarden teneinde ervoor te zorgen dat een beleidsprogramma als legitiem wordt ervaren. Wat is bijvoorbeeld de legitimiteit van een nodale oriëntatie van de politie, gelet op de vrijheid die burgers – met name in termen van een mogelijke schending van de persoonlijke levenssfeer – moeten inleveren in relatie tot de bescherming en de veiligheid die het concept van de nodale politie pretendeert te hebben?

Terecht heeft Ringeling (1987) erop gewezen dat het denken in termen van beleidstheorieën niet moet worden gezien als de ontwikkeling van wetenschappelijke theorieën voor beleid. Beleidstheorieën moeten veeleer worden gezien als handelingstheorieën. Kenmerkend voor een handelingstheorie is dat gebruik wordt gemaakt van theoretische/wetenschappelijke en op ervaring gebaseerde inzichten die kunnen helpen bepaalde beleidsconcepten te onderbouwen. In dat licht willen wij dit onderzoek dan ook vooral plaatsen, hetgeen ook gevolgen heeft voor de werkwijze die we in dit onderzoek volgen (zie paragraaf 1.4).

1.3.2 Veronderstellingen achter de nodale oriëntatie

In het veiligheidsconcept dat in 'Politie in Ontwikkeling' wordt gehanteerd, is de geografische ruimte waarbinnen de politie een aantal functies uitoefent, onderverdeeld in woongebieden (wijken in de stad, dorpen), de open ruimte daarbuiten en de infrastructuur (p. 83). De nodale oriëntatie van de politie heeft vooral betrekking op het uitoefenen van controles, die gericht zijn op het ontanonimiseren en het identificeren van kwaad op de knooppunten van de infrastructuur. De intensiteit van deze controles neemt toe, naarmate het schaalniveau van de infrastructuur hoger is (p.83). Daarbij wordt de infrastructuurverdeeld in verschillende niveaus:

- de intrastedelijke infrastructuur zoals doorgaande routes in de stad;
- de interstedelijke infrastructuur zoals het nationale wegennet;
- de internationale infrastructuur, bijvoorbeeld het Europese wegennet, het internationale luchtverkeer); en
- de virtuele infrastructuur(bijvoorbeeld computernetwerken).

Wat zijn de veronderstellingen achter dit concept zoals die door de opstellers van het visiedocument worden verwoord?

Causale veronderstellingen

De ontwikkeling van deze nodale oriëntatie dient te worden begrepen in het licht van een aantal maatschappelijke en technologische ontwikkelingen die ook hebben bijgedragen aan een veranderend crimineel gedrag. Ontgrenzing, mobiliteit en anonimiteit staan daarin centraal. Deze ontwikkelingen staan haaks op de traditionele organisatie van veiligheid die vooral gericht is op begrenzing, waarbij criminaliteitsbestrijding zich vooral afspeelt binnen een stad of een land; dit alles in combinatie met het koppelen van een bepaalde identiteit aan een bepaalde (woon)plaats. Internationaal opererende criminele organisaties trekken zich echter niets aan van allerlei internationale grenzen, zijn uiterst mobiel en maken optimaal gebruik van de anonimiteit die een open en complexe samenleving biedt. Tegelijkertijd bieden ook allerlei technologische ontwikkelingen nieuwe controlemogelijkheden, terwijl tegelijkertijd ook de bevoegdheden om te kunnen controleren de afgelopen jaren zijn toegenomen (p. 84-85). Om deze ontwikkeling te begrijpen wordt een uitstapje gemaakt naar de theorievorming over de informatiesamenleving of de netwerksamenleving.
Het interessante is dat de transformatie van de industriële samenleving naar de informatiesamenleving niet alleen het belang laat zien van informatie en informatietechnologie, maar dat ook het begrip ruimte van karakter is veranderd. Voor de politie is dit van belang, omdat de Nederlandse politie altijd sterk gericht is geweest op een gebiedsgebonden aanpak, waarbij 'kennen' en 'gekend worden' binnen dit gebied een belangrijk principe was (p. 85). Volgens de opstellers van het rapport moet hieraan een nieuwe dimensie worden toegevoegd.

Kenmerkend voor de informatiesamenleving is dat de dominante processen in onze hedendaagse samenleving steeds meer bepaald worden door stromen van mensen, goederen, geld en vooral informatie. Dit geldt ook voor als onwenselijk bestempelde verschijnselen in termen van criminaliteit en terreur. Hierdoor ontstaat een stromenland (de door de opstellers aangehaalde socioloog Castells noemt dit 'spaces of flows') waarin bepaalde fysieke locaties (volgens Castells 'space of places') nog steeds een belangrijke ontmoetingsplaats zijn waar mensen wonen en werken (zoals een wijk, een stad of een vliegveld). Maar deze leefruimte wordt in toenemende mate beïnvloed door het stromenland. De wisselwerking tussen leefruimte en stromenland beïnvloedt in toenemende mate de soort van onveiligheid die wordt ervaren, maar biedt tegelijkertijd ook aanknopingspunten voor de bestrijding ervan (p.85).
In het licht van deze ontwikkelingen wordt een pleidooi gehouden voor de ontwikkeling van een aanvullende oriëntatie: het hebben van meer aandacht voor stromen en de plaatsen waar deze stromen bij elkaar komen, de zogenaamde knooppunten (ook wel 'nodes' genoemd). De infrastructuur in al zijn gedaanten wordt daarmee het nieuwe aangrijpingspunt: wegennet, vaarwater, luchthaven en communicatienetwerken. Mensen, goederen, geld en informatie verplaatsen zich immers door gebruik te maken

van de infrastructuur en genereren daarmee tegelijkertijd stromen. Daar waar deze stromen bij elkaar komen, liggen voor de politie interessante interventiekansen (p.87).

Finale veronderstellingen

Door niet alleen aanwezig te zijn op plaatsen maar ook op stromen kan het afnemende handelingsvermogen bij de overheid door de opkomst van de informatiesamenleving worden gecompenseerd. Het verlies van dit handelingsvermogen komt deels voor rekening van allerlei technologische ontwikkelingen. Tegelijkertijd bieden deze technologische ontwikkelingen ook een antwoord op bovenstaande uitdagingen. Dit geldt zeker voor de controle op fysieke stromen (infrastructuur en knooppunten) en de controle op (virtuele) informatiestromen. De idee is dat de veiligheid van plaatsen in toenemende mate kan worden geborgd door meer controle in stromenland. Twee voorbeelden worden genoemd als onderbouwing. Een gebiedsgebonden benadering van ramkraken door Oost-Europese criminele organisaties is gedoemd te mislukken zonder aanvullende aandacht voor de infrastructuur. Een ander voorbeeld is dat een succesvolle aanpak van terrorisme alleen maar mogelijk is door de koppeling van plaatsgebonden vormen van signalering in de wijk met relevante, soms wereldwijde stromen van mensen, goederen, geld en informatie (p.86).

Deze gedachtegang wordt ook wel de nodale oriëntatie van de politiefunctie genoemd, dit in tegenstelling tot de locale oriëntatie. In operationele zin gaat het dan om het toezicht houden op de infrastructuur en de stromen van mensen, goederen en geld die zich over deze infrastructuur verplaatsen. Daartoe controleert de politie op knooppunten van de netwerken (ringwegen rond steden, overslagpunten, havens, luchthavens) van uiteenlopende geografische schaal en van verschillende aard (stedelijk, interstedelijk, interstatelijk en virtueel). De controlefunctie is derhalve gericht op het opheffen van de anonimiteit en onzichtbaarheid en het identificeren van het 'kwaad' in de vorm van potentiële en actuele bedreigingen van de veiligheid. De controlefunctie is bovendien meer gericht op personen of groepen van personen dan op delicten. Dat betekent onder meer dat de onderverdeling in specialismen (bijvoorbeeld voertuigveiligheid, alcohol in het verkeer, verkeersovertredingen) minder interessant wordt ten gunste van controles gerichte op de breedte van het vakgebied. Naar verwachtingen zal ook technologie steeds belangrijker worden. Daarbij denkt men vooral aan hightech toepassingen zoals catch-ken technieken, waarbij waarnemingen en registraties van personen en voertuigen worden vergeleken met uiteenlopende databases (bijvoorbeeld openstaande boetes, gestolen voertuigen, vermiste kentekenplaten, bekende verdachten) (p.90). Kortom, in de nodale oriëntatie gaat het dus om ontanonimiseren, het onderscheppen van kwaad en om tegenhouden, daarbij ontgrenzing en mobiliteit als uitgangspunt nemend (p.86,87, 90).

Verder wordt naar voren gebracht dat een oriëntatie op de infrastructuur grote mogelijkheden biedt voor interregionale en internationale samenwerking van de politie en voor samenwerking tussen de politie en andere bijzondere opsporingsdiensten.

Tot slot wordt een aantal randvoorwaarden genoemd die in acht moeten worden genomen, zijnde (p. 91-95):

- het belang van informatiegestuurd werken, waarbij het opsporingsproces meer gekoppeld wordt aan het informatieproces teneinde de informatiepositie van de politie te versterken, zodat meer informatie eerder en beter en op een meer intelligente manier voor allerlei uiteenlopende strategische, tactische en operationele doelen kan worden gebruikt;
- het belang van een betere landelijke en internationale informatie-uitwisseling binnen de politieorganisatie en de diverse onderdelen die daarin te onderscheiden zijn maar ook met andere opsporings- en handhavingsorganisaties;
- heldere verantwoordelijkheden en bevoegdheden; en
- een gedeeld veiligheidsconcept tussen alle betrokken partners, waarin duidelijkheid bestaat over de intenties en een gedeeld beeld van adequaat optreden.

Normatieve veronderstellingen

Daarnaast willen we ook nog aandacht schenken aan de wijze waarop de opstellers van het visiedocument aankijken tegen de maatschappelijke en politieke legitimatie van dit concept. Immers, de realisatie ervan kan ingrijpende consequenties hebben voor de persoonlijke levenssfeer van burgers. De opstellers verwachten dat de bevoegdheden in stromenland uitgebreider kunnen zijn dan in de leefomgeving, zonder dat de maatschappelijke legitimering van de politie wordt aangetast. (p. 86). De bevoegdheden op de infrastructuur zijn dan het wisselgeld in een sociaal contract, waarbij tegenover de enorm toegenomen vrijheid van burger enkele andere, cruciale bevoegdheden staan. Aanwezigheid van de politie in stromenland voorkomt, aldus de opstellers, dat buitenproportioneel inbreuk wordt gemaakt op de persoonlijke levenssfeer, bijvoorbeeld met het oog op de bestrijding van terreur.

De aantasting van privacy varieert met het schaalniveau van het netwerk waarop van bepaalde bevoegdheden gebruik wordt gemaakt (p. 91). Op het lage schaalniveau, bijvoorbeeld intrastedelijk, is de anonimiteit relatief laag ('kennen en gekend worden') en zal de inzet van de bevoegdheden van de politie beperkt zijn, waarbij de privacy beter beschermd is. Naarmate het schaalniveau hoger is en de anonimiteit toeneemt, kan de politie zwaardere bevoegdheden en middelen inzetten en zal de bescherming van de privacy minder zijn, zonder dat dit tot grote weerstand hoeft te leiden. Immers, zo wordt verondersteld, niemand staat verbaasd op Schiphol te kijken als men bij de 'poortjes' de jas en schoenen moet uittrekken (p.91).

In ons onderzoek gebruiken we de inzichten uit 'Politie in Ontwikkeling' als een eerste aanzet tot de ontwikkeling van een beleidstheorie voor de nodale oriëntatie. Dit onderzoek heeft niet de intentie deze beleidstheorie te toetsen. Het gaat vooral om een verdere beleidsmatige uitwerking van de 'oriëntatie', waarbij nadrukkelijk andere inzichten en ervaringen worden meegenomen.

1.4 Werkwijze en opzet

Om inzicht te krijgen in de vraag voor welke problemen de nodale oriëntatie een mogelijk antwoord zou kunnen zijn, zal eerst een verkenning plaats vinden van een aantal sociologische, technologische, criminologische, politicologische en juridische leerstukken en inzichten; inzichten die iets zeggen over de veranderende aard van onze samenleving en de wijze waarop de criminaliteit zich binnen onze samenleving ontwikkelt, alsmede de normatieve kaders die hierop van toepassing zijn, met het oog op de legitimering van het concept. Op deze manier trachten we meer inzicht te krijgen in de verschillende soorten (causale, finale en normatieve veronderstellingen) die achter het concept verscholen zitten. In hoofdstuk drie worden deze aannames inzichtelijk gemaakt en verder uitgewerkt. Daarmee wordt de eerste vraag uit de probleemstelling beantwoord. Tevens trachten we telkens aan te geven in hoeverre de door ons aangereikte leerstukken en inzichten bouwstenen bevatten voor een verdere ontwikkeling van het concept van de nodale oriëntatie. Deze verkenning heeft plaats gevonden door gebruik te maken van literatuuronderzoek, documentenonderzoek en het houden van verkennende diepte-interviews met vijf experts binnen de wereld van politie, justitie, criminologie en veiligheidswetenschap.

Vervolgens willen we vooral kijken naar de manifestatie van de nodale oriëntatie in de bestaande praktijk van de politie en naar praktijken buiten de politie (bijvoorbeeld andere opsporingsdiensten), die een sterke verwantschap vertonen met de nodale oriëntatie. Met name staat de vraag centraal, of en onder welke condities, de nodale oriëntatie als interventiestrategie en de middelen die in dat verband worden ingezet, een effectieve en efficiënte bijdrage hebben geleverd aan het ontanonimiseren en onderscheppen van ongewenst gedrag binnen een knooppunt of binnen een stroom. In hoofdstuk vier wordt deze exercitie uitgevoerd en daarmee wordt tevens de tweede en derde vraag uit de probleemstelling beantwoord. Meer in het bijzonder worden de volgende verkenningen van een aantal nodale manifestaties ter hand genomen:

a) vormen van digitale recherche, gericht op computercriminaliteit en het gebruik van het internet ter ondersteuning van crimineel en/of terroristisch gedrag;
b) de monitoring van groepen van voetbalvandalen en het (preventief) ingrijpen in relatie tot risicowedstrijden;

c) de monitoring van verkeersbewegingen en verkeersstromen op en rondom knooppunten, bijvoorbeeld door camerabewaking en catch-ken technieken, zoals thans geschiedt in de Hoeksche Waard;
d) vormen van financiële recherche, gericht op bijvoorbeeld het opsporen van crimineel geld en het witwassen van dit geld, of fraude in het betalingsverkeer zoals creditcardfraude, waarvan de opsporing ter hand wordt genomen door de FIOD en/of door de banken zelf;
e) de opsporing van drugs- en andere vormen van smokkel in bijvoorbeeld havens door gebruik te maken van risicoanalyses en risicoprofielen zoals thans al plaats vindt in de havens van Rotterdam;
f) de elektronische identificatie van risicovolle passagiers en ladingen op Schiphol.

De voorbeelden a t/m c zijn voorbeelden die gelokaliseerd zijn binnen de politie, terwijl de voorbeelden d t/m f betrekking hebben op voorbeelden buiten de politiewereld waarbij andere publieke en private opsporingsorganisaties een leidende rol vervullen. In het kader hiervan hebben diepte-interviews plaats gevonden met ervaringsdeskundigen binnen de onderzochte cases en zijn relevante documenten bestudeerd.

Tenslotte wordt in hoofdstuk 4 de balans opgemaakt en wordt op hoofdlijnen een uitwerking geven van een mogelijke beleidstheorie voor de nodale politie en de condities waaronder deze gerealiseerd zou kunnen worden.

2 AANNAMES ACHTER DE NODALE ORIËNTATIE

2.1 Inleiding

In dit hoofdstuk gaat het om de vraag, voor welke problemen en maatschappelijke ontwikkelingen de nodale politie een antwoord is. Hoe zien die ontwikkelingen eruit? Wat betekenen ze voor de inhoud van het concept van de nodale oriëntatie? Door deze vragen te beantwoorden zijn we in staat om de aannames achter het concept beter te begrijpen en deze verder uitwerken. We richten ons op een aantal relevante causale, finale en normatieve veronderstellingen die achter het concept verscholen gaan. Om deze veronderstellingen inzichtelijk te maken, maken we gebruik van een aantal (in onze ogen relevante) sociologische, criminologische, technologische en politicologisch-juridische leerstukken. Telkens zullen we per paragraaf aangeven wat de implicaties van deze leerstukken zijn voor de verdere ontwikkeling van het concept van de nodale oriëntatie.

2.2 Sociologische verkenningen: over de anatomie van de netwerksamenleving

De netwerksamenleving moet worden begrepen als de uitkomst van een transformatie, waarbij met name de aard van het productieproces in de industriële samenleving fundamenteel is veranderd. Wat zijn de kenmerken van dit transformatieproces? Het is immers dit transformatieproces, zoals dit onder meer door Castells (1996, 1997, 1998) is beschreven, dat ervoor gezorgd heeft dat de politie andere strategische accenten moet zetten. In het visiedocument 'Politie in Ontwikkeling' wordt bijvoorbeeld nadrukkelijk verwezen naar de idee van de samenleving als een 'stromenland' als inspiratiebron voor de nodale oriëntatie. We volgen daartoe het spoor dat door Castells is getrokken. Daarnaast willen we tevens aandacht vragen voor een ander belangrijk perspectief op de netwerksamenleving, namelijk dat van de kwetsbaarheid van de netwerksamenleving zoals dat vooral tot uitdrukking komt in Becks notie van de risicosamenleving (Beck, 1999).

2.2.1 Kenmerken van de netwerksamenleving

De netwerksamenleving is een samenleving geworden waarin informatie en kennis de belangrijkste grondstof zijn geworden voor de productie van diensten en in mindere mate van goederen. Diensten in de netwerksamenleving zijn primair door informatie en kennis voortgedreven diensten, terwijl de producten die worden aangeboden in essentie producten zijn waarbij informatie en kennis wordt verschaft of waarvoor kennis en informatie nodig is om ze op hun waarde te kunnen schatten. Dit geldt

bijvoorbeeld voor de diensten en producten in de bank en verzekeringswereld, in de wereld van het onroerend goed, de consultancy, de advocatuur, in de marketing en de pr. Als we bijvoorbeeld kijken naar het functioneren van de kapitaalmarkt, dan zien we dat het merendeel van de activiteiten die daar plaats vinden alleen maar gericht is op het verzamelen, bewerken en verwerken, distribueren en interpreteren van informatie: informatie over koersen, over marktontwikkelingen, over tussentijdse winst en verliescijfers, deelnemingen, fusies etc. Werk dat bijvoorbeeld beursanalisten doen. Maar ook in de wereld van de logistiek, waar bijvoorbeeld schepen en vrachtwagens goederen vervoeren, blijkt dat kennis en informatie over de logistieke keten en de schakels daarin van onschatbare waarde is om als producent en distributeur effectief te kunnen opereren. Kortom, heel veel processen in ons dagelijks bestaan zijn gericht op het ontginnen, verwerken, bewerken, veredelen en distribueren van kennis en informatie, hetgeen allerlei informatiestromen tussen organisaties genereert. ICT speelt hierin een steeds belangrijkere rol, temeer daar deze kennis en informatie gedigitaliseerd kan worden en daardoor gemakkelijker getransporteerd en gemanipuleerd kan worden. In het voetspoor hiervan zien we ook nieuwe producten ontstaan, namelijk informatieproducten, die gericht zijn op het kopen en verkopen van informatie, zoals bijvoorbeeld marketinginformatie of beursinformatie.

Globalisering

Deze informatiestromen zijn mede het resultaat van het feit dat onze samenleving een hypergefragmenteerde en georganiseerde samenleving is, waarbij organisaties - mede op grond van allerlei schaalvoordelen – slechts gespecialiseerde taken voor hun rekening nemen. Het gevolg is dat tussen deze organisaties een intensief ruilverkeer tot stand komt, terwijl tegelijkertijd de wederzijdse afhankelijkheid tussen de organisaties alleen maar toeneemt. De omvang en intensiteit van dit ruilverkeer neemt nog verder toe, omdat onze moderne productie- en consumptiepatronen een wereldwijd karakter hebben, terwijl het vermogen om 'realtime' te kunnen werken op wereldschaal steeds belangrijker wordt. Globalisering is daarom een van de belangrijkste kenmerken van de netwerksamenleving, zowel in termen van arbeidsdeling als in termen van concurrentie. ICT wordt vooral ingezet om de noodzakelijke verbindingen tussen organisaties te realiseren, zodat - ongeacht tijd en locatie - mensen en organisaties effectief kennis en informatie met elkaar kunnen delen en met elkaar kunnen communiceren. Hierdoor ontstaan ook nieuwe organisatievormen met veelal een netwerkachtig karakter. Dit wordt ook wel de netwerklogica van ICT genoemd.

Vervlechting van infrastructuren

ICT-infrastructuren spelen een vitale rol in het totstandbrengen van deze verbindingen. Dit betekent niet dat andere infrastructuren hierin geen rol spelen, zoals het stelsel van weg en waterwegen, het vliegverkeer of distributienetwerken voor elektriciteit, gas of water. Het interessante is echter dat in de netwerksamenleving deze infrastructuren steeds meer met elkaar vervlochten raken, en dus ook meer afhankelijk van elkaar worden (Bekkers et al, 2002; Bekkers & Thaens, 2005). In het

kader van de regulering en monitoring van verkeersstromen op de weg, op het spoor en in de lucht speelt bijvoorbeeld ICT een cruciale rol; hetzelfde geldt ook voor de distributie van bijvoorbeeld elektriciteit.
Deze convergentie heeft niet alleen betrekking op het naar elkaar toe groeien van infrastructuren. Het geldt tevens voor allerlei technologietoepassingen, die overigens steeds kleiner in omvang worden. Een mooi voorbeeld is de mobiele telefoon die ons niet alleen in staat stelt om telefoongesprekken te voeren, maar die ook de mogelijkheid biedt om te internetten, muziek te luisteren en ook steeds vaker is uitgerust met de mogelijkheid van 'global positioning' (GPS).

De kwetsbaarheid van de netwerksamenleving

Kenmerkend voor de netwerksamenleving is niet alleen het bestaan van stromen en knooppunten, maar ook de kwetsbaarheid als gevolg van de koppeling van deze stromen en infrastructuren, alsmede de kwetsbaarheid van knooppunten waarin deze stromen en infrastructuren bij elkaar komen (Bekkers et al, 2002). Het feit dat ICT volgens Castells gepenetreerd is in de haarvaten van onze samenleving, heeft ingrijpende gevolgen voor de wijze waarop we naar netwerken en infrastructuren in onze moderne samenleving dienen te kijken. De functionele grenzen tussen allerlei fysieke infrastructuren en netwerken (het routestelsel voor het weg, water-, spoor- en luchtverkeer), allerlei energiedistributienetwerken (het pijpleidingenstelsel voor gas, water en elektriciteit), telecommunicatienetwerken (telefoon, mobiele telefonie, internet, televisie etc.) en allerlei sociaal-organisatorische netwerken (steden, havens, wijken etc.) zijn in toenemende mate vervaagd. Er is sprake van een grote mate van wederzijdse vervlechting, hetgeen vitale kwetsbaarheden oproept. Immers een verstoringen in het ene netwerk heeft ook gevolgen voor het functioneren van andere netwerken en kan daardoor de samenleving als geheel ontwrichten; een samenleving die immers gedragen wordt door de vervlechting van allerlei netwerken en infrastructuren. Een stroomstoring leidt er bijvoorbeeld toe dat telecommunicatie deels wordt plat gelegd en belemmert vervolgens ons dagelijkse leven en werken. Een computervirus dat zich verspreidt via ICT-netwerken kan ook penetreren in de ICT-systemen die verkeersstromen reguleren maar kan ook de distributie van gas, water en elektriciteit ernstig verstoren - en daarmee ook ons dagelijkse leven.
Een dergelijke verstoring en de effecten die dit oproept is door Beck (1999) – als de founding father van het denken over de 'risicosamenleving' – als volgt beschreven. Veel risico's hebben implicaties die niet langer meer beperkt zijn tot een bepaalde locatie, terwijl ze ook steeds meer tijdsonafhankelijk zijn. "It becomes an event with a beginning and no end; an 'open-ended festival' of creeping, galloping and overlapping waves of destruction" (Beck, 1999:54,77). Een ICT-virus kan zich razendsnel verspreiden en wereldwijde effecten hebben. Maar het stelen van de identiteit van mensen uit allerlei databases, bijvoorbeeld van creditcardmaatschappijen, kan er bijvoorbeeld voor zorgen dat het handels- en kapitaalverkeer op wereldwijde schaal onbetrouwbaar wordt.
In bijvoorbeeld 'Politie in Ontwikkeling' wordt aandacht gevraagd voor het bestaan van stromenland, maar er bestaat relatief weinig aandacht voor de kwetsbaarheden van dit

stromenland, terwijl deze kwetsbaarheden voor de georganiseerde criminaliteit en allerlei terroristische groeperingen een interessant perspectief vormen; en dit geldt zeker voor de stedelijke knooppunten in de netwerksamenleving. Denk daarbij bijvoorbeeld aan allerlei mogelijkheden die bestaan op het terrein van 'Information Warfare'. Dit roept de vraag op of de kwetsbaarheid van allerlei infrastructuren niet veel explicieter een rol zou moeten spelen in de uitwerking van de nodale oriëntatie; niet alleen in instrumentele zin maar ook in relatie tot de legitimering van het concept.

Knooppunten

Kenmerkend voor de netwerksamenleving is niet alleen het bestaan van allerlei informatie- en kennisstromen, maar ook dat deze stromen op bepaalde punten bij elkaar komen. Knooppunten spelen in de netwerksamenleving daarom een vitale rol. New York, Tokyo en London zijn bijvoorbeeld knooppunten van kennis over de financiële wereld, van allerlei internationaal opererende consultancybureaus en andere hoogwaardige dienstenaanbieders. Maar ook tussen deze knoppunten kan sprake zijn van arbeidsdeling. Chicago en Singapore, ook belangrijke financiële knooppunten, zijn bijvoorbeeld leidend in de wereld van de 'futures'. Silicon Valley is weer een voorbeeld van een ander knooppunt, waar hoogwaardige ICT-kennis gebundeld wordt en innovaties plaats vinden, terwijl de haven van Rotterdam een voorbeeld is van een logistiek knooppunt.
Een analyse van de netwerksamenleving dient daarom ook niet alleen aandacht te hebben voor de aard en het verloop van allerlei stromen, maar ook voor de aard en de activiteiten die plaats vinden in allerlei fysieke knooppunten, die echter wereldwijde betekenis hebben. Vaak zijn dat grootstedelijke of metropolitaanse gebieden (Castells, 1996).

Spaces of flows

We hebben een aantal karakteristieken van de netwerksamenleving beschreven, maar we kunnen nog een stap verder gaan door de anatomie van de netwerksamenleving te ontrafelen. Hierin speelt het begrip 'spaces of flows' een belangrijke rol; in 'Politie in Ontwikkeling' vertaald als 'stromenland'. 'A space of flow' wordt door Castells (1996:412) omschreven als "the material organization of time sharing social practices that works through flows". Wat bedoelt hij hiermee?
Elke vorm van leven en werken kan alleen maar op een betekenisvolle manier plaats vinden, indien mensen een locatie met elkaar delen. Effectief organiseren betekende voorheen dat mensen en middelen op één plek gelokaliseerd moeten worden, binnen een bepaalde ruimte. Daarom hebben we bijvoorbeeld ook scholen. Kennis over verschillende vakken wordt op een plek aangeboden aan leerlingen. Kenmerkend voor de netwerkmaatschappij is dat deze ruimte niet langer fysiek hoeft te zijn, maar ook virtueel kan zijn; of juist een combinatie van beide is. In de ogen van Castells zijn het juist ICT-infrastructuren of netwerken die nieuwe virtuele ruimten creëren. De internationale kapitaalmarkt is een markt die fysiek te lokaliseren valt op de beursvloer van Amsterdam, maar tegelijkertijd - door middel van ICT - een mondiaal

karakter heeft en waar kennis en informatie over koersen voortdurend worden aangeboden. De haven van Rotterdam is een fysieke plaats waar mensen en middelen bij elkaar gebracht zijn om goederen te laden, te lossen of over te slaan, maar tegelijkertijd is die haven van Rotterdam door middel van ICT verbonden met allerlei wereldwijde logistieke processen. Informatie hierover is van vitaal belang voor het efficiënt en effectief organiseren voor het laden, lossen en overslaan van goederen, zoals bijvoorbeeld informatie over de lading van een schip, over mogelijke vertragingen etc. Kortom, binnen deze fysieke en/of virtuele ruimte spelen allerlei informatiestromen een vitale rol, omdat mensen op grond van deze informatie en kennis handelen of ergens een bepaalde betekenis aan toekennen. Bijvoorbeeld het combineren van informatie over een lading, de reputatie van een rederij en informatie over de vertrekhaven van een schip kan ertoe leiden dat een schip als risicovol wordt getypeerd en door de Douane extra zal worden gecontroleerd.

De gelaagdheid van de knooppunten

Van belang is ook aandacht te hebben voor de gelaagdheid van knooppunten. De eerste laag wordt gevormd door de ICT-infrastructuur die deze kennis- en informatiestromen ondersteunt en die mensen fysiek of virtueel bij elkaar brengt om te wonen en te werken (Castells, 1996).
De tweede laag wordt gevormd door geografische knooppunten en centra ('hubs and nodes') in een netwerk van stromen, die hierin bij elkaar komen en met elkaar verbonden worden. Wall Street is zo'n knooppunt van wereldwijde kapitaal en informatiestromen, terwijl de haven van Rotterdam niet alleen een fysiek knooppunt is van logistieke stromen maar ook een knoppunt van logistieke informatiestromen is. Sassen (1994) wijst erop dat het belangrijk is om deze knooppunten vooral te lokaliseren in een stedelijke context, zeker in het licht van een globaliserende economie. Daar vindt het werk plaats, ook al kan het gaan om wereldwijde activiteiten. Volgens Sassen heeft elke economie, ook een door informatie en ICT voortgedreven economie, fysieke locaties nodig. Dit betekent dus ook per definitie dat locale en fysieke factoren ertoe doen.
De derde laag wordt gevormd door een bepaalde elite, die toegang heeft tot deze ruimte van stromen en de kennis en informatie die daar wordt aangeboden, ook gebruikt ter ondersteuning van hun belangen en posities. Voor criminele organisaties is het daarom van belang om toegang te krijgen of deel uit te gaan maken van deze elite en de instituties van de elite; onder andere met het oog op het witwassen van crimineel geld.

Netwerken voor netwerken

De transformatie van de industriële samenleving in een netwerksamenleving heeft ook gevolgen voor de wijze waarop we ons organiseren, aldus Castells (1996: 190 e.v.). Nieuwe organisatievormen zien derhalve het licht; vormen die zelf ook een sterk netwerkachtig karakter hebben.

Op tal van plaatsen, verspreid over de wereld, treffen we volgens Castells (1996:171) de netwerkonderneming aan. Kenmerkend voor een netwerkorganisaties is - ten eerste - het vermogen om ruisloze communicatie tussen de verschillende onderdelen van de netwerkorganisaties te organiseren (in termen van interconnectiviteit). Hierdoor kan informatie en kennis efficiënt en effectief worden uitgewisseld of worden gedeeld, ongeacht tijd en plaats. Een tweede kenmerk is de consistentie van de deelnemende organisaties. Ondanks het feit dat de samenstellende onderdelen vaak andere doelen hebben, is er defacto sprake van een bepaald, gedeeld belang.
Door deze twee factoren is een netwerkorganisatie in staat zich vrij snel aan te passen aan veranderende omstandigheden. Deze organisatievorm wordt daarom op tal van plaatsen op de wereld aangetroffen, waarbij tevens moet worden aangetekend dat in sommige landen - zoals in Oost Azië – deze vorm van organiseren past in een bepaalde culturele traditie van samenwerken.
Volgens Castells zijn er twee hoofdredenen waarom deze organisatievorm belangrijk is om te kunnen overleven in de netwerksamenleving. Netwerkorganisaties bieden de meeste kans om te kunnen overleven in een situatie van wereldwijde concurrentie die steeds harder wordt. De globalisering van markt- en productieverhoudingen vraagt om wisselende vormen van samenwerking rondom bepaalde hulpbronnen, zoals kennis en informatie maar ook rondom het delen van een bepaalde infrastructuur. Tegelijkertijd kunnen risico's beter worden gespreid. Dit geldt ook voor criminele organisaties die immers optimaal gebruik maken van netwerkachtige structuren.
Een van de meest krachtige netwerken in de netwerksamenleving die optimaal gebruik maakt van de mogelijkheden die deze samenleving biedt, is volgens Castells het productie- en distributienetwerk van verdovende middelen zoals cocaïne. Op een zeer geraffineerde manier zijn de locaties waar de cocaïne wordt verbouwd in Peru en Bolivia verbonden met laboratoria en hoofdkwartieren in Colombia –zoals Medellin of Cali - die op hun beurt weer verbonden zijn met allerlei financiële centra zoals Miami, Panama, de Kaaiman-eilanden, IJsland en Luxemburg. Maar dit geldt ook voor allerlei distributiecentra in de Verenigde Staten en Europa, waarvan de Rotterdamse haven er een is.

2.3 Implicaties voor de nodale oriëntatie

Bovenstaand argumentatie maakt duidelijk dat de veranderende aard van de samenleving consequenties heeft voor de strategie van de politie. Een politie die tracht in te spelen op veranderende maatschappelijke en economische processen, dient daarom expliciet rekening te houden met de rol die netwerken, infrastructuren en stromen spelen in onze hedendaagse samenleving. In het rapport 'Politie in Ontwikkeling' wordt dit als uitgangspunt genomen. De interpretatie die daar plaats vindt is correct, maar soms onvolledig. Ook op grond van bovenstaande literatuurverkenning en een aantal verkennende interviews willen we aandacht vragen voor de volgende kanttekeningen die in een verdere uitwerking van het concept aan de orde moeten komen.

2.3.1 Stromenland

Stromen en infrastructuren

In 'Politie in Ontwikkeling' wordt wel gesproken over 'stromenland' maar wordt het accent vooral gelegd op het bestaan van verschillende soorten infrastructuren, waarbij vooral de aandacht wordt gevestigd op de verkeersinfrastructuur. Volgens ons het is belangrijk om dit stromenland open te breken en te relateren aan verschillende soorten van infrastructuren. Door meer oog te hebben voor de variëteit in dit stromenland ontstaan er ook meer aangrijpingspunten voor interventie. In ieder geval gaat het om de volgende stromen en infrastructuren:

- personen, veelal gebruik makende van fysieke infrastructuren die gelokaliseerd kunnen worden binnen een geografisch bepaalde en fysieke ruimte zoals het wegenverkeersnet;
- goederen, veelal gebruik makende van fysieke infrastructuren die gelokaliseerd kunnen worden binnen een geografisch bepaalde en fysieke ruimte zoals het wegenverkeersnet of het spoorwegennet;
- energie (gas water, elektriciteit), veelal gebruik makende van fysieke distributie-infrastructuren die gelokaliseerd kunnen worden binnen een geografisch bepaalde fysieke ruimte zoals het pijpleidingennetwerk;
- kapitaal, dat veelal gebruik maakt van een virtuele ICT- infrastructuur en wier bewegingen zich vooral afspelen binnen een virtuele ruimte (wereldwijde kapitaalmarkt) en een fysieke ruimte (infrastructuur van banken en andere financiële instellingen); en
- informatie en communicatie, veelal gebruik makende van een fysieke infrastructuur (het electriciteit- en vaste en mobiele telefoonnetwerk) en zich bewegende in een wereldwijde, virtuele ruimte die gecreëerd wordt door de koppeling van computernetwerken (de virtuele infrastructuur). Hierbij gaat het niet alleen om bijvoorbeeld diensten die via het internet worden aangeboden zoals elektronisch winkelen, maar ook de uitwisseling van informatie over het verloop van bovengenoemde personen, kapitaal, goederen, energie en informatiestromen (meta-informatie).

Open- en geslotenheid

Een belangrijke complicatie is het open en het gesloten karakter van bovenstaande stromen en de infrastructuren waarover deze stromen gaan. Ook dit heeft gevolgen voor de opsporing en interventie in deze stromen en op deze knooppunten. Veel infrastructuren hebben een open karakter, omdat ze een publieke functie hebben zoals de verkeersinfrastructuur. Andere infrastructuren hebben daarentegen een gesloten karakter zoals de computernetwerken die het kapitaalverkeer tussen banken ondersteunen of de infrastructuren die het vervoer van gas, water, telefoon en elektriciteit voor hun rekening nemen. Stromen kunnen zelf ook een open dan wel een gesloten karakter hebben. Veel discussies op het internet hebben een open karakter, terwijl het (mobiele) telefoonverkeer een gesloten karakter heeft.
Dit gesloten karakter heeft vaak iets te maken met het eigenaarschap van de infrastructuur of de mate waarin bepaalde stromen vanwege bijvoorbeeld privacyredenen gesloten dienen te zijn.

Twee aangrijpingspunten

Dit alles betekent dat de aard van de stroom en de infrastructuur waarvan gebruik wordt gemaakt, ook gevolgen heeft voor de soort van nodale oriëntatie van de politie en te gebruiken instrumenten en de effectiviteit ervan. Kortom, de invulling van de nodale oriëntatie dient dus te variëren met de aard van de stroom. Daarbij kunnen twee soorten aangrijpingspunten worden onderscheiden.
Ten eerste kan een nodale oriëntatie zich richten op de toegangen en uitgangen van de betreffende infrastructuur, bijvoorbeeld door het opzetten van fysieke of virtuele fuiken. Bij de verkeersinfrastructuur kan dit de toegang tot een snelweg zijn. In het geval van de ICT infrastructuur kan dit de server van een internetprovidor zijn. Het scannen van containers op nucleair materiaal in de haven van Rotterdam of de irisscan als identificatiemiddel op Schiphol zijn andere voorbeelden. De effectiviteit van de monitoring van het betreffende verkeer en mogelijke interventie hierop neemt echter toe, wanneer er sprake is van een beperkt en daarmee gecontroleerd aantal toe- en uitgangswegen. Een vliegveld heeft bijvoorbeeld een beperkt aantal toe- en uitgangen. Het wordt echter lastiger als er sprake is van een uitgebreid netwerk van toe- en uitgangswegen tot bijvoorbeeld de kapitaalmarkt in het geval van het witwassen van geld of het wereldwijde verkeer op het internet.
Ten tweede kan de nodale oriëntatie zich ook richten op het meebewegen met de stroom binnen een bepaalde infrastructuur. Voorbeelden zien we daarvan terug op de snelwegen waar de nodale oriëntatie vooral gestalte krijgt door patrouilles van de verkeerspolitie; hetzelfde geldt voor het surfen over het internet op zoek naar bijvoorbeeld kinderporno, of het deelnemen aan discussie in een rechts-extremistische of religieus-fundamentalistische chatroom.

Op grond van deze overwegingen kunnen we deze nadere operationalisering als volgt weergeven.

