Inzicht in toezicht: toezicht door inzicht

Peter Marks, Arie van Sluis en Victor Bekkers

Inleiding

In 2005 publiceerde de Raad van Hoofdcommissarissen een nieuw visiedocument voor de Nederlandse politie met als titel 'Politie in Ontwikkeling' (PIO[1]). In PIO worden tien punten op de horizon gezet die richtinggevend zouden moeten zijn voor de politie de komende jaren. Een van meest innovatieve en spraakmakende van de tien punten van PIO is ongetwijfeld de 'nodale oriëntatie': de focus van de politie op de knooppunten van stromen van mensen, goederen, geld en informatie, als aanvulling op de traditionele gebiedsgerichtheid van de politie. Daar waar deze stromen bij elkaar komen, zijn er voor de politie en andere organisaties die zich met veiligheid bezighouden interessante kansen om te interveniëren.[2] De interventies zijn dan vooral gericht op het zichtbaar maken en ontanonimiseren van potentieel crimineel gedrag binnen deze stromen en op deze knooppunten.

De keuze voor een nodale oriëntatie dient begrepen te worden vanuit zowel maatschappelijke als technologische ontwikkelingen die ook hebben bijgedragen aan een veranderend crimineel gedrag.[3] De samenleving is drastisch veranderd: ontgrenzing, een grote mobiliteit en anonimiteit zijn typische kenmerken van de moderne samenleving die zich geleidelijk ontwikkelt tot een netwerksamenleving, waarin stromen van mensen, goederen, geld en vooral informatie steeds belangrijker worden.[4] Fysieke locaties zijn weliswaar nog steeds een belangrijke ontmoetingsplaats waar mensen wonen, werken of verblijven. Deze ruimte is echter niet langer uitsluitend fysiek, maar ook virtueel door middel van ICT, of een combinatie van beide. De internationale kapitaalmarkt is een fysieke markt op de beursvloer van Amsterdam, maar heeft tegelijkertijd een mondiaal karakter waar kennis en informatie over koersen voortdurend worden aangeboden via ICT-stromen.

Deze ontwikkelingen brengen nieuwe dreigingen met zich mee.[5] Een verstoring in het ene netwerk kan ook gevolgen hebben voor het functioneren van andere netwerken en daarmee de samenleving als geheel ontwrichten. Een stroomstoring leidt er bijvoorbeeld toe dat telecommunicatie deels wordt plat gelegd en dat belemmert vervolgens ons dagelijkse leven en werken. Deze kwetsbaarheden vormen voor de georganiseerde criminaliteit en allerlei terroristische groeperingen een interessant perspectief. Dit geldt zeker voor de stedelijke gebieden in de netwerksamenleving, waarin verschillende stromen en knooppunten samenkomen. Kenmerkend voor de netwerksamenleving is immers 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.

ICT en andere technologische ontwikkelingen bieden mogelijkheden om vooral de anonimiteit van individuele bewegingen binnen 'stromenland' op te heffen. In de nodale oriëntatie moeten nieuwe technologieën worden toegepast waarmee men mensen of goederen kan volgen