Stroom	Infrastructuur (publieke)	Interventie op de toegang van de stroom	Interventie door meebewegen met de stroom
Mensen	Verkeersinfrastructuur (open) - wegen; - vaarwegen; - luchtwegen - spoorlijnen	Toegangswegen tot hoofdwegen en tot knooppunten zoals havens, luchthavens en stations	Patrouilles
Goederen	Verkeersinfrastructuur (open) - wegen; - vaarwegen; - luchtwegen - spoorlijnen	Toegangswegen tot hoofdwegen en tot knooppunten zoals havens, luchthavens en stations	Patrouilles
Energie	Gas, water en elektriciteitsdistributie netwerk (gesloten)	Productielocaties zoals electriciteitscentrales Distributieknooppunten zoals schakelstations	Monitoring van bewegingen
Kapitaal	ICT-infrastructuur (deels open deels gesloten)	Toegang tot (databanken) van banken, verzekeringsmaatschappijen en andere financiële dienstverleners zoals wisselkantoren en kredietverstrekkers	Monitoring van kapitaalbewegingen (bijv. melding grote transacties)
Informatie en communicatie	Internet (open) Telefoon (gesloten) Mobiele telefoon (gesloten) Satelliet (gesloten)	Websites als knooppunt van communicatie Servers Schakelstations Databases en andere registratiesystemen	Aftappen, afluisteren Participatie in internet discussiegroepen

Tabel 2.3.1: Soorten van stromen in relatie tot infrastructuur en interventiemogelijkheden

Het ontanonimiseren van ongewenst gedrag binnen bepaalde stromen betekent derhalve dat gezocht moet worden naar specifieke aangrijpingspunten die recht doen aan de kenmerken van de stroom en de gebruikte infrastructuur. In een aantal documenten over de nodale politie vindt een zekere vernauwing van de mogelijkheden van het concept plaats, door vooral aandacht te hebben voor het met behulp van catch-ken technieken volgen en zichtbaar maken van verkeersbewegingen op de toegangswegen c.q. toegangspoorten tot stedelijke gebieden. Hierdoor wordt te weinig recht gedaan aan de potentie van de nodale oriëntatie van de politie.

2.3.2 Het internationale karakter van de stromen

De netwerksamenleving is een samenleving die gekenmerkt wordt door de globalisering van bovenstaande stromen, en waarin het lokale en globale nadrukkelijk met elkaar verbonden zijn. Een XTC-lab in een woonwijk kan lokale veiligheidsriscio's met zich mee brengen (in termen van ontploffingsgevaar) maar kan ook wereldwijde effecten hebben als door internationale handel kwalitatief slechte pillen worden

verspreid. Immers kenmerkend voor stromen is hun landsgrensoverstijgende karakter. Soms wordt de overschrijding van die landsgrenzen nadrukkelijk gemarkeerd, bijvoorbeeld door een bepaald knooppunt zoals een luchthaven; soms is sprake van een diffuse overschrijding van de landsgrenzen, hetgeen ook gevolgen heeft de soort van interventies. In het laatste geval is bijvoorbeeld sprake van een website die weer bestaat uit onderdelen van websites die weer gehost worden door verschillende servers uit verschillende landen.
Dit alles impliceert per definitie dat de nodale oriëntatie van de politie nadrukkelijk een internationale component moet hebben. In het visiedocument is bijvoorbeeld weinig aandacht welke extra eisen de nodale oriëntatie stelt aan de kwaliteit (aard en intensiteit) van internationale samenwerking die noodzakelijk is om de nodale oriëntatie te ondersteunen. Dit kan overigens variëren met de aard van de stroom.

2.3.3 Analyse van stedelijke knooppunten en stromen

Knooppunten binnen knooppunten

De stromen in de netwerksamenleving komen bij elkaar in met name stedelijke knooppunten, maar wat weten we eigenlijk over die knooppunten. Wat zijn dan relevante Nederlandse knooppunten? Hoe zitten die knooppunten in elkaar, welke soorten van stromen komen hier bij elkaar en welke functies vervullen deze knooppunten? Dit veronderstelt een relatief gedetailleerd beeld van bepaalde knooppunten zoals de haven van Rotterdam, het financiële centrum van Amsterdam-Zuidoost, of de luchthaven van Schiphol. Tegelijkertijd zien we dat binnen deze grootstedelijke knooppunten zich ook weer allerlei knooppunten bevinden. Twee voorbeelden maken dit duidelijk. Ten eerste zien we dat binnen de luchthaven Schiphol de bagageruimte een dergelijk knooppunt is. In de criminaliteitsanalyse van een dergelijk knooppunt gaat het niet alleen om het werken met risicoprofielen van bepaalde soorten van bagage uit bepaalde landen en bepaalde luchtvaartmaatschappijen, maar ook de betrouwbaarheid van het personeel (en de screening van dat personeel) dat bepaalde functies vervult ten aanzien van vitale en kwetsbare stromen, zoals in dit geval bagage). Een ander voorbeeld is het World Fashion Centre als knooppunt van financiële stromen binnen het Amsterdamse financiële centrum. Ook daar zien we een kwetsbaar knooppunt waar corrupte financiële stromen zich vermengen met vastgoed, waar boven- en onderwereld en de daarmee samenhangende elites met elkaar vervlochten raken.
Inzicht in deze knooppunten dient echter niet alleen gebaseerd te zijn op een statisch beeld van een dergelijk knooppunt, maar de stromen die zich binnen deze knooppunten afspelen vragen echter ook om een dynamisch beeld; gebaseerd op actuele informatie die recht die doet aan de verschillende kenmerken van een knooppunt, dat bovendien een lokale en wereldwijde betekenis heeft. Dit stelt zeer hoge eisen aan de kwaliteit van de informatievoorziening die een actueel (deels realtime) beeld dient te geven van de bewegingen binnen de bepaalde stromen en knooppunten. We komen daar dadelijk nog uitgebreider op terug.

Samenwerking rondom knooppunten en stromen

De nodale oriëntatie veronderstelt lokale en internationale samenwerking met verschillende soorten van organisaties (andere opsporingsdiensten zoals bijvoorbeeld de douane, publieke organisaties zoals bijvoorbeeld een Kamer van Koophandel of een gemeentelijke dienst en private organisaties zoals bijvoorbeeld banken) en de bereidheid om betrouwbare kennis en informatie te delen. In het visiedocument wordt aandacht gevraagd voor de mogelijkheden van samenwerking met andere partijen, maar essentieel is de vraag, hoe en onder welke condities deze bredere en intensievere vormen van samenwerking gestalte moeten krijgen; ook in het licht van de bestaande samenwerkingsverbanden? Onder welke condities zijn partijen bereid om kennis en informatie met elkaar te delen?
Een eerste stap is het in kaart brengen van het specifieke samenwerkingsnetwerk van partijen rondom een bepaalde stroom, knooppunt of infrastructuur. In een nodale oriëntatie op personen horen bijvoorbeeld de Koninklijke Marechaussee, de Douane en de IND thuis; een op kapitaalstromen gerichte nodale oriëntatie vraagt bijvoorbeeld om samenwerking met de FIOD, de Belastingdienst en De Nederlandsche Bank. Dit kan ook worden gedemonstreerd aan de hand van onderstaande tabel.

Stroom	Infrastructuur (publieke)	Knooppunt	Noodzakelijke samenwerking met andere publieke en private partijen
Mensen	Verkeersinfrastructuur - wegen; - vaarwegen; - luchtwegen - spoorwegen	Verkeersknooppunten; Toegangs- en ringwegenstelsels Havens Luchthavens Stations, incl. Metrostations	KLPD; Douane; Koninklijke Marechaussee; IND; Vreemdelingenpolitie; Havenautoriteit
Goederen	Verkeersinfrastructuur - wegen; - vaarwegen; - luchtwegen - spoorwegen	Havens Luchthavens Stations	Douane; Inspectie V & W; Waren- en Voedsel Autoriteit; Algemene Inspectie Dienst; Havenbedrijven en havenautoriteiten
Energie	Gas, water en elektriciteitsnetwerk	Distributiecentra Productiecentra	Energiebedrijven; NMA (voorheen DtE)
Kapitaal	ICT-infrastructuur	Banken Verzekeringsmaatschappijen Beurs Vastgoedmaatschappijen Notarissen	Banken Verzekeringsmaatschappijen Beurs NMA, FIOD, SIOD Notariaat Vastgoedmaatschappijen
Informatie en com-municatie	Internet Telefoon Mobiele telefoon Satelliet	Telecombedrijven Internetproviders AMS-IX (Amsterdam Internet Exchange)	Digitale recherche Telecom- en internet providers OPTA Agentschap Netwerken Buma/Stemra

Tabel 2.3.3: Relatie tussen stroom, infrastructuur, knooppunt en samenwerkingspartners

Tegelijkertijd maakt deze tabel ook duidelijk dat rondom de opsporing en handhaving van verdachte activiteiten binnen een stroom of knooppunt vaak meerdere partijen betrokken zijn. Soms zijn dat andere publieke opsporingsdiensten soms zijn dat private organisaties. Dit laat in sommige gevallen zien dat het primaat ten aanzien van opsporing en handhaving bij andere organisaties ligt en veel minder bij de politie. Vandaar dat de politie zich per knooppunt, infrastructuur of stroom nadrukkelijk de vraag moet stellen, welke gevolgen dit heeft voor de rol die de politie kan en wil innemen (onder meer op grond van de verdeling van formele taken, bevoegdheden en verantwoordelijkheden) met betrekking tot de invulling van de specifieke nodale oriëntatie die men ten aanzien van deze stroom, knooppunt of infrastructuur wenst te ontwikkelen. Wie is bijvoorbeeld de regisseur van de handhavingsactiviteiten rondom een bepaald knooppunt? Is dit een andere opsporingsdienst, of dient dit juist de politie te zijn, zeker als andere 'trekkers' ontbreken. Tegelijkertijd maakt bovenstaande tabel het belang van vormen van integrale handhaving duidelijk. In ieder geval is het van belang om afspraken te maken over de uitwisseling van relevante informatie en in welke gevallen de politie wel en niet wordt ingeschakeld.

Het netwerk als organisatieprincipe

Overigens laat bovenstaande tabel nog een ander relevant aspect zien, dat nog meer betekenis krijgt als we bedenken dat in de netwerksamenleving het netwerk als organisatieprincipe de meest effectieve vorm van organiseren is. Dit heeft niet alleen gevolgen voor de soort van samenwerkingsrelaties die met andere publieke en private partijen (zie boven; alsmede ook internationaal) worden aangegaan, maar ook voor de interne organisatie van de politie. Vandaar dat het interessant is om na te gaan wat de behoefte aan meer centralisatie, standaardisatie en formalisering binnen de Nederlandse politie organisatie betekent voor de verdere uitwerking van de nodale oriëntatie, waarin netwerkvorming essentieel is. Overigens hoeven die twee ontwikkelingen elkaar niet te verzwakken maar kunnen ze elkaar juist versterken. Bijvoorbeeld een uniforme ICT-infrastructuur kan netwerkvorming vergemakkelijken, omdat er geen technische barrières zijn die de flexibele uitwisseling van informatie kunnen belemmeren.

2.3.4 Strategische kennis en informatiepositie

In de netwerksamenleving zijn informatie en kennis een vitale grondstoffen. Dat geldt dus ook voor de politie. Inzicht in het reilen en zeilen van de netwerksamenleving is alleen maar mogelijk, indien de politie een informatiestrategie ontwikkelt die recht doet aan de wijze waarop knooppunten en stromen in elkaar zitten; daarbij gaat het niet alleen om relatief statische informatie over relevante aspecten van bijvoorbeeld Schiphol of de haven van Rotterdam. Het gaat om dynamische informatie; actuele informatie over de concrete en recente bewegingen binnen een stroom of binnen een netwerk.

Gelet op de omvang van veel stromen en de intensiteit van (bijvoorbeeld het internet of kapitaal) verkeer is het noodzakelijk om met risicoprofielen te werken ten aanzien van bepaalde gedragingen in een stroom of knooppunt.
Tegelijkertijd laat de kwetsbaarheid van deze stromen en netwerken ook zien dat het belangrijk is om actuele kwetsbaarheidanalyses te maken van deze knooppunten, zoals bijvoorbeeld ook hebben plaats gevonden in het kader van de millenniumproblematiek en de analyses die thans ook plaats vinden met betrekking tot de mogelijkheid van terroristische aanslagen ten aanzien van vitale sectoren.
Dit veronderstelt een andere inrichting van de informatievoorziening en het opbouwen van een strategische informatiepositie. In 'Politie en Ontwikkeling' wordt hierop deels gewezen, daar waar gesproken wordt over informatiegestuurd werken. In ieder geval dient in het opbouwen van die strategische informatiepositie aandacht te zijn voor:

- de hoogwaardige kennis die nodig is om de aard en het verloop van bepaalde stromen te begrijpen, bijvoorbeeld daar waar het gaat om het begrijpen van witwasoperaties waarbij gebruik wordt gemaakt van de complexiteit en verwevenheid van kapitaalstromen;
- het in kaart brengen van de condities waaronder andere organisaties die over de kennis beschikken bereid en in staat zijn om deze kennis te delen; en
- het ontwikkelen van een technologische en organisatorische infrastructuur die dat ondersteunt.

2.4 Criminologische verkenningen

In deze paragraaf verleggen we onze aandacht door op zoek te gaan naar een aantal criminologische inzichten en concepten die van belang kunnen zijn voor de vraag, voor welke problemen de nodale oriëntatie een oplossing is. In het visiedocument 'Politie in Ontwikkeling' wordt verondersteld dat de aard van de hedendaagse criminaliteit vraagt om het ontanonimiseren van de stromen in de netwerksamenleving; stromen die ontstaan omdat criminaliteit steeds meer mobieler wordt en zich nauwelijks iets van allerlei soorten van grenzen (ontgrenzing) aantrekt en gebruik maakt van de toegenomen anonimiteit van de samenleving. Wat zijn in dat verband relevante inzichten?

Anonimiteit, ontgrenzing en mobiliteit

Ten eerste moet gewezen worden op de toegenomen anonimiteit van de samenleving ten gevolge van het proces van individualisering dat zich gedurende de laatste decennia met name heeft voltrokken en dat tevens een vruchtbare voedingsbodem biedt voor criminaliteit. In veel gevallen gaat individualiseringsproces hand in hand met verstedelijking en massaliteit, hetgeen onder meer leidt tot een verlies aan sociale binding en sociale controle in wijken en buurten (Schnabel, 2004). Dit bevordert crimineel gedrag en biedt tevens een dekmantel voor het ongestoord kunnen opzetten en verrichten van criminele activiteiten.

Door de uitbreiding van de Europese Unie en daarmee het openstellen van de grenzen voor vrij verkeer van personen, goederen en diensten, zien we tevens een toename van de grensoverschrijdende georganiseerde criminaliteit alsmede een toenemende mate van geografische spreiding van de internationale criminaliteit (Europol, 2004). Dit betekent dat meer landen met internationale criminaliteit te maken hebben gekregen en de aantallen en manifestaties van misdaad toenemen. Bovendien is door het wegvallen van de scheiding tussen West- en Oost-europa een intensivering van allerlei internationale samenwerkingsverbanden op gang gekomen. Zo is een groeiende tendens te zien van roofcriminaliteit of 'banditisme'[1], vooral door bendes die afkomstig zijn uit het voormalige Oost-Europa. Hiermee wordt bedoeld dat criminelen in Nederland goederen stelen (al dan niet op bestelling) en vervolgens met de buit teruggaan naar het land van herkomst. Op deze ontwikkeling wordt al gereageerd door bijvoorbeeld het houden van grote nachtelijke controles op snelwegen richting het oosten van Nederland zoals met regelmaat op de A1; dit alles onder de naam 'Ochtendgloren'. In het licht van de toenemende globalisering van de internationale gemeenschap wordt de aard van georganiseerde criminaliteit al gekenschetst als '*transnationaal fenomeen'* (Veiligheidsatlas, 2003).

Flexibele netwerken

De georganiseerde criminaliteit gaat steeds meer opereren volgens het organisatieprincipe van de netwerksamenleving. Het beeld van sterk hiërarchisch georganiseerde piramidale criminele organisaties wordt steeds meer als uitzondering beschouwd. Eerder is sprake van fluïde en dynamische samenwerkingsverbanden op basis van 'afhankelijkheidsrelaties' en taakverdelingen, waarin bepaalde personen rondom specifieke hulpbronnen als geld, transport of contacten aan te merken zijn als centrale 'knooppunten' en hun faciliteiten aanbieden aan andere criminele netwerken. Een andere belangrijke constatering is dat door het dynamisch karakter en het vermogen tot aanpassing en substitutie van (onderdelen van) het netwerk, criminelen in staat zijn na arrestaties, inbeslagname of andere justitiële interventies op relatief eenvoudige wijze via andere schakels in het netwerk activiteiten te continueren (Kleemans, 2002).
Verder blijkt dat bepaalde delen van het netwerk niet of nauwelijks met elkaar verbonden zijn; hetzij door taalbarrières, geografische factoren of etnische verschillen. Deze ontbrekende schakels worden aangemerkt als "structural holes". Degenen die in staat zijn in deze lacune te positioneren zijn van grote strategische waarde in het netwerk. Vaak zijn dit personen die zelf wat verder af staan van de uitvoering van directe criminele activiteiten, maar activiteiten ontplooien in de ondersteuning van de noodzakelijke communicatie of het doen van financiële transacties. Een recent voorbeeld is de in 2004 geliquideerde Willem Endstra.
Verder blijkt dat het karakter van het criminele netwerk te omschrijven is als 'conflictvermijdend' met andere criminele netwerken en 'confrontatiemijdend' richting

[1] NRC Handelsblad, "*meer banditisme Litouwers en Polen"*, 20 oktober 2005

de overheid. De anonimiteit van bepaalde criminele operaties wordt hierdoor verder versterkt.

Cybercrime

Het toegenomen belang van ICT heeft tevens geleid tot hiermee samenhangende, 'eigen soorten' van criminaliteit die tevens bijdragen aan de kwetsbaarheid van de samenleving. Vormen van computercriminaliteit kunnen daarmee een belangrijke ontwrichtende werking hebben, bijvoorbeeld in het geval van virussen, het digitaal plunderen van bankrekeningen of het kraken van de identiteit van de houders van creditcards. Hierdoor wordt niet alleen geld gestolen maar kan ook identiteitsfraude worden gepleegd.
Tenslotte zien we ook dat de anonimiteit en de laagdrempeligheid van internet ruimte biedt aan criminele en andere (bijvoorbeeld terroristische) organisaties om elkaar te ontmoeten en met elkaar te communiceren teneinde hun criminele activiteiten te kunnen coördineren of producten uit te wisselen en te verspreiden (bijv. in het geval van kinderporno).

Voorgaande ontwikkelingen zijn relatief algemene ontwikkelingen die gelden voor de meeste Europese landen. Naast deze trends gelden voor Nederland nog een aantal specifieke factoren.

Infrastructurele positie

De aanwezigheid van relatief hoogwaardige economische, technische en fysieke infrastructuren alsmede de centrale positie van Nederland als bruggenhoofd van Europa betekent, dat Nederland een aantrekkelijke uitvalsbasis en doorvoerland isvoor verschillende soorten van georganiseerde internationale criminaliteit. Dit is ook de conclusie van de WODC-criminaliteitsmonitor: de georganiseerde criminaliteit in Nederland heeft een sterk transitiekarakter; dit wil zeggen veel grensoverschrijdend handelsverkeer. Criminelen en criminele organisatie weten op geraffineerde (en soms zelfs legale) wijze gebruik te maken van staande, legale, infrastructuren voor de uitvoering van criminele activiteiten (WODC, 2002).

Financiële dienstverlening

Naast de bovengenoemde infrastructurele voorzieningen en de centrale geografische ligging is in Nederland uitgebreide expertise aanwezig wat betreft financiële dienstverlening. De internationale positie van Nederland als een handelsnatie maakt ons aantrekkelijk voor illegale handel, waarbij criminelen hun opbrengsten, goederen en diensten kunnen verbergen in het legale (financiële) handelsverkeer door fraude of witwassen. De invloed en omvang van het witwassen van crimineel geld is door het ministerie van Financiën becijferd op ongeveer 3,8 miljard euro uit criminele activiteiten binnen Nederland en daarbij ongeveer nog eens 14,7 miljard euro dat door

of in het land stroomt als opbrengsten uit buitenlandse criminele activiteiten[2]. Gebleken is dat, tot op heden, het een eerder positief dan een negatief economisch effect heeft gehad (WODC, 2002). Witwassen trekt echter criminaliteit aan en heeft dus een gevaarlijke langetermijneffect, omdat het de economische, sociale en politieke stabiliteit van een land kan ondermijnen.
Het toenemende belang van deze vorm van criminaliteit is ook af te leiden uit het feit dat het in kaart krijgen en brengen van witwaspraktijken steeds meer internationale aandacht krijgt. Een van de verklaringen hiervoor is de bestrijding van financiële stromen die bedoeld zijn als ondersteuning en financiering van terreurnetwerken of terroristische organisaties.

Migratie

Vanaf de jaren 60 heeft Nederland te maken gehad met een aanzienlijke instroom van migrantengroepen. De beperkte mate (en mogelijkheden) van integratie en kansen om een bepaald welvaartsniveau te bereiken, spelen eveneens een rol van betekenis. De marginale positie van minderheden in de Nederlandse samenleving alsmede de positie als doorvoerland en de criminaliteit en sociale contacten in het land van herkomst bieden in dat verband interessante mogelijkheden. Met name de sociale context zoals sterke familiebanden zijn belangrijk in internationale criminele organisaties. Zo stelt Kleemans bijvoorbeeld (2002:308) dat de goede Nederlandse infrastructuur gecombineerd met effectieve transnationale sociale banden en familienetwerken de handel in Colombiaanse cocaïne, Turkse heroïne en Marokkaanse hasj helpt en maakt dat Nederland een belangrijk doorvoerland voor drugs in Europa.

2.5 Implicaties voor de nodale oriëntatie

In deze paragraaf willen we de implicaties van de zojuist beschreven ontwikkelingen voor de nodale oriëntatie nader in kaart brengen.

2.5.1 De nodale oriëntatie van de georganiseerde criminaliteit

De eerste conclusie die we moeten trekken is dat met name de georganiseerde misdaad en terroristische organisaties optimaal gebruik weten te maken van de mogelijkheden die netwerksamenleving en de rol die knooppunten en stromen daarin spelen. Dit is een belangrijke legitimatie voor de nodale oriëntatie van de politie. Bovendien biedt de anonimiteit en het individualistische karakter van de netwerksamenleving, zeker in grootstedelijke gebieden, dit soort van organisaties de gewenste achtergronden om bepaalde activiteiten te ontplooien.
Een andere conclusie is dat ook misdaad- en terroristische organisaties zich bewust zijn van de wijze waarop 'stromenland' functioneert, hetgeen een ander argument is ter ondersteuning van het belang van een nodale oriëntatie. Zo zorgen de

[2] Ministerie van Financiën. persbericht | 17-02-2006 | nr 06-011 | Directie Voorlichting, 17 februari 2006

toegenomen internationalisering van de criminaliteit, de taakspecialisatie tussen criminele organisaties en de daarmee samenhangende noodzaak van samenwerking alsmede de toegenomen mobiliteit van criminele organisaties ervoor dat er een intensief verkeer van personen en goederen ontstaat. Dit vereist dat informatie moet worden gedeeld en uitgewisseld, met als gevolg dat deze organisaties optimaal gebruik maken van ICT en ICT-netwerken. In hun strategisch gedrag is nodale oriëntatie een leidend beginsel.
Verder maakt bovenstaande schets duidelijk dat er nieuwe vormen van criminaliteit ontstaan zoals computercriminaliteit, die optimaal gebruik maakt van wereldwijde informatiestromen of die optimaal gebruik maakt van de vervlechting van stromen, bijvoorbeeld tussen kapitaal en informatiestromen. Bovendien zorgt deze technologie voor nieuwe vormen van criminaliteit, zoals identiteitsfraude. Het feit dat identiteiten steeds beter te manipuleren zijn heeft echter ook gevolgen voor het vaststellen van de identiteit of status van bepaalde van personen en hun betrokkenheid in allerlei personen, goederen, kapitaal en informatie- en communicatiestromen; en dit was juist een van de hoekstenen van de nodale oriëntatie.
Een laatste conclusie verwijst naar de rol van knooppunt die Nederland vervult. De infrastructurele positie van Nederland als toegangspoort tot Europa, alsmede zijn rol als financiële dienstverlener, benadrukken eveneens het belang van een nodale oriëntatie.

Kortom, als we kijken naar de ontwikkeling van de criminaliteit in Nederland, dan is eigenlijk alleen maar één conclusie gerechtvaardigd, namelijk dat de politie in haar strategische positionering het netwerkkarakter van de samenleving als belangrijk uitgangspunt moet nemen; een besef dat immers in criminele kringen al langer is doorgedrongen. Een verdere uitwerking van de nodale oriëntatie van de politie is daarin een gewenste vervolgstap.

2.5.2 Een criminologische analyse van knooppunten en stromen

Veel misdaadanalyses die de politie maakt zijn gericht op het in kaart brengen van het netwerk van personen c.q. bedrijven rondom een persoon c.q. een bedrijf, waarvan het vermoeden bestaat dat er sprake is van criminele activiteiten. Vanuit de nodale oriëntatie gaat het vooral op het maken van twee andere soorten van misdaadanalyses:

a) het maken van een risico-analyse van knooppunten waarvan het vermoeden bestaat dat ze een draaischijf zijn voor criminele activiteiten of van knooppunten die erg kwetsbaar zijn. Twee voorbeelden daarvan zijn eerder genoemd, namelijk de bagageruimte van Schiphol en het World Fashion Centre.
b) Het maken een risico-analyse van bepaalde stromen of bewegingen binnen stromen, waarvan het vermoeden bestaat dat hier regelmatig activiteiten worden ontplooid die het daglicht niet kunnen verdragen. Eventueel zou men

vanuit een knooppunt de stromen kunnen volgen naar eventuele bronnen. Een voorbeeld daarvan is de analyse van extra activiteit in het telefoonverkeer, op het internet binnen bepaalde discussiegroepen, of de bewegingen van groepen van hooligans op weg naar een voetbalwedstrijd.

Beiden soorten laten dus zien dat een nodale oriëntatie zich niet richt op de relatie tussen een persoon en (het vermoeden van) een delict, maar op de relatie tussen knooppunten en mogelijke delicten en/of de relatie stromen en mogelijke delicten, waarachter vervolgens personen of bedrijven schuil gaan. Dit vereist niet alleen een andere werkwijze, maar veronderstelt ook dat analisten een gedegen vakinhoudelijke kennis hebben van een knooppunt en de bewegingen en stromen die daar plaats vinden. Kortom, dergelijke analyses doen een beroep op een bredere kennisbasis waarin ook andere dan criminologische factoren in ogenschouw moeten worden genomen.

In onderstaande tabel hebben we bij wijze van exercitie in kaart gebracht wat mogelijke soorten van delicten zijn, waarbij we geredeneerd hebben vanuit de eerder benoemde stromen.

STROOM	SOORT VAN DELICTEN (VOORBEELDEN)
MENSEN	Vermogensdelicten door veelplegers Mensensmokkel Mobiel banditisme Terrorisme
GOEDEREN	Smokkel van drugs, wapens, sigaretten en andere goederen Autodiefstal
ENERGIE	Aftappen van electriciteit i.v.m. hennepteelt
KAPITAAL	Verplaatsen en witwassen van criminele gelden Financiering van terroristische activiteiten
INFORMATIE EN COMMUNICATIE	Identiteitsfraude Verspreiden van computervirussen Hacken van computers en netwerken Kinderporno Terrorisme Verspreiding van rechts-extremistisch of religieus-fundamentalistische of ander gedachtegoed

Tabel 2.5.2: Voorbeelden van een stroomgeoriënteerde benadering van delicten

2.5.3 Het concept 'tegenhouden'

De nodale oriëntatie kent een zekere verwantschap met een eerder ontwikkelde interventieconcept, namelijk dat van 'tegenhouden'. Tegenhouden kan worden gedefinieerd als het zodanig beïnvloeden van gedrag en van omstandigheden dat criminaliteit of andere inbreuken op de veiligheid en de maatschappelijke integriteit

worden voorkomen (Tegenhouden troef, p. 35). Dit heeft ook gevolgen voor de verdere ontwikkeling van de nodale politie.

Ten eerste behelst tegenhouden dat vooral gekeken wordt naar de samenhang tussen relevante elementen die te ontwaren zijn in de concrete manifestatie van bepaalde criminele activiteiten of bepaalde problemen. (Tegenhouden troef, p. 36). En in dat systeemperspectief op criminele activiteiten spelen stromen en knooppunten een essentiële rol.
Voor de doelstelling van dit onderzoek heeft dit twee implicaties. Ten eerste dat een bepaalde criminele activiteit veel nadrukkelijker in samenhang moet worden beschouwd met de stromen van personen, goederen, geld en informatie die deze activiteit oproept en waarvan ze gebruikt maakt, alsmede van de knooppunten waarvan men gebruikt maakt. Dit betekent dat de productie van XTC niet alleen gezien moet worden als het oprollen van een XTC-laboratorium, maar dat het functioneren van dit laboratorium veel meer in samenhang moet worden geanalyseerd met de stromen van mensen, goederen, geld en informatie, de knooppunten waar deze samenkomen en de bronnen van waaruit zij ontstaan.
Even zo interessant is de tweede implicatie. Is het mogelijk om door een intensievere controle van stromen van mensen, goederen, geld en informatie effectiever te zijn en eerder en beter zicht te krijgen op deze locale manifestaties van crimineel gedrag? Een recent voorbeeld hiervan is het volgen van de bewegingen van groepen van hooligans op weg naar bijvoorbeeld het Wereldkampioenschap. In dat geval wordt een strategie van tegenhouden gebruikt die van stromen naar de locatie gaat in plaats van locatie naar stromen.

Bovendien gaat de idee van tegenhouden uit van een multidisciplinaire aanpak, waarbij verschillende soorten van kennis en instrumenten worden gebruikt. Bijvoorbeeld door niet alleen gebruik te maken van strafrechtelijke middelen maar ook door de mogelijkheden die het bestuursrecht of het privaatrecht biedt. Dit betekent dat al naar gelang de aard van de problematiek, het instrument wordt aangewend dat het meest effectief is en dat hoeft niet altijd gebaseerd te zijn op opsporing door de politie. Zo is in een aantal steden de Vreemdelingenwet ingezet in de strijd tegen tippelprostitutie en straatroof door illegaal in Nederland verblijvende vreemdelingen. Dit betekent derhalve dat een dergelijke aanpak (internationale) samenwerking veronderstelt tussen de meest belanghebbende partijen - ook al hebben deze verschillende taken, verantwoordelijkheden en bevoegdheden - die met een bepaald probleem of een bepaalde activiteit worden geconfronteerd. Dit betekent derhalve dat het tegenhouden van crimineel gedrag binnen een stroom niet alleen via het strafrecht kan plaats vinden, maar ook via andere juridische regimes, zoals het innen van niet betaalde belastingen. Een ander voorbeeld – gericht op de controle van goederenstromen - is de samenwerking met de Douane in de haven Rotterdam om verdachte containers eerder en beter te kunnen opsporen. Daarbij wordt niet alleen gebruik gemaakt van elkaars kennis, maar ook van elkaars taken,

verantwoordelijkheden en bevoegdheden, wanneer dit de mogelijkheid biedt om effectiever te kunnen optreden buiten bijvoorbeeld het strafrecht om.

Tegenhouden is verder vooral gericht op het tussentijds verstoren van een 'stroom' of van een knooppunt, desnoods met andere dan strafrechtelijke middelen. De nodale oriëntatie gaat eigenlijk nog een stap verder, namelijk door aandacht te vragen voor het via het volgen van de stroom achterhalen van de bronnen van bepaalde criminele activiteiten en daarmee samenhangen groepen (voor zover dat mogelijk is in een sterk verweven en verknoopt netwerk van stromen).

Een laatste belangrijkste implicatie van het concept 'tegenhouden' voor de verdere uitwerking van de nodale oriëntatie is dat onderkend moet worden dat voor het effectief signaleren, voorkomen en opsporen van criminele activiteiten, het noodzakelijk is om verschillende soorten van kennis ook daadwerkelijk te gebruiken om een beter inzicht te krijgen in het functioneren van een stroom of knooppunt. Financiële kennis bijvoorbeeld is noodzakelijk om kapitaaltransacties te kunnen doorgronden, terwijl ICT kennis noodzakelijk is voor het begrijpen van het functioneren van het internet. Vaak ook is juist de combinatie van verschillende soorten kennis cruciaal. Dit betekent dat samenwerking met die private en publieke organisaties die een belangrijke rol spelen in de aansturing van bepaalde functies binnen bepaalde stromen en het toezicht op deze stromen, essentieel is. Een voorbeeld – gericht op de controle van geldstromen - is de verplichting van banken om in het kader van de antiterreurwetgeving de identiteit van hun klanten bij bepaalde soorten van transacties, die als risicovol worden beschouwd, eerder door te geven aan opsporingsdiensten.

2.6 Technologische verkenningen

In 'Politie in ontwikkeling' wordt naar voren gebracht dat de keuze voor een nodale oriëntatie begrepen dient te worden vanuit zowel maatschappelijke als technologische ontwikkelingen die ook hebben bijgedragen aan een veranderend crimineel gedrag. Tegelijkertijd biedt ICT ook allerlei mogelijkheden om met name de anonimiteit van individuele bewegingen binnen 'stromenland' op te heffen. Vandaar dat het belangrijk is om stil te staan bij een aantal robuuste technologische ontwikkelingen. In het visiedocument worden echter geen relevante technologische ontwikkelingen genoemd, terwijl er ook geen aandacht is voor de strategische betekenis van deze ontwikkelingen voor de verdere vormgeving en instrumentalisering van de nodale oriëntatie. Er wordt alleen verwezen naar zogenaamde catch-ken technologieën.

De volgende technologische ontwikkelingen zijn van belang om expliciet in ogenschouw te nemen bij een verdere uitwerking van de nodale oriëntatie.

Samensmelting en multimedialisering

Verschillende soorten van technologische infrastructuren (telefoon, kabel, televisie, internet) integreren steeds verder. Zo is het thans al mogelijk om via de kabel te telefoneren, televisie te kijken en te internetten. Ook worden steeds meer toepassingen geïntegreerd. Met de gemiddelde mobiele telefoon is het mogelijk om te telefoneren, te internetten, te fotograferen en MP3 files c.q. FM-radio te beluisteren. Dit laatste voorbeeld laat ook een andere ontwikkeling zien, namelijk multimedialisering. Geluid, beeld, tekst en andere data kunnen via dezelfde toepassing worden ontvangen, bewerkt en verzonden. Een ander voorbeeld is de automatische matching van de gelaatstrekken die door middel van videobeelden zijn verzameld (bijvoorbeeld van voetbalhooligans) met persoonsgegevens en andere informatie die beschikbaar is in allerlei databestanden.

Ontdrading en mobiel

Bovenstaand voorbeeld illustreert ook een tweede belangrijke ontwikkeling. Communicatie en informatie-uitwisseling vindt steeds meer via de ether plaats, zonder tussenkomst van allerlei draden en kabels. Deze vormen van draadloze communicatie zorgen ervoor dat het mogelijk is steeds gemakkelijker mobiel te kunnen communiceren volgens het principe: "anytime, anyplace and anywhere".

Gegevensverwerkingscapaciteit en transporteerbaarheid

De integratie van zowel infrastructuren als (multimedia)applicaties leidt ertoe dat niet alleen de gegevensverwerkingscapaciteit van de chips in allerlei systemen nog steeds exponentieel toeneemt, maar dat ook de transportomvang en transportsnelheid van steeds groter worden hoeveelheid data een factor van betekenis is. Ook deze zal nog steeds verder toenemen, gelet op allerlei ontwikkelingen op het terrein van breedband (glasvezel, WiFi, ADSL, UMTS).

Locatie-georiënteerde technologie

Een andere interessante ontwikkeling is de opkomst van geografische informatieverwerkingsprocessen, die het mogelijk maken om uiteenlopende geografische informatiebronnen (dit wil zeggen informatie waarin een locatiecomponent zit) aan elkaar te koppelen, om vervolgens deze locatiegeoriënteerde informatie weer te koppelen aan andere informatie. Dit heeft als voordeel dat de complexe samenhang van veel problemen inzichtelijker en transparanter kan worden gemaakt en dat de effecten van bepaalde maatregelen ook relatief eenvoudiger zichtbaar kunnen worden gemaakt. Criminaliteitsgegevens van een buurt kunnen daardoor gemakkelijker worden gekoppeld aan andere kenmerken van deze buurt, zoals aantal koop- of huurwoningen, soort van bewoners (jong/oud, allochtoon/autochtoon) etc. Informatie kan daardoor meer integraal en meer toegesneden op de specifieke locatie worden aangeboden. Maar dit geldt ook voor het inzichtelijk maken van met name fysieke stromen (zoals verkeersstromen en personen

en goederenstroom) en de samenhang hiertussen binnen een bepaald geografisch gebied (bijvoorbeeld binnen een knooppunt zoals een haven). Dit geldt zeker als deze informatie wordt gekoppeld aan een andere belangrijke ontwikkeling op het terrein van de geografische informatiesystemen, namelijk global positioning systemen. De combinatie van satelliet technologie en geografische informatiesystemen maakt het zo relatief eenvoudig om te kunnen bepalen waar iemand zich bevindt.

Virtualisering en simulatie

De combinatie van het koppelen van allerlei soorten van databestanden (waaronder geografische) en de inzet van allerlei multimedia toepassingen, maakt mogelijk om fictieve maar wel levensechte (virtuele) werkelijkheden te creëren dan wel te simuleren. Dit betekent bijvoorbeeld dat stromen in knooppunten, zoals havens en luchthavens, metrostations etc. relatief eenvoudig kunnen worden nagebootst, waardoor ook de effecten van bepaalde verstoringen c.q. interventies relatief gemakkelijk zichtbaar kunnen worden gemaakt.

Miniaturisering en reflexiviteit

Geheugenchips worden steeds kleiner en steeds flexibeler. Dit heeft twee gevolgen. Ten eerste wordt het gemakkelijker om deze geheugenchips te implanteren. Ten tweede neemt hierdoor ook de reflexiviteit c.q. het leervermogen van personen, voorwerpen en allerlei soorten van processen op bepaalde locaties toe, omdat hieraan een stukje intelligentie wordt toegevoegd. Zo wordt onder meer gesproken van 'smart places'. Het resultaat is dat op afstand bestuurbare (in combinatie met draadloze technologie) of zelfsturende mechanismen kunnen worden ontworpen; maar dat tegelijkertijd ook meer mogelijkheden voor monitoring en controle worden gecreerd. Het gevolg is dat ook de stromen en knooppunten in de samenleving steeds intelligenter worden, hetgeen nieuwe interessante aangrijpingspunten voor een nodale oriëntatie kan bieden.
Deze ontwikkeling is ook wel beschreven in termen van 'ambient intelligence'. Een interessant voorbeeld hiervan is 'Radio Frequency IDentification' (RFID); een technologie die de komende vijf jaren op grotere schaal zal worden uitgerold. Het gaat dan om met name 'slimme' detectietechnologie die steeds gemakkelijker kan worden ingepast in onze natuurlijke leef- en werkomgeving. RFID maakt bijvoorbeeld gebruik van allerlei radiosignalen om informatie door te geven, waardoor personen en goederen, uitgerust met een minuscule chip die bijvoorbeeld deel uitmaakt van de coating van een pak melk maar ook van een auto, permanent kan worden gevolgd. Deze soort van technologie (die bijvoorbeeld de barcode in de supermarkt zal vervangen en waardoor automatisch de rekening kan worden opgemaakt als iemand door een poortje loopt met zijn wagentje vol boodschappen) is bij uitstek geschikt voor het verwerven van overzicht in relatief chaotische contexten (bijv. in een stad, een haven of op een vliegveld). RFID chips zijn thans al opgenomen in de Australische paspoorten (en worden binnenkort ook opgenomen in het Nederlandse paspoort), waardoor het gemakkelijker wordt om bepaalde personen te identificeren en op te

sporen. Een andere toepassing van deze minuscule chip is ze te implanteren in het menselijk lichaam. Voor exclusieve leden van een Rotterdamse discoclub wordt thans de mogelijkheid geboden deze chip te implanteren. Het voordeel is dat ze zich automatisch identificeren bij de toegang tot de club, terwijl het scannen van deze chip ook gebruikt wordt voor de registratie van consumpties die vervolgens automatisch worden afgeschreven.

Datamining

Een andere belangrijke ontwikkeling is het vermogen om uit bestaande informatie nieuwe informatie te creëren. De Kerckhove (1996) noemt dit 'gekoppelde intelligentie'. Door middel van allerlei nieuwe software ontwikkelingen en het feit dat steeds meer databestanden en uitwisselingsnetwerken gebaseerd zijn op open, internationaal erkende standaarden, wordt niet alleen technologie veel flexibeler maar dat geldt ook voor allerlei soorten van data en databestanden waardoor ze gemakkelijker gekoppeld kunnen worden, bijvoorbeeld met het oog op verificatie van gegevens. Een andere mogelijkheid is het maken van dwarsdoorsneden en profielen (bijv. risicoprofielen) waarbij gegevens binnen een of tussen verschillende databases met elkaar worden gekoppeld (Van Duivenboden, 1999).

2.7 Implicaties voor de nodale oriëntatie

Wanneer we deze technologische ontwikkelingen bezien vanuit het licht van de nodale oriëntatie van de politie, dan heeft dit op zijn minst de volgende implicaties voor de politie. Implicaties die zowel kansen als bedreigingen omvatten.

2.7.1 Intelligence Led Policing

Het belang dat op grond van de voorgaande verkenningen wordt gehecht aan het pro-actief verzamelen van (dynamische) informatie over bewegingen in allerlei knooppunten en binnen bepaalde stromen, maakt duidelijk dat de nodale politie een sterk informatiegedreven politie wordt. Dit wordt ook onderkend in 'Politie In Ontwikkeling' waarin gesproken wordt van een informatiegestuurde politie. Tegelijkertijd maken de in de voorgaande paragraaf beschreven technologische ontwikkelingen duidelijk dat er allerlei technologische mogelijkheden zijn die het belang van een informatiegestuurde politie ondersteunen.
Vandaar dat wij bepleiten om in de verdere uitwerking van de notie 'nodale politie' aansluiting te zoeken bij concepten die in dit verband zijn ontwikkeld, namelijk 'Intelligence Led Policing'. Dit wordt gezien als een uitwerking van de idee van 'smart policing', waarbij getracht is de doelmatigheid en doeltreffendheid van het politiewerk in de praktijk te verbeteren met gebruik van ICT. Tevens wordt 'smart policing' gezien als een meer pro-actieve (en dus een minder reactieve) vorm van politiewerk die vooral gericht is op 'law enforcement', op 'strafrechtelijke handhaving' (Tilley, 2003).

Achterliggende gedachte is dat getracht wordt een gedetailleerde en actuele foto te maken van patronen in criminaliteit, waardoor criminele netwerken kunnen worden ontmanteld, activiteiten eventueel kunnen worden verstoord (vergelijk de relatie met tegenhouden) en daders kunnen worden verwijderd; dit alles op basis van systematisch gebruik van informatie en een gerichte op de criminaliteit georiënteerde en gecoördineerde aanpak (Tilley, 2003). Dit veronderstelt echter wel dat er sprake is van een diepgaande kennis over de soort van activiteiten die zich binnen een crimineel netwerk afspelen. Volgens Versteegh (2005) is het belangrijk dat de gebruikte informatie niet alleen afkomstig is uit de databestanden van de politie, maar dat ook gebruik wordt gemaakt van informatie uit andere bronnen, van andere opsporingsdiensten. Daarnaast is het belangrijk om inzicht te krijgen in bijvoorbeeld de perceptie van burgers.

Binnen deze aanpak worden doorgaans vier informatieproducten onderscheiden, te weten (Tilley, 2003; Versteegh, 2005):

- Strategische analyses en beoordeling, gericht op lange termijn trends en voorspellingen voor de toekomst
- Tactische analyses en beoordelingen, die inzicht geven in lokaties en tijden waar en wanneer problemen zich voordoen (hotspots en hottimes).
- Daderprofielen, gericht op het in kaart brengen van een bepaalde dader of groep van daders bijvoorbeeld in relatie tot veelplegers en hun (terugkerende) gedragingen.
- Operationele analyses en beoordelingen, die inzicht geven in de vraag of in relatie tot een concrete casus de juiste dingen worden gedaan of dat in relatie tot een bepaalde proces de juiste dingen op een adequate manier worden gedaan.

Bovenstaande producten passen goed in een nodale oriëntatie. Geredeneerd vanuit een nodale oriëntatie zou het dan vooral gaan om strategische beoordelingen van de risico's die bepaalde stromen en knooppunten kunnen opleveren. Daarbij kan dan worden gedacht aan bijvoorbeeld de verkeersstromen in de haven van Rotterdam; de analyse van een specifieke stroom of een specifiek knooppunt in een groter knooppunt, zoals een bepaald expeditiebedrijf dat in de haven fungeert als draaipunt voor bepaalde criminele activiteiten waarbij gebruik wordt gemaakt van bepaalde waterwegen en verkeerswegen. Ook zou het in een dergelijke tactische of locatiegerichte probleembeoordeling kunnen gaan om een website of discussiegroep op het internet, of een analyse van de stromen en activiteiten binnen de bagageruimte van de luchthaven Schiphol. Van belang in dit alles is dat in deze producten de slag naar knooppunten en stromen moet worden gemaakt; deels wordt dit al gedaan, daar waar het gaat om probleem- en daderprofielen die gekoppeld zijn aan een hot spot.

Wanneer we de idee van Intelligence Led Policing meer nadrukkelijker in kaart willen brengen met de idee van het transparant maken van stromen in de

netwerksamenleving, dan gaat het om de volgende soort van interventies die door middel van technologie mogelijk worden, te weten (Bannister 2005):

- het volgen van personen c.q. het monitoren van het gedrag van personen bijvoorbeeld in het kader van camerabewaking;
- het onderscheppen van de communicatie tussen personen, bijvoorbeeld in het kader van afluisteren en onderscheppen van een e-mailbericht;
- het ontsluiten van data in diverse publieke en private databestanden, zoals het toegang krijgen tot data van banken waarin transacties zijn opgeslagen; en
- de interpretatie van bestaande data door ze op een bepaalde manier met elkaar in verband te brengen of te aggregeren, waardoor 'intelligence' ontstaat. Deze integratie van op zich zelf staande informatie moet nieuwe informatie opleveren die een beter beeld geeft van de gedragingen van bijvoorbeeld een persoon of bedrijf.

Wij willen er echter op wijzen dat 'intelligence' niet alleen verwijst naar informatie (sec) maar ook naar het vermogen om deze informatie in combinatie met reeds bestaande kennis en ervaring te kunnen beschouwen in hun context. Zo wordt informatie namelijk intelligentie. Dit is met name van belang wanneer het concept van de informatiegestuurde politie wordt toegepast op het analyseren en volgen van bewegingen in stromen en knooppunten waaraan immers verschillende soorten van (kennis en ervaringsaspecten) te onderscheiden zijn. Dit veronderstelt kennis van de context van een bepaald knooppunt en bepaalde stromen en van de complexiteit ervan.

Daarnaast betekent Intelligence Led Policing dat meer met risicoprofielen moet worden gewerkt om te bepalen welk soort gedrag binnen een stroom of van bepaalde soorten van bewegingen binnen een knooppunt (bijvoorbeeld de combinatie van een rederij, de eerder bezochte havens en de soort van lading in het geval van bijvoorbeeld drugssmokkel via zeehavens) als verdacht moet worden beschouwd. De nodale oriëntatie vraagt om een dergelijke benadering (zie ook par. 2.6). ICT kan het werken met dergelijke profielen ondersteunen.
Belangrijk is echter oog te hebben voor de risico's van een dergelijke benadering. Ten eerste kan worden gewezen op de betrouwbaarheid van de gegevens waarop deze profielen zijn gebaseerd. Ten tweede kan er een kloof bestaan tussen statistische relevante verbanden die niet altijd feitelijk waar behoeven te zijn. Zo kan er sprake zijn van een statistische verband (bijvoorbeeld op grond van factoranalyse) waardoor een groepsprofiel kan worden samengesteld, terwijl in de praktijk, in het geval van een concrete persoon, er weliswaar sprake is van een match (die wijst in de richting van verdacht), maar blijkt na kennisneming van andere factoren, dat een ander oordeel gerechtvaardigd was. Kortom, er kan een kloof zijn tussen het theoretische kenmerken en feitelijke kenmerken. Een verdenking betekent in dat geval dat aan bepaalde profielkenmerken wordt voldaan - hetgeen kan kloppen - maar nog niet behoeft te leiden tot een gerede verdenking. Ten derde bestaat er de kans dat risicoprofielen een eigen leven gaan leiden en dat alleen die risico's serieus worden

genomen die gebaseerd zijn op een risicoprofiel, waardoor sommige risico's bewust aan de aandacht ontsnappen. Dit is met name van belang omdat in de nodale oriëntatie getracht wordt de status van personen die zich bewegen in relatief anonieme stromen transparant te maken. Achterliggende gedachte is dat iedereen die aan een bepaald profiel voldoet, in eerste instantie als verdacht moet worden aangemerkt.

2.7.2 Detectietechnologie en 'Network centric warfare'

Een van de belangrijkste uitdagingen voor de nodale politie is het ontanonimiseren van personen zo stellen de opstellers van het visiedocument 'Politie in Ontwikkeling'. Technologie maakt het gemakkelijker om het verloop maar ook de status van goederen, personen en andere bewegingen door middel van een combinatie van monitoring/detectie/identificatietechnieken, al dan niet in combinatie met biometrie, te identificeren. Het aftappen van het (mobiele) telefoon en internetverkeer door de Echelon-organisatie is een typisch voorbeeld van het gebruik van technologie om de communicatiestromen in de netwerksamenleving en de inhoud van de uitgewisselde boodschappen te volgen. Vandaar dat het voor de verdere uitwerking van de nodale oriëntatie belangrijk is om de mogelijkheden van bepaalde soorten van detectie te koppelen aan de kenmerken van bepaalde knooppunten en de daarin plaatsvindende stromen.
In 'Politie in Ontwikkeling' wordt verwezen naar zogenaamde catch-kentechnieken, waarbij het scannen van bijvoorbeeld kentekens van voorbij rijdende voertuigen volautomatisch en realtime gekoppeld wordt met informatie uit allerlei registers, zoals de politieregisters, de kentekenregistratie en de GBA. Hierdoor kan snel informatie worden verkregen over de status van een voertuig of persoon. Een dergelijke techniek kan bijvoorbeeld inhouden dat op de 'toegangen' tot een knooppunt 'elektronische fuiken' worden opgesteld. Voorbeelden hiervan vinden op dit moment al plaats, daarbij denkende aan de irisscan/identificatie op Schiphol, het scannen van containers in de haven van Rotterdam, of het monitoren van de toegangswegen tot steden zoals Amsterdam. Om dit mogelijk te maken is het plaatsen van een 'elektronische fuik' niet persé noodzakelijk. De KLPD is thans in staat haar surveillance auto's uit te rusten met deze technieken. Door mee te bewegen in de verkeersstroom is de KLPD in staat om mobiel en volautomatisch informatie te matchen met andere informatie.

Een interessant voorbeeld van deze ontwikkeling is een technologisch geïnspireerd defensieconcept dat 'network-centric warfare' heet en dat door de VS reeds gebruikt is in Afghanistan en Irak. In dit concept worden de kenmerken van netwerktechnologie optimaal ingezet ter ondersteuning van interventies doordat verscheidene netwerken en infrastructuren aan elkaar gekoppeld zijn en er realtime informatie beschikbaar is, die voortdurend gesynchroniseerd wordt met andere systemen (bijv. strategische intelligence) maar ook 'battle information' systemen die veel gebruik maken van allerlei sensoren. Hierdoor krijgen eenheden die daadwerkelijk de gevechtshandelingen moeten verrichten een strategische informatievoorsprong op hun tegenstanders. Network centric warfare heeft de volgende voordelen: a) het ondersteunt on-line samenwerking ter plekke omdat informatie kan worden gedeeld, ongeacht waar

iemand zich bevindt; b) er ontstaat een gedeeld beeld van de situatie, omdat informatie 'realtime' ter beschikking komt, en c) men is in staat dit beeld te visualiseren waardoor veel sneller gereageerd kan worden. Dit concept is overigens niet alleen in oorlogstijd beproefd maar wordt ook gebruikt voor het vroegtijdig signaleren van verdachte bewegingen en preventief ingrijpen. Voorbeelden hiervan zijn te vinden bij politie van New York en in Louisiana (www.mitre.org). Een dergelijk concept zou interessant kunnen zijn in de uitwerking van de nodale oriëntatie, mits het nadrukkelijk wordt gekoppeld aan de specifieke kenmerken van een bepaald knooppunt en de daarin gelokaliseerde stromen. In ieder geval gaat het daarbij om knooppunten en stromen die sterk verweven zijn met de fysieke infrastructuur.

2.7.3 Informatiestrategie en kwaliteit informatievoorziening

Voor de uitwerking van de nodale oriëntatie van de politie technologie speelt technologie als instrument een zeer belangrijke rol; alleen de betekenis hiervan wordt vooral thans geduid in termen van te ontwikkelen applicaties. Het is echter belangrijk om op een andere manier naar technologie te kijken; een manier die verder reikt dan ' toys for the boys'.

Essentieel is om technologische ontwikkelingen in een breder perspectief te plaatsen door ze relateren aan het opbouwen van een strategische informatie- en kennispositie van de politie, waarin applicaties, informatiestromen en allerlei basisvoorzieningen vanuit een infrastructureel perspectief (dus in samenhang) worden beschouwd. Verder is het aanbevelenswaardig om deze ICT-strategie dienend te laten zijn aan de nodale oriëntatie. Hoe kunnen de informatie- en kennisbehoeften bij verschillende soorten van partijen die een rol spelen in de nodale oriëntatie van de politie worden ondersteund door middel van ICT? Wat betekent dit voor de organisatie en het verloop van relevante processen binnen de politie? En wat betekent dit voor de uitwisseling van kennis en informatie met andere partijen buiten de politie en in het buitenland? Daarbij dient ook de vraag aan de orde te worden gesteld, of de huidige organisatie van de informatievoorziening van de politie wel voldoende in staat is om deze nodale oriëntatie ondersteunen.

Tenslotte is het belangrijk om in de te ontwikkelen informatiestrategie rekening te houden met de politieke en maatschappelijke effecten van de inzet van technologie. In politieke, juridische en maatschappelijke discussies over de nodale oriëntatie zal bijvoorbeeld worden gewezen op het onderkennen van de ongewenste effecten van technologie. Dit brengt ons meteen op een andere verkenning die van belang is om inzicht te krijgen in de veronderstellingen die ten grondslag liggen aan het concept van de nodale politie, namelijk de normatieve veronderstellingen.

2.8 Politicologische en juridische verkenningen

Achter de idee van de nodale oriëntatie gaat een aantal veronderstellingen schuil die verwijzen naar de potentiële normatieve betekenis van het concept. In 'Politie in Ontwikkeling' wordt daarvoor aandacht gevraagd. Met name wordt dan verwezen naar het ontstaan van een nieuw sociaal contract tussen politie en burger, waarbij burgers bereid zijn op een hoger schaalniveau, een mogelijke aantasting van hun persoonlijke levenssfeer - die ontstaat doordat vooral technologie wordt ingezet om de verschillende stromen in netwerksamenleving te ontanonimiseren - in te ruilen voor het verkrijgen van meer veiligheid. Hier wordt een 'trade-off' verondersteld tussen vrijheid en veiligheid. In deze paragraaf trachten we de veronderstellingen achter deze en andere 'trade-offs' verder uiteen te rafelen door een aantal relevante politicologische en juridische leerstukken naar voren te brengen, terwijl tegelijkertijd ook moet worden bedacht dat de inzet van technologie – waarop de nodale oriëntatie sterk leunt – niet neutraal is maar 'waardegeladen' is.

De staat als panopticum

Ten eerste kan de verdere ontwikkeling van de idee van nodale oriëntatie worden gezien als een illustratie van het vermogen van (netwerk- en andere) technologie om vanuit elk willekeurig punt in de samenleving bepaalde processen in 'stromenland' transparant te maken. Dit is onder meer mogelijk door het koppelen van bestaande informatiebronnen waardoor nieuwe informatie en kennis wordt gegenereerd. Deze potentie wordt door De Kerckhove (1996) gedefinieerd als 'gekoppelde intelligentie' . Vervolgens zet deze transparantie de deur open voor intensievere en meer verfijnde vormen van controle (Bekkers, 1994). Lyon (1992) heeft deze ontwikkeling beschreven in termen van het realiseren van een digitaal panopticum. Het gevolg van deze concentratie van informatie op verschillende plekken in de samenleving – waardoor een 'totaalbeeld' kan worden gecreëerd – is dat er ook diverse machtscentra gaan ontstaan. Informatie is immers macht. Dit roept de vraag op, hoe de bundeling van informatiebronnen tot informatiemacht effectief kan worden gecontroleerd (Bekkers, 1998).

Het normatieve karakter van technologie

Deze ontwikkeling krijgt nog meer reliëf wanneer bedacht wordt dat technologie geen neutraal en dus waardevrij instrument is. Drie overwegingen onderstrepen dit.
Ten eerste laat onderzoek zien dat technologie een politiek instrument is, en daarmee ook een machtsbron, dat wordt ingezet voor de articulatie en bescherming van specifieke belangen van bepaalde partijen en de wereld- en mensbeelden die daaraan ten grondslag liggen; belangen en referentiekaders die ook de vormgeving en gebruik van technologie beïnvloeden (Bijker et al., 1987). Technologie is daardoor ook een kneedbaar (Bijker et al, 1987; Winner, 1988).
Ten tweede wijzen andere erop dat technologie per definitie gericht is op controle en disciplinering. Dit is inherent aan de aard van technologie (Beniger, 1990). Bij

informatie- en communicatietechnologie wordt het inherente controlepotentieel nog eens versterkt door het reflexieve karakter van deze technologie. Wat bedoelen we hiermee? Het gebruik van ICT laat overal digitale sporen achter, waardoor het gedrag van mensen veel gemakkelijker kan worden gereconstrueerd of worden gevolgd (Zuboff, 1988; Frissen, 1989). De betekenis hiervan wordt nog vitaler, indien we bedenken dat ICT is doorgedrongen tot in de haarvaten van onze samenleving, hetgeen impliceert dat er legio digitale sporen zijn die transparant kunnen worden gemaakt en kunnen worden gecombineerd. De vraag is echter welke veronderstellingen aan deze combinaties ten grondslag liggen.
Ten derde wordt vaak gewezen op de onbedoelde effecten van technologie. Ook al wordt technologie met de beste bedoelingen van de wereld ingezet, vaak zien we dat allerlei onbedoelde (gewenste en ongewenste) effecten optreedt, omdat technologie, wanneer deze eenmaal is ingezet, een eigen dynamiek heeft (Frissen, 2004).

De afweging tussen vrijheid en veiligheid

De politieke en daarmee ook normatieve discussie over de nodale politie staat ten eerste in het teken van het spanningsveld tussen enerzijds vrijheid - in de zin van mogelijke aantasting van de persoonlijke levenssfeer van burgers - en anderzijds het bieden van veiligheid aan diezelfde burger. Juist het bieden van veiligheid kan van oudsher beschouwd worden als een van de kerntalen van de staat en van haar politieorganisatie (Stone, 2003). Defacto gaat het om twee grondrechten die mogelijkerwijs op gespannen voet staan met elkaar. Een kader voor het maken van deze keuze wordt geboden door de Wet Bescherming Persoonsgegevens. Daarin wordt een aantal criteria naar voren gebracht waaraan het College Bescherming Persoonsgegevens de afweging probeert te maken, namelijk:

a) er moet sprake zijn van doelbinding, gegevens mogen niet worden gebruikt voor andere doeleinden dan waarvoor ze zijn verzameld, zij het dat daar onder specifieke voorwaarden van kan worden afgeweken;
b) er moet sprake zijn van causaliteit, dit wil zeggen dat er sprake moet zijn van een oorzakelijk verband waarbij een bepaald gedrag leidt tot bepaalde ongewenste effecten, hetgeen vervolgens een rechtvaardiging kan opleveren om dit gedrag transparant te maken'
c) er moet sprake zijn van proportionaliteit, dit wil zeggen dat een mogelijke, zij het tijdelijke, aantasting van de privacy in verhouding moet staan tot daadwerkelijk aantoonbare en feitelijk te realiseren opbrengsten; en
d) er moet sprake zijn van het optimaal mogelijk gebruik maken van de bestaande bevoegdheden op grond waarvan een aantasting van de privacy mogelijk wordt. Daarbij dient tevens specifiek te worden aangegeven, lettende op de aard van het betreffende geval, waarom eventuele aanvullende bevoegdheden nodig zijn.

De afweging tussen veiligheid en efficiency

Een andere waarden afweging die van belang is, heeft betrekking op de kosten die moeten worden gemaakt om een bepaald gewenst niveau van veiligheid te kunnen bieden en de feitelijk beoogde resultaten te behalen (Stone, 2003). Bijvoorbeeld de kosten die moeten worden gemaakt en de inspanningen die moeten worden geleverd om een bepaald veiligheidsniveau op Schiphol te realiseren. Tegelijkertijd is het lastig om deze feitelijke resultaten zichtbaar te maken, omdat de genomen veiligheidsmaatregelen ook nog een preventieve werking hebben, die niet in cijfermatige resultaten kunnen worden weergegeven.

De afweging tussen veiligheid en gelijkheid

Een laatste trade-off heeft betrekking op de mate waarin de behoefte om van staatswege meer veiligheid te bieden al dan niet te koste gaat van de gelijkheid van burgers c.q. gelijke behandeling van burgers (Stone, 2003). Kortom, in het bieden van bescherming van burgers door de staat dient rekening te worden gehouden met de politieke en ook rechtsstatelijke wens om 'alle gelijke gevallen op gelijke, en alle ongelijke gevallen op een ongelijke manier' te behandelen. Essentieel is de vraag of er ruimte is voor differentiatie en maatwerk.

Afwegingen en risico's

De nodale oriëntatie dwingt tot het maken van afwegingen tussen politieke waarden. Hoe deze afweging uitvalt is onder meer afhankelijke van de in het geding zijnde risico-inschatting. Van belang is erop te wijzen dat het inschatten van risico's geen calculeerbare activiteit is - Beck (1999) spreekt in dit geval over de zogenaamde risico calculus. Ook hier is het van belang om het normatieve karakter van risico's in ogenschouw te nemen. Het gaat immers om de perceptie van mogelijke risico, waarbij moet worden bedacht dat aan deze perceptie immers altijd bepaalde veronderstellingen ten grondslag liggen; veronderstellingen ten aanzien van wat een organisatie of een samenleving als ongewenst, als risicovol definieert en welke waarden, mens- en wereldbeelden hierbij in het geding zijn. Dit is niet altijd een gegeven, maar een vraag die per definitie een politieke en maatschappelijke discussie impliceert (Douglas & Wildavsky, 1983). Het is volgens Beck (1999) echter de vraag of deze discussie wel wordt gevoerd.

2.9 Implicaties voor de nodale oriëntatie

In de vorige paragraaf is een aantal leerstukken behandeld die van belang zijn voor de discussie over de normatieve implicaties van de nodale oriëntatie. Wij zullen in dit rapport hierin geen stelling nemen. Een afweging tussen de normatieve veronderstellingen die ten grondslag liggen aan de (verdere uitwerking van de) nodale oriëntatie is per definitie een politieke keuze en behoort inzet te zijn van een politiek en maatschappelijk debat. Wij geven alleen maar aan wat de agenda van deze

discussie zou kunnen zijn, wanneer we bovenstaande inzichten toepassen op de nodale oriëntatie.

2.9.1 'Checks and balances' in de panoptische staat

Een belangrijk aandachtspunt in de normatieve discussie over de nodale oriëntatie is de mate waarin de concentratie van informatiemacht - die ontstaat wanneer bestanden aan elkaar worden gekoppeld en het gedrag van personen wordt gevolgd - ook daadwerkelijk is ingebed in een systeem van controle en verantwoording. Wie controleert in dit geval de controleur? En, zijn we de in te zetten technologie wel degelijk de baas (De Mul, 2001)? Kortom, voor de verdere uitwerking van het concept van de nodale oriëntatie is het noodzakelijk om deze in te bedden in een systeem van 'checks and balances' teneinde de kans op machtsmisbruik te voorkomen (Bekkers, 1998).

De noodzaak om dit systeem te ontwikkelen is niet alleen verdedigbaar vanuit het perspectief van de individuele burger. Er is nog een andere ontwikkeling die hiertoe noopt. Samenwerking tussen de politie en andere opsporingsdiensten – zowel in de publieke als private sfeer – is namelijk een ander belangrijk kenmerk van de nodale oriëntatie. Het gevolg is dat de grenzen tussen deze organisatie gaan verschuiven met als resultaat dat een 'grenzeloze overheid' ontstaat (Bekkers, 1998). Grenzen vervagen of worden opgerekt, hetgeen ook van invloed is op de jurisdicties van deze organisaties. De notie van een jurisdictie verwijst naar de exclusieve toebedeling van bepaalde taken, verantwoordelijkheid en bevoegdheden en een daarmee samenhangende beleidsvrijheid, op grond waarvan een organisatie bepaalde rechten en plichten kan toebedelen aan burgers, terwijl de notie tegelijkertijd verwijst naar het afleggen van politieke en juridische verantwoording over het gebruik van deze bevoegdheden (Bekkers, 1994). Dit betekent dat in een verdere uitwerking van de nodale politie in ieder geval drie vragen moeten worden beantwoord:

- waar is de macht gelokaliseerd die op grond van de verzameling en combinatie van informatie wordt gegenereerd;
- Wat is de reikwijdte van die macht; en
- Welke politieke waarden moeten tegen elkaar worden afgewogen teneinde er voor te zorgen dat de macht die in het concept van de nodale politie besloten ligt, op een zorgvuldige en controleerbare manier wordt toegepast?

In de volgende paragraaf gaan we in ieder geval in op de 'trade-offs' tussen een aantal politieke waarden. Het lastige daarbij is dat 'de nodale oriëntatie' niet bestaat, maar dat het beantwoorden van deze vragen sterk afhankelijk is van de context waarbinnen een nodale oriëntatie wordt ontwikkeld. Tevens dient bij beantwoording van deze vragen nadrukkelijk rekening te worden gehouden met het feit dat ICT geen neutraal en waardevrij instrument is. De inzet van technologie en het optreden van beoogde resultaten worden mede bepaald door bepaalde belangen en daarmee samenhangende mens- en wereldbeelden, terwijl er tevens onbedoelde effecten optreden; effecten die een eigen dynamiek krijgen, hetgeen de controleerbaarheid en stuurbaarheid van de technologie ondermijnt, ondanks alle goede intenties.

In 'Politie in Ontwikkeling' wordt onder meer naar voren gebracht dat er sprake is van een groot vertrouwen van burgers in de politie, omdat willekeur en machtsmisbruik niet tot de traditie en cultuur van de politie behoren. Dit laat zien dat er binnen de politie voldoende informele 'checks and balances' zin. Toch verdient het aanbeveling te streven naar een formeel systeem van checks and balances, de waarschuwing van Madison – een van de 'founding fathers' van de Amerikaanse constitutie- in acht nemend*:"if men were angels no government would be necessary. If angels were to govern men, neither external controls nor internal controls would be necessary"(Hamilton, Madison & Jay, 1966:160).*

2.9.2 Enkele afwegingen tussen politieke waarden

In de vorige paraaf hebben we laten zien dat tenminste drie soorten van waardenafwegingen van belang zijn; afwegingen die ten grondslag liggen aan de normatieve inbedding en legitimatie van de nodale oriëntatie.

De eerste relevante normatieve afweging die voor de uitwerking van de nodale oriëntatie van belang is, is die tussen vrijheid en veiligheid, waarbij vrijheid met name wordt geconcretiseerd in termen van de bescherming van de persoonlijke levenssfeer. In het geval van de nodale oriëntatie is aantasting van de privacy mogelijk het gevolg van a) het volgen van personen c.q. het monitoren van het gedrag van personen bijvoorbeeld in het kader van camerabewaking, b) het onderscheppen van de communicatie tussen personen, bijvoorbeeld in het kader van afluisteren en onderscheppen van een e-mailbericht, c) het onsluiten van data in diverse publieke en private databestanden, zoals het toegang krijgen tot data van banken waarin transacties zijn opgeslagen, en d) de interpretatie van bestaande data door ze op een bepaalde manier met elkaar in verband te brengen of te aggregeren, waardoor 'intelligence' ontstaat. Deze integratie van op zich zelf staande informatie moet nieuwe informatie opleveren die een beter beeld geeft van de gedragingen van bijvoorbeeld een persoon of bedrijf (Bannister, 2005)
Van belang is om deze afweging te concretiseren. De nodale oriëntatie als concept leent zich hiervoor niet. Van belang is deze afweging inzichtelijk te maken aan de hand van een concrete manifestatie van de nodale oriëntatie, alsmede dit te laten variëren met de risico's die hierbij op het spel staan. Daarbij is in ieder geval het onderscheid van belang tussen een verdachte en een niet-verdachte, zeker daar waar het gaat om het ont-anonimiseren van personen binnen bepaalde stromen zonder dat op voorhand duidelijk is wie een potentiële verdachte is.
Tegelijkertijd staat daar ook een andere gedachte tegenover, die met name ook in 'Politie In Ontwikkeling' naar voren wordt gebracht: het bieden van meer veiligheid teneinde de vrijheid van burgers te kunnen garanderen, waarbij de vrijheid van het zich veilig kunnen voortbewegen binnen een bepaalde publieke ruimte (zowel fysiek als virtueel) gepaard gaat met een bepaalde aantasting van de persoonlijke levenssfeer. Maar ook hier geldt dat deze afweging alleen handen en voeten krijgt,

indien ze concreet wordt gemaakt door ze te relateren aan een bepaalde praktijk en niet aan bepaalde 'abstracte' schaalniveaus.

Een tweede afweging betreft de afweging tussen vrijheid en efficiency. Een eerste vraag betreft de kosten die moeten worden gemaakt c.q. de investeringen die moeten worden gedaan om het gedrag van bepaalde personen transparant te maken. Dit moet in verhouding staan tot het doel. In hoeverre kan bijvoorbeeld de vrijheid van grote groepen burgers die zich binnen bepaalde stromen en knooppunten bewegen worden aangetast, om zo meer veiligheid te kunnen bieden.

Een derde afweging betreft de afweging tussen veiligheid en gelijkheid. De nodale oriëntatie is gericht op het bieden van veiligheid binnen bepaalde stromen en knooppunten, hetgeen in veel gevallen betekent dat er niet op voorhand sprake is van een bepaalde verdachte. In veel gevallen gaat het om het volgen en/of ont-anonimiseren van grote groepen van in principe niet verdachte personen die echter als 'verdachte' worden aangemerkt. Verdachten en niet-verdachten worden dan als gelijk behandeld, louter vanwege het feit dat zij zich binnen een bepaalde stroom of knooppunt bewegen. Maar ook ten aanzien van deze afweging geldt dat 'gelijke behandeling' verdedigbaar is op grond van de in het geding zijnde risico's; een afweging die echter alleen maar inhoud krijgt, wanneer ze geconcretiseerd kan worden aan de hand van een specifieke praktijksituatie.
Tegelijkertijd kan ook naar voren worden gebracht dat juist door de mogelijkheid die ICT biedt tot allerlei vormen van profilering er meer maatwerk mogelijk is, waardoor 'gelijke gevallen' eerder kunnen worden opgespoord. Daar staat echter tegenover dat deze vormen van profilering gebaseerd zijn op theoretische en statistische verbanden, waardoor er sprake is van een theoretisch gerede verdenking die echter geen recht doen aan de feitelijke situatie waarin een bepaalde persoon zich bevindt.

Wij hebben in deze paragraaf in kaart gebracht welke afwegingen in het geding zijn. Het heeft volgens ons geen zin om deze afwegingen in zijn algemeenheid te verkennen en allerlei algemene voor- en nadelen in kaart te brengen. Essentieel is het duidelijk maken wie verantwoordelijk is voor een afweging en hoe deze afweging wordt gemaakt (Bannister, 2005). Van belang is deze afwegingen concreet te maken aan de hand van bepaalde praktijkvoorbeelden en de dilemma's en grenzen concreet in dialoog met bijvoorbeeld het College Bescherming Persoonsgegevens te verkennen. Tegelijkertijd zou het interessant kunnen zijn voor de politie om over de concrete uitwerking van de nodale oriëntatie een maatschappelijke debat te organiseren over de normatieve grenzen waarbinnen burgers en maatschappelijke organisaties een nodale oriëntatie al dan niet acceptabel vinden.

2.10 Samenvatting

In dit hoofdstuk stond de vraag centraal, voor welke problemen en maatschappelijke ontwikkelingen de nodale politie een antwoord is. Hoe zien die ontwikkelingen eruit? Wat betekenen ze voor de inhoud van het concept van de nodale oriëntatie? Door deze vragen te beantwoorden zijn we in staat geweest om de aannames achter het concept beter te begrijpen en deze verder uitwerken. Om deze veronderstellingen inzichtelijk te maken, maken we gebruik van een aantal, in onze ogen relevante, sociologische, criminologische, technologische en politicologisch-juridische leerstukken. Telkens weer hebben we per paragraaf aangeven wat de implicaties van deze leerstukken zijn voor de verdere ontwikkeling van het concept van de nodale oriëntatie.

3 MANIFESTATIES VAN DE NODALE ORIËNTATIE: PRAKTIJKVOORBEELDEN

3.1 Inleiding

In het vorige hoofdstuk hebben we reeds enkele malen verwezen naar diverse praktijkvoorbeelden van een nodale oriëntatie bij de politie maar ook bij andere (zowel publieke als private) opsporingsdiensten. In dit hoofdstuk willen we deze voorbeelden pregnanter aan de orde stellen. Daarmee wordt dan ook voldaan aan de tweede vraag uit de probleemstelling: *Welke toepassingen van deze nodale oriëntatie zijn denkbaar en waarop hebben deze betrekking?* Daarnaast willen we aandacht schenken aan de condities waaronder voorbeelden al dan niet succesvol zijn geweest. Daarmee geven we dan ook een antwoord op de derde vraag uit de probleemstelling*: Wat zijn de te verwachten condities (bijv. menskracht, expertise, ICT, bevoegdheden) waaronder deze toepassingen gerealiseerd kunnen worden, wat zijn mogelijke effecten en mogelijke kritische succes- en faalfactoren?*

In de selectie van onze praktijkvoorbeelden hebben we getracht zoveel mogelijk recht te doen aan de eerdere indeling van nodale oriëntaties die we in het vorige hoofdstuk hebben onderscheiden. In onderstaande tabel worden deze voorbeelden hieraan gerelateerd.

STROOM	PRAKTIJKEN VAN DE NODALE ORIENTATIE
PERSONEN	Monitoring en tegenhouden van voetbalhooligans Monitoring personen en hun bagage binnen knooppunt Schiphol
INFORMATIE	Digitaal rechercheren/cybercrime
GOEDEREN	Monitoring en opsporing van verdachte ladingen in de haven Rotterdam (knooppunt) door de Douane
VERKEER	Catch-ken Hoeksche Waard Ochtendgloren KLPD
FINANCIËN	Fraude en opsporing verdachte transacties in het creditcardbetalingsverkeer door Equens Nederland (voorheen Interpay)

Tabel 3.1: Praktijkvoorbeelden nodale oriëntatie per stroom

In de navolgende paragrafen worden deze praktijken kort beschreven. Het gaat hierbij om 'quick scans'. We hebben niet de pretentie om uitgebreide case studies te presenteren. We hanteren hierbij de volgende werkwijze. Ten eerste beschrijven we een aantal relevante achtergronden zoals de aanleiding voor de het ontwikkelen van een nodale oriëntatie, de doelstellingen die worden beoogd. Ten tweede trachten we de kenmerken van de nodale oriëntatie die in praktijk wordt gebracht te beschrijven alsmede de ambities die men voor de nabije toekomst heeft. Ook besteden we aandacht aan de wijze waarop het project is opgezet en de geboekte resultaten. Ten derde beschrijven we een aantal relevante kritische factoren, zoals die vooral door de geïnterviewde personen naar voren worden gebracht. Nadat we deze uiteenlopende praktijken hebben beschreven en geanalyseerd, zal een korte case vergelijking plaats vinden waarin een aantal lessen zullen worden getrokken met het oog op de verdere uitwerking van de nodale oriëntatie.

3.2 Goederenstroom: DOUANE IN DE HAVEN VAN ROTTERDAM

3.2.1 Achtergrond

De douane is een generieke controledienst die toezicht houdt op het grensoverschrijdende goederenverkeer, dus op de invoer, de doorvoer en de uitvoer van goederen. De douane voert de facto lijnstoezicht uit. De werkzaamheden van de douane worden voor een groot deel bepaald door haar rol als bewaker van de buitengrens van de Europese Unie. Zij fungeert immers als 'poortwachter' tot de Europese interne markt. In tegenstelling tot bijvoorbeeld de politie is de douane goederengericht; goederen die samenhangen met het internationale handelsverkeer. De douane gaat over zendingen, vracht en containers en schepen, terwijl de politie maar ook de marechaussee voornamelijk over personen gaat. In deze handel spelen allerlei tussenpersonen, zoals expediteurs, een belangrijke rol (Bedrijfsplan belastingdienst 2006-2010, p. 22). Een betere controle van de buitengrenzen op het terrein van veiligheid moet ertoe leiden dat bij grensoverschrijdende goederenbewegingen de *safety* van mensen en de *security* van goederen gegarandeerd zijn (Bedrijfsplan Belastingdienst 2006-2010). Om dit mogelijk te maken wil de douane zich verder ontwikkelen in de richting van een sterk door informatie en informatietechnologie gedreven organisatie. Dit vereist niet alleen een adequaat functionerende informatievoorziening, maar ook een duidelijke strategie die sturing geeft aan de inrichting van een dergelijke informatievoorziening.
In de Rotterdamse haven is de douane vooral gericht op inkomende goederen, niet op uitgaande. Jaarlijks wordt 380 miljoen ton goederen ingevoerd. Dit volume aan goederen is uiteraard veel te groot om allemaal te kunnen controleren. Vandaar dat belangrijk is om de schaarse middelen geconcentreerd in te zetten.

3.2.2 Nodale oriëntatie

De interventiestrategie van de douane is gericht op het opbouwen van een informatiepositie in een knooppunt van vooral inkomende, internationale goederenstromen. Er zijn twee aangrijpingspunten. Ten eerste tracht de douane een beeld te krijgen van de bewegingen van bepaalde containers binnen bepaalde goederenstromen. Getracht wordt om een dynamisch beeld te krijgen op het moment dat een container onderweg is. Door containers meer en beter te monitoren beweegt de douane als het ware mee met de goederenstromen, die voor haar werk van belang zijn. Op grond van dit beeld wordt een risicoprofiel opgesteld. Dit kan ertoe leiden dat nader fysiek onderzoek wordt ingesteld. Een daarmee komen we bij het tweede aangrijpingspunt, de toegang tot de haven of binnen de haven. Hier worden nadere controles uitgevoerd, waarin de zogenaamde containerscan een belangrijke rol speelt.

Risico-selectie

De douane werkt momenteel met een systeem voor risicoselectie, PRISMA genaamd. 95% van alle informatie over goederenzendingen wordt elektronisch aangeleverd. PRISMA moet de douane in staat stellen om potentieel risicovolle zendingen te selecteren, die vervolgens worden gecontroleerd. Het systeem genereert automatische hits op basis van risicoprofielen. Deze profielen worden periodiek bijgesteld op basis van actuele informatie, gedane constateringen en in kaart gebrachte ervaringen. Een profiel kan worden gezien als de neerslag van gecumuleerde ervaringskennis.
Op grond van PRISMA wordt ongeveer 60% van alle zendingen als niet-risicovol beschouwd. De douane hoeft deze dan ook niet te zien. Naar de resterende 40%, ongeveer een miljoen zendingen, wordt nader onderzoek uitgevoerd. Soms gaat het om meerdere containers, soms om een container met veel zendingen. Dit geschiedt door analisten. Dit zijn functionarissen die een analistenopleiding hebben gevolgd. Zij kennen PRISMA, maar werken daarnaast op ervaringskennis en intuïtie ('Fingerspitzengefühl). Hun belangstelling wordt getriggered door zaken die niet deugen of niet logisch zijn. Op basis daarvan wordt besloten tot een containerscan. Op deze manier wordt de inbreng van de menselijke factor in het proces van risico-analyse en –selectie gewaarborgd.

'Alles aan rumoer en signalen wordt vastgelegd. We zoeken op naam, op goederen, op boot, op land. Dan constateer je, er is wat en doen wij een scan. Het is de menselijke factor. Je krijgt het niet allemaal in de machine. Een groot deel wordt weggestreept'. (Bron: interview)

Nieuwe constateringen worden ingevoerd in PRISMA, waardoor het systeem met feiten en ervaringen wordt gevoed. Het resultaat is dat een zelflerend systeem ontstaat, waardoor nog meer verfijnde risicoprofielen kunnen worden opgesteld.

De containerscan

Bestaat er twijfel over de overeenkomst tussen formeel beschreven en de feitelijke inhoud van een container, dan wordt besloten om de betreffende container door een containerscan te halen. Er worden jaarlijks ongeveer 50.000 foto's van ladingen van containers gemaakt. De analisten bestuderen de foto's om mogelijke discrepanties tussen beschreven en feitelijke lading te ontdekken. Het voordeel van een scan is dat een lading per blok uit een totaaloverzicht kan worden geselecteerd om deze vervolgens te kunnen vergroten, te kunnen in- of uitzoomen. Bij twijfel wordt de container gelost, dat wil zeggen opengemaakt. Er vindt dan een feitelijke inspectie plaats.
Binnen de Rotterdamse haven ontwikkelt de scantechniek zich vrij snel. Bij de ECT worden vanaf 2007 alle vrachtauto's door poortjes geloodst. Deze poortjes zijn uitgerust met meetapparatuur die het mogelijk maakt om nucleaire straling op te sporen. Binnenkort zullen ook treinen een zelfde behandeling moeten doorlopen. In het geval bepaalde meters gaan piepen, komen ambtenaren uit de centrale commandopost om met behulp van sterkere meetapparatuur een nader onderzoek in te stellen. Blijft het piepen aanhouden, dan is er een gerede kans dat een container nucleair materiaal bevat. Dan wordt de container veilig gesteld en wordt het ministerie van VROM erbij gehaald.

Een ontwikkeling in de nabije toekomst is het gebruik van zogenaamde '*container security devices'.* Dat zijn apparaten die bij vertrek aan een container worden bevestigd en die de route van containers vastleggen. Bij binnenkomst van een container, kunnen deze gegevens, net als bij de zwarte doos in een vliegtuig, worden gelezen en kan bijvoorbeeld worden nagegaan of de deuren open zijn geweest, of de container gestopt is of beschadigd is. Als bij het uitlezen van deze gegevens, een piepsignaal wordt afgegeven, volgt nadere controle. Op de langere termijn wil de douane een *'controlestraat'* op de weg naar de Maasvlakte, met scans, detectiepoorten en 'container security devices' gaan aanleggen Dit wordt een soort afvangplek voor zowel het binnenkomende als het uitgaande goederenverkeer. In de nabije toekomst zal ook gebruik gemaakt worden van *radio frequency identifiaction devices* (RFID's). Hiermee komt het permanent volgen van containers per satelliet binnen handbereik.

Ambitie

De douane heeft de ambitie zich op grond van haar kennis van goederen, handelaren en logistieke processen, te ontwikkelen tot mederegisseur van het veiligheidsbeleid, zodat burgers met één loket te maken hebben. Politie, marechaussee en douane moeten optreden als één overheid. Goederencontroles moeten niet achter elkaar maar met elkaar worden uitgevoerd en burgers moeten terechtkunnen bij één loket. Het idee van gezamenlijkheid is ook cruciaal voor informatiemanagement. De Douane wil in de komende jaren uitgroeien tot het knooppunt waar alle informatie die betrekking heeft op het grensoverschrijdende goederenverkeer bij elkaar komt. Informatie zou gezamenlijk opgeslagen en gezamenlijk gebruikt moeten worden. Maar dat is nog toekomstmuziek. In de toekomst moeten er gezamenlijke risicoanalyses van schepen

gemaakt worden. Dit moet ondersteund worden door gezamenlijk beheer en met voor alle partijen toegankelijke databestanden en systemen die voor gezamenlijke trajecten geraadpleegd kunnen worden, wel met beperkingen voor autorisatie, bijvoorbeeld vanwege privacy gevoelige informatie over individuen. Het kernprobleem voor de douane blijft alle relevante informatie van een grensoverschrijding tijdig bij elkaar te krijgen. Risicomanagement blijft daarbij de hoeksteen voor de douane. Informatie is voor de douane van levensbelang om selectief te kunnen controleren. De ontwikkeling van de *intelligence*-functie zal de komende jaren daarom grote aandacht krijgen (Bedrijfsplan belastingdienst 2006-2010, p. 24).

	DOUANE ROTTERDAMSE HAVEN
TYPE STROOM	Goederen
INTERVENTIE	Toegang tot knooppunten controleren en meebewegen
OMVANG	selectieve controle
EFFECT	ongehinderde doorstroom
INTENSITEIT	Continu (up-to-date houden)
GEOGRAFISCH	Vast op vooraf bepaalde punten én mobiel
MANIFESTATIE	Zichtbaar(controlestraat) en onzichtbaar (risico-analyses)
RISICO SELECTIE	bepaald door kracht van **observatie en technologie** - Verzamelde en opgebouwde informatie (PRISMA) - Human Factor
REFERENTIE	containers/goederen

Tabel 3.2: samenvatting kenmerken casus Douane Rotterdamse Haven

3.2.3 Kritische factoren

Het opbouwen van een strategische informatiepositie door de douane is echter alleen mogelijk indien expliciet aandacht wordt besteed aan de kwaliteit van de informatie-uitwisseling met andere publieke en private partijen. Immers de betreffende interventiestrategie leunt sterk op de betrouwbaarheid en snelheid waarmee informatie door andere partijen wordt aangeleverd. Dit betekent dan ook dat de douane het belang van samenwerking als expliciet punt van aandacht ziet in de ontwikkeling van haar nodale oriëntatie. Ook hierop gaan we nader in.

Samenwerking en partnerships

Samenwerking en informatie-uitwisseling met private partijen, andere opsporingsdiensten en douane organisaties in andere landen is voor de douane van groot belang. Zo werkt de douane aan het ontwikkelen van een 'partnership' met

bedrijven. Een bedrijf dat bewezen heeft 'compliant' te zijn, wordt vergunninghouder. Deze bedrijven krijgen faciliteiten zoals toestemming om goederen in het eigen bedrijf op te slaan, zonder dat vooralsnog belasting moet worden betaald. Zij stellen zich echter wel borg voor de goederen die zij opgeslagen hebben. Hun voordeel is dat zij dus niet elke binnenkomst van een nieuwe lading moeten melden aan de douane. Dit kan ook achteraf geschieden. Daar staat echter een informatieplicht van bedrijven tegenover. Zij moeten de douane informeren over de soort van lading, de herkomst, het vervolgtraject enz. Op deze manier tracht de douane gezonde en open informatierelaties te ontwikkelen met partijen in de haven.

De idee hierachter is dat niet alleen de overheid verantwoordelijk is voor handhaving. De douane wil uiteindelijk het bestaande vergunningenproces verbreden tot een systeem van certificering, waarin veiligheid centraal zal staan. Klanten worden gecertificeerd op de integriteit van de processen, de organisatie en het daarin werkzame personeel. De douane maakt daarbij zoveel mogelijk gebruik van de veiligheidsprocedures en –initiatieven die ondernemingen zelf al hebben ontwikkeld. Op grond van deze gecertificeerde processen wordt tevens meer en betere informatie gegenereerd waardoor ook het bestaande risico-selectieproces kan worden versterkt. Op de wat langere termijn wordt het stelsel van vergunninghouders uitgebouwd en zal worden aangesloten bij de definities die de Europese Commissie ontwikkelt voor de zogenoemde *Authorised Economic Operators* (AEO's). Dit houdt in dat de zendingen van een AEO in beginsel ongehinderd de buitengrens van de EU kunnen overschrijden. Fysieke controles worden vooral toegepast ten aanzien van niet-gecertificeerde en onbekende klanten.

Een ander belangrijke punt is dat er binnen de Rotterdamse haven veel en goede samenwerkingsrelaties bestaan met andere opsporingsdiensten, zowel beleidsmatig als operationeel. Deze zijn gebundeld in het Expertisecentrum Haven. In het Expertisecentrum Haven werken zeehavenpolitie, douane en havenbedrijf samen om de veiligheidsrisico's en criminaliteitsontwikkelingen in het haven- en industriecomplex te inventariseren en beoordelen. Daarin participeren zowel de zeehavenpolitie als het Openbaar Ministerie. Verder werken ook de douane en politie nauw samen, omdat beiden immers op de schepen komen: zij varen beiden. Er is samenwerking in het gebruik van boten en het gebruik van informatie. Er is ook een platform samenwerking controlediensten. Hierin worden zendingen goederen op één tijdstip op één plek gecontroleerd. Een probleem voor de douane in de samenwerking met de politie is de zelfstandigheid van politieregio's. De douane moet zijn netwerk over meerdere korpsen verspreiden. Samenwerking staat of valt met goede contacten. Goederen houden immers niet op bij regiogrenzen. Het volgen van bepaalde transporten vanuit naar de grens kost relatief veel inspanning omdat hierbij verschillende politieregio's betrokken zijn.

Informatie-uitwisseling

Met andere diensten wordt informatie uitgewisseld, maar binnen de kaders én de beperkingen van de wettelijke grenzen. Douanewerk bestaat in essentie uit het omgaan met informatie over vier bronnen: actoren, goederen, zendingen en geld. Vroeger bevonden deze zich allen op één plek. Ten aanzien van een gebeurtenis, namelijk het overschrijden van een grens, moet al deze informatie bij elkaar gebracht worden; informatie die meestal aanwezig is bij andere diensten. Dit roept problemen op.

Ten eerste is het lastig om de informatiesystemen van de verschillende hierbij betrokken te koppelen. Er is een veelheid aan niet-compatibele systemen. Hieraan liggen allerlei technische en informatiekundige oorzaken ten grondslag. Daarbij kan worden gedacht aan het 'legacy' karakter van veel systemen maar ook het ontbreken van eenduidige gegevensdefinities en basisregistraties.

Ten tweede is het ook de vraag of het koppelen van deze bestanden en daarin opgeslagen gegevens juridisch wel mag. Informatie mag alleen worden aangewend voor het doel waar het voor is verzameld, bijvoorbeeld belasting heffen of andere fiscale taken. Deze informatie is niet bedoeld voor opsporing. Deze bescherming heeft te maken met de angst voor misbruik van informatie en de noodzaak om de integriteit van het overheidsoptreden te waarborgen. Een nodale oriëntatie betekent echter dat de traditionele en wettelijk vastgelegde scheiding (in termen van 'checks and balances') die in Nederland wordt gehanteerd tussen enerzijds controle en anderzijds opsporing, steeds meer ter discussie wordt gesteld. In andere landen zoals VS en het Verenigd Koninkrijk is dit onderscheid inmiddels opgeheven vanwege het toegenomen politieke en maatschappelijke belang dat aan veiligheid wordt gehecht. In het Verenigd Koninkrijk is het bijvoorbeeld mogelijk dat de douane gegevens over de personenstroom koppelt aan de goederenstroom. Dit gebeurde ook al voor 11 september. In het geval van Nederland moet de douane zich beperken tot informatie over goederen. Dit bemoeilijkt ook de samenwerking met de douanediensten in andere landen. De douane wisselt immers ook informatie uit met de douane in andere landen. De Rotterdamse haven is een partner in het CSI, Container Security Initiative.[3] Op het niveau van zendingen wordt informatie uitgewisseld met de Verenigde Staten. Rotterdam vormt een 'second line of defense'. Zendingen voor de VS worden in Rotterdam gecontroleerd. De douane mag echter geen informatie uitwisselen met douane-instellingen over personen, vanwege wettelijke beperkingen en de scheiding tussen controle en opsporing.

[3] *The Container Security Initiative (CSI) was launched in 2002 by the U.S. Bureau of Customs and Border Protection (CBP), an agency of the Department of Homeland Security. Its purpose was to increase security for container cargo shipped to the United States. The CSI program offers its participant countries the reciprocal opportunity to enhance their own incoming shipment security. CSI partners can send their customs officers to major U.S. ports to target ocean-going, containerized cargo to be exported from the U.S. to their countries (Bron: Wikipedia)*

Ten derde moet ook worden gewezen op het 'precaire spel' van informatie halen en brengen dat telkens weer tussen de verschillende opsporingsdiensten wordt gespeeld, waarbij elke dienst zijn eigen bevoegdheden heeft; bevoegdheden die wel in tact gelaten moeten worden.

> *'Wij zien soms export zendingen met vier oude Mercedessen in een container, opgehangen of zelfs nieuwe Mercedessen. Dat gaat naar een land waarvan wij denken, wat een raar transport. En als we de exporteur ook niet kennen, gaat het waarschijnlijk om gestolen auto's. Nee, dan begint het spel, wie start het onderzoek, welke informatie geef je aan elkaar.' (Bron: interview)*

Om dit informatie-politieke spel te vergemakkelijken vindt er afstemming plaats binnen het Expertisecentrum Haven, maar dit alles zonodig onder de bevoegdheid van een officier van justitie. Dit kan gebeuren als een strafzaak wordt voorbereid. Voor de douane zit echter ook in kleine zaken, voordat ze bij het OM komen, veel waardevolle informatie.
Een ander knelpunt in de informatieuitwisseling is meer van 'culturele aard' die samenhangt met de scheiding tussen specialisten en generalisten. De recherche als specialist haalt informatie bij de 'generalist' (de douane), maar geeft vervolgens geen of nauwelijks informatie terug, die ook voor de douane van nut kan zijn. De door de recherche gebruikte en veredelde informatie kan namelijk ook interessant zijn voor het verder ontwikkelen van de risicoprofielen binnen PRISMA. Het gevolg is dat kennis vooral gedefinieerd wordt als een bron, waardoor extra barrières kunnen ontstaan die een optimale uitwisseling van informatie in de weg kunnen staan.

3.3 Verkeersstromen: CATCH-KEN IN HOEKSCHE WAARD EN KLPD OPERATIES 'OCHTENDGLOREN'

3.3.1 Achtergrond

Het Korps Landelijke Politiediensten bestaat uit een dertiental uitvoerende diensten met als belangrijkste primaire taken de aanpak van de zware, georganiseerde criminaliteit, terreurbestrijding, het toezicht op de Nederlandse hoofdinfrastructuur (verkeer-, spoor- en waterwegen), informatiecoördinatie en de beveiliging van leden van het Koninklijk Huis[4]. Belangrijkste overeenkomst tussen deze uiteenlopende taken is dat deze binnen de Nederlandse politie allemaal landelijk georganiseerd zijn, hetgeen niet onverlet laat dat de KLPD vaak samenwerkt met regionale korpsen. De Dienst Verkeerspolitie is belast met het toezicht op - en de bijdrage aan – een veilig en betrouwbaar verkeers- en vervoerssysteem in Nederland. Voor het onderzoek naar de nodale oriëntatie van de politie is binnen het KLPD gekeken naar de controles die worden gehouden in het kader van "Ochtendgloren" door de dienst Verkeerspolitie en de samenwerkende opsporingsdiensten.

De aanleiding voor Ochtendgloren lag in de toenemende criminaliteit op en rond autosnelwegen in het Oost-Nederland. Trends die werden gesignaleerd waren in toenemende mate roofovervallen op geparkeerde vrachtwagens en vormen van mobiel banditisme; het overschrijden van de landsgrens vanuit Oost-Europa om in Nederland criminele activiteiten te plegen om vervolgens tegen het *'ochtendgloren'* huiswaarts te keren. Om dit tij te keren heeft de KLPD het initiatief genomen om samen met de betrokken korpsen Twente, IJsselland en Gelderland gemeenschappelijke controles in te stellen. Deze controles zijn niet zozeer gericht op het handhaven van de verkeersveiligheid maar op de criminaliteitsbestrijding op en rond de snelwegen, waarbij geïntervenieerd wordt binnen de verkeersstroom op de verkeersinfrastructuur. Bovendien is Ochtendgloren interessant omdat nadrukkelijk wordt samengewerkt met andere opsporingsdiensten, onder andere om een gemeenschappelijke informatiepositie op te bouwen.

Er is echter ook nog een ander interessant initiatief met een nodale oriëntatie, dat zich vooral richt op toezicht uitoefenen door mee te bewegen op de verkeersstroom. Dit is mogelijk omdat inmiddels verschillende regionale politiekorpsen gebruik maken van zogenaamde 'Catch-ken' apparatuur. Dit systeem werkt met, vaste of mobiele fotoapparatuur en software die in staat is kentekens van voertuigen direct te controleren aan de hand van bijvoorbeeld de database van de RDW of politie. Op deze wijze kan effectief, efficiënt en grootschalig (continu, 24u/24u) worden nagegaan of er 'gesignaleerde' voertuigen passeren, openstaande boetes zijn, sprake is van verlopen APK-keuring, onverzekerd wordt rondgereden etc. Geeft het systeem een "hit" dan kan

[4] http://www.politie.nl/KLPD/

de politie dit registreren, het voertuig volgen of direct optreden door het betreffende voertuig aan de kant te zetten. Onder andere de politie Amsterdam-Amstelland en het district Hoeksche Waard van de regio Zuid Holland Zuid werken inmiddels met deze technologie.

Belangrijk in de Hoeksche Waard is dat met name veelplegers, komende van buiten de Hoekse Waard, gebruik maken van de verkeersinfrastructuur om binnen de Hoeksche waarde met name woning- en bedrijfsinbraken te plegen (vermogensdelicten), terwijl de lokale criminaliteit vooral bestaat uit vernielingen en geweldsdelicten. Om met name een eind te maken aan overlast die criminelen van buiten de Hoeksche Waard genereren, is besloten gebruik te maken van de geografisch voordelen van het gebied, namelijk de insluiting van het gebied door verschillende snelwegen. Als pilot in Nederland is men in de Kiltunnel begonnen met een systeem dat kentekens van voertuigen kan lezen en herkennen (Automatic Numberplate Recognition- kortweg ANPR). Daarnaast is en wordt er gewerkt met een mobiele versie van het systeem.

3.3.2 De Nodale Oriëntatie

De nodale oriëntatie in deze twee casus komt enerzijds tot uitdrukking in het registreren, identificeren en volgen van verkeersbewegingen op de infrastructuur door de inzet van ANPR (meebewegen op de stroom) en anderzijds door de interventies op de toegang en doorgang van de verkeersstroom op de verkeersinfrastructuur, waarbij meerdere opsporingsdiensten samenwerken in operaties zoals 'Ochtendgloren'. Feitelijk biedt het ANPR ook de mogelijkheid om na een 'hit' een voertuig aan te houden en zo dus de toegang tot de infrastructuur te controleren. We zullen de karakteristieken van beide benaderingen wat uitgebreider bespreken.

Identificeren van risico's en afwijkingen binnen de verkeersstroom

ANPR Hoeksche Waard
Het ANPR biedt de politie een viertal verschillende mogelijkheden[5] om verkeersstromen 'in beeld te krijgen' , te volgen en te bepalen of een signaal moet leiden tot een bepaald interventiescenario;

1. *Controle van voertuigen door koppeling aan de database van de RDW of bij de politie staat gesignaleerd, bijv. in het kader van opsporingsonderzoek.*
2. *Inzicht geven in bewegingen van usual suspects (veelplegers); hiervoor is een koppeling met de database van veelplegers, notoire verkeersovertreders etc. staande houding hoeft niet altijd noodzakelijk gevolg te zijn; signalering kan ook voldoende zijn, teneinde inzicht in bewegingen te krijgen.*
3. *Het registeren én bewaren van alle verkeersbewegingen (stromen). Het achteraf verbinden, en het matchen aan voorgevallen criminaliteit.*
4. *Opbouwen van systematische fenomeenkennis. Hierbij bestaan er op voorhand risicoprofielen op basis waarvan, pro-actief, bewegingen worden herkend en of er*

[5] "*Veiligheidsbeleid en nodale oriëntatie*", Openbaar Bestuur, april 2006, p.20-23

sprake is van afwijkingen van regulier gedrag of er een bepaalde kans op ongewoon gedrag bestaat.

De controle van verkeersstromen gebeurt op dit moment nog zoals omschreven onder 1 en 2. Dit betekent dat de monitoring betrekking heeft op álle passerende voertuigen maar dat het systeem alleen 'aanslaat', indien vanuit de systemen (databases en software) daarvoor aanleiding wordt gegeven. De belangrijkste bronnen die op dit moment het ANPR voeden bestaan uit gegevens van RDW, de database bekende veelplegers, ernstige verkeersovertreders, openstaande boetes, gestolen kentekenplaten en gesignaleerde personen/voertuigen. Het systeem geeft bij het passeren van een voertuig dat voldoet aan één of meerdere kenmerken uit de database, een signaal naar de dienstdoende agent met het daarbij direct het bijpassend protocol; een protocol dat aangeeft op grond van welke feiten het voertuig staande gehouden moet worden en welke actie ondernomen moeten worden. Dit kan betekenen dat een specifieke interventie of scenario beschreven kan worden op het niveau van een uniek kenteken, waardoor maatwerk kan worden geboden, bijvoorbeeld in het geval er melding wordt gemaakt van vuurwapengevaarlijk.

In dit systeem is het uitgangspunt de kentekenregistratie van de RDW die vervolgens gekoppeld wordt aan andere databases op grond waarvan inzicht kan worden verkregen in de feiten die gerelateerd zijn aan de houder van een bepaald kenteken. Dit betekent dat het noodzakelijk is data te verrijken met andere data. Dit kan zowel andere regionale, bovenregionale of landelijke politie-informatie zijn als informatie die afkomstig is van derden zoals andere opsporingsdiensten. Verrijking vindt ook plaats doordat er handelingsperspectief aan wordt gekoppeld. Immers aangegeven is hoe gehandeld moet worden in het licht van de geconstateerde feiten. Momenteel vindt deze verrijking vooralsnog handmatig plaats, daar waar het betreft het verzamelen van specifieke verbanden en het kunnen leggen van verbanden alsmede het continue up-to-date houden hiervan.
Het aantal hits dat gegenereerd wordt en leidt tot een gericht interventiescenario is in de Hoeksche Waard in de periode van de pilot 3507 op de vaste opstelling en 211 op de mobiele opstelling van de ANPR. In het eerste geval werden in totaal ruim 1 miljoen voertuigen geregistreerd, in het tweede geval 65.000. In beide gevallen ging het om minder dan 1 % van het totaal aantal passanten. In Hoeksche Waard laten de criminaliteitscijfers thans een daling zien, maar het is nog onvoldoende duidelijk of er een rechtstreeks verband bestaat tussen de ingezette daling en het gebruik van de ANPR, mede omdat pas ongeveer 1 jaar met het systeem gewerkt wordt en effecten nog niet zijn uitgekristalliseerd (pijplijneffecten).

KLPD Ochtendgloren
Tijdens de Ochtendgloren operaties worden risico's of afwijkingen geconstateerd, doordat alle voertuigen ter plekke worden nagetrokken. Het moment waarop de controles plaatsvinden wordt maar in beperkte mate bepaald door specifieke te verwachten risico's. Wel wordt rekening gehouden met een aantal basisgegevens die van te voren bekend zijn zoals de vakantieperioden en de data waarop grote

evenementen gepland zijn. Feitelijk wordt het tijdstip met name bepaald door capaciteitsoverwegingen van de deelnemende diensten. Ook wordt in de keuze van het tijdstip rekening gehouden met de gegevens die beschikbaar zijn gekomen op grond van de evaluatie van de vorige operatie. Overigens krijgt men wel steeds meer inzicht in trends en patronen, waarmee rekening kan worden gehouden. Bijvoorbeeld op maandag en dinsdag reizen verhoudingsgewijs veel drugskoeriers, terwijl in de weekenden met name alcohol overtredingen plaat vinden.
Tijdens Ochtendgloren worden álle voertuigen gecontroleerd in de het kader de Wegenverkeerswet (100% controle). Het bepalen in hoeverre voertuigen al dan niet *bijzondere* aandacht verdienen gebeurd op basis van informatie uit verschillende databases van aanwezige opsporingsdiensten maar ook de intuïtie en kennis van de politie agent en inspectiemedewerker speelt een belangrijke rol.

> *"Een auto met daarin een ouder echtpaar dat zegt van de verjaardag van hun kleindochter terug te komen is sneller door de controle dan een paar ongure types in een snelle auto met een buitenlands kenteken. Dat is een kwestie van ervaring en intuïtie".*

Tegelijkertijd wordt een mobiele versie van het ANPR ter plaatste ingezet waarbij aanvullende selectie plaatsvindt op basis van informatie uit andere databases zoals ook beschreven is onder de Hoeksche Waard. Indien er vanuit andere aanwezige inspecties belangstelling is voor een bepaald voertuig - bijvoorbeeld de Vreemdelingendienst - dan wordt dat voertuig aan nadere inspectie onderworpen in de controlestraat.

Uit criminaliteitscijfers blijkt het aantal woninginbraken, overvallen op en rond de snelweg aanzienlijk te zijn verminderd (vaak tot min 50%). In Deventer ging het aantal roofovervallen terug van 12 naar 3 gevallen.

Ambities

ANPR Hoeksche Waard
De mogelijkheden die ANPR in de toekomst kan bieden zijn vooral gericht op (pro actieve) informatieanalyse, datamining en het systematisch versterken van de informatiepositie van de politie. Doelstelling is het ontdekken van trends, patronen en profielen om daar passende interventiescenario's voor te kunnen opstellen of zelfs "criminaliteitsvoorspellingen" uit te kunnen destilleren (zie punt 3 en 4 in voorgaand overzicht). Feitelijk is bij de verkeerspolitie nog niet veel praktijkervaring opgedaan met het opbouwen van fenomeenkennis dat is gebaseerd op patronen en 'afwijkingen in gedrag'. De ANPR zou bijvoorbeeld veel gerichter kunnen worden ingezet ter bestrijding van mobiel banditisme door nachtelijke verkeersbewegingen achteraf te matchen met bijvoorbeeld openingstijden van horeca of fabrieken en voorgevallen criminaliteit. Tijdens de proef is wel al resultaat geboekt met de aanhouding van verdachten die met aan de hand van een dergelijke analyse achteraf in beeld kwamen. Van een systematische inzet of kennisopbouw is echter nog geen sprake. Op grond van de verzamelde data en analyses zouden zelfs voorspellingen kunnen worden

gedaan over criminaliteitsverwachting. De nadruk ligt thans nog te veel aan het versterken van de betrouwbaarheid en volledigheid van de kentekendatabase.
In de toepassing van gegevensanalyse en het ontwikkelen van patronen/profielen speelt het vraagstuk van het registreren, vastleggen en bewaren van verkeersbewegingen op het niveau van kentekens een belangrijke rol. Op dit moment is de beleidslijn van het OM dat de inzet van ANPR ter uitvoering van de Wegenverkeerswetgeving is toegestaan en dat het tevens mag dienen als selectiemiddel in relatie tot geregistreerde veelplegers. Ook de registratie van reguliere bewegingen (sec) is toegestaan (zonder dat dit leidt tot staande houdingen) maar of deze gegevens kunnen en mogen worden gebruikt als een systematische bron voor ondersteuning van de informatiepositie politie is nog een vraag die openstaat, gelet op de vigerende privacywetgeving en de standpunten van het College Bescherming Persoonsgegevens. Er wordt daarom thans gewerkt aan de ontwikkeling van een privacyreglement voor met name de inzet van de ANPR.

Voor de verdere ontwikkeling van het ANPR wordt gedacht aan uitbreiding met andere partners zoals de Marechaussee, andere inspectiediensten, de Belastingdienst, de FIOD, maar mogelijke ook private partijen. Uitbreiding met allerhande IP-camera's die nu al aanwezig zijn in en rond bedrijven(terreinen) is eveneens een reële optie. De ICT-infrastructuur biedt hiervoor al de mogelijkheden. Tevens zijn er mogelijkheden om een koppeling met flitspalen te realiseren, alsmede de camera's die worden ingezet op trajectcontroles op de ring A10, A12 en A13. Wat betreft de informatiepositie wordt gewerkt aan een landelijke centrale dataserver waaruit landelijk getapt kan worden en waaraan informatie *geleverd* kan worden door locale ANPR signaleringen. Verder is het niet ondenkbaar dat een signaal wordt doorgegeven aan andere opsporingsdiensten.

KLPD Ochtendgloren
De kracht maar ook de doelmatigheid bij Ochtendgloren zit vooral in het uitgebreide palet aan bevoegdheden dat ter plekke vertegenwoordigd is: de regiopolitiekorpsen IJsselland, Twente, Noord en Oost Gelderland, Vreemdelingendienst (VD), het permanent autoteam (PAT), KLPD verkeerspolitie, Inspectie Verkeer en Waterstaat (IVW), Koninklijke Marechaussee (KM), Openbaar Ministerie parket Zwolle, Parketpolitie, Douane, Centraal Bureau Motorrijtuigenbelasting Zwolle, Voedsel en Waren Autoriteit (VWA) Sociale Opsporings- en Inlichtingen Dienst (SIOD), Algemene Inspectie Dienst, (AID), Rijkswaterstaat en Autobahnpolizei NI-Osnabrück. De douane is daarbij een belangrijke partner. De bevoegdheden van al deze partijen zijn in belangrijke mate aanvullend op die van de politie, met name daar waar het gaat om het doorzoeken van voertuigen. Voor de toekomst zou nog met meer opsporingsinstanties kunnen worden uitgebreid.
Daarnaast krijgt de actie ook met enige regelmaat een internationaal karakter; door anticiperend gedrag van daders (die na verloop van tijd op de hoogte raken van de tactische opstelling van Ochtendgloren) is het zaak de politiestrategie aan te passen en mee te veranderen. Wat dus al gebeurt, is dat er een internationale opschaling

plaatsvindt waarbij de gehele controle zich afspeelt tussen Amsterdam tot aan Warschau.

De locatie waarop de operatie Ochtendgloren gericht is, wordt ook gebruikt om de inzet van moderne technologieën zoals de mobiele scanmobiel (vergelijkbaar met schiphol röntgenscan) te testen, waaronder de 'backscatter'. Dit is een voertuig dat om het verdachte voertuig heenrijdt en een volledige 3d-scan maakt. Zonder dat hiervoor het voortuig doorzocht of geopend hoeft te worden. Dit kan ook op personen worden ingezet. Dit wordt ook wel "virtuele fouillering[6]" genoemd.

Ten tijde van de controle leidt hard bewijsmateriaal (aantreffen van wapens, drugs) tot registratie en vervolging. De controles worden echter ook in toenemende gebruikt om 'soft info' te registreren; het noteren/vastleggen van verdachte of opmerkelijke zaken rondom personen of voertuigen die in de toekomst wellicht bij te kunnen dragen aan onderzoek of te kunnen bijdragen als ondersteunende bewijslast.

In onderstaande tabel vatten we de karakteristieken van de nodale oriëntaties die in beide praktijken worden gebruikt nog een keer samen.

	ANPR	OCHTENDGLOREN
TYPE STROOM	Verkeersinfrastructuur	Verkeersinfrastructuur
INTERVENTIE	Toegang controleren en meebewegen	Toegang controleren
OMVANG	100% (stille) controle	100% controle
EFFECT	ongehinderde doorstroom	verminderde doorstroom
INTENSITEIT	continue 24/24	periodiek, 11x per jaar
GEOGRAFISCH	Vast op vooraf bepaalde punten én mobiel (hot-spots/evenementen)	Beperkt (deel van snelweg Oost-Nederland)
MANIFESTATIE	Onzichtbaar	zichtbaar
RISICO SELECTIE	bepaald door kracht van **technologie** - systeeminformatie (databases) - vooraf gedefinieerd (profielen)	bepaald door kracht van **samenwerkende opsporingsdiensten** - ter plaatse ingeschat (human factor) - systeeminformatie (databases)
REFERENTIE	kenteken en geregistreerd profiel	Inzittenden, kenteken, situationele omstandigheden

Tabel 3.3: Kenmerken casus Verkeersstromen

Natuurlijk gaat de uitvoering van praktijken niet zonder slag of stoot. Vandaar dat het belangrijk is om een aantal kritische factoren voor het voetlicht te brengen.

[6] http://journalist.web-log.nl/journalist/2005/05/rntgenapparaat_.html

3.3.3 Kritische factoren

Zowel binnen de proef met het ANPR als Ochtendgloren zijn in het licht van de nodale oriëntatie een aantal relevante randvoorwaarden die in acht moeten worden genomen. In de interviews en door ons bestudeerde documenten wordt vooral betekenis gehecht aan de volgende factoren en randvoorwaarden.

Samenwerking

Uit ons onderzoek blijkt dat het succes van beide praktijken vooral wordt bepaald door de kwaliteit van de samenwerking met andere diensten. Deze samenwerking leidt vervolgens tot het beter gebruik maken van elkaars taken, verantwoordelijkheden en bevoegdheden (versterking complementariteit) waardoor het mogelijk wordt om vormen van integrale handhaving te ontwikkelen, door het delen van kennis en kunde en door het ontwikkelen van een samenwerkingscultuur. We zullen dit hieronder nader toelichten.

Ochtendgloren
De kracht van de effectiviteit van Ochtendgloren drijft grotendeels op de samenwerking met andere opsporingsdiensten. De aanwezige bevoegdheden tijdens Ochtendgloren vormen tezamen een complementair palet waarmee men in staat is 'volledige toegangscontroles' uit te voeren. Er wordt door de verschillende diensten gebruik gemaakt van bestaande bevoegdheden en waar dat niet mogelijk was zijn maatoplossingen bedacht. Een voorbeeld is de aanwezigheid van de marechaussee;

> *"De marechaussee is een belangrijke partner wat betreft specialistische kennis van document- en geldherkenning (Authenticatie). De inzet van de bevoegdheden van de marechaussee is echter beperkt in gebieden waar sprake is van een geconstateerde grensoverschrijding. Schiphol en de landsgrenzen dus. Voor de inzet bij ochtendgloren is door alle hoofdofficieren van de betrokken arrondissementen schriftelijke toestemming gegeven om het gebied van ochtendgloren aan te wijzen binnen de bevoegdheden van de marechaussee."*

Naast bepaalde bevoegdheden ontbreekt het de politie in bijzondere gevallen – logischerwijs - ook aan kennis en kunde om bepaalde zaken te kunnen herkennen, zoals het kunnen constateren van het (moeten) hebben van een werkvergunning van Poolse arbeiders die in de nacht terugrijden uit het westen (SIOD) of identificeren van al dan niet beschermde schelpdieren (AID). Een ander praktijkvoorbeeld waarin maatregelen zijn genomen om het uitvoeren van de controle-activiteiten te bevorderen is de wijziging van de Algemene Plaatselijke Verordening gemeente Rijssen-Holten[7]:

> *"De gemeenteraad van Rijssen-Holten heeft de burgemeester de bevoegdheid verleend om veiligheidsrisicogebieden te duiden waar preventief fouilleren kan worden toegestaan. Dit is vooral van belang voor de grootscheepse controles op de A1 ('Ochtendgloren'). Bij deze controles zijn in het verleden 'bij toeval' grote wapens aangetroffen. Sinds 2004 bestaat de mogelijkheid om, ter voorkoming van verstoring van de openbare orde door de aanwezigheid van wapens, voertuigen en bagage te doorzoeken en inzittenden te fouilleren.*

[7] Raadsvoorstelnummer: 2004-II-18, 27 januari 2004

De rol van het KLPD bij Ochtendgloren is door alle opschaling met andere diensten nog maar beperkt. Het KLPD heeft al in het eerste stadium initiatief genomen tot de uitbouw van deze samenwerking en is de aangewezen partij waar het gaat om de facilitaire taken die er zijn rond het fysiek inrichten van de controle op de snelweg en de uitvoering van de Wegenverkeerswetgeving. Gebleken is dat de samenwerking veelal afhangt van de informele contacten en interpersoonlijke vaardigheden. Als positieve spin-off naast het directe resultaat van de 'vangsten' tijdens de controles (cijfers) noemt men in het bijzonder ook de resultaten achter het resultaat; door de samenwerking die zo'n 10 keer per jaar plaatsvindt, de voorbereiding, uitvoering en evaluatie zijn er tussen de verschillende eilanden van bevoegdenheden en taken van verschillende diensten bruggen en verbindingen ontstaan, die ook op andere momenten worden benut.

> *"Als collega's tijdens een reguliere snelwegsurveillance een vrachtauto met vee zien rijden in een gebied waarvan zij denken dat een vervoersverbod van kracht is, zie je nu eerder dat 'even contact' wordt gezocht met collega's van de AID. Deze contacten kent men dan vanuit de samenwerking die rond Ochtendgloren plaatsvindt. Wat je dus ziet, is dat collega's van andere opsporingsdiensten op deze manier een uitbreiding vormen in de signalerende capaciteit."*

ANPR

De effectiviteit van het toezicht op de verkeersstroom hangt op dit moment in grote mate af van samenwerking die in de 'backoffice' is georganiseerd. De inzet van het instrument ANPR is in hoge mate afhankelijk van de betrouwbaarheid van de informatie, zeker omdat in het geval van een bepaalde signalering een geautomatiseerd en daarbij passend handelingsprotocol/interventiescenario vooraf gegenereerd wordt. Pas na een staande houding kan de agent ter plaatse een inschatting maken, of dit daadwerkelijk correct is geweest. Dit betekent dat vooral aandacht moet worden besteed aan de kwaliteit van de operationele follow up. De follow-up na een hit ligt nu nog geheel bij de politie Dit is niet altijd even makkelijk, omdat men ongeveer 10 minuten heeft om een auto staande te houden, voordat deze het gebied alweer verlaten kan hebben. Bovendien speelt bij het in toenemende mate voeden van de database vanuit verschillende diensten en externe bronnen ook de vraag wie, waarvoor en wanneer verantwoordelijk is bij de inzet van het ANPR.

Technologie en kwaliteit informatie

Een andere vitale factor is de inzet van technologie. De inzet van nieuwe technologie zoals ANPR betekent een forse verbetering van de kwaliteit van werkproces – zowel in doelmatigheid als doeltreffendheid. Hits worden nu geautomatiseerd en systematisch - 24 uur per dag en 7 dagen per week – gegeneerd, terwijl dit voorheen op individuele basis en incidenteel plaats vond, op grond van aannemelijke vermoedens. Verder zien we dat door gebruik te maken van on-line en realtime gegevens, de ANPR

en de 'back scatter' getracht wordt om het oponthoud van automobilisten zo beperkt mogelijk te laten zijn.
Belangrijker dan de toepassing van bepaalde geavanceerde technologieën is echter de kwaliteit van de informatiehuishouding binnen de politie. Hoe betrouwbaar is de voorhanden zijnde informatie, hoe kan deze worden ontsloten. Hetzelfde geldt ook voor informatie die wordt gebruikt uit databestanden die worden beheerd door andere korpsen of andere opsporingsdiensten.

Draagvlak

Omdat de inzet van catch-ken als bij de operaties rond ochtendgloren een fundamentele aantasting van de privacy tot gevolg hebben, is een belangrijke factor het maatschappelijke en politiek bestuurlijke draagvlak van dit soort praktijken. Tot nu toe blijkt dat dit draagvlak wordt versterkt doordat zichtbare resultaten zijn geboekt. Nader onderzoek zal echter moeten uitwijzen of er een directe relatie bestaat tussen deze praktijken en de daling van de criminaliteit. Tot op heden blijkt dat er een daling van criminaliteit is te zien. Bij Ochtendgloren wordt de mening van de gecontroleerde automobilisten regelmatig gevraagd en in kaart gebracht met behulp van enquêtes Over het algemeen kan men rekenen op grote waardering en steun. Nadeel is dat bij gunstige criminaliteitsontwikkeling de vraag opkomt of controles dan nog wel nodig zijn c.q. geaccepteerd worden.

Cultuur en competenties

De zojuist beschreven manier van opsporing staat haaks op de bestaande en in allerlei gedragspatronen, routines en procedures verankerde praktijk van opsporing die namelijk delictgericht is. Een meer pro-actieve kennisvergaring en het werken met daaraan gekoppelde preventieve interventiescenario's (zeker in het geval van het ANPR) vraagt om een heel andere benaderingswijze. Niet alleen vereist het dat de politie-organisatie in staat moet zijn om een explosief groeiende hoeveelheid van verschillende soorten van data te kunnen verwerken, bewerken en te kunnen combineren, maar deze data moet ook op hun merites worden beoordeeld. Dit vereist ook een heel andere kennis en andere vaardigheden.

3.4 Stromen van personen: HOOLIGANS IN BEELD

3.4.1 Achtergrond

Onder naam "Hooligans in Beeld" is een aanpak ontwikkeld om risicosupporters in het betaald voetbal in beeld te krijgen. De aanleiding hiervoor was het voetbalvandalisme; de toenemende mate van ongeregeldheden rond voetbalwedstrijden en de omvangrijke politie inzet. Doelstelling was het verbeteren van de informatiepositie ten aanzien van het voetbalgeweld en met name de personen die hierbij een centrale rol spelen door hen uit de anonimiteit van de groep/stroom te halen[8]. Met het verzamelen van informatie van en over personen en groepen en deze te delen met andere partijen, is men beter in staat om daarop toegesneden passende interventiestrategieën te ontwikkelen - zowel op individueel als op groepsniveau.

Hooligans in Beeld is een aanpak die vanaf 2002 door de Regionale Inlichtingen Dienst (RID) van de regio Gelderland-Midden is ontwikkeld rond de wedstrijden van voetbalclub Vitesse. Als pilot zijn, ter toetsing van de ontwikkelde aanpak, daarna vergelijkbare trajecten vanaf 2003 gehouden in Rotterdam-Rijnmond (Feyenoord), IJsselland (Go Ahead Eagles) en Brabant Zuid-Oost (PSV). De aanpak in Gelderland-Midden heeft geleid tot een voorbeeld van good-practice dat is vastgelegd in een praktisch toepasbare methodiek. Na ook in andere regio's te hebben bewezen een succesvolle aanpak te zijn, krijgt de toepassing van deze methodiek een landelijk vervolg.

3.4.2 De Nodale Oriëntatie

Risico-identificatie en afwijkingen binnen de stroom

Hooligans is Beeld is gericht op een dadergerichte aanpak, waarbij men uit de stroom/groep personen toonaangevende figuren wil identificeren die in belangrijke mate verantwoordelijk zijn voor overlast in en rond het voetbalstadion, waarbij het voetbalstadion wordt gezien als een knooppunt van risicovol gedrag. Om beter inzicht te krijgen in de mogelijke risico's die samenhangen met de bewegingen van bepaalde supportergroepen en de ontmoeting van bepaalde – rivaliserende - groepen op een bepaalde locatie (binnen of buiten het stadion), is men begonnen met het 'duiden' van groepen op grond van participerende observatie. Daartoe is de politie in het stadion aanwezig en wordt het gedrag dat in de vakken plaats vindt geobserveerd en geregistreerd.

[8] Ferwerda, H.B., Adang, O.M.J. "*Hooligans in beeld"*, Advies- en onderzoeksgroep Beke (iov. Politie en Wetenschap), Apeldoorn/Arnhem, 2005, p.8

Deze observaties leiden tot een eerste indeling in een drietal categorieën:

1- Hinderlijk gedrag; maar gevoelig voor autoriteit van politie
2- Overlastgevend, lichte criminaliteit; doelbewust en provocerend bezig
3- Crimineel gedrag, ook buiten het stadion; gewelddadig, uit op financieel gewin.

Vervolgens wordt binnen groepen gekeken naar de concentratie van problemen, aantallen betrokken personen en subgroepen en het gedrag van deze personen en subgroepen. Ook geworden hiërarchische verhoudingen, de samenstelling van de groep, wisselingen en onderlinge groepsrelaties in kaart gebracht. Daarnaast wordt onderzocht of er andere locaties (zoals horeca in de binnenstad) zijn waar dezelfde groepen voor overlast zorgen. De observaties beperken zich eerst tot het niveau van de groep en zijn dus relatief anoniem. Vervolgens wordt ingezoomd op meest 'toonaangevende' individuen die zelf, of anderen aanzetten tot het veroorzaken van aanmerkelijke overlast. Vervolgens worden deze toonaangevende personen uit de anonimiteit gehaald, door hen aan te spreken; dit kan plaats vinden vanuit de politie of vanuit de club.
Grote groepen voetbalhooligans bestaan uit meelopers die vanuit de beschutting van de anonimiteit meedoen, al dan niet onder invloed van alcohol of drugs. Het ontanonimiseren van toonaangevende personen heeft vaak tot resultaat dat personen zich terugtrekken op de achtergrond, omdat men niet als (leidende) hooligan met naam en toenaam bekend wil staan (gezichtsverlies op werk, woonomgeving en familie). Een andere reactie kan zijn, dat men zich hiervan niets aantrekt. In dit laatste geval gaat de politie over tot het creëren van een breder beeld van deze persoon (sociale context, voorgaand politieverleden etc.). Dit verzwaard toezicht betekent dat op alle dagen van de week personen gevolgd worden en dat dit aan de persoon kenbaar gemaakt wordt met als doel verstoring van ongewenst gedrag.

Het selecteren van personen uit de stroom gebeurt door daarvoor opgeleide politiemedewerkers (spotters). Na de groep uitgebreid in beeld te hebben gebracht, wordt selectief ingezoomd op centrale personen (trechteren). Het komen tot bepaalde interventies gebeurt doordat informatie systematisch wordt verzameld, vastgelegd en geanalyseerd op afwijkende patronen (het opbouwen van de informatiepositie). De waarnemingen worden getoetst aan en overlegt met mensen die dagelijks werken in het stadion, supporterbegeleiders (stewards) etc. Onderdeel van participerende observaties is ook het deelnemen aan stromen (meebewegen) door undercover rechercheurs, die zich bevinden zich tussen supporters op de tribune en die trachten te participeren in het feitelijke groepsproces. De waarneming en informatieverzameling op groepsniveau is anoniem, pas op het moment van het kunnen identificeren van toonaangevende personen komt men op het niveau van het individu.

Dit alles levert 25% minder inzet van politie, minder vernielingen, een daling in het aantal aanhoudingen, incidenten rond de wedstrijden en een afname van de ernst van delicten op. Daarnaast zijn er ook sociale opbrengsten in termen van een toegenomen gevoel van veiligheid, voorkomen van ziekenhuiskosten en slachtofferhulp. Het aantal wedstrijden dat nog wordt aangemerkt als risicovol is gedaald van 7 naar 1. Dankzij het succes van de methode voorziet men thans in landelijke implementatie.

Ambities

Hooligans in Beeld richt zich met de kennis en beelden uit stromen op passende interventies die gericht zijn op 'voorkomen' dan wel 'verstoren'. In de sfeer van bevoegdheden ziet men dat er nog belangrijke winstpunten zijn te behalen. Gezien de huidige, delictgerichte oriëntatie en daarop afgestemde bevoegdheden zou een uitbreiding van bevoegdheden, gebaseerd op de idee van tegenhouden, kunnen bijdragen aan een substantiële verbetering in termen van opbrengsten. Te denken valt aan het tijdelijke telefoontap voorafgaand aan en tijdens wedstrijden.

Een van de doelstellingen is de focus op 'incidenten' verder te verlaten en veel meer vooraf invloed te gaan uitoefenen met het oog op voorkomen dan wel verstoren. Dit voorkomen kan alleen als een adequate informatiepositie wordt opgebouwd; een positie die al begint met informatie te verzamelen en de delen over factoren die buiten het stadion liggen, bijvoorbeeld informatie die vanuit (probleem)woonwijken komt. Ook kan het 'aftappen' van data uit meerdere en gecombineerde databases nog verder worden uitgebreid, waardoor meer inzicht kan worden verkregen in de context van bepaalde personen. Daarbij kan worden gedacht aan de databases van de Belastingdienst, SIOD, FIOD etc. De bevoegdheden hiervoor schieten soms te kort, juist vanwege de delictgerichte oriëntatie. De ambitie is niet méér bevoegdheden maar andere bevoegdheden die veel meer gericht zijn op effectief voorkomen.

In onderstaande tabel hebben we de belangrijkste karakteristieken van de nodale oriëntatie in deze opsporingspraktijk nog een keer in kaart gebracht.

	HOOLIGANS IN BEELD
TYPE STROOM	Personen
INTERVENTIE	Toegang tot knooppunten controleren en meebewegen
OMVANG	Bottum-up getrechterde (stille) controle
EFFECT	ongehinderde doorstroom
INTENSITEIT	Continue (up-to-date houden)
GEOGRAFISCH	Vast op vooraf bepaalde punten én mobiel (hot-spots/evenementen)
MANIFESTATIE	Zichtbaar en onzichtbaar
RISICO SELECTIE	bepaald door kracht van **observatie** - Verzamelde individuele- en groepsinformatie (aangevuld met politie databases) - Human Factor
REFERENTIE	Groepen en individuen

Tabel 3.4: kenmerken casus Hooligans in Beeld

3.4.3 Kritische factoren

Verbeterde informatiepositie

De belangrijkste randvoorwaarde bij de methodiek Hooligans in Beeld is het actueel en up-to-date houden van het beeld dat is opgebouwd van supportersgroepen. Dit blijft een uitermate dynamisch proces waarbij steeds weer veranderingen optreden in het aantal groepen, de onderlinge relaties en het ontstaan van nieuwe 'leiders'. Gegevens van een jaar geleden kunnen al dusdanig veranderd zijn, dat strategieën hierop aangepast moeten worden. Daarnaast kunnen supporters proberen de politie bewust op het verkeerde been zetten.

> *"Een nadeel van de methode is dat bij goede resultaten, toenemende mate van rust en een afname van het aantal incidenten, men op hoger niveau gauw geneigd is te roepen dat de inzet wel gestopt of verminderd kan worden. Dit is een valkuil gezien de dynamiek van de stroom."*

Een effectieve informatiepositie dient tevens om te kunnen anticiperen op verschuivingen naar plaatsen buiten het stadion; het uitgaanscentrum Korenmarkt, het terrein van de Rijnhal of dance festivals. De systematiek blijft hier ook hetzelfde toepasbaar.

> *"Wat met regelmaat voorkomt is dat er sprake is van de 'day before', de avond voorafgaand aan een wedstrijd. Dit kan zich dan afspelen op- of rond De Korenmarkt in het centrum van de stad. Wat je dan ziet, is dat bekende personen en groepen uit het stadion daar overlast veroorzaken. Door dit centraal te registeren draagt dit bij aan een adequate beeldvorming van groepen en kunnen interventie daarop aangepast worden."*

Hooligans in Beeld gaat uit van actieve observatie en undercover 'participatie'. De verzamelde meta-informatie over kenmerken van stromen en groepen leidt vervolgens door analyse en verrijking van deze gegevens tot een selectieve en passende aanpak. Dit is alles vereist maatwerk in soort van interventie die wordt gepleegd. Dit kan locatie- situatie-, persoons- of groepsgericht zijn, maar het kan ook bestaan uit het aanbieden van bepaalde vormen van hulpverlening.

Competenties

De kennis en kunde die vereist is bij het werken zoals bij een aanpak als Hooligans in Beeld is essentieel anders dan in het reguliere politiewerk. Het accent ligt niet meer primair op de delictgerichte aanpak of noodhulpverlening, maar veel meer op informatieverzameling, analyse en interpretatie. Een belangrijke competentie is het leren kijken naar structuren en groepsprocessen en hierbij de juiste interventie te formuleren en dit in werkprocessen te incorporeren.
Verder is ook belangrijk dat geleerd wordt van eerdere optredens bij delicten of bij de verlening van noodhulp. Dit betekent dat deze ervaringen moeten worden

gecodificeerd. Onderzoek heeft geleerd dat maar ten hoogste 20% van de informatie die hierop betrekking had, is geregistreerd. Daardoor is sprake van een beperkt leervermogen. Kortom, een dergelijk aanpak is gebaat bij de ontwikkeling van kennismanagement die politiemensen in staat stelt om te kunnen leren.
Tenslotte is ook belangrijk dat politiemensen in staat zijn om harde en zachte informatie op hun merites te kunnen beoordelen en te kunnen combineren, waardoor meer inzicht verkregen wordt in de specifieke context van zowel individueel als groepsgedrag.
Dit alles vereist niet alleen bepaalde kennis en kunde maar het vereist ook een bepaalde hoeveelheid analysecapaciteit.

Samenwerking en informatieuitwisseling

Om de methode Hooligans in Beeld adequaat te kunnen toepassen is samenwerking tussen verschillende instanties en afdelingen onontbeerlijk. Belangrijke partners zijn de regionale inlichtingendiensten, de recherche, de burgemeester en Openbaar Ministerie voor de juridische vervolging maar ook samenwerking met instanties die zich meer in de sfeer van de hulpverlening bewegen zoals het jeugd- en jongerenwerk. De verbreding naar andere domeinen zoals het uitgaansleven en of woonwijken en andere gelegenheden dan het voetbalstadion, vraagt om het uitwisselen van informatie met bijvoorbeeld de wijkagent, de woningbouwcorporatie en de horeca.

3.5 Stromen van personen: PASSAGIERS OP LUCHTHAVEN SCHIPHOL

3.5.1 Achtergrond

De Schiphol Group is eigenaar en exploitant van Amsterdam Airport Schiphol, Rotterdam Airport en Lelystad Airport en bezit 51% van de aandelen in Eindhoven Airport (www.schipholgroup.com). De Schiphol Group N.V. exploiteert luchthavens en ontwikkelt 'Airport Cities'. Een AirportCity is een dynamische omgeving waar mensen en bedrijven, logistiek en winkels, informatie en entertainment samenkomen en elkaar versterken. Het is behalve een efficiënt en multimodaal vervoersknooppunt ook een locatie die haar gebruikers 24 uur per dag alle benodigde diensten biedt. De idee is dat een luchthaven een vlekkeloze tussenstop in het reisproces is.
Bij de Schiphol Group werken bijna 2200 mensen In totaal werken zo'n 58.000 mensen bij 543 bedrijven op de luchthaven. Samenwerking met partners is een cruciale succesfactor voor de duurzame ontwikkeling van de luchthaven (Jaarverslag verantwoord Ondernemen, 2005). Veiligheid wordt steeds belangrijker, mede door de gebeurtenissen op 11 september. Er wordt een onderscheid gemaakt tussen safety en security.

Safety

Onder safety vallen luchtveiligheid, ARBO-veiligheid, milieuveiligheid, verkeersveiligheid en brandveiligheid. Op het gebied van luchtvaartveiligheid kregen in 2005 vooral 'runway incursions' en 'birdstrikes' veel aandacht.
Alle bedrijven die werken op Schiphol, hun klanten en hun medewerkers hebben belang bij veilig werken. Veiligheid is daarom een zaak van ieder bedrijf zelf én van alle bedrijven samen. "Samen werken aan Veiligheid" is het motto van de bedrijven die op het gebied van veiligheid samenwerken in het Veiligheidsplatform Schiphol. Het Veiligheidsplatform is een samenwerkingsverband van alle bedrijven die een rol spelen in het luchtvaartproces. Dat zijn de Nederlandse en buitenlandse luchtvaartmaatschappijen, Amsterdam Airport Schiphol, Luchtverkeersleiding Nederland, afhandelingsbedrijven, cateringbedrijven, schoonmaakbedrijven en tankdiensten. Het doel van hun samenwerking is de veiligheid op Schiphol te waarborgen en integraal te verbeteren. Na de Bijlmerramp werd een integrale aanpak van de veiligheid op Schiphol ook een eis van de overheid.
Alle deelnemende bedrijven hebben een eigen veiligheidsmanagementsysteem voor de eigen bedrijfsprocessen. Het Veiligheidsplatform Schiphol richt zich op de raakvlakken van deze processen en de samenhang tussen de verschillende veiligheidsmanagementsystemen. Het Veiligheidsplatform Schiphol kijkt naar het gehele luchtvaartproces en maakt de gehele veiligheidsketen zichtbaar. Onder het platform opereren werkgroepen. Daarnaast komen incidentonderzoekers van alle

bedrijven maandelijks met hun analyses bij elkaar. Zo worden patronen zichtbaar, bijvoorbeeld in het terugduwen van vliegtuigen (push backs). Sinds kort werkt het platform met een jaarplan. Er is een beleidsverklaring opgesteld, die alle partijen hebben ondertekend. De vrijblijvendheid is er afgehaald.

Security

Security heeft betrekking op veiligheid en beveiliging van de luchthaven Schiphol. Hier gaat het om de publieke veiligheid. Er wordt veel gedaan op dit gebied op Schiphol, maar in het verborgene. Per jaar wordt 200 miljoen geïnvesteerd. Dat heeft alles te maken met 11 september. De kosten van beveiligingsmaatregelen zijn opgenomen in de luchthavengelden die betaald worden door de luchtvaartmaatschappijen. De luchtvaartmaatschappijen berekenen deze kosten door aan hun passagiers via een beveiligingsheffing op de vliegtickets.
Amsterdam Airport Schiphol is zelf wettelijk verantwoordelijk voor de uitvoering van preventieve beveiligingstaken op de luchthaven. De Koninklijke Marechaussee houdt toezicht op de taakuitoefening, terwijl het Ministerie van Justitie eindverantwoordelijk blijft. Particuliere beveiligingsbedrijven voeren de werkzaamheden uit. Verder wordt er intensief samengewerkt met Korps Landelijke Politie Dienst, Douane, Immigratie en Naturalisatie Dienst, Algemene Inlichtingen en Veiligheid Dienst, Leger des Heils, Meldpunt M en natuurlijk diverse vertegenwoordigers binnen de luchtvaartsector. Schiphol voert uit, maar onder controle van de overheid. Schiphol is een commercieel bedrijf, een NV. Schiphol doet dit niet zelf, uit efficiëntieoverwegingen Hiervoor worden 2800 private medewerkers ingehuurd van diverse bedrijven. Op Schiphol zijn honderd medewerkers belast met de aansturing van deze private beveiligers. De politietaken op Schiphol worden uitgevoerd door de Koninklijke Marechaussee. Die taak omvat ook de beveiliging van de luchtvaart tegen terroristische aanslagen. Ook de exploitant van de luchthaven en de luchtvaartmaatschappijen hebben beveiligingstaken en verantwoordelijkheden (website ministerie van Verkeer en Waterstaat).

Europees beleid

De maatregelen die in Nederland worden genomen ter beveiliging van de luchtvaart zijn bijna allemaal gebaseerd op internationaal beleid. Het internationale beveiligingsbeleid is grotendeels EU-beleid, via rechtstreekse verordeningen. Dit zijn de zogenaamde regels beveiliging luchthavens, die gelden voor alle lidstaten. De luchtvaartsector had eerst aversie tegen deze regels, maar is nu bijgedraaid. Harmonisatie is een probleem, maar er treedt verbetering op.

Integrale veiligheid

De diamantroof in februari 2005 was in een aantal opzichten een keerpunt. De roof vond plaats op het terrein van Schiphol en had veel impact. De gestolen auto kon immers ongehinderd het terrein verlaten. De diamantroof leidde tot onderzoek van de Tweede kamer en de oprichting van de commissie Toegangsbeheer Schiphol

(Commissie-Oord). Ook ontstond het Platform Beveiliging en Publieke Veiligheid Schiphol. De commissie-Oord had tot taak te bezien in welke mate de effectiviteit van maatregelen ter beveiliging van de burgerluchtvaart van invloed is op het tegengaan van (veelvoorkomende) criminaliteit op Schiphol.
Op 25 januari werd het Platform Beveiliging en Publieke Veiligheid Schiphol opgericht. Hiermee werd een begin gemaakt met een centrale (publieke/private) regie op de beveiliging en criminaliteitsbeheersing op Schiphol. (TK, 2e voortgangsrapportage implementatie aanbevelingen commissie Oord). Betrokken publieke en private partijen werken in dit platform samen om veiligheid en beveiliging in samenhang op te pakken. Uitgangspunt is de beheersing van risico's als gevolg van terroristische dreigingen van aanslagen/kapingen, illegale immigratie, drugs/wapensmokkel, diefstallen en openbare orde. Een betere informatiepositie, ondersteund door techniek en integratie van activiteiten maakt een gezamenlijke risicoanalyse met oog voor samenhang mogelijk, zo wordt veronderstelt. Met een gezamenlijke risicoanalyse zijn de risico's in de beveiliging/veiligheid beter beheersbaar, worden doublures vermeden en kunnen partijen hun processen beter stroomlijnen.
Het voorzitterschap van het Platform wordt gedeeld tussen de Nationaal Coördinator Terrorismebestrijding en de President van de Schiphol Group. In het platform nemen verder vertegenwoordigers van Defensie, Verkeer en Waterstaat, AIVD, Financiën, Vreemdelingenbeleid en Integratie, de KLM, het Openbaar Ministerie en het openbaar bestuur deel. De feitelijke regiefunctie voor de beveiligings- en veiligheidsprocessen op Schiphol vindt plaats in een stuurgroep. De stuurgroep benadert de beveiliging en veiligheid vanuit de processen en het is haar taak de regie te voeren op de samenhang van activiteiten die gericht zijn op de verbetering van kwaliteit, effectiviteit en efficiency. Voorbeelden van de nieuwe (publiekprivate) aanpak zijn het plan voor de gemeenschappelijke controlekamer en voor de toepassing van nieuwe technieken, waarop dadelijk terug komen.

3.5.2 De Nodale Oriëntatie

Schiphol is een knooppunt dat verschillende soorten verschillende infrastructuren met elkaar verbindt (lucht, weg, rail) en waar binnen zich in ieder geval personen en goederenstromen zich bewegen. We richten ons in dit onderzoek met name op de personenstroom.

Self service airport

Essentieel in de beheersing van de passagiersstroom is het brede concept van de 'self service airport', dat ook gevolgen heeft voor de wijze waarop het beveiligingsvraagstuk wordt aangepakt. Als onderdeel hiervan heeft Schiphol een geheel nieuw afhandelingsconcept ontwikkeld, het zogenaamde Redesign Passenger Process. Dit moet binnen enkele jaren operationeel zijn. Uitgangspunt is het reisgedrag van toekomstige passagiers. Passagiers komen binnen door de 'front door' en gaan weg via de 'boarding area' , zogenaamde 'de back door'. Hoe verloopt dit proces thans?

'Dat begint bij thuis inchecken, mensen weg bij de ticketbalie. Dat kost immers geld en tijd. Het gaat veel sneller. Aan de balie wordt nu alles opnieuw ingetypt. Ik doe het met twee drukken op de knop. Het duurt nu 10 minuten. Je moet weten hoe de reiziger in de toekomst gaat reizen. Je komt het terrein op, bied je paspoort aan aan de machine. Die registreert dat, stuurt informatie naar de gate waar jij naar toe moet. Bij deze gate vinken zij af of dit de juiste passagier is. Zo kun je Schengen opheffen. Je hebt een personal file, waaruit blijkt dat je zonder enige controle kunt vertrekken. Die meneer achter je uit Ghana moet wel gecontroleerd worden. Er is veel meer mogelijk. Wij hebben daar een visie voor gemaakt. Meer informatie hoeven wij niet te gebruiken.'

Ambitie

Het instapproces voor passagiers wordt echter verregaand geautomatiseerd (Algemeen Dagblad d.d. 5-8-2006; Volkskrant 7-8-2006). De huidige incheckbalies en -zuiltjes worden vervangen door poortjes die geopend kunnen worden door het paspoort en ticket op een scanner te leggen. Daar kunnen passagiers ook een stoel uitzoeken en een bagagelabel printen. Daarna zet de reiziger zijn koffer op een transportband en loopt ongehinderd door naar taxfree winkels of naar de 'gate'. Aan de 'gate' komt een geavanceerd type detectiepoort waar opnieuw paspoort en ticket moeten worden getoond. Dat poortje controleert op metaal en op explosieven. Ook de handbagage moet hier in een scanner. Grondstewardessen en marechaussee komen alleen nog in actie als een passagier om hulp vraagt of als het alarm van een detectiepoortje afgaat. Zo worden kosten en wachttijden teruggebracht en kan de luchthaven meer passagiers verwerken.

Ook op het terrein van de luchthaven wordt gewerkt aan een 'security-wasstraat' voor de honderden voertuigen die dagelijks het terrein op willen. In samenwerking met TNO ontwerpt Schiphol een grote poort met röntgenscanner om de lading van elk voertuig te kunnen bekijken. Daarnaast staat een detectiepoort voor de chauffeurs. Dit systeem moet in 2008 gereed zijn.

Schiphol heeft een reeks van maatregelen genomen op gebied van beveiliging. Enkele daarvan zijn geïmplementeerd, anderen zijn nog ontwikkeling. Op een aantal van deze ontwikkelingen gaan we nader in.

Privium program

Privium biedt leden voorrang, snelheid en comfort, zoals gegarandeerd vooraan parkeren in P2 of P3, inchecken bij 'business class' balies en een snelle grenspassage met de irisscan. Per 1 maart deden al 30000 mensen mee in dit programma. Voor €200,00 kun je je als reiziger inkopen in een Privium programma, zodat je er via een aparte Privium lane door de paspoortcontrole kunt, zeer bruikbaar voor zakenlieden. Sommigen vliegen bijna elke dag.

Het levert veel tijdswinst op ten opzichte van de handmatige paspoortcontrole. Er zijn eigen Privium incheckbalies. Vaak zijn dit de business class balies, ongeacht de klasse van het ticket. Bij deelname aan Privium worden opnamen gemaakt van zowel het linker- als het rechteroog. Bij de grenspassage worden de gegevens in de chip vergeleken met de gegevens van het echte oog. Hierna worden de gegevens direct uit de apparatuur verwijderd.
Na de scan worden de irisdetails alleen op de chip van de Priviumkaart opgeslagen en niet ook daarnaast in een database. Respect voor privacy blijkt uit onder andere uit een aantal maatregelen die zijn genomen, zoals: [9]

- Verification to a token
- No storage of template in databases or systems
- Only conscious capture possible
- No long distance or unconscious recognition
- Protected against identity theft
- No skimming possibility
- Encrypted storage of data on the token
- Encrypted communication to authentic systems
- Use of non-hackable private keys (no public part).

Staff Access

Alle stafleden worden gescreend, hetgeen betekent dat alle personeelsleden een veiligheidsonderzoek en een pasje krijgen. Criminele en politieke antecedenten worden onderzocht. Schiphol verstrekt zelf de pasjes. Vroeger gaf de overheid alleen een advies over de toekenning. Nu is navolging wettelijk verplicht. Screenen gebeurt nu in drie uur via elektronische kanalen.
Stafleden - captains, stewardessen - worden nu op dezelfde wijze gecontroleerd als passagiers, tot hun grote ergernis. Voor deze controles gelden Europese richtlijnen. Er wordt handmatig gefouilleerd. Body scans zijn in ontwikkeling, onder druk van piloten die klagen over de handmatige fouilleringen aan het lichaam. De body scans worden samen ontwikkeld met de overheid. Body scans roepen een privacy discussie op. Je kunt alles gezien op het lichaam. De private delen worden afgeschermd. Mensen die scans bekijken zitten nu afgeschermd. Zij zien alleen een pop, niet de persoon bij wie het hoort. De stewardessen vinden dit een goede oplossing. Het werkt perfect, maar de EU moet deze werkwijze nog goedkeuren. Het zou ook gebruikt kunnen worden voor de controle op drugs en drugsgelden, maar tot op heden wordt dit nog niet toegepast op passagiers, omdat de EU hierop nog studeert. Verder zijn personeelspassen met biometrische kenmerken versneld geïntroduceerd.
In de loop van 2005 is een aantal personeelsdoorgangen voorzien van apparatuur, waarmee deze biometrische gegevens van de Schipholpas gecontroleerd kunnen worden. Op personeelspasjes staat een digitale afbeelding van de iris. In vergelijking

[9] Presentatie Van Beek voor de Club van Amsterdam d.d. 1-3-2006.

met andere Europese landen loopt Schiphol hiermee voorop. Dit systeem levert veel interessante informatie op. Waarom gebruikt iemand zijn personeels pas op een bepaald tijdstip terwijl hij niet werkt? Indien dit wordt geconstateerd, dan vindt vervolgens nader onderzoek plaats door de bedrijfsbeveiliging. Passen worden overigens ingetrokken als iemand toegang geeft tot een ander. Ook wordt gewerkt aan software die het mogelijk maakt om verdachte passages sneller en gemakkelijker op te merken, waardoor de betreffende persoon ook eerder en effectiever kan worden gevolgd.

Controle handbagage

Vanaf 1 december 2004 zijn extra beveiligingsmaatregelen geïmplementeerd voor passagiers en bagage uit landen buiten de Europese Unie die op Schiphol overstappen op een vlucht naar één van de lidstaten. Voor de handbagage wordt X-ray technologie gebruikt, terwijl voor de controle op bagage in de kelder gebruikt wordt gemaakt van CT-scans. De controle is vooral gericht op het opsporen van explosieven. Hiermee kunnen doorsnede beelden gemaakt worden. Dit is een volautomatisch systeem dat vanaf 2002 in de EU wordt toegepast bij de bagagecontrole. Voordien werden koffers niet bekeken. Thans is 100 procent bagagecontrole, een controle die sinds 2006 wereldwijd plaats vindt. Het resultaat is dat er veel geld en drugs in de bagage worden aangetroffen. Deze vondsten moeten wettelijk worden gemeld aan de Marechaussee.

Cameratoezicht

Met de Nederlandse Spoorwegen worden thans proeven gedaan met gericht cameratoezicht op de treinperrons onder de terminal. Op die manier kan onbeheerde bagage tijdig gesignaleerd worden. Ook op de rijbaan voor de vertrekhal is een proef geweest met gericht cameratoezicht, waarbij gericht kentekens werden geverifieerd. Zo werden er relatief veel gestolen auto's gesignaleerd. De eerste maand waren er bijvoorbeeld 50 'hits'. Er is nu elke week wel een 'hit'. Parkeerterreinen worden bijvoorbeeld door criminelen gebruikt om gestolen auto's een tijdje weg te zetten.

> *'Soms hebben wij gestolen auto's die de politie nog niet in haar register heeft. De verzekering is sneller. We zijn gekoppeld aan het opsporingsregister van de politie én het systeem van de verzekeringsmaatschappijen'. (Bron: interview)*

De nieuwste ontwikkeling zijn camera's op Schiphol zelf. Er zijn er nu ongeveer 1200 camera's operationeel, waar de meeste recent geplaatst zijn. Schiphol wil meer toezicht uitoefenen met behulp van camera's en wil minder personeel inzetten. Ook de marechaussee zou dan in omvang terug kunnen. Naarmate meer technologie wordt ingezet voor de paspoort c.q. identiteitscontrole, zou ook de marechaussee Schiphol in aantal terug gebracht kunnen worden.

> *'Ons doel is zo min mogelijk partijen in dit proces hebben. Wij willen dit allemaal zelf afhandelen en niemand tegenkomen. Zo gaat het veel sneller. Paspoortcontroles kunnen wij*

nog niet overnemen. Wij zijn ermee bezig om hier machines voor in te stellen. Zo kan de marechaussee fors terug in omvang'.

Schiphol wil in de nabije toekomst 'slimme camera's', die aanslaan als iemand zich in de massa verdacht gedraagt of als zich andere verdachte situaties voordoen. Camerabeelden worden nu vooral achteraf gebruikt, bijvoorbeeld bij de reconstructie van de diamantroof. Het is interessant om camerabeelden veel pro-actiever te gebruiken, waardoor eerder en sneller en dus ook preventief kan worden ingegrepen.

	SCHIPHOL
TYPE STROOM	personen, goederen
INTERVENTIE	Toegang controleren en meebewegen
OMVANG	(stille) 100% controle
EFFECT	ongehinderde doorstroom
INTENSITEIT	Continu
GEOGRAFISCH	locaties rond Schiphol Airport
MANIFESTATIE	Zichtbaar en onzichtbaar
RISICO SELECTIE	Bepaald door kracht van technologie en observatie. - selectie aan de hand van verzamelde individuele- en groepsinformatie (systeeminformatie) - Human Factor
REFERENTIE	personen

Tabel 3.5:kenmerken casus Schiphol

3.5.3 Kritische factoren

Publiek-private samenwerking

Schiphol weet dat het zich bevindt in het brandpunt van een aantal politieke en maatschappelijke ontwikkelingen, door de eerdere genoemde diamantroof en het risico van terroristische aanslagen. Er ontstond zo een groot gevoel van urgentie om de veiligheid op en de beveiliging van Schiphol op een hoger plan te tillen, met gebruik van de mogelijkheden van de moderne technologie. Daarnaast werd onderkend dat Schiphol een knooppunt is van infrastructuren en van activiteiten waar vele private en publieke organisaties functioneren. Daarom is publiekprivate samenwerking op het bedrijventerrein Schiphol een belangrijke succesfactor. Er is immers een samenloop van belangen en er zijn gemeenschappelijke belangen.
Bij Schiphol is de aanvankelijke aversie tegen het platform - vanwege de spanning tussen commerciële belangen (belastingvrije verkoop, parkeren) en publieke belangen

- verdwenen. Samenwerking met de overheid wordt gezien als onvermijdelijk. Het platform slecht grenzen tussen bedrijfsleven en overheid en maakt onderwerpen bespreekbaar. Win-win situaties treden steeds gemakkelijker op, waardoor gezamenlijke initiatieven eerder van de grond komen. Voorbeelden zijn de toepassing van software voor slimme camera's en de gezamenlijke servicebus. De kosten worden gedeeld met de overheid op 50-50 basis. Voorheen kwam het leeuwendeel van de technische innovaties die op Schiphol werden ontwikkeld en werden ingevoerd voor rekening van Schiphol, maar hierin is nu verandering opgetreden. Het platform biedt ook een mogelijkheid om elkaar te informeren over mogelijke innovaties. Voorheen wisten partijen van elkaar niet wat waar en door wie werd ontwikkeld.

Integrale aanpak

Het platform maakt een integrale benadering en een samenhangende aanpak mogelijk van criminaliteits- en beveiligingsproblemen door de introductie van centrale besturing. Door het voorzitterschap van de NCTB zijn bovendien korte lijnen gecreëerd met 'Den Haag' waardoor politieke steun kan worden gemobiliseerd als dat nodig is. De vrijblijvendheid is er af gehaald en daadkracht en realisatiemacht zijn toegenomen.

Informatie en informatiemanagement

De initiatieven die het platform heeft genomen zorgen voor een betere informatiepositie. Voor de gezamenlijke meldkamer - de servicebus - hebben alle partijen hun wensen kunnen inbrengen, Vreemdelingenzaken, justitie, douane, rechtshandhaving, Marechaussee, Defensie en KLM. Alle informatie wordt in de servicebus opgeslagen en op basis van autorisatie kan iedereen de informatie er uithalen die hij nodig heeft, op basis van getekende contracten. Informatie kan voor meerdere doelen worden gebruikt. Maar uitwisseling en stapeling van informatie verlopen nog niet altijd zonder problemen.
Schiphol verzamelt gegevens voor de eigen bedrijfsvoering en voor de dienstverlening aan klanten. Hier zit ook waardevolle informatie in voor overheidsinstanties.

> *'Bij de meeste parkeerterreinen op Schiphol is kentekenherkenning. Waarom? Wij willen onze reguliere klanten advies geven over waar het goedkoopste parkeren. Vaste klanten willen wij herkennen. Kortgeleden hebben wij deze informatie voor onze bedrijfsvoering gedeeld met de marechaussee. Uit vergelijking met het kenteken registratiesysteem bleken 21 auto's gestolen te zijn. Deze stonden in de parkeergarage. De Marechaussee wil nu een kopie van alle bedrijfsvoering gegevens van Schiphol. Daar wil men op aansluiten. Wettelijk mag dit nog niet. Aan dit wettelijk kader wordt gewerkt. Technisch kan het en gebeurt het feitelijk ook al. Het is van de gekke het niet te doen. De vraag is in welk domein welke taken liggen. Primaire doel is bedrijfsvoering en dienstverlening aan klanten'. (Bron: interview)*

Schiphol geeft geen informatie door over passagiers. De passagiergegevens liggen bij de luchtvaartmaatschappijen. Hiervoor gelden specifieke regels. Ook de Marechaussee geeft gegevens door, omdat zij de paspoortcontrole doet. Schiphol kijkt vooral naar de

dingen die iemand bij zich heeft en veel minder naar de persoon. Dit laatste wordt gezien als een overheidstaak. Men wil niet op de stoel van de politie gaan zitten. De onderlinge uitwisseling van informatie kan beter.

> *'Terroristen moet je arresteren voordat ze op Schiphol komen. Hierover moet meer informatie worden uitgewisseld. De AIVD wist ons niet te vertellen welke voorwerpen zo een dreiging had veroorzaakt in de Londense metro'. (Bron: interview)*

Voor de uitwisseling van informatie moeten protocollen worden ontwikkeld. Hier wordt nu over gesproken. Het platform bewijst ook hierin zijn nut, omdat het een forum biedt voor moeilijke onderwerpen zoals de privacy problematiek bij cameratoezicht en de kwaliteit van de informatie-uitwisseling. Het College Bescherming Persoonsgegevens is bij deze discussie betrokken.

Rol van de Marechaussee

De politie kan volgens Schiphol nog beter samenwerken maar blijft op afstand. De Marechaussee die immers de politiefunctie uitvoert, is minder gericht op innovatie en zoekt vooral oplossingen in een uitbreiding van de bestaande capaciteit in plaats van in technologische vernieuwing. Technologische vernieuwing heeft als voordeel dat veiligheid en klantgerichtheid niet als tegenstrijdige belangen worden gezien maar toch op zekere hoogte gecombineerd kunnen worden. Bij Schiphol zijn klantgerichtheid en het gevoel voor urgentie sterker ontwikkeld dan bij de Marechaussee.

> *'Knooppunten als Schiphol, de haven, grote stations en daar veel informatie vragen er wel echt met elkaar samenwerken, dan boek je veel winst. De politie sluit mondjesmaat aan bij het platform. Men is bang te worden opgeheven of taken kwijt te raken. De politiek ziet de marechaussee wel als het 27e korps dat niet mag staken en overeind blijft als alle anderen falen. Dat beeld laat men zich graag aanleunen'.(Bron: interview)*

Cruciaal voor samenwerking is onderling vertrouwen. Hierin is verbetering mogelijk.

> *'Op bedrijventerreinen valt meer samen te werken, maar het zijn soms wel Poolse landdagen. De AIVD zegt soms; ik kan je geen bedreigingsinformatie geven, want er zitten partijen aan tafel die dit niet mogen weten. Dan gaan er mensen de kamer uit en zeggen ze: het dreigingsbeeld is onveranderd. Dat gaat nergens over. Als je samenwerkt moet je ook vertrouwen hebben.'(Bron: interview)*

3.6 Financiële stromen: CREDITCARDFRAUDE

3.6.1 Achtergrond

In Nederland omvat het dagelijkse betalingsverkeer vele miljoenen transacties van banken en financiële instellingen, hun klanten, bedrijven en individuele consumenten onderling. Het bedrijf Equens Nederland, voorheen bekend als Interpay, is verantwoordelijk voor een adequate, betrouwbare, efficiënte en snelle verwerking van deze transacties. Het aantal transacties dat via Equens Nederland wordt verwerkt, loopt jaarlijks in de miljarden: jaarlijks 3,3 miljard girale betalingen en 1,7 miljard toonbankbetalingen en autorisaties van geldopnames[10]. Hiermee is Equens Nederland één van de grootste verwerkers van betalingsverkeer in Europa. Om deze omvangrijke stroom van betalingsverkeer te kunnen verwerken, maakt men gebruik van geavanceerde computersystemen en loopt men voorop bij de ontwikkeling en toepassing van nieuwe innovatieve technologieën in de procesoptimalisatie van het betalingsverkeer maar ook in het kunnen signaleren van fraude en detectie van (mogelijk) misbruik binnen deze financiële stroom.

3.6.2 De Nodale Oriëntatie

Het Nederlandse betalingsverkeer genereert een heleboel verschillende stromen waarin verschillende soorten van financiële transacties worden afgewikkeld. Enerzijds heeft Equens Nederland de verantwoordelijkheid voor de verwerking en adequate uitvoering van betalingsverkeer (*doorstromen*) en tegelijkertijd is men in staat afwijkingen binnen transacties, patronen en gedrag te identificeren en hier passende interventies bij de formuleren. Dit zonder een belemmering te vormen in de doorstroming van het verkeer. Kortom, de nodale oriëntatie komt vooral tot uitdrukking in het volgen/monitoren van bewegingen, transacties en het maken van 'risico-beoordelingen'.

Identificeren van risico's en afwijkingen binnen de stroom.

Aan het begin van de jaren '90 is een begin gemaakt met het systematisch analyseren van betalingsverkeer op signalen van fraude en misbruik. Binnen het betalingsverkeer richt men zich op een drietal substromen:

1. Betalingen met creditcard;
2. PIN-transacties;
3. Automatische incasso's.

De risico (fraude) detectie richt zich met name op transacties binnen de stroom van creditcard betalingen (bij PIN transacties en automatische incasso's komen maar in

[10] "*Partner in processing*", Interpay 2006, p1.

beperkte mate excessen voor, die detectie noodzakelijk maken). Detectie is in zekere zin de laatste schakel in de toezichtsketen. Het inrichten van detectievoorzieningen heeft alleen nut indien de genomen preventiemaatregelen niet (meer) afdoende zijn. Het zoeken naar een balans tussen preventieve beveiligingsmaatregelen en gebruikersgemak van een betaalmiddel leidt soms tot een gereduceerde hoeveelheid preventieve maatregelen. Voorbeelden hiervan zijn legitimatie bij betalingen (boven bepaalde bedragen), het gebruiken van een terminal met pincode en de introductie van een chip op de creditcard. Bij transacties met bankpassen is de PIN al lang geleden geïntroduceerd en ook met automatische incasso's zijn risico's beperkt. Wanneer nieuwe preventieve maatregelen van kracht worden, betekent dat de noodzaak en de vorm van detectie opnieuw wordt bepaald.

Om een beeld te krijgen van alle betalingen die met creditcards worden gedaan en daadwerkelijk te kunnen controleren of er mogelijk sprake is van misbruik, is het noodzakelijk dat een omvangrijke hoeveelheid data wordt verzameld en geanalyseerd, gelet op het feit dat het aantal Nederlandse creditcard transacties dat door Equens Nederland wordt verwerkt, maandelijks miljoenen is. Wanneer een kaarthouder een betaling met zijn creditcard wil doen, wordt inmiddels in (vrijwel) alle gevallen online en realtime een verbinding met Equens Nederland gezocht. Door middel van een geautomatiseerd systeem ("Authorizer") worden betalingsaanvragen direct getoetst aan criteria die door de bank van de kaarthouder zijn bepaald. Dit kunnen criteria zijn als: de vervaldatum van de kaart, bestedingslimiet en een check of een kaart al dan niet geblokkeerd is. Vervolgens wordt een signaal teruggeven of de bank akkoord is en zal de transactie voltrokken worden. De betaling wordt van het limiet afgeboekt en maandelijks van de rekening afgeschreven. Dit autorisatieproces wordt gedefinieerd volgens de richtlijnen van de banken waarbij Equens Nederland verantwoordelijk is voor de technische afhandeling en efficiënte uitvoering ervan.

Het autorisatieproces is vanuit het oogpunt van opsporing van fraude het moment om tijdig te kunnen interveniëren. Equens Nederland past hiervoor zogenaamde 'regels' en statistisch modellen toe op alle betalingsverkeer. Deze regels kunnen worden gezien worden als een set van vooraf bepaalde kenmerken of patronen waaraan alle transacties geautomatiseerd worden getoetst. Het aangrijpingspunt voor het toepassen van deze regels ligt in de korte tijd tussen aanvraag en autorisatie, op het moment dat de transactie nog niet is voltooid. Bepaalde afwijkende waarden op de regels kunnen leiden tot vooraf omschreven interventies (tijdelijk blokkeren creditcard, weigering transactie etc). Het verloop van PIN-transacties verloopt op een vergelijkbare wijze ook via Equens Nederland.

Om binnen de stroom betalingsverkeer risico's te kunnen signaleren gaan álle gegevens die door de Authorizer zijn verwerkt door middel van een "dump" naar de afdeling Risk Detection (RD). Risk Detection vormt tezamen met Risk Investigation, Operation Security en Risk Consultancy de afdeling Risk Management. RD heeft tot taak incidenten met een specifieke betaalkaart, die afwijken van normaal en historisch gedrag, op te sporen. Het gaat er dan niet om te bepalen óf en in hoeverre er sprake

is van fraude, maar om het constateren van afwijkingen die, op basis van historische data en meer andere opvallende of onmogelijke kenmerken, opmerkelijk zijn ten opzichte van het regulier betalingspatroon van een specifieke kaart. Bij aannemelijke verdenking van fraude wordt de afdeling Risk Investigation ingeschakeld. Deze afdeling start vervolgens een onderzoek naar de oorzaak/bron van de afwijkingen. Men gaat hierbij aanvullende aanwijzingen verzamelen om de patroonafwijking te verklaren of te herkennen.

De fraudeparameters (regels) die worden toegepast op de 'dump' uit de Authorizer worden ingesteld door Equens Nederland. Hiervoor is Equens Nederland gemachtigd door de banken (klanten van Equens Nederland). Doordat regels direct kunnen worden aangepast als daarvoor aanleiding bestaat, kan Equens Nederland tot snelle interventie komen. De bepaling wat de definitie van regels is gebeurd door mensen maar vindt tevens plaats op basis van historisch gegevens.

Ambities

In de toekomst zijn verdere ontwikkelingen te verwachten in de toepassing van intelligente software en mogelijke vormen van geavanceerde datamining. Met de ontwikkeling van Artificial Intelligence, oftewel zelflerende systemen is men beter in staat patronen en logische verbanden te herkennen, dit gegeven de exponentieel groeiende omvang van data die geanalyseerd moet worden. Systemen kunnen door analyse van eigen handelingen zichzelf trainen. Toch zijn deze technieken nog sterk in ontwikkeling en leiden nog niet in alle gevallen tot de gewenste resultaten. Het opstellen van profielen en parameters is nu dan ook nog grotendeels mensenwerk dat gebaseerd is op systematische (historische) kennisopbouw van het betalingsverkeer.

Het toezicht op creditcard betalingen gaat vanaf volgend jaar terug naar de banken zelf. Vanuit wet- en regelgeving worden financiële instellingen verplicht een uitgebreid klantprofiel op te bouwen ("ken uw klant"-verplichting). Dat betekent dat niet alleen de reguliere PIN en creditcard transacties worden verzameld, maar ook lopende kredieten, hypotheken, inkomsten – en uitgavenpatronen etc. De 'ken-uw-klant' verplichting is gericht op het tegengaan- en de opsporing van:

1. Witwassen;
2. Terrorisme;
3. Fraude.

Dit maakt deel uit van de toezichtwet 'Wet financiële dienstverlening'. Hiermee beoogd men van overheidswege te komen tot vergaande transparantie over de financiële situatie van klanten van financiële dienstverleners, recent ook merkbaar aan de oproepen van de Postbank aan haar klanten zich op het postkantoor te komen legitimeren. Deze ontwikkelingen beperken zich niet tot Nederland maar ontstaan in internationale afspraken en staan ook onder invloed van de Verenigde Staten.

Kort samengevat zijn de belangrijkste kenmerken beschouwd vanuit nodaal perspectief als volgt:

	CREDITCARDFRAUDE
TYPE STROOM	Financiën (betalingsverkeer)
INTERVENTIE	meebewegen & toegangscontrole
OMVANG	100%
EFFECT	ongehinderde doorstroom
INTENSITEIT	Continu
GEOGRAFISCH	Virtueel (overal)
MANIFESTATIE	Onzichtbaar
RISICO SELECTIE	bepaald door kracht van **technologie** - Systematische kennisopbouw: -historische data -patroonherkenning/profiling - Human Factor
REFERENTIE	(credit)kaartnummer

Tabel 3.6: Kenmerken casus creditcardfraude

3.6.3 Kritische factoren

Het adequaat kunnen volgen van de stroom betalingsverkeer en het tegelijkertijd kunnen detecteren van mogelijke risico's wordt bepaald door onder meer de volgende kritische factoren.

Informatieanalyse

Alle informatie betreffende het betalingsverkeer dat wordt verwerkt door de Authorizer wordt getoetst aan de set van regels die zijn opgesteld rond fraudedetectie. De vaststelling van deze regels is een proces dat continu moet worden aangepast en actueel gehouden. De selectie van mogelijke risico's vindt immers plaats op basis van deze regels en is dus, mede gezien de omvang van de stroom, van cruciaal belang in de monitoring van afwijkingen binnen de stroom. Opgebouwde kennis van historische data vormt belangrijke input voor de zuiverheid/efficiëntie van regels. Anderzijds zijn bepaalde regels maar een beperkte periode nuttig; criminelen passen hun strategie aan naar gelang bepaalde vormen van misbruik niet meer werken of schijnbaar tegenhouden worden. Dit maakt het proces zeer dynamisch. Het vaststellen van patronen, afwijkingen en logische verbanden kan echter álleen op basis van historische gegevens. Dit betekent dat alle betalingsverkeer wordt vastgelegd.

Het detecteren van fraude is dus in eerste instantie sterk afhankelijk van de inzet van afgestelde technologie waarna vervolgens de human factor in de follow-up steeds belangrijker wordt; om werkelijk te kunnen bepalen of er sprake is van fraude of misbruik heeft Equens Nederland dagelijks contact met klanten over als 'afwijkend'

gekwalificeerd betalingsgedrag. De analyse van gedrag en afwijkingen wordt bepaald op het niveau van de kaart, en is dus strikt genomen op dat moment niet op personen herleidbaar. Pas op het moment dat na de systeemselectie en de informatie analisten een verdergaand onderzoek gerechtvaardigd is worden persoonsgegevens achter de kaart 'zichtbaar', dit conform duidelijk geprotocolleerde richtlijnen.

Samenwerking

Bij het constateren van mogelijke fraude is het van belang dat samenwerking met opsporingsdiensten geregeld is. Voor het betalingsverkeer heeft Equens Nederland een belangrijke signaalfunctie. Van de andere kant is Equens Nederland ook partner voor de politie als men bij invalacties creditcards vindt en de herkomst en betalingen wil traceren.
Een voorbeeld van samenwerking is rond het "skimmen" van bankpassen: hierbij wordt een voorzetmond op een pinautomaat gezet en de pas gekopieerd. Tegelijk wordt of door een persoon of door een camera de pincode gezien. Men is vervolgens in staat bankpas en code te gebruiken voor geldopname. De transactie/geldopname waarbij de kaart wordt geskimd is als zodanig niet te detecteren als vorm van fraude; dit gebeurt immers duizenden keren per uur en valt onder regulier betalingsverkeer zolang de eigenaar geen melding van verlies/diefstal heeft gedaan. Wanneer echter grote sommen geld en/of in korte tijd achter elkaar worden besteed wordt dit wel gedetecteerd. Vervolgens kan bij alle getroffen kaarthouders worden nagegaan waar de laatste transacties zijn verricht waarna uiteindelijk de betreffende automaat in beeld komt.

Gevallen van fraudedetectie hebben echter niet altijd een adequate follow-up. Dit komt doordat op bepaalde momenten dit soort vormen van criminaliteit een lagere prioriteit kan hebben bij politie.

" *Misbruik van creditcardgegevens bij internetfraude kan worden gedetecteerd. Bijvoorbeeld rond de handel op www.marktplaats.nl. Het is nu nog wel eens lastig om in samenwerking met politie en justitie tot een adequate follow up te komen. Vaak liggen prioriteiten bij andere vormen van criminaliteit of komt men pas in actie na aangiften van oplichting. Met de informatie die uit het detectiesysteem kan soms veel eerder geintervenieerd worden en eigenlijk worden 'voorkomen'.*"

De informatie die binnen het betalingsverkeer afwijkend is of vermoedelijk duidt op misbruik wordt gedetecteerd en kan voor politie en justitie aanvullend bewijs leveren. Dit soort signalen rond personen/kaarthouders zou door politie veel meer en beter kunnen worden vastgelegd (soft-info). In principe werkt dit hetzelfde als de signaleringen/meldingen die gedaan worden in het kader van de regelgeving rond de Melding Ongebruikelijke transacties (MOT); bij verdachte aangemerkte transactie worden deze ter beschikking gesteld aan (Bijzondere) Opsporings-, Inlichtingen- en Veiligheidsdiensten in binnen- en buitenland ter versterking van de kwaliteit van opsporing en vervolging.[11]

[11] *Jaaroverzicht 2005 en vooruitblik 2006 Meldingen Ongebruikelijke Transacties, 2005*

Competenties, kennis en kunde

Het risk detection systeem genereert duizenden gevallen van mogelijke fraude of misbruik. Al deze gevallen worden uitgelicht en door analisten beoordeeld. Hier spelen opleiding, ervaring, intuïtie en kennis een rol in het proces deze te reduceren tot een aantal zaken die verder uitgezocht dienen te worden. De technologie die wordt toegepast is in staat in hele korte tijd een selectie te maken in de omvangrijke stroom van data en hieruit mogelijke risico's te selecteren. Het is echter complementair aan de human factor, hoe goed je de parameters (regels) ook definieert en hoe up-to-date deze ook zijn. De human factor speelt in de uiteindelijke analyse de doorslaggevende rol.

De inzet van menskracht in termen van arbeidskosten en daarbij de kosten van (het beheer van) detectietechnologieën zijn tezamen tot driemaal lager dan de mogelijke schade die zou ontstaan als risico's niet gesignaleerd zouden worden.

3.7 Informatie- en communicatiestromen: CYBERCRIME

3.7.1 Achtergrond

Cybercrime is een relatief nieuw fenomeen binnen de criminaliteit. Niet alleen criminelen, maar tegenwoordig ook terroristen, hebben de mogelijkheden van digitale technieken voor hun praktijken ontdekt. Computercriminaliteit is sterk in ontwikkeling. Cybercrime is een bijeffect van de komst van het digitale tijdperk. Cybercrime is niet een zelfstandig criminaliteitsterrein zoals drugs, fraude, mensenhandel, milieucriminaliteit, kinderporno en dergelijke. Kenmerkend is dat informatie- en communicatietechnologie (ICT) de criminele activiteit in haar essentie faciliteert, vergemakkelijkt of zelfs maskeert (Hetzschold, 2005).
De KLPD omschrijft cybercrime als elke strafbare en strafwaardige gedraging, voor de uitvoering waarvan het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is. Strafwaardig is gedrag waarvan verwacht wordt dat het binnen afzienbare tijd strafbaar wordt gesteld. Anders geformuleerd, hightech crime bestaat uit misdaden die zijn verricht met, of gericht tegen informatie en communicatietechnologie (NHTCC, 2005).

De veronderstelde toename van cybercriminaliteit werkte meer aandacht voor de aanpak ervan in de hand. In 2004 zijn twee projecten van start gegaan gericht op versterking van de aanpak van cybercrime. Het project National High Tech Crime Center (NHTCC) concentreerde zich primair op het vormgeven van de pro-actieve taak van de overheid en meer specifiek van de politie, op het gebied van de bestrijding van ICT criminaliteit. Dit was een project van de ministeries van Binnenlandse zaken en Koninkrijksrelaties (BZK), Economische Zaken (EZ) en Justitie in samenwerking met het Korps landelijke politiediensten (KLPD).
Daarnaast werd een project Aanpak Cybercrime (NPAC) gestart vanuit het platform criminaliteitsbeheersing. Dit project richtte zich op de niet-strafrechtelijke bestrijding door het versterken van de informatie-uitwisseling, samenwerking, en coördinatie tussen publieke en private partijen. Het uiteindelijke gevolg was het gezamenlijk opstellen van een ontwerp voor een Nationale Infrastructuur gericht op de bestrijding van cybercrime. Deze activiteit concentreert zich op publiekprivate samenwerking. Financier is het Ministerie van Economische Zaken en Werkgelegenheid.
De Nationale Infrastructuur heeft sinds 2005 enkele grote onderzoeken gestart. Één daarvan richt zich op het midden- en kleinbedrijf, een ander op de bankwereld. Er zijn twee andere experimentele onderzoeken in voorbereiding. Een nieuw experiment is het informatieknooppunt. Hierin wordt getracht tussen enkele sectoren, beginnend bij de financiële sector en bij overheidsorganisaties met een informatiepositie op het

gebied van hightech crime – KLPD, GOVCERT[12], AIVD- periodiek informatie uit te wisselen over dreigingen en de betekenis daarvan voor een sector.

Het Project NHTCC is begin 2006 beëindigd. Binnen de Dienst Nationale Recherche is uitvloeisel van dit project een team hightech crime opgericht voor de bestrijding van (inter-)nationale complexe vormen van cybercrime. Hier wordt dus specifiek capaciteit voor vrijgemaakt voor de opsporing van cybercrime. Daarnaast is het de bedoeling om meer inzicht te krijgen in de aard en omvang van cybercrime en input te leveren voor het nationaal dreigingsbeeld dat door de Dienst Recherche Informatie van het KLPD wordt opgesteld. Het team digitale expertise binnen de nationale recherche heeft een kennis- en innovatierol. Ook ondersteunt het andere units. Bij de nationale recherche heeft elke unit zijn digitale en Internet rechercheurs. Ook de UCTA[13] heeft zijn eigen digitale en internet expertise.

3.7.2 Nodale oriëntatie

Cybercrime speelt zich af in een virtuele omgeving, op het Internet. Dat geldt ook voor de transacties en de daders. Daders hebben virtuele identiteiten en kunnen ook nog eens snel wisselen van identiteit (nicknames). Ook modus operandi en gedragingen kunnen snel veranderen. Daarbij opereren daders in een internationale context op het wereldwijde web.
Het voormalige National Hightech Crime Center (NHTCC) onderscheidt vier vormen van cybercrime:

- **Illegale communicatie**. Criminelen bedienen zich van publieke netwerken voor onderlinge communicatie voor het uitwisselen van strafbare zaken, zoals bijvoorbeeld kinderporno. Het netwerk wordt eigenlijk gebruikt waarvoor het is bedoeld: gegevensuitwisseling.
- **Inbreuk op de integriteit van gegevensbeheer**. Het netwerk wordt gebruikt om ergens binnen te komen voor het moedwillig beschadigen van gegevens of voor het stelen van gegevens. Dit wordt 'computervredebreuk' genoemd.
- **Beschadiging van het netwerk**. Niet gegevens op het netwerk zijn het eerste doelwit, maar het netwerk of aangesloten apparatuur zelf. Waardoor die apparatuur bijvoorbeeld niet meer werkt, of werkt volgens de specificaties van degene die inbreuk maakt, zoals in het geval van botnets.[14]

---

[12] *Staat voor Governmental Computer Emergency Response Team ondersteunt de overheid bij preventie en afhandeling van ICT- gerelateerde veiligheidsincidenten. GOVCERT.NL. is voor de overheid het centrale meldpunt voor veiligheidsincidenten met betrekking tot ICT, zoals computervirussen, hacking en fouten in applicaties en hardware, verstrekt informatie en ondersteunt bij preventie van en reactie op veiligheidsincidenten.*

[13] *De Unit Contra Terrorisme en Activisme (UCTA) is begin 2005 in Nederland opgerichte eenheid van de Dienst Nationale Recherche van het Korps landelijke politiediensten (KLPD) die zich bezig houdt met de bestrijding van terrorisme en gewelddadig activisme. De door het kabinet in november 2004 aangekondigde tientallen extra politiemensen voor terrorismebestrijding binnen het KLPD zijn onder meer naar deze eenheid gegaan.*

[14] Een bot is een programma dat zelfstandig geautomatiseerd werk kan uitvoeren (NHTCC, 2005). Een botnet 'refer to a collection of compromised machines running programs, usually referred to as worms, Trojan horses, or backdoors, under a common command and control

- **Legale communicatie voor illegale doeleinden.** Bellen via internet, mailen en chatten maar ook het doen van financiële transacties valt onder regulier gebruik, of dat nu door een crimineel of een niet-crimineel plaatsvindt. Kenmerkend is dat het gebruik van het netwerk op zich zichzelf genomen niet illegaal is, ook al gaat het voor het uitvoeren of bespreken van duistere zaken. (Ontwerp Nationale Infrastructuur Bestrijding Cybercrime, 2006).

Er zijn misdaden die gepleegd worden met ICT als doelwit en misdaden die worden gepleegd met behulp van ICT, zoals blijkt uit de volgende opsomming van het NHTCC:

Misdaden met ICT als doelwit:

1) Aanvallen op computer- of informatiesystemen (denial of service-aanvallen) of op vitale informatie-infrastructuren van logistieke knooppunten. Deze aanvallen kunnen leiden tot uitschakeling van de voorzieningen die gebruik maken van de computer- of informatiesystemen;
2) Inbraak in computer- of informatiesystemen of in computerprogramma's (hacking/cracking);
3) Vernieling/wijziging/verwijdering van informatie in computersystemen (virussen en Trojans) of informatie op internet (defacing).

Misdaden verricht met behulp van ICT:

4) Terrorisme - voorbeelden: *online* verdachte financiële transacties, propaganda, rekrutering, communicatie, bedreigingen, *online* beschikbaar zijn van gevoelige of vertrouwelijke informatie; eventueel bruikbaar voor terreuractiviteiten;
5) Spionageactiviteiten – gegevens van computergebruikers onderscheppen met behulp van ogenschijnlijk onschuldige softwareapplicaties (*spyware*) waarmee men de gebruiker ongemerkt kan afluisteren of bespioneren;
6) Fraude op internetwinkels, veiling- of verkoopsites;
7) Fraude met internetwinkels, veiling- of verkoopsites;
8) Fraude met internetbetalingen (bancaire transacties, '*phishing*');
9) Fraude met inbelnummers (0900-fraude, *autodailers*);
10) Handelen met voorkennis door afspraken te maken met gebruik van besloten *online chatsites*, discussieruimten.
11) Gebruik van (*online*) discussieruimten voor criminele activiteiten/communicatie door criminele organisaties;
12) Verzoeken tot het verrichten van dubieuze investeringen of betalingen (*advance fee fraud, Nigerian scams, lottery scams*);
13) Merkvervalsing op het internet, software piraterij; kopiëren en illegaal uitwisselen en verkopen van films, muziek etc.;

infrastructure. A botnet's originator ('bot herder') can control the group remotely' (Wikipedia.com).

14) Bedreiging, chantage, afpersing en *stalking* via het internet of met behulp van GPS-systemen;
15) Drugshandel op of via het internet (*online*-verkooppunten);
16) Illegale handel in geneesmiddelen op of via het Internet;
17) Illegale kansspelen op het Internet;
18) Kinderpornografische afbeeldingen op het Internet of het lokken van kinderen via chatsites (*grooming*);
19) Racisme, discriminatie, smaad en laster op of via het internet;
20) Diefstal en misbruik van (*online*) persoonsgegevens of profielen;
21) Illegaal kopiëren van betaalpassen, toegangspassen of online-betaalkaartgegevens (*skimming*). *Bron: NHTCC*

De samenhang tussen de technische complexiteit, het internationale karakter, de snelheid, de diversiteit en de veelvuldigheid van sommige vormen van high tech-criminaliteit stelt de aanpak van cybercrime door de politie voor grote problemen. Een voorbeeld:

> *'In een zaak die wij onderzocht hebben, heeft een persoon een virus gemaakt voor criminelen in het Oostblok. Dit is een stukje code met als doel over de gehele wereld van mensen financiële gegevens te downloaden. Veel computers zijn geïnfecteerd. Zij vormen dan een botnet, een netwerk van geïnfecteerde computers. Dit botnet geeft een commando om zodra iemand bijvoorbeeld www. postbank.nl intikt, alle toetsaanslagen op te slaan en die toetsaanslagen naar een gehackte computer te sturen die deze persoon in zijn macht heeft. Zo verzamelt zo een botnet van duizenden geïnfecteerde pc's waardevolle informatie. Als politie moet je bewijzen dat iemand een virus heeft geschreven, met als doel bankgegevens te verzamelen (het functioneren dus uit te leggen). Dat gaat ver. Je moet aantonen dat iemand het commando voert over zo een botnet. Het zijn allemaal codes met enen en nullen. Ook nog eens verspreid over computers over de gehele wereld. Dit is globaal het proces. Dit is anders dan traditioneel onderzoek' (Bron: interview).*

Een actueel aandachtspunt is de bestrijding van terrorisme, met name de dreiging van een mogelijk elektronische aanval of digitale dreiging van terroristen. Terroristen kunnen in principe het Internet, luchtverkeersleidingen en energiebedrijven platleggen. Dit onderwerp is erg actueel in het project Nationale Veiligheid van het ministerie van BZK. Uit het buitenland zijn voorbeelden. Enkele jaren terug verschafte een hacker in Australië zich toegang tot het waterleiding systeem en het rioleringssysteem. Hij heeft de kleppen opengezet waardoor vervuild water bij het drinkwater kwam. In Amerika heeft iemand zich toegang verschaft tot een energiecentrale. In Nederland zou zoiets zich ook kunnen voordoen. Ook in Nederland gebruiken wij SCADA[15], geautomatiseerde systemen waarmee industriële processen, zoals chemische processen of energiecentrales bestuurd worden. Het is een veel gebruikte technologie in de meet- en regeltechniek. Indien deze systemen met internet verbonden worden, zouden er kwetsbaarheden kunnen ontstaan waarmee

[15] *SCADA is een afkorting voor: "Supervisory Control And Data Acquisition", het verzamelen en doorsturen van meet- en regelsignalen op verschillende machines in grote industriële systemen.*

dergelijke systemen misbruikt kunnen worden. Echte incidenten hebben zich nog niet voorgedaan.

Terrorisme op Internet manifesteert zich nu nog in het zaaien van haat en het rekruteren van terroristen[16]. Maar dreigingen worden nu in beeld gebracht, als onderdeel van een strategie tegen terroristische aanslagen. Voorkomen is cruciaal.

> *'Er is nog geen terroristische aanval geweest. Maar stel, je pleegt een bomaanslag in Amsterdam en tegelijkertijd leg je via digitale weg het noodnet plat. Dan heb je een dubbel effect.' (Bron: interview)*

Tegenwoordig heeft de politie in totaal 200 digitale experts in dienst; van taakaccenthouders tot specialisten bij het Nederlands Forensisch Instituut en de KLPD die zich met cybercrime bezighouden. Cybercrime-fighters hebben naar eigen zeggen voldoende zicht op de aard van dreigingen op het Internet, maar niet in termen van omvang en frequenties. Er bestaat ook weinig systematisch inzicht in daders en kenmerken van daders; wie zitten er achter de botnets, wat is hun levensloop? Meer inzicht op dit gebied kan impliceren dat de politie minder incidentgericht hoeft te werken en meer aandacht kan geven aan preventie. Tegelijkertijd is het aanpakken van daders alleen ook niet in alle gevallen effectief. De strategie van 'tegenhouden' kan een passend onderdeel zijn van de bestrijding van cybercrime en politiewerk in een virtuele omgeving.

> *'Een aantal jaren terug werd de site van de overheid, aangevallen door een ddos-aanval. Het netwerk werd platgelegd zodat de digitale loketten niet meer werkten. Deze bleken kwetsbaar. Een van de daders werd opgepakt. Hij maakte gebruik van een botnet en zegt dat hij, voordat hij de gevangenis inging voor een paar dagen, er 10.000 in had zitten. Als hij terugkomt uit de gevangenis zegt hij, het botnet is gegroeid. Ik heb er nu 20.000Gedurende de tijd dat de dader in de gevangenis zat, groeide het door gebruikte botnet significant. Dat is bijna autonome groei. Dus al pak je de crimineel op, de criminele feiten in de informatiestroom kunnen gewoon doorgang vinden. In andere zaken zijn de botnets ontmanteld. Je moet criminaliteit stoppen. Dat is onze verplichting. Je moet dus niet alleen op de opsporing zitten, maar ook andere manieren proberen strafbare activiteiten te stoppen.' (bron: interview)*

Andere methodieken die de politie bijvorbeeld kan gebruiken in de bestrijding van terrorisme, zijn het monitoren van allerlei communities op het Internet en undercover meedoen in chatkanalen. Dit is de intelligence-kant van het politiewerk, waarmee de informatiepositie kan worden verbeterd.
De politie heeft als ambitie om ook in virtuele omgevingen meer pro-actief te werken. Dit streven stuit op het probleem dat ontwikkelingen in de ICT en op het Internet dermate snel gaan dat cybercrime fighters niet aan de voorkant van het probleem komen. Het ene verschijnsel is nog niet geanalyseerd of het andere doemt weer op.

[16] *Jihadisten en het Internet.* Nationaal Coördinator terrorismebestrijding, Den Haag, 2006

Criminelen proberen voortdurend gebruik te maken van beveiligingsgaten of juridische mazen; wat ook steeds opnieuw lukt. Daar moet de markt weer op reageren, wat weer een nieuwe uitdaging voor de criminelen met zich meebrengt. Daarmee is de wedloop een feit (Nationale infrastructuur).

	CYBERCRIME
TYPE STROOM	informatie en communicatie
INTERVENTIE	Toegang controleren en meebewegen
OMVANG	(stille) selectieve controle
EFFECT	ongehinderde doorstroom
INTENSITEIT	Continue monitoring
GEOGRAFISCH	virtueel (overal)
MANIFESTATIE	onzichtbaar
RISICO SELECTIE	bepaald door kracht rechercheren, observatie en technologie - monitoring van gedragingen - Verzamelde individuele- en groepsinformatie (databases) - Human Factor
REFERENTIE	personen/IP-nummer

Tabel 3.7: kenmerken casus Cybercrime

3.7.3 Kritische factoren

Uit de evaluatie van het project NHTCC kwam naar voren dat een succesvolle aanpak van cybercrime valt of staat met:

- Snelle uitwisseling van relevante informatie tussen politie en het bedrijfsleven over internetdiensten, logging en registratiegegevens, gebruiks- en verbruiksgegevens en gebruikte software en hardware etc.
- Snel te starten samenwerking met andere overheidsinstanties door het uitwisselen van inlichtingen en informatie over verdachte(n), activiteiten, doelwit en de mogelijke consequenties van het handelen van de verdachte(n)
- 'Grensoverschrijdend' informatie uitwisselen
- Delen van de geleerde lessen met alle betrokkenen/belanghebbenden,ter voorkoming van toekomstige incidenten
- Integrale aanpak. Voor die integrale aanpak is het vanzelfsprekend dat nauw wordt samengewerkt met diverse partijen van zowel de publieke als private sector, inclusief opsporing. (Nationale Infrastructuur)

Informatiemanagement

Een succesfactor is informatiemanagement, het vergaren, analyseren, bewerken en vervolgens delen van informatie uit verschillende bronnen met uiteenlopende informatieregimes.

Samenwerking met zusterorganisaties

Om effectief te kunnen werken is de politie afhankelijk van andere partijen. Binnen de politie zijn Interpol en Europol belangrijke partijen. Internationale rechtshulp en de formele informatie-uitwisseling zijn belangrijk omdat soms veel naspeuringen in het buitenland gedaan moeten worden om een higtech crime zaak tot een goed einde te brengen. Er zijn officiële kanalen voor informatie-uitwisseling, zoals Interpol, Europol of Schengen. Naast operationele informatie-uitwisseling gaat het ook om het uitwisselen van kennis en expertise, ervaringen en best practices. Kennis veroudert snel. Deze moet frequent op peil worden gehouden. Immers, *'tools cannot replace fools'*. Daarnaast zijn samenwerking met zusterorganisaties in het buitenland van belang (Nationale Infrastructuur).
Daarnaast zijn er ook in andere landen hightech crime units. Dit soort criminaliteit is per definitie internationaal. Dat maakt internationale samenwerking en informatie-uitwisseling met zusterorganisaties onontkoombaar. Ook deelname aan internationale taskforces en het bevorderen van joint investigation teams zijn belangrijke succesfactoren.

Ketensamenwerking

Maar de noodzaak tot samenwerking strekt verder. Het NHTCC noemt de aanpak van cybercrime een ketenproces met als stappen: pro-actie, preventie, preparatie, signalering, opvolging, terugkoppeling, resultaat en evaluatie. Bestrijding van cybercrime wordt niet gezien als alleen een zaak voor de politie' maar vergt een multi-agency aanpak. Immers, de politie is sterk afhankelijk van anderen, juist voor het ontwikkelen van een proactieve aanpak. Belangrijk zijn partnerships met Internet providers, hosting providers en andere organisaties die een deel bezitten van de infrastructuur van computers. Anderen hebben informatie die voor de politie van belang is. In de aanpak van computercriminaliteit spelen de computer emergency response teams een rol. Daar komt informatie binnen. Samenwerking en informatie-uitwisseling moeten echter georganiseerd worden. Een goede informatiepositie veronderstelt formele en informele samenwerking. In deze tak van sport is snel reageren op informatie cruciaal. Je moet weten waar de informatie te halen. Het hebben van contacten met securityafdelingen van bedrijven en govcert communities is belangrijk om snel stappen te kunnen zetten.

Publiekprivate samenwerking

Naast deze emergency response teams zijn ook private partijen van belang, met verschillende rollen en informatieposities, die actief zijn of kunnen worden in verschillende stappen van het bestrijdingproces. Voorbeelden zijn private partijen die 'slachtoffer' zijn van hightech crime, bijvoorbeeld als leverancier van de informatie-infrastructuur of softwareontwikkelaar. Partijen zoals internet providers, de antivirus-industrie of grote technologische bedrijven beschikken ook over belangrijke kennis met betrekking tot het strafbare feit, de gebruikte methodes of zelfs met betrekking tot de dader(s). Private partijen kunnen ook over veel kennis, ervaring en informatie over

ICT beschikken omdat zij bijvoorbeeld of eigenaar, beheerder of gebruiker zijn van een vitale structuur die van belang is voor de vergroting van de weerbaarheid van de samenleving (bancaire sector, luchthaven Schiphol). Waar het gaat om vitale informatie-infrastructuur is publiekprivate samenwerking nodig. Veel grote bedrijven en providers hebben eigen teams met informatie over wat misgaat op het Internet. Ook de antivirus industrie is een belangrijke partij, de AVI-industrie, zoals Microsoft en andere grote firma's. De politie staat nog aan het begin met het opbouwen van deze netwerken. Er is veel samenwerking, maar veelal informeel en nog niet echt geïnstitutionaliseerd (bron: interview). Steeds meer blijkt dat contacten met de (internet-)industrie waardevol zijn bij het speuren naar internationaal opererende cybercriminelen.
Verdergaande samenwerking met sleutel partners, de cert-communities en de bedrijven die zich bezighouden met Internet technologie en de antivirusindustrie kunnen eveneens als kritische factoren worden beschouwd.

3.8 De nodale oriëntatie in de praktijk: een vergelijking

In dit hoofdstuk hebben we een aantal nodale praktijken beschreven op grond van een quick scan van de inhoud en vormgeving van deze praktijk, de bereikte resultaten en belangrijkste kritische factoren. Op grond van het beperkte aantal praktijken die ook nog eens verdeeld zijn over verschillende soorten van stromen/infrastructuren en knooppunten en het beperkte karakter van beschrijvingen en analyses, hebben we niet de pretentie om algemene uitspraken te doen over de condities waaronder de nodale oriëntatie van de politie gestalte kan krijgen. Vandaar dat deze case-vergelijking een indicatief karakter heeft en met name gelezen moet worden als een agenda voor verdere uitwerking. We zetten de belangrijkste bevindingen op een rijtje teneinde inzicht te krijgen in de meerwaarde van de nodale oriëntatie.

Bevindingen ten aanzien van de aard van de nodale oriëntatie

In de zes door ons bestudeerde praktijken zien we een opsporingspraktijk die doelbewust gericht is op het ontanonimiseren van het gedrag dat zich beweegt binnen bepaalde stromen en binnen bepaalde knooppunten. In iedere casus is duidelijk een nodale oriëntatie aanwezig, waarbij de aanknopingspunten overigens variëren. In sommige gevallen gaat het om het zichtbaar maken van de stroom door controles in te stellen op de toegang en uitgang van de stroom, met name daar waar stromen bij elkaar komen in een bepaald knooppunt (bijvoorbeeld Schiphol, Rotterdam, creditcard fraude, operatie 'ochtendgloren', dan wel door mee te bewegen met de betreffende stroom (mobiele catch-ken, internet criminaliteit).
Kenmerkend voor al deze opsporingspraktijken is het opbouwen van een strategische informatiepositie (gericht op het verzamelen van 'intelligence'), waarbij het succes van de opsporing wordt bepaald door de unieke identificatie van de status van een persoon of voertuig (bijv. op grond van de kentekenregistratie of het paspoort) in combinatie

met data die in andere databestanden voorhanden zit; bestanden die of bij de politie, bij andere opsporingsdiensten of private organisaties is op geslagen en die kan worden ontsloten. Het opbouwen van deze strategische informatiepositie is vooral gericht op het kunnen maken van verantwoorde risico-analyses, hetgeen impliceert dat risico-definitie en risicoselectie en risico-interpretatie nauw verbonden is met de nodale oriëntatie. Op grond van deze risico-analyses worden interventiescenario's worden ontwikkeld. Heel duidelijk komt dit naar voren in het geval van de ANPR scan, hooligans in beeld, de Rotterdamse haven en de fraude met creditcards.
In sommige gevallen gaat het om praktijken waarin politiediensten het voortouw hebben (in het geval van de controle op de verkeersstroom, de aanpak van hooligans en het internetverkeer); in andere gevallen heeft een andere opsporingsdienst het voortouw en schuift de politie zonodig aan (bijvoorbeeld in het geval van de Rotterdamse haven); in weer andere gevallen zijn het private partijen die een nodale opsporingspraktijk hebben ontwikkeld (bijvoorbeeld in het geval van Schiphol en in het geval van Equens Nederland en de banken).
Ook zien we dat in alle gevallen een effectieve nodale oriëntatie stoelt op samenwerking met andere publieke en private partijen; tegelijkertijd laten deze praktijken zien dat deze samenwerking ook een internationaal karakter heeft, omdat - door de toegenomen globalisering van het economische en maatschappelijke verkeer - stromen per definitie een internationaal c.q. grensoverschrijdend karakter hebben. We zien dit bijvoorbeeld terug in de participatie van de Duitse politie in de operaties ochtendgloren op de Nederlandse snelwegen, de haven van Rotterdam en de luchthaven van Schiphol. Het is met name de kwaliteit van deze samenwerking die het succes bepaalt van de nodale oriëntatie in de praktijkvoorbeelden. Het belang hiervan wordt ook nog eens gedemonstreerd in de cybercrime case. Het internet is immers per definitie een wereldwijd netwerk met lokale knooppunten maar met internationale stromen.
Overigens zien we dat, ondanks het feit dat op heden systematisch onderzoek naar de relatie tussen een nodale opsporingspraktijk en de daarin ingezette instrumenten nog ontbreekt, er voldoende indicaties zijn voor het succes van dergelijke aanpakken (bijvoorbeeld het aantal 'hits' en de daling van criminaliteitscijfers).

Bevindingen ten aanzien van de meerwaarde van de nodale oriëntatie
De beschreven praktijkvoorbeelden laten duidelijk zien dat er sprake is van een meerwaarde van de nodale oriëntatie. Deze meerwaarde wordt bepaald door de volgende overwegingen:

- een erkenning door bepaalde publieke en private opsporingsorganisaties van het feit dat de criminele en terroristische organisaties optimaal gebruik maken van de knooppunten en de (internationale) stromen in de netwerksamenleving, alsmede van de anonimiteit van de netwerksamenleving. Dit impliceert dat de politie en andere organisaties dus ook deze stap zullen moeten maken;
- sommige centrale knooppunten in de Nederlandse samenleving (Rotterdamse haven, Schiphol) een strategisch groeiperspectief hebben ontwikkeld dat gebaseerd is op de (internationale) functie van deze knooppunten en de daarin

bij elkaar komende stromen en waarin veiligheid een belangrijk aandachtspunt is;

- door het kiezen van knooppunten, infrastructuren en stromen als belangrijk referentiekader voor het ontwikkelen van een strategisch opsporingsbeleid, worden bestaande misdadige praktijken in een ander perspectief gezet (re-framing) waardoor nieuwe mogelijkheden voor opsporing worden gezien (Schiphol, Rotterdam, operatie ochtendgloren, hooligans); worden zich nieuw ontwikkelende criminele praktijken (bijvoorbeeld internet criminaliteit, creditcard fraude) eerder en beter zichtbaar (framing). Dit alles impliceert soms een breuk met de bestaande vooral individuele delicten gerichte opsporingspraktijk, hetgeen ook weer ruimte biedt voor innovatie en de zoektocht naar innovatieve technologieën (Schiphol, Rotterdamse haven, catch-ken, ochtendgloren);
- criminaliteit in en rondom knooppunten en stromen wordt in samenhang gezien met andere activiteiten, die plaats vinden binnen en rondom deze knooppunten en stromen. Hierdoor wordt de noodzaak en het nut van integrale handhaving eerder zichtbaar, hetgeen de effectiviteit van de opsporing kan versterken. Bovendien biedt dit meer mogelijkheden om van elkaars bevoegdheden gebruik te maken;
- de eerste resultaten spreken in veel gevallen tot de verbeelding en hebben geleid tot het formuleren van verregaande ambities ten aanzien van de uitwerking van de nodale oriëntatie.

Dit alles betekent dat de nodale oriëntatie als strategisch uitgangspunt een bestaande praktijk is, die zowel binnen als buiten de politie vooral in projecten handen en voeten heeft gekregen; een praktijk die gelet op de ambities die we in de beschrijvingen hebben aangetroffen alleen nog maar verder ontwikkeld zal worden. Dit betekent voor de politie dat een verdere uitwerking van het concept zonder meer vruchtbaar is. We komen hierop in de volgende paragraaf terug. De meerwaarde van het concept wordt echter ook duidelijk door nadrukkelijk een aantal technologische en andere randvoorwaarden voor het voetlicht te brengen.

Bevindingen ten aanzien van de rol van technologie

Technologie speelt een belangrijke rol in de ontwikkeling van de nodale opsporingspraktijken zoals wij die hebben aangetroffen. In alle praktijken, tot op zekere hoogte met uitzondering van de case 'hooligans in beeld', wordt getracht door de inzet van technologie een strategische informatiepositie op te bouwen. Interessant is te bezien hoe de verhouding tussen de inzet van technologie en de nodale oriëntatie in de praktijkvoorbeelden precies in elkaar zit. Volgt de technologie het strategisch concept? Of, volgt het strategisch concept de strategie? In de door ons bestudeerde cases zien we beide terug.

In het geval van Schiphol en Rotterdam zien we dat de opsporingsdiensten ter plekke een strategisch concept hebben ontwikkeld waarin het inzichtelijk maken van bewegingen binnen de goederen en passagiersstroom en het interveniëren hierin, indien er verdachte bewegingen zijn; een concept dat tevens past in een bredere visie

op het functioneren en de toekomst van deze knooppunten als zeehaven en als luchthaven. In het geval van de catch-ken in de Hoekse waard maar ook de mobiele scans van de KLPD zien we dat het nog vooral gaat om technologisch gedreven projecten, waarvan de strategische betekenis wel zichtbaar wordt maar nog tamelijk op zichzelf staat. In het geval van de cybercrime case moet we zelfs stellen dat in een dergelijke technologische omgeving technologie het enige instrument is, dat effectief kan worden ingezet om deze vorm van criminaliteit op te sporen. Criminaliteit die bijvoorbeeld gebruik maakt van het internet, kan alleen maar door gebruik te maken van datzelfde netwerk worden opgespoord. De in te zetten technologie is zowel strategie als instrument.

De functie die technologie vervult ligt vooral op het terrein van identificatie en authenticatie, waarbij het primair gaat om het vaststellen van de status van iets of iemand. Verder zien we dat de rol van technologie zich uitstrekt tot het kunnen koppelen van databestanden, ook al bevinden die zich binnen andere organisaties, alsmede het kunnen maken van dwarsdoorsneden en profielen binnen een database of door de combinatie van databases. Daardoor vervult technologie een belangrijke rol in het vergroten van toegankelijkheid van informatie en het creëren van transparantie, ten einde controle mogelijk te maken. Dit alles met het oog op het opbouwen van een strategische informatiepositie.
Overigens constateren we ook dat het vermogen van technologie om verbindingen te leggen tussen organisatiegrensoverschrijdende databases en het vermogen om steeds geavanceerde dwarsverbanden te creëren, leidt tot een eigen dynamiek. In alle cases zien we de ambities om nog meer informatie en bestanden te betrekken teneinde een meer en verfijnd, maar ook pro-actief beeld te krijgen van de bewegingen die zich binnen bepaalde stromen en knooppunten afspelen.

Bevindingen ten aanzien van relevante kritische factoren en condities

In alle cases zien we dat de volgende kritische factoren naar voren worden gebracht ter verklaring van het succes van de betreffende nodale opsporingspraktijken. In onderstaande tabel hebben we deze factoren nog een keer samengevat.

	KRITISCHE FACTOREN							
TYPE STROOM	**JURIDISCH**	**ECONOMISCH**	**POLITIEK/BESTUURLIJK**	**TECHNOLOGIE**	**SAMENWERKING**	**COMPETENTIES**	**INFORMATIEPOSITIE**	**TOEKOMST/AMBITIE**
VERKEER (KLPD EN ANPR)	Bestaande bevoegdheden worden gebruikt. In bepaalde gevallen bijzondere ontheffing.	Technologie is relatief goedkoop Mankracht: hoge kosten	Resultaten werken twee kanten op: resultaat van het initiatief leidt tot steun. Vermindering van criminaliteit (resultaat) kan daarna leiden tot afnemend draagvlak voor maatregelen (noodzaak wordt minder)	Cruciaal (en deels autonoom) bij ANPR Ondersteunend bij controles/ werkzaamheden opsporings-ambtenaren (KLPD)	Cruciaal voor zuiverheid database en bepalen van hits/follow-up(ANPR) Integraliteit door samenwerking is de doorslaggevende factor (KLPD)	Naar Informatie analyse/kunde Verbetering samenwerking (KLPD)	Efficiënt door pro-actief profiel (ANPR) Registratie van soft-info (KLPD) en meta informatie (kengetallen)	Koppeling databases ANPR landelijk/uploaden KLPD: nog meer diensten betrekken, nieuwe technologieën tbv. Werkproces optimalisatie
GOEDEREN (DOUANE)	Beperkt wettelijke kader voor uitwisselen van informatie (‘checks and balances’)	Technologie is niet duur. Controles kosten capaciteit, mankracht is relatief schaars	Afstemming met andere opsporingsdiensten in Expertisecentrum haven onder bevoegdheid OM	Cruciaal (kwaliteit risicoanalyses koppeling informatiesystemen van anderen)	Cruciaal, met andere opsporingsinstanties en partnerships met ‘compliant’ bedrijven	Naar meer samenwerking en informatieuit-wisseling	Profiling mbv PRISMA (op basis van gecumuleerde ervaringskennis)	Gezamenlijke risicoanalyses, uitbouw intelligence, inzet nieuwe technologie (o.a. container security devices en controlestraat Maasvlakte)
PERSONEN (HOOLIGANS)	Bestaande bevoegdheden	Opbrengsten staan in verhouding tot kosten mankracht	Steun van burgemeester: openbare orde aangelegenheid met daarbij behorende bevoegdheden	Ondersteunend bij observatie, registratie (clubcard) en handhaving sancties (stadionverbod)	Belangrijk oa. in follow-up (justitie) En informatie verzameling woonomgeving (wijkagent)	Andere wijze van observeren (van delictgericht, naar sof-info)	Contextanalyse brede informatie-verzameling/ soft-info informatiedeling	Samenwerking organisaties, database taps Aangepaste/andere bevoegdheden tav. ‘tegenhouden’
FINANCIËN (EQUENS NEDERLAND)	Gegevens worden vastgelegd op niveau van kaart. Koppeling aan personen geprotocolleerd	kosten van detectie tech-nologie en arbeidskracht zijn tot 3x lager dan de mogelijke schade		Cruciaal is risicoselectie (en deels autonoom)	goed regelen van follow up bij fraude aansluiting politie en justitie	specialist in authenticatie, identificatie, afwijkingen en patroonherkenning	Continue aanpassen van detectieregels systematische (historische) opbouw kennispositie	Artificial Intelligence, datamining wet- en regelgeving “ken uw klant” West financiële dienstverlening en MOT regelgeving
SCHIPHOL (SAFETY&SECURTY)	Bevoegdheden mbt delen van informatie tussen publiek en private partijen	Hoge kosten voor innovatie voor veiligheid en wie hiervoor opdraait	Korte lijnen met “’Den Haag”via deelname NCTB in platform	‘Smart technology’ cruciaal op meerdere infrastructurele knooppunten	Publiekprivate samenwerking		Gezamenlijke meldkamer creëert betere informatiepositie	Automated borders (idee van fully automated airport)
DIGITALE RECHERCHE	Privacy op het Internet	Veel onzichtbare (slachtofferloze) schade van cybercriminaliteit		Cruciaal	Cruciaal, samenwerking met zusterorganisaties en internet-industrie	Naar meer samenwerking en profiling		Profilering proactieve aanpak cybercrime (‘tegenhouden’)

Tabel 3.8: overzicht kritische factoren naar casus

We willen op grond van dit overzicht meer in het bijzonder nog aandacht schenken aan de volgende factoren:

Samenwerking

Ten eerste betekent een nodale oriëntatie per definitie dat nauw moet worden samengewerkt met andere politiekorpsen, andere publieke opsporingsdiensten maar ook met allerlei private partijen. Samenwerking is per definitie niet een gegeven maar moet worden verdiend. In de cases zien we dat er verschillende motieven zijn voor samenwerking, te weten:

- onderkenning wederzijdse afhankelijkheid bijvoorbeeld omdat alle betrokken partijen binnen een bepaald knooppunt (luchthaven Schiphol, haven van Rotterdam, het voetbalstadion) of binnen en rondom een stroom die zich binnen een bepaald gebied beweegt (bijv. verkeersstromen of the creditcardbetalingsverkeer door de banken en Equens Nederland) een gemeenschappelijke problematiek delen (zoals aanpak criminaliteit rondom snelwegen, veiligheid van en op de luchthaven, opsporen van risicovolle ladingen in de zeehaven, overlast door hooligans, opsporen van creditcardfraude) en daardoor een gedeeld belang hebben;
- vertrouwen wordt gezien als smeerolie waardoor men elkaar eerder en beter weet te vinden, hetgeen een proces van samenwerking kan entameren of verbeteren;
- een min of meer evenredige verdeling van kosten en baten. Zeker in samenwerkingsprocessen is het belangrijk dat niet een partij alle investeringen voor zijn rekening moet nemen c.q. kosten moet maken terwijl andere partijen alleen maar kunnen profiteren van de opbrengsten c.q. baten van met name de technologische maatregelen die zijn genomen. Kosten en baten moeten tot op zekere hoogte in evenwicht zijn, dan wel moeten onevenredig grote investeringen of hoge kosten worden gecompenseerd. Het belang hiervan werd met name duidelijk in de Schiphol cases, waarbij de overheid een deel van de kosten van de beveiligingsmaatregelen voor zijn rekening heeft genomen.

Deze samenwerking is ook nodig omdat men vervolgens door de complementariteit van (strafrechtelijke en bestuursrechtelijke) bevoegdheden effectiever kan optreden; een idee dat ook terugkomt in de notie van 'tegenhouden'.
Tegelijkertijd heeft deze samenwerking niet alleen gevolgen voor de effectiviteit van de preventie (het op voorhand kunnen delen en combineren van gegevens uit verschillende bronnen bij verschillende organisaties teneinde risico-profielen te kunnen opstellen) maar ook voor de effectiviteit van de follow-up, namelijk de daadwerkelijke interventie die plaatsvindt.

Kwaliteit informatie

Ten tweede zien we dat we dat technologie belangrijk is, maar dat geavanceerde technologische toepassingen hun betekenis verliezen, indien geen betrouwbare en

geldige informatie voorhanden is en indien de verbindingen die nodig zijn om informatie uit te wisselen en databases te koppelen (in termen van een betrouwbare infrastructuur), gebrekkig zijn. De centrale rol die 'intelligence' speelt binnen de betreffende nodale opsporingspraktijken onderstreept dit.
Overigens moet hierbij worden aangetekend dat de eisen ten aanzien van de kwaliteit van informatie niet alleen betrekking hebben op de kwaliteit van formele en vaak kwantitatieve data die is opgeslagen in allerlei bestanden en registers, maar ook om de afweging tussen formele data en informele data, waarin ervaring, intuïtie en andere zachte informatie nog steeds een belangrijke rol speelt. We zien dit terug bij de opsporingsactiviteiten van de douane binnen de Rotterdamse haven, in de aanpak van overlast door hooligans, in de aanpak van creditcardfraude maar ook binnen de operaties ochtendgloren .

Cultuur
Ten derde zien we in alle cases dat een nodale oriëntatie betekent dat een andere opsporingsstijl moet worden ontwikkeld die ook leidt tot andere werkwijzen, routines en procedures. Het accent verschuift van een delictgerichte opsporing naar een pro-actieve opsporing waarbinnen op grond van de verzameling en interpretatie van informatie – afkomstig vanuit verschillende bronnen – op zoek wordt gegaan naar specifieke verbanden die als risicovol kunnen worden aangemerkt. Daarmee komen we op een vierde vitale factor.

Risicodefinitie
Ten vierde is de kwaliteit van risicodefinitie, analyse en evaluatie een punt van aandacht, gelet op het belang dat wordt toegekend aan risico-profielen. Hieraan zit een statistisch aspect en een human resource aspect. Ten aanzien van het statistische aspect gaat het om de betrouwbaarheid van de informatie waarop statistische profielen zijn gebaseerd; zeker indien deze profielen steeds verder verfijnd worden met behulp van nieuwe informatie en reeds opgebouwde ervaringen. Ten tweede vereist het specifieke kennis en vaardigheden die verder reiken dan statistische kennis en vaardigheden. Het gaat vooral om kennis en vaardigheden om bepaalde patronen te zien, te herkennen maar deze ook te relativeren (een statistisch verband hoeft nog een feitelijk verband te zijn). Ook is het van belang om deze patronen te kunnen interpreteren door oog te hebben voor de specifieke context waarbinnen een patroon al dan niet optreedt. Verder vraagt het werken met dergelijke profielen om vakinhoudelijke kennis van het reilen en zeilen binnen een stroom of binnen een knooppunt. In bijna alle cases werd het belang hiervan onderstreept.

Privacy
Ten vijfde zien we in alle voorbeelden het privacy-vraagstuk terug. Van de ene kant stelt de bescherming van de persoonlijke levenssfeer noodzakelijkerwijs normatieve grenzen aan datgene wat mogelijk is. Van de andere kant zien we dat de mogelijkheden die er zijn ook benut worden (ook al is er technologisch nog meer mogelijk), indien aannemelijk wordt gemaakt dat ertussen mogelijke schending van de

persoonlijke levenssfeer en het gericht kunnen opsporen van crimineel gedrag een causale relatie bestaat, die bovendien proportioneel is. Om deze balans goed te kunnen maken is het belangrijk om het College Bescherming Persoonsgegevens hierin actief te betrekken.

De rol van de politie

Ten zesde zien we dat de rol van de politie in deze praktijken varieert. In sommige gevallen is ze de regisseur van een zich verder ontwikkelde nodale opsporingspraktijk (bijvoorbeeld op het terrein van cybercrime); in een aantal gevallen speelt zij slechts een bescheiden rol en ligt de regie en het initiatief bij andere opsporingsdiensten of zelfs bij bepaalde private partijen. Interessant is echter dat juist in de twee knooppunten die we onderzocht hebben (Schiphol en Rotterdam) de politie of de organisatie die politietaken uitvoert (in het geval van Schiphol de Marechaussee), nog niet een natuurlijke plek heeft weten te vinden binnen de samenwerking die daar thans plaats vindt. Deels heeft dat iets te maken met verschil in bevoegdheden (delictoriëntatie), deels heeft dat ook iets te maken met de cultuur van de politie (of de Marechaussee).

4 BOUWSTENEN VOOR DE NODALE ORIËNTATIE: SAMENVATTING, CONCLUSIES EN AANBEVELINGEN

4.1 Inleiding

In dit hoofdstuk willen we een aantal bouwstenen die zijn verzameld op grond van diverse sociologische, criminologische, technologische en politicologisch-juridische verkenningen bij elkaar brengen. Verkenningen, waarin we ons vooral gericht hebben op een verduidelijking van de aannames die achter het concept van de nodale oriëntatie verscholen zitten en verkenningen van praktijkvoorbeelden die een sterke gelijkenis vertonen met de nodale oriëntatie. Hiermee worden de contouren van een 'beleidstheorie' voor de nodale oriëntatie langzamerhand zichtbaar; een beleidstheorie die echter vooral moet worden gezien als een handelingsperspectief voor de politie met het oog op de verdere ontwikkeling van het concept. Dit hoofdstuk moet dan ook worden gezien als een zelfstandig leesbaar hoofdstuk.

Allereerst gaan we in op de herkenbaarheid van het concept en de meerwaarde van het concept, dat vooral gelegen ligt in het vermogen om bepaalde praktijken te 'framen' en 'reframen' (paragraaf 2). Vervolgens trachten we de nodale oriëntatie specifieker in te vullen, door aandacht te schenken aan de verschillende soorten van aangrijpingspunten van de nodale oriëntatie (namelijk de aanwezigheid van verschillende soorten van knooppunten, stromen en infrastructuren), de condities waaronder op grond van de nodale oriëntatie kan worden geïntervenieerd en de instrumenten die daarbij kunnen worden ingezet (paragraaf 3). De normatieve inbedding van het concept komt aan de orde in paragraaf 4. In paragraaf vijf geven we nog een aantal suggesties voor de verdere doorontwikkeling van het concept en in paragraaf zes geven we een aantal concrete aanbevelingen, die bij de doorontwikkeling in ogenschouw kunnen worden genomen.

4.2 Over de meerwaarde van de nodale oriëntatie

Conclusie

De conclusie die we trekken op grond van ons onderzoek is dat de nodale oriëntatie zonder meer een belangrijke meerwaarde heeft voor de politie. Deze conclusie is gebaseerd op de volgende overwegingen.

Noodzakelijke strategische aanpassing

De nodale oriëntatie geeft ten eerste uitdrukking aan het feit dat de politie zich bewust is van haar positie in de netwerksamenleving en de wijze waarop criminele organisaties gebruik maken van de netwerksamenleving, hetgeen ook gevolgen heeft voor de wijze waarop zij in die netwerksamenleving wil optreden. De nodale oriëntatie kan daarmee ook worden gezien als een concept waarin de politie probeert een 'strategic fit' te realiseren tussen haar taken en de veranderende omgeving waarin zij moet opereren; een 'strategic fit' die veel criminele en terroristische organisaties al enige tijd geleden hebben gemaakt. Hierdoor vindt een proces van noodzakelijke strategische aanpassing plaats, hetgeen per definitie essentieel is voor de effectiviteit en legitimiteit van de politie-organisatie. In dit aanpassingsproces vervult de nodale oriëntatie als '*sensitizing concept*' een belangrijke rol, omdat het een referentiekader biedt voor strategie-ontwikkeling.

Een zich vestigende praktijk

Ten tweede zien we dat het begrip nodale oriëntatie als strategisch concept weliswaar nieuw is, maar zijn er binnen de politie praktijken tot ontwikkeling gebracht c.q. projecten gestart die een sterke verwantschap vertonen met een nodale oriëntatie. Voorbeelden zijn de aanpak van hooligans rondom voetbalstadia of de aanpak van criminaliteit rond snelwegen, zoals plaatsvindt in de operaties ochtendgloren. Ook bestaan er werksoorten die zich nadrukkelijk richten op opsporing en handhaving binnen verschillende soorten van infrastructuren zoals de verkeerspolitie van de KLPD of vormen van digitaal rechercheren. Tegelijkertijd zien we ook dat andere opsporingsdiensten en zelfs private organisaties een nodale oriëntatie ontwikkelen in het licht van hun verantwoordelijkheid voor het reilen en zeilen van bepaalde knooppunten en stromen. We treffen dit aan in de wijze waarop de douane optreedt in de haven van Rotterdam, hoe de Schiphol Groep de veiligheid en beveiliging van de luchthaven ter hand neemt, maar ook in de manier waarop banken fraude met het betalingsverkeer trachten tegen te gaan.
Kortom, de conclusie is derhalve gerechtvaardigd dat de nodale oriëntatie een gevestigde en een zich verder ontwikkelende praktijk is – binnen en buiten de politie. Door te kiezen voor een nodale oriëntatie (zoals in 'Politie in Ontwikkeling' geschiedt) wordt de strategische betekenis van de praktijk onderkend. Een betekenis die vooral ligt in 'framing en reframing'.

Framing en reframing

De kracht van het concept van de nodale oriëntatie is ten derde dat het een strategisch perspectief biedt door bestaande praktijken en projecten te 'reframen' en nieuwe praktijken te 'framen'
Bestaande praktijken, die wellicht relatief geïsoleerd zijn ontstaan en waarin pioniers een belangrijke rol hebben gespeeld, kunnen nu worden onderbouwd vanuit een strategische visie. Een voorbeeld is de ANPR scan in de Hoekse Waard. Aanvankelijk gaat het hierbij om een belangrijke technologische innovatie, die vanuit een bepaalde

problematiek is ontwikkeld. Deze technologische toepassing krijgt echter een heel andere betekenis indien het potentieel ervan kan worden verbonden met bepaalde strategische concepten. Ook is het mogelijk om andere strategische concepten, zoals het concept tegenhouden, met het concept van de nodale oriëntatie te verbinden, waardoor synergie kan ontstaan, omdat beide concepten een aantal gemeenschappelijke uitgangspunten kent (zie par. 2.5.3).
Daarnaast biedt het concept ook de mogelijkheid tot 'framing'. Vanuit het concept nodale oriëntatie kan de politie derhalve meer systematisch nadenken over de wijze waarop zij haar strategische informatiepositie ten opzichte van bepaalde stromen en knooppunten kan opbouwen, wat de rol van risicoselectie daar in is en welke rol de politie voor zichzelf weggelegd ziet in de opsporing van criminele activiteiten in bepaalde knooppunten en binnen bepaalde stromen. Neemt de politie daarin het voortouw, blijft zij op de achtergrond of is zij de regisseur van de samenwerking binnen en rondom een bepaald knooppunt of een bepaalde stroom? Kortom, de nodale oriëntatie dwingt de politie eveneens nadrukkelijk na te denken over haar eigen kerntaken in relatie tot het functioneren van bepaalde knooppunten en stromen.

Criminologische ontwikkelingen

Het strategische belang van het concept wordt ten vierde onderstreept door te verwijzen naar een aantal criminologische ontwikkelingen. De nodale oriëntatie moet derhalve worden gezien als het strategische antwoord op deze ontwikkelingen. Deze ontwikkelingen vormen derhalve een belangrijke inhoudelijke legitimatie voor de (door-)ontwikkeling van een nodale oriëntatie door de politie. Een aantal conclusies zijn in dit verband (zei paragraaf 2.4 en 2.5).
Ten eerste weten met name de georganiseerde misdaad en terroristische organisaties optimaal gebruik te maken van de kansen die de netwerksamenleving en de rol die knooppunten en stromen daarin spelen bieden. Bovendien biedt de anonimiteit en het individualistische karakter van de netwerksamenleving, zeker in grootstedelijke gebieden, dit soort van organisaties de gewenste anonimiteit om bepaalde activiteiten te ontplooien.
Een andere conclusie is dat ook misdaad- en terroristische organisaties zich bewust zijn van de wijze waarop 'stromenland' functioneert, hetgeen een ander argument is ter ondersteuning van het belang van een nodale oriëntatie. Zo zorgen de toegenomen internationalisering van de criminaliteit, de taakspecialisatie tussen criminele organisaties en de daarmee samenhangende noodzaak van samenwerking alsmede de toegenomen mobiliteit van criminele organisaties ervoor dat er een intensief verkeer van personen en goederen ontstaat; informatie hiervoor wordt weer gedeeld doordat optimaal gebruik wordt gemaakt van moderne informatie- en communicatietechnologie. In hun strategisch gedrag is nodale oriëntatie een leidend beginsel.
Verder ontstaan er nieuwe vormen van criminaliteit zoals computercriminaliteit, die gebruik maakt van wereldwijde informatiestromen of die optimaal gebruik maakt van de vervlechting van stromen, bijvoorbeeld tussen kapitaal en informatiestromen. Bovendien blijkt dat het door deze technologie mogelijk is om de identiteiten steeds

beter te manipuleren, hetgeen gevolgen heeft voor het vaststellen van de identiteit of status van bepaalde van personen en hun betrokkenheid in allerlei personen, goederen, kapitaal en informatie- en communicatiestromen.
Een laatste conclusie verwijst naar de rol van knooppunt die Nederland vervult. De infrastructurele positie van Nederland als toegangspoort tot Europa, alsmede zijn rol als financiële dienstverlener, benadrukken eveneens het belang van een nodale oriëntatie.

Meerwaarde uit de praktijkvoorbeelden

Ook de beschreven praktijkvoorbeelden laten ten vijfde duidelijk zien dat de nodale oriëntatie duidelijk een meerwaarde heeft. Deze meerwaarde wordt bepaald door de volgende overwegingen:

- een erkenning door bepaalde publieke en private opsporingsorganisaties van het feit dat de criminele en terroristische organisaties optimaal gebruik maken van de knooppunten en de (internationale) stromen in de netwerksamenleving, alsmede van de anonimiteit van de netwerksamenleving. Heel duidelijk is dit in de Rotterdamse haven, de luchthaven Schiphol, internetcriminaliteit, creditcardfraude en de operaties 'ochtendgloren van het KLPD. Dit impliceert dat de politie en andere organisaties dus ook deze stap zullen moeten maken;
- sommige centrale knooppunten in de Nederlandse samenleving (Rotterdamse haven, Schiphol) hebben een strategisch groeiperspectief ontwikkeld, dat gebaseerd is op de (internationale) functie van deze knooppunten en de daarin bij elkaar komende stromen en waarin veiligheid een belangrijk aandachtspunt is;
- door het kiezen van knooppunten, infrastructuren en stromen als belangrijk referentiekader voor het ontwikkelen van een strategisch opsporingsbeleid, worden bestaande misdadige praktijken in een ander perspectief gezet (re-framing) waardoor nieuwe mogelijkheden voor opsporing worden gezien (Schiphol, Rotterdam, operatie ochtendgloren, hooligans); worden zich nieuw ontwikkelende criminele praktijken (bijvoorbeeld internet criminaliteit, creditcard fraude) eerder en beter zichtbaar (framing). Dit alles impliceert soms een breuk met de bestaande vooral individuele delicten gerichte benadering, hetgeen ruimte biedt voor innovatie;
- criminaliteit wordt in en rondom knooppunten en stromen in samenhang gezien met andere activiteiten, die plaats vinden binnen en rondom deze knooppunten en stromen. Hierdoor wordt de noodzaak en het nut van integrale handhaving eerder zichtbaar, hetgeen de effectiviteit van de opsporing kan versterken. Bovendien biedt dit meer mogelijkheden om van elkaars bevoegdheden gebruik te maken (bijv. Schiphol en de Rotterdamse haven en de operaties 'ochtendgloren');
- de eerste resultaten spreken in veel gevallen tot de verbeelding en hebben geleid tot het formuleren van verregaande ambities ten aanzien van de uitwerking van de nodale oriëntatie (bijv. de catch-ken in de Hoeksche Waard, operatie ochtend gloren, creditcard fraude).

Tegelijkertijd moet worden bedacht dat de feitelijke meerwaarde ook wordt bepaald door de mate waarin rekening wordt gehouden met de concrete vormgeving van de nodale oriëntatie (immers de nodale oriëntatie bestaat niet), bepaalde kritische factoren en relevante condities.

4.3 Aangrijpingspunten, condities en instrumenten

In deze paragraaf trachten we, in samenvattende en concluderende zin, de nodale oriëntatie nader vorm en inhoud te geven op grond van de eerdere uitgevoerde verkenningen naar de veronderstellingen achter het begrip en de praktijkvoorbeelden die we hebben bestudeerd. Achtereenvolgens komen aan de orde de aard van de nodale oriëntatie, de vorm die de nodale oriëntatie kan aannemen, de instrumenten die hiermee samenhangen en de condities waaronder een nodale oriëntatie met name vorm en inhoud kan krijgen.

Interventies in stromenland: aard van de nodale oriëntatie

Kenmerkend voor de nodale oriëntatie is het centraal stellen van de verschillende knooppunten in de netwerksamenleving en de (vervlochten) stromen die deze knooppunten met elkaar verbinden. Door meer oog te hebben voor de variëteit in dit stromenland, ontstaan er ook meer aangrijpingspunten voor interventie. In ieder geval gaat het om de volgende stromen van (zie ook paragraaf 2.2 en 2.3.1):

- Personen, veelal gebruik makende van fysieke infrastructuren die gelokaliseerd zijn binnen een geografisch bepaalde fysieke ruimte zoals het wegenverkeersnet;
- Goederen, veelal gebruik makende van fysieke infrastructuren die gelokaliseerd zijn binnen een geografisch bepaalde fysieke ruimte zoals het wegenverkeersnet;
- Energie (gas water, elektriciteit), veelal gebruik makende van fysieke distributie-infrastructuren die gelokaliseerd zijn binnen een geografisch bepaalde fysieke ruimte zoals het pijpleidingennetwerk;
- Kapitaal, dat veelal gebruik maakt van een virtuele ICT- infrastructuur en wier bewegingen zich vooral afspelen binnen een deels virtuele ruimte (wereldwijde kapitaalmarkt) en een deels fysieke ruimte (infrastructuur van banken en andere financiële instellingen); en
- Informatie en communicatie, veelal gebruik makende van een fysieke infrastructuur (het elektriciteitsnetwerk en het vaste en mobiele telefoonnetwerk) en zich bewegend in een wereldwijde, virtuele ruimte die gecreëerd wordt door computernetwerken (de virtuele infrastructuur). Hierbij gaat het niet alleen om bijvoorbeeld diensten die via het internet worden aangeboden zoals elektronisch winkelen, maar ook de uitwisseling van informatie over het verloop van bovengenoemde personen, kapitaal, goederen, energie en informatiestromen (meta-informatie).

Een belangrijke complicatie is verder het open en het gesloten karakter van de stromen en de infrastructuren waarover deze stromen gaan. Ook dit heeft gevolgen voor de opsporing en interventie in deze stromen en op deze knooppunten. Veel infrastructuren hebben een open karakter, omdat ze een publieke functie hebben zoals de verkeersinfrastructuur. Andere infrastructuren hebben een gesloten karakter, zoals de computernetwerken die het kapitaalverkeer tussen banken faciliteren of de infrastructuur die het transport van gas, water, telefoon en elektriciteit voor hun rekening neemt.
Ook stromen kunnen een open en gesloten karakter hebben. Veel discussies op het internet hebben een open karakter, terwijl het (mobiele) telefoonverkeer een gesloten karakter heeft. Dit gesloten karakter heeft vaak iets te maken met het eigenaarschap van de infrastructuur of de mate waarin bepaalde stromen vanwege bijvoorbeeld privacyredenen gesloten dienen te zijn om.

Dit alles betekent dat de aard van de stroom en de infrastructuur waarvan gebruik wordt gemaakt, ook gevolgen heeft voor de soort van nodale oriëntatie van de politie en te gebruiken instrumenten en de effectiviteit van deze instrumenten. Kortom, de invulling van de nodale oriëntatie dient dus te variëren met de aard van de stroom. Daarbij kunnen twee soorten aangrijpingspunten worden onderscheiden.
Ten eerste kan men zich richten op de toegangen en uitgangen van de betreffende infrastructuur door het opzetten van fysieke of virtuele fuiken. Ten tweede kan men zich richten op het meebewegen met de stroom binnen een bepaalde infrastructuur.

Op grond van deze overwegingen kunnen we deze nadere operationalisering als volgt weergeven.

Stroom	Infrastructuur (publieke)	Interventie op de toegang van de stroom	Interventie door meebewegen met de stroom
Mensen	Verkeersinfrastructuur (open) - wegen; - vaarwegen; - luchtwegen - spoorlijnen	Toegangswegen tot hoofdwegen en tot knooppunten zoals havens, luchthavens en stations	Patrouilles
Goederen	Verkeersinfrastructuur (open) - wegen; - vaarwegen; - luchtwegen - spoorlijnen	Toegangswegen tot hoofdwegen en tot knooppunten zoals havens, luchthavens en stations	Patrouilles
Energie	Gas, water en elektriciteitsdistributie netwerk (gesloten)	Productielocaties zoals electriciteitscentrales Distributieknooppunten zoals schakelstations	Monitoring van bewegingen
Kapitaal	ICT-infrastructuur (deels open deels gesloten)	Toegang tot (databanken) van banken, verzekeringsmaatschappijen en andere financiële dienstverleners zoals wisselkantoren en kredietverstrekkers	Monitoring van kapitaalbewegingen (bijv. melding grote transacties)
Informatie en communicatie	Internet (open) Telefoon (gesloten) Mobiele telefoon (gesloten) Satelliet (gesloten)	Websites als knooppunt van communicatie Servers Schakelstations Databases en andere registratiesystemen	Aftappen, afluisteren Participatie in internet discussiegroepen

Tabel 4.3a: Soorten van stromen in relatie tot infrastructuur en interventiemogelijkheden

Als deze stromen en knooppunten een mogelijk aangrijpingspunt voor opsporing zijn, dan rijst de volgende vraag: Wat weten we eigenlijk over die knooppunten en stromen?

Vandaar dat een volgende stap in de uitwerking van de nodale oriëntatie gericht dient te zijn op het analyseren van met name stedelijke knooppunten en stromen (zie par. 2.3.3). Dit alles is echter alleen mogelijk, indien we een relatief gedetailleerd beeld hebben over de aard van deze knooppunten, de functies die ze vervullen, de stromen die er door heen lopen en de wijze waarop die stromen met elkaar verweven zijn en welke risico's hiermee samenhangen. Knooppunten zijn er echter in allerlei soorten en maten. Dit kan de haven van Rotterdam zijn maar ook de bagageruimte van Schiphol of een voetbalstadion.

Derhalve is het belangrijk om systematisch na te denken hoe de nodale oriëntatie, gericht op een specifiek knooppunt of een specifieke stroom, er concreet uit zou

moeten zien. De aard van deze specifieke nodale oriëntatie kunnen we verder operationaliseren door het - op grond van de cases - aanreiken van een referentiekader. In dit kader worden een aantal punten genoemd, die in ieder geval geadresseerd moeten worden. Onderwerpen zijn onder meer de soort van interventie, de soort van risicoselectie en technologie en de soort van samenwerking die nodig is om gericht in stromen en knooppunten te interveniëren. Schematisch ziet dit model er als volgt uit (tabel 4.3b). De cellen zijn ingevuld op grond van de vergelijking tussen de twee interventiestrategieën op de verkeersinfrastructuur, namelijk de ANPR scan in het district Hoeksche Waard en operatie ochtendgloren. De indeling in de tabel laat zien welk soort van operationele vragen gesteld kunnen worden wanneer voor een bepaalde stroom of knooppunt een nodale strategie wordt ontwikkeld.

INTERVENTIE	Toegang controleren en meebewegen	Toegang controleren
OMVANG	100% (stille) controle	100% controle
EFFECT VAN CONTROLE OP STROOM	ongehinderde doorstroom	verminderde doorstroom
INTENSITEIT VAN CONTROLE	continue 24/24	periodiek, 11x per jaar
GEOGRAFISCH ORIENTATIE	Vast op vooraf bepaalde punten én mobiel (hot-spots/evenementen)	Beperkt (deel van snelweg Oost-Nederland)
MANIFESTATIE VAN CONTROLE	Onzichtbaar	zichtbaar
RISICO SELECTIE	bepaald door kracht van **technologie** - systeeminformatie (databases) - vooraf gedefinieerd (profielen)	bepaald door kracht van **samenwerkende opsporingsdiensten** - ter plaatse ingeschat (human factor) - systeeminformatie (databases)
REFERENTIE	Kenteken en geregistreerd profiel	Inzittenden, kenteken, situationele omstandigheden

Tabel 4.3b: Voorbeeld van de uitwerking van de nodale oriëntatie

Op grond van deze tabel zien we dat informatie een belangrijke rol speelt. Informatie die nodig is om bijvoorbeeld risico's te kunnen definiëren. En daarmee zijn we gekomen op een andere belangrijk aspect van de aard van de nodale oriëntatie.

Strategische risico-informatie: aard van de nodale oriëntatie

Bovenstaand betoog laat ons nog een ander aspect zien van de nodale oriëntatie. Stromen en knooppunten zijn belangrijke aanknopingspunten, maar kenmerkend voor de aard de nodale oriëntatie is ook:

a) het opbouwen van een strategische informatiepositie (intelligence led policing), waarin niet alleen statische en statistische informatie wordt verzameld maar ook dynamische, kwalitatieve en real-time informatie, waardoor een actueel beeld wordt verkregen van de actuele bewegingen binnen een stroom;

b) het werken met criminaliteitsanalyses waarin nadrukkelijk rekening wordt gehouden met de contextinformatie en kennis van de specifieke stroom of het specifieke knooppunt;

c) het werken met risicoprofielen, gericht op het herkennen van patronen – zowel achteraf als pro-actief; en

d) het maken van kwetsbaarheidsanalyses, omdat de vervlechting van verschillende stromen rondom bepaalde knooppunten dusdanige kwetsbaarheden kan oproepen, dat de stabiliteit en de voorspelbaarheid van het economische en maatschappelijke verkeer rondom een dergelijk knooppunt (met nationale en internationale uitstralingseffecten) in gevaar wordt gebracht.

Criminaliteitsanalyse als instrument

Criminaliteitsanalyses zijn een belangrijk instrument in ontwikkeling van deze strategische informatiepositie. Van belang is dat deze analyses zich niet alleen maar richten op de relatie tussen een bepaalde vorm van criminaliteit en daarbij behorende daderprofielen. Vanuit een nodale oriëntatie is het interessant om te kijken naar mate waarin bepaalde soorten van criminaliteit samenhangen met bepaalde stromen en de context waarbinnen een bepaalde stroom zich beweegt. Daardoor wordt een daderprofiel veel nadrukkelijker gepositioneerd in de context van de netwerksamenleving. In onderstaande tabel hebben we getracht criminaliteitssoorten te koppelen aan bepaalde stromen (tabel 4.3c, zie ook 2.5.2).

STROOM	SOORT VAN DELICTEN (VOORBEELDEN)
MENSEN	Vermogensdelicten door veelplegers Mensensmokkel Mobiel banditisme Terrorisme
GOEDEREN	Smokkel van drugs, wapens, sigaretten en andere goederen Autodiefstal
ENERGIE	Aftappen van elektriciteit i.v.m. hennepteelt
KAPITAAL	Verplaatsen en witwassen van criminele gelden Financiering van terroristische activiteiten
INFORMATIE EN COMMUNICATIE	Identiteitsfraude Uitzetten van computervirussen Hacken van computers en netwerken Kinderporno Terrorisme Verspreiding van rechts-extremistisch of religieus-fundamentalistische of ander gedachtegoed

Tabel 4.3c: Voorbeelden van een stroomgeoriënteerde benadering van delicten

Risicoselectie als instrument

Kenmerkend voor de nodale oriëntatie is het opsporen van crimineel gedrag in knooppunten en stromen op grond van risicoprofielen (zie verder ook par. 2.3.4, 2.7.1. en 2.7.3). Essentieel is de kwaliteit van definitie, analyse en evaluatie van mogelijke risico's. Hieraan zijn zowel een statistisch aspect als een human resource aspect te onderscheiden. Ten aanzien van het statistische aspect gaat het om de betrouwbaarheid van de informatie waarop statistische profielen zijn gebaseerd; zeker indien deze profielen steeds verder verfijnd worden met behulp van nieuwe informatie en reeds opgebouwde ervaringen. Ten tweede gaat het om specifieke kennis en vaardigheden, die verder reiken dan statistische kennis en vaardigheden. Het gaat vooral om kennis en vaardigheden om bepaalde patronen te zien, te herkennen maar ook deze te relativeren (een statistisch verband hoeft nog een feitelijk verband te zijn). Ook is het van belang - om deze patronen te kunnen interpreteren - oog te hebben voor de specifieke context waarbinnen een patroon al dan niet optreedt. Verder vraagt het werken met dergelijke profielen om vakinhoudelijke kennis van het reilen en zeilen binnen een stroom of binnen een knooppunt.

Informatievoorziening als instrument en voorwaarde

Essentieel in de nodale oriëntatie is het kunnen beschikken over informatie die afkomstig is uit verschillende bronnen om criminaliteits- en risicoanalyses te kunnen maken. Vandaar dat het kunnen opbouwen van een strategische informatiepositie kan worden gezien als een noodzakelijke voorwaarde voor de ontwikkeling van een nodale oriëntatie.
In het geval van het opbouwen van een strategische informatiepositie gaat het in ieder geval om:

- toegang en beschikbaarheid over de hoogwaardige kennis en informatie; daar waar het bijvoorbeeld gaat om het begrijpen van witwasoperaties waarbij gebruik wordt gemaakt van de complexiteit en verwevenheid van kapitaalstromen;
- het in kaart brengen van de condities waaronder andere organisaties die over de kennis en informatie beschikken, bereid en in staat zijn om deze kennis en informatie te delen; en
- het ontwikkelen van een technologische en organisatorische infrastructuur die dat ondersteunt en die ook nieuwe organisatieconcepten (zoals network centric warfare, zie par. 2.7.2) mogelijk maakt, die veel meer gebaseerd zijn op het door technologie real-time koppelen en visualiseren van activiteiten en informatieverwerkingsprocessen. Het belang van deze punten werd ook in de praktijkvoorbeelden nadrukkelijk naar voren gebracht als relevante kritische factoren. Dit brengt ons op een volgend punt.

Technologie speelt hierin een zeer belangrijke rol, zo niet een leidende. Hierbij gaat het vooral om enerzijds technologie die het mogelijk maakt om de status van bepaalde

personen die zich bewegen in een knooppunten of bepaalde handelingen binnen een stroom verrichten op een unieke manier identificeren (identificatie) en anderzijds om het kunnen koppelen van deze informatie gekoppeld aan andere informatie, waardoor samenhangen transparant kunnen worden gemaakt. Alleen de betekenis hiervan wordt binnen de politie vooral geduid in termen van te ontwikkelen applicaties. Het is echter belangrijk om op een andere manier naar technologie te kijken die verder reikt dan ' toys for the boys'.

Essentieel is het om technologische ontwikkelingen in een breder perspectief te plaatsen door ze relateren aan het opbouwen van een strategische informatie- en kennispositie door de politie, waarin applicaties, informatiestromen en allerlei basisvoorzieningen vanuit een infrastructureel perspectief (dus in samenhang) worden beschouwd. Het gaat echter niet alleen om het creëren van een politiebreed perspectief op informatievoorziening maar ook om te kijken hoe dit past in informatiestrategieën die worden ontwikkeld ter ondersteuning van het verloop van de stromen en daarmee samenhangende bedrijfsprocessen en toezichtprocessen die binnen een bepaald knooppunt kunnen worden ontwaard. Schiphol is een duidelijk voorbeeld hiervan. Daar wordt het strategische informatiebeleid nadrukkelijk gekoppeld aan een breder concept, namelijk dat van de 'self service airport'. Ook de douane in de haven Rotterdam werkt aan de ontwikkeling van een dergelijke strategische visie. Hoe kan ik informatie- en kennisbehoeften bij verschillende soorten van partijen die een rol spelen in de nodale oriëntatie van de politie ondersteunen door middel van ICT? Wat betekent dit voor de organisatie en het verloop van relevante processen binnen de politie? En wat betekent dit voor de uitwisseling van kennis en informatie met andere partijen buiten de politie en in het buitenland? Daarbij is het tevens belangrijk zich de vraag te stellen of de huidige organisatie van de informatievoorziening van de politie wel in staat is de nodale oriëntatie van de politie te kunnen ondersteunen. Tenslotte is het essentieel dat in een te ontwikkelen informatiestrategie voor de nodale oriëntatie rekening wordt gehouden met de politieke en maatschappelijke effecten van de inzet van het soort van technologie dat eerder is beschreven (zie uitgebreid 2.6 en 2.7).

Samenwerking en regie als instrument en voorwaarde

Binnen en rondom een knooppunt of stroom zijn veelal andere publieke en private organisaties aanwezig met uiteenlopende taken, verantwoordelijkheden en bevoegdheden op het terrein van inspectie, handhaving en opsporing. Kenmerkend voor een knooppunt en een stroom is dat het meerdere 'eigenaren' heeft met uiteenlopende belangen (bijvoorbeeld in het geval van Schiphol de afweging tussen klantvriendelijkheid en efficiency versus veiligheid). In alle praktijkvoorbeelden die we hebben bestudeerd werd het belang van een goede samenwerking, gebaseerd op het onderkennen van wederzijdse afhankelijkheid en vertrouwen, als een van de meest vitale factoren onderstreept.

Tegelijkertijd beperkt deze samenwerking zich niet alleen tot het Nederlandse grondgebied. In een netwerksamenleving, die immers gekenmerkt wordt door landsgrensoverschrijdende productie-, dienstverlenings- en handelsstromen ten

gevolge van de verregaande globalisering van economische, sociale en culturele verhoudingen, betekent de focus op knooppunten, infrastructuren en stromen per definitie dat ook een goede internationale samenwerking uiterst belangrijk is. We zagen dat met name terug in de cases die betrekking hadden op de haven van Rotterdam, de luchthaven Schiphol maar ook de operaties ochtendgloren (zie ook par. 2.3.3).

STROOM	INFRASTRUCTUUR (PUBLIEKE)	KNOOPPUNT	NOODZAKELIJKE SAMENWERKING MET ANDERE PUBLIEKE EN PRIVATE PARTIJEN
MENSEN	Verkeersinfrastructuur - wegen; - vaarwegen; - luchtwegen - spoorwegen	Verkeersknooppunten; Toegangs- en ringwegenstelsels Havens Luchthavens Stations, incl. Metrostations	KLPD; Douane; Koninklijke Marechaussee; IND; Vreemdelingenpolitie; Havenautoriteit
GOEDEREN	Verkeersinfrastructuur - wegen; - vaarwegen; - luchtwegen - spoorwegen	Havens Luchthavens Stations	Douane; Inspectie V & W; Waren- en Voedsel Autoriteit; Algemene Inspectie Dienst; Havenbedrijven en havenautoriteiten
ENERGIE	Gas, water en elektriciteitsnetwerk	Distributiecentra Productiecentra	Energiebedrijven; NMA (voorheen DtE)
KAPITAAL	ICT-infrastructuur	Banken Verzekeringsmaatschappijen Beurs Vastgoedmaatschappijen Notarissen	Banken Verzekeringsmaatschappijen Beurs NMA FIOD SIOD Notariaat Vastgoedmaatschappijen
INFORMATIE EN COM-MUNICATIE	Internet Telefoon Mobiele telefoon Satelliet	Telecombedrijven Internetproviders AMS-IX (Amsterdam Internet Exchange)	Digitale recherche Telecom- en internet providors OPTA Agentschap Netwerken Buma/Stemra

Tabel 4.3d: Relatie stroom, infrastructuur, knooppunt en samenwerkingspartners

Bovenstaande tabel maakt tevens duidelijk dat in de specifieke ontwikkeling van een nodale oriëntatie op een bepaalde stroom, knooppunt of infrastructuur, tenminste twee vragen moeten worden beantwoord:

- waar ligt het primaat van de opsporing, hetgeen niet noodzakelijkerwijs bij de politie behoeft te liggen,
- wat betekent dit voor de rol van de politie?

Tegelijkertijd maakt bovenstaande tabel het belang van vormen van integrale handhaving duidelijk, hetgeen Schiphol duidelijk illustreert. Kortom, de nodale oriëntatie dwingt de politie veel explicieter na te denken over hun rol en positie in bepaalde integrale handhavingsnetwerken in en rondom bepaalde knooppunten. In ieder geval is het van belang om afspraken te maken over de uitwisseling van

relevante informatie en in welke gevallen de politie wel en niet wordt ingeschakeld. Indien deze netwerken niet bestaan, dan zou de politie juist een regisseursrol kunnen vervullen in het opzetten van deze netwerken rondom bepaalde vitale knooppunten.

Pro-actieve opsporingstijl als instrument en voorwaarde

Tenslotte laat het onderzoek van met name de praktijkvoorbeelden bovendien zien, dat zich een heel andere opsporingsstijl ontwikkelt c.q. moet worden ontwikkeld, die kansen maar ook bedreigingen biedt. Het accent verschuift van een delictgerichte opsporing naar een pro-actieve opsporing waarbinnen op grond van de verzameling en interpretatie van informatie – afkomstig vanuit verschillende bronnen – op zoek wordt gegaan naar specifieke verbanden die als risicovol kunnen worden aangemerkt. Dit leidt niet alleen tot andere werkwijzen, routines en procedures, maar ook tot een andere cultuur en waardering van andersoortige kennis. Een nodale oriëntatie zal daarom ook rekening moeten houden met de beperkende invloed van de bestaande cultuur binnen de politie.

4.4 De normatieve inbedding van de nodale oriëntatie

De ontwikkeling van de nodale oriëntatie roept een aantal normatieve vragen op. Een voor de hand liggende vraag is die naar de bescherming van de persoonlijke levenssfeer, zoals ook blijkt uit de bestudeerde praktijkvoorbeelden. In de meeste van de door bestudeerde praktijken voorbeelden blijkt dat een balans gevonden is tussen enerzijds de bijdrage die bepaalde technologietoepassingen kunnen bieden aan het transparant maken en opsporen van crimineel gedrag en anderzijds de grondwettelijk en Europees-rechtelijk vastgelegde rechten en plichten jegens de bescherming van de persoonlijke levenssfeer. Wij pleiten ervoor om deze discussie niet te voeren in termen van 'wij' en 'zij', waarbij zowel technologische mogelijkheden, het maatschappelijke probleem of de privacybescherming verabsoluteert dan wel gebagatelliseerd worden. Van belang is een zakelijke discussie te voeren en nadrukkelijk afweging tussen politieke waarden te laten plaats vinden aan de hand van een concrete opsporingspraktijk. De nodale oriëntatie maakt duidelijk dat het hierbij gaat om een afweging van politieke waarden en dat de uitkomst van deze afweging een politiek proces is, dat in een democratische rechtsstaat volgens bepaalde regels en spelregels dient te verlopen.

Als onderzoekers betreden we niet de inhoud van deze waarden afweging, maar we kunnen wel op grond van onze verkenning duidelijk maken dat de legitimiteit van de nodale oriëntatie zich afspeelt binnen bepaalde spanningsvelden. Het is van belang die spanningsvelden te onderkennen en hierover ook een publieke en politieke dialoog te voeren. Bovendien is het belangrijk dat de afweging concreet wordt gemaakt. Een discussie over de normatieve inbedding van 'de' nodale oriëntatie is namelijk gedoemd te mislukken. Van belang is ze te richten op concrete situaties binnen stromen en

knooppunten. In die afweging spelen in ieder geval de volgende overwegingen een rol. De eerste relevante normatieve afweging die voor de uitwerking van de nodale oriëntatie van belang is, is die tussen vrijheid en veiligheid, de tweede betreft de afweging tussen vrijheid en efficiency en de derde afweging betreft die tussen vrijheid en gelijkheid (zie voor een uitgebreidere weergave par. 2.9.)
Daarnaast moet onderkend worden dat de nodale oriëntatie en de wijze waarop technologie hierin wordt ingezet, leidt tot een bepaald soort overheid; een overheid die eerder is beschreven als de 'panoptische staat' , waarin de staatsmacht in ultieme vorm gebaseerd is op de combinatie van zwaardmacht en informatiemacht. Essentieel is dat in de verdere ontwikkeling van het concept van de nodale oriëntatie – ook al is er een groot vertrouwen in de politie en ook al heeft de politie geen traditie en cultuur van machtsmisbruik – nagedacht over de inbedding van deze visie in een systeem van 'checks and balances': wie controleert de controleurs?.
Tevens dient in de discussie over de normatieve inbedding van de nodale oriëntatie gewaakt te worden voor naïef instrumentalisme. Technologie is niet alleen een instrument; het is een kneedbaar instrument, het instrument dat de belichaming van bepaalde belangen en waarden, en dat ook een eigen dynamiek kan genereren en daarmee zijn eigen onbedoelde effecten. Ook hier is de normatieve vraag gerechtigd: hoe en wie controleren de inzet van technologie?

4.5 Strategische agenda

We hebben laten zien dat de nodale oriëntatie op de opsporing van criminele activiteiten een gevestigde en een zich verder ontwikkelende praktijk is, die niet alleen vorm en inhoud krijgt binnen de politie maar ook daarbuiten. Dit roept verschillende specifieke agenda's voor uitwerking op.

Strategische agenda

Van de ene kant raakt de doorontwikkeling van het concept op zijn minst nog drie andere zaken die van strategische betekenis zijn.
Ten eerste is het belangrijk om een strategische en dus inhoudelijke visie te ontwikkelen op specifieke stromen en knooppunten, waarbij rekening wordt gehouden met de specifieke aard van een stroom of een knooppunt en rol die andere publieke en private partijen vervullen in de opsporing van crimineel gedrag binnen deze stroom of binnen dit knooppunt. Dit, omday er ook gevolgen zijn voor de rol van de politie en aard van samenwerking. De ontwikkeling en toepassing van technologische applicaties is hierin de uitkomst van deze visie.

Ten tweede dient het concept van de nodale oriëntatie nadrukkelijker te worden verbonden met het strategische en technologische innovatiebeleid van de politie. Daarin gaat het niet alleen om de vraag welke soort van individuele technologietoepassingen ontwikkeld moet worden ten einde een nodale oriëntatie te ondersteunen. Het is belangrijk om vanuit de behoeften die rondom de aanpak van

criminaliteit binnen stromen en knooppunten bij verschillende partijen leven, een gemeenschappelijk perspectief te creëren op de bijdrage van technologische innovatie aan de wijze waarop in de stroom of in het knooppunt wordt geïntervenieerd. Voorkomen moet worden dat er sprake is van eilandinnovatie, waarbij innovaties geïsoleerd worden ontwikkeld.
Verder is het belangrijk om na te denken over de diffusie en adoptie van innovatie door andere partijen, bijvoorbeeld andere korpsen, zodat optimaal gebruik kan worden gemaakt van leerervaringen die elders zijn ontwikkeld (Bekkers, Korteland, Simons, 2006). De catch-ken technologie zoals deze wordt ingezet in Hoekse Waard kan worden gezien als een relatief geïsoleerde innovatie, waarin bepaalde pioniers een voortrekkersol hebben vervuld, maar het succes hiervan is mede afhankelijk van de gepercipieerde meerwaarde voor andere korpsen.

Ten derde is het belangrijk om de uitwerking van de nodale oriëntatie nadrukkelijk te koppelen aan de kerntakendiscussie die thans ook binnen de politie speelt (zie ook het eerste punt). In de bestudeerde praktijkvoorbeelden zien we dat in sommige gevallen de politie de trekker is van de nodale oriëntatie, terwijl zij in andere gevallen een bescheiden rol vervult. Kortom, het benadrukken van een nodale oriëntatie als interventiestrategie, betekent dat de vraag gesteld moet worden wie in een knooppunt of binnen een bepaalde stroom de regisseur van de nodale oriëntatie is. Dit raakt ook de vraag wat de kerntaak van de politie ten aanzien van een bepaalde stroom of knooppunt is. Tegelijkertijd zien we dat het belang dat in de nodale oriëntatie wordt toegekend aan 'intelligence' ook vragen oproept met betrekking tot de verhouding en soort van samenwerking met andere partijen, die zich met opsporing en met het verzamelen van 'intelligence' bezighouden.

Operationele en tactische agenda

Van de andere kant roept de uitwerking de doorontwikkeling van het concept een heleboel operationele en tactische uitwerkingsvragen op. In de paragraaf drie van dit hoofdstuk zijn verschillende zaken aan de orde gesteld. Genoemd kunnen worden:

- de uitwerking van de strategische informatiepositie van de politie ten aanzien van concrete stromen en knooppunten;
- de rol, kwaliteit en soort van risicodefinities en misdaadanalyses die gericht zijn op het in kaart brengen van het functioneren van knooppunten en stromen en minder op dader- of groepsprofielen;
- de kwaliteit van de informatievoorziening binnen de politie in relatie tot de ontwikkeling van een politiebrede infrastructuur die tevens mogelijkheden biedt om effectiever en efficiënter gegevens uit te wisselen met andere partijen;
- de noodzaak tot kennismanagement (gericht op inhoudelijke kennis van en de context waarbinnen stromen en knooppunten functioneren en het vermogen tot patroonherkenning (zowel achteraf als vooraf);
- cultuurverandering ter ondersteuning van een pro-actieve in plaats van een op delictgerichte opsporingsstijl; en

- het versterken van de bereidheid tot en het vermogen om samenwerking, hetgeen cultuur en attitudeaspecten kent.

Onderzoeksagenda

We hebben in dit onderzoek een verkenning gedaan naar die bouwstenen die nodig zijn om de nodale oriëntatie van de politie een stap verder te brengen. Daartoe is een aantal relevante ontwikkelingenen zijn leerstukken en enkele praktijkvoorbeelden verkend door middel van een 'quick scan'. Wat ons betreft zou de verdere ontwikkeling van de nodale oriëntatie in ieder geval gebaat zijn met een verdere, grondige bestudering van deze of andere nodale praktijken. Daarbij is het tevens interessant om deze praktijken te vergelijken met praktijken zoals die zich in het buitenland hebben ontwikkeld.
Verder is het interessant om specifieker in kaart te brengen welke eisen aan de strategische kennis- en informatiepositie moeten worden gesteld en hoe deze verder kunnen worden geoperationaliseerd om een nodale oriëntatie mogelijk te maken; om verder te bezien of die eisen mogelijk verschillen per stroom en per infrastructuur. Dit alles ook in het licht van de recente discussie over een nieuwe informatievoorziening voor de politie die meer op een concern-leest geschoeid zou moeten worden.
Daarnaast zou het interessant kunnen zijn om de bestaande criminologische kennis op het terrein van misdaadanalyses te 're-framen' vanuit het perspectief van stromen en knooppunten. Hoe kan de criminologie dit oppakken en wat betekent dit voor de samenwerking met andere disciplines?
Tenslotte zou het interessant kunnen zijn om de vraag welke soort van innovaties de nodale oriëntatie vraagt, verder uit te diepen alsmede aan te geven wat dit betekent voor de diffusie en adoptie van deze innovatie door andere korpsen of andere diensten buiten de politie.

Synthese: experimentele agenda

Deze verschillende soorten van agenda's kunnen ook bij elkaar worden gebracht in de vorm van het opzetten van een experiment of proeftuin. Op grond van de overwegingen in dit onderzoek zou voor een specifieke stroom of een specifiek knooppunt (of een combinatie van beiden) een nodale oriëntatie kunnen worden ontwikkeld, waarbij ook aandacht is voor de te ontwikkelen instrumenten daarbij. Vervolgens zou deze oriëntatie in een proeftuin uitgevoerd kunnen worden om te bekijken welke kritische factoren een rol spelen, alsmede inzicht te krijgen in de wijze waarop leerervaringen worden opgedaan en hoe deze kunnen worden verspreid. Dit alles zou op een wetenschappelijk verantwoorde manier moeten worden gedocumenteerd, beschreven, geanalyseerd en geëvalueerd. Op deze manier zou belangrijke ervaringskennis kunnen worden vastgelegd die belangrijk is voor de verdere ontwikkeling van de nodale oriëntatie.

In dit hoofdstuk hebben we de contouren van een beleidstheorie voor de nodale oriëntatie uitgewerkt. Hierna vatten wij onze aanbevelingen met het oog op de verdere uitwerking van het concept nog eens samen.

4.6 Aanbevelingen

1 De nodale oriëntatie heeft een meerwaarde voor de politie. De politie moet voortbouwen op nodale praktijken en projecten die reeds zijn gestart en deze verder tot ontwikkeling brengen rondom specifieke stromen, infrastructuren en knooppunten. De nodale oriëntatie moet uitgewerkt en gespecificeerd danwel gedifferentieerd worden per stroom, knooppunt of infrastructuur.

2 Knooppunten en stromen hebben meerdere eigenaren. Per stroom, knooppunt of infrastructuur moet de politie zich de vraag stellen welke rol zij voor zichzelf ziet weggelegd, in hoeverre zij zich ziet als regisseur of het voortouw wenst te nemen of een rol speelt op de achtergrond. Kortom, wat haar kerntaken zijn in samenwerkings-netwerken in relatie tot specifieke knooppunten en stromen. Dit veronderstelt het uitwerken van een inhoudelijke visie.

3 Daar waar rondom vitale knooppunten geen samenwerkingsnetwerken bestaan, zou de politie de regisseursfunctie op zich moeten nemen in het creëren van deze netwerken.

4 Een nodale oriëntatie veronderstelt samenwerken met andere publieke en private partijen. Dit veronderstelt een bereidheid om, onder voorwaarden, kennis en informatie te delen en uit te wisselen op basis van onderkenning van wederzijdse afhankelijkheid en onderling vertrouwen.

5 De politie dient te onderzoeken in hoeverre de huidige informatievoorziening en informatiestrategieën de nodale oriëntatie voldoende ondersteunen dan wel blokkades vormen.

6 Voor de verdere uitwerking van het concept van de nodale oriëntatie is een geformaliseerd systeem van 'checks and balances' noodzakelijk teneinde de kans op machtsmisbruik te voorkomen. De vraag is: wie controleer de controleurs? Het gaat hier met name om aantasting van de persoonlijke levenssfeer als mogelijk gevolg van de nodale oriëntatie door:
   b) het volgen van personen c.q. het monitoren van het gedrag van personen bijvoorbeeld in het kader van camerabewaking;
   c) het onderscheppen van de communicatie tussen personen, bijvoorbeeld in het kader van afluisteren en onderscheppen van een e-mailbericht;

d) het ontsluiten van data in diverse publieke en private databestanden, zoals het toegang krijgen tot data van banken waarin transacties zijn opgeslagen, en;
e) de interpretatie van bestaande data door ze op een bepaalde manier met elkaar in verband te brengen of te aggregeren. Essentieel is dat transparant is wie de afweging maakt, wie hiervoor verantwoordelijk is, hoe deze afwegingen worden gemaakt en hoe zij getoetst worden.

7 De politie kan in dialoog met het College Bescherming Persoonsgegevens de grenzen en dilemma's van de nodale oriëntatie verkennen. Hiervoor zijn concrete casuïstiek en voorbeelden uit de praktijk het meest geëigend, concrete situaties binnen stromen en knooppunten, niet abstracte schaalniveaus. Ook zou de politie een maatschappelijke debat kunnen organiseren over de normatieve grenzen waarbinnen burgers en maatschappelijke organisaties een nodale oriëntatie al dan niet acceptabel vinden.

8 Ga na in hoeverre bestaande criminaliteitsanalyses zich in voldoende mate richten op relaties tussen stromen/knooppunten en mogelijke delicten en in hoeverre de huidige competenties van misdaadanalisten passen bij een nodale oriëntatie. Het gaat met name om risicoanalyses van kwetsbare en criminogene knooppunten en stromen.

9 De nodale praktijken tot nu toe zijn te typeren als eilandinnovatie met een belangrijke rol voor pioniers. Het is aan te bevelen dat de politie nu een doordacht leertraject uitzet en regie ontwikkelt over de diffusie en adoptie van de nodale oriëntatie, zodat gebruik kan worden gemaakt van leerervaringen die elders zijn ontwikkeld.

10 Voor de verder uitwerking van de nodale oriëntatie zou gebruik kunnen worden gemaakt van een experiment of een proeftuin. Voor een specifieke stroom of een specifiek knooppunt (of een combinatie van beiden) zou een nodale oriëntatie kunnen worden ontwikkeld, inclusief het ontwerpen van instrumenten. Vervolgens zou deze oriëntatie in een proeftuin uitgevoerd moet worden om te kijken welke kritische factoren zich voordoen alsmede inzicht te krijgen in de wijze waarop leerervaringen worden opgedaan en hoe deze kunnen worden verspreid.

11 De verdere ontwikkeling van de nodale oriëntatie zou gebaat zijn met een verdere, grondige bestudering van deze of van andere nodale praktijken.

BIJLAGE A LIJST VAN GEÏNTERVIEWDE PERSONEN

De heer B. Mos
Senior officer security
Amsterdam Airport Schiphol
Schiphol Group N.V.

Mevrouw mr. V.H. Brouwer
College Bescherming Persoonsgegevens (CBP)

Mevrouw drs. R. Kats
Risk Management
Equens Nederland B.V.

De heer prof.dr. H.G. van de Bunt
Hoogleraar Criminologie, Faculteit der Rechtsgeleerdheid
Erasmus Universiteit Rotterdam

De heer drs. A.J. van Dijk
Adviseur
Politieregio Amsterdam-Amstelland

De heer drs. S. Eschen MPA
Ministerie van Justitie, directie Algemene Justitiële Strategie

De heer mr. A.J. Groenendijk
voorzitter managementteam
Customs Rotterdam

De heer P. M.A. Homminga
Districtschef district Hoeksche Waard
Politieregio Zuid-Holland-Zuid, thans chef Divisie Uitvoeringsondersteuning (DUO)

De heer prof.dr. A.B. Hoogenboom
hoogleraar Forensic Business Studies
NIVRA-Nyenrode School of Accountancy

De heer L.Th.C. Kuijs
Korpschef
Politieregio BrabantZuid-Oost

De heer drs. E. Lagerweij
senior officer safety & environment
Amsterdam Airport Schiphol
Schiphol Group N.V.

De heer drs. G.O. van de Klashorst
Hoofd Communicatie
College Bescherming Persoonsgegevens (CBP)

De heer mr. J. Kohnstamm
voorzitter College Bescherming Persoonsgegevens.
College Bescherming Persoonsgegevens (CBP)

De heer H. Markerink
Coördinator
Korps Landelijke Politiediensten (KLPD), dienst Verkeerspolitie unit Wolfheze

De heer ir. J. van Os
Senior Adviseur Expertise
Korps Landelijke Politiediensten

De heer drs. J. Regterschot
Hoofd regionale Inlichtingendienst (RID)
Politieregio Gelderland-Midden

De heer H. Schönfeld MCM
Director Business-strategy and Processes
Politieregio Amsterdam-Amstelland

De heer prof.dr. C.D. van der Vijver
Hoogleraar Instituut voor Maatschappelijke Veiligheidsvraagstukken (IPIT)
Universiteit Twente

BIJLAGE B LITERATUUR

B&A Groep Beleidsonderzoek & -Advies, Intomart GfK, *Bevolking 2004: landelijke rapportage,* Hilversum, 2004

Bannister, F., *The panoptic state. Privacy, surveillance and the balance of risk*, in: I*nformation Polity*, 2005, vol. 10, nr.1-2, pp. 65-80.

Beck, U., *World Risk Society*. Polity Press, Malden, 1999

Beer M. de e.a., *Aanpak criminaliteit*, B&A Groep BV, Den Haag, 1997

Bekkers, V. e.a., *De keerzijde van verbonden netwerken*, Eburon, Delft 2002

Bekkers, V., *Grenzeloze overheid*, Samsom, Alphen aan de Rijn, 1998

Bekkers, V., *Nieuwe vormen van sturing en informatisering*, Eburon, Delft, 1994.

Bekkers, V. & M. Thaens, *Interconnected networks and the governance of trust*, in: *Information Polity*, 2005, vol. 10, nr.1-2, pp, 37-50.

Beniger, J., Conceptuzalizing, information technology as organization and vice versa, in Fulk, J. & Ch. Steinfeld (eds.), *Organizations and communication technology*, Sage, Newbury Park, 1990, pp. 229-249.

Bijker, W.E. et al., *The social construction of technological system*., Cambridge University Press, Cambridge, 1987

Castells, M., *The Rise of the Network Society, The Information Age: Economy, Society and Culture.* Blackwell*,* Cambridge, 1996.

Castells, M., *The Power of Identity, The Information Age: Economy, Society and Culture.* Blackwell, Cambridge, 1997

Castells, M., *The End of the Millennium, The Information Age: Economy, Society and Culture*. Blackwell, Cambridge, 1998

College Bescherming Persoonsgegevens, "*Camera's in het publieke domein*", Den Haag, 2004

Douglas, M. &, A. Wildavsky, *Risk and Culture,* University of California Press, Berkeley, Los Angeles, London, 1983

Duivenboden, H. van., *Koppeling in uitvoering*, Eburon, Delft, 1999

Europol, "*2004 European Union Organised Crime Report OPEN VERSION*", Europol, 2004

Eggen A.Th.J. e.a., *Criminaliteit en rechtshandhaving 2004; ontwikkelingen en samenhangen*", CBS, 2004

Ferwerda, H.B., Adang, O.M.J. *Hooligans in beeld*, Apeldoorn/Arnhem, 2005

Frissen, P., *Bureaucratische cultuur en informatisering*, Sdu, Den Haag,1989

Frissen, V., *De domestificatie van technologie*, oratie, Erasmus Universiteit Rotterdam, 2004

Hamilton, A., J. Madison, & J. Jay, *The federalist papers*, Doubleday New York, 1966

Hoogerwerf, A., *Beleid berust op veronderstellingen: de beleidstheorie,* in: Lehning, P. B.(red.), Handboek beleidswetenschap, Boom, Meppel, 1987, pp. 23-41

Interpay, "*Partner in processing*", Interpay, Utrecht, 2006, p1.

Kerckhove de, D., *Gekoppelde intelligentie*, Ede, SMO, 1996

Kleemans, E.R., Brienen M.E.I., Van de Bunt, H.G., "*Georganiseerde criminaliteit in Nederland, Tweede rapportage op basis van de WODC-monitor*", Den Haag, WODC, 2002

KLPD/DNRI , "*Jaaroverzicht 2005 en vooruitblik 2006 Meldingen Ongebruikelijke Transacties*", 2005

Lammers, J. e.a., *Landelijke criminaliteitskaart 2004*, KLPD-DNRI, Zoetermeer, 2004

Lyon, D., *The electronic eye*, Polity Press, Cambridge, 1992

Ministerie van Financiën. persbericht | 17-02-2006 | nr 06-011 | Directie Voorlichting, 17 februari 2006

Mul, J de. et. al., *ICT de baas?* in: Frissen, P. e.a., *Internet en openbaar bestuur*, Tilburg, 2002

Politie Brabant-Noord i.s.m. instituut IVA-Tilburg, "*Veiligheidsatlas*", IVA Tilburg, 2003

Projectgroep Visie op de politiefunctie, "*Politie in ontwikkeling; visie op de politiefunctie*", NPI, Den Haag, in opdracht van de Raad van Hoofdcommissarissen, 2005

Projectgroep Opsporing-2, "*Tegenhouden troef*", Groningen, in opdracht van de Raad van Hoofdcommissarissen, 2003

Ringeling, A.B., *Beleidstheorieen en theorieen over beleid*, in: Lehning, P. B.(red.), Handboek beleidswetenschap, Boom, Meppel, 1987, pp. 41-53

Sassen, S., *Cities in a world economy*, Pine Forge Press, Thousand Oaks, 1994

Schnabel P., *Individualisering en sociale integratie*, Sociaal en Cultureel Planbureau, Den Haag, 2004

Stol W., *Cybercrime*, WODC, Den Haag, in: Justitiële verkenningen december 2004 nr. 08

Stone, D., *The policy paradox*, Norton, New York, 2003

Versteegh, Peter, *Informatiegestuurde Veiligheidszorg, Stichting Maatschappij, Veiligheid en Politie*, Dordrecht, 2005

Winner, L., *Do artifacts have politics*?, in: Kraft, M. & N. Vigs (eds), *Technology and politics*, Duke University Press, Durham, 1988, pp. 33-53

Sociaal en Cultureel Planbureau, *Sociaal en Cultureel Rapport 2004*, Den Haag, 2004

Tilley, Nick., *Community policing, problem-oriented policing and intelligence-led policing*. In: Tim Newburn (ed.) Handbook of Policing, Willan Publishing, Devon, 2003

Zuboff, S., *In the age of the smart machine*, Heineman, Oxford,1988

Overige bronnen

Meer banditisme Litouwers en Polen, verschenen in NRC Handelsblad 20 oktober 2005

Cybercrime, Justitiële verkenningen, WODC,Den Haag , 2004

Justitiële verkenningen nr. 2, WODC,Den Haag, 2006

Dossier: Terreur in Europa, verschenen in Elsevier januari 2006

Veiligheidsbeleid en nodale oriëntatie, verschenen in Openbaar Bestuur, april 2006, p.20-23

Gemeente Rijssen-Holten, *Raadsvoorstelnummer: 2004-II-18*, 27 januari 2004

Belastingdienst, *Bedrijfsplan belastingdienst*, 2006-2010, 2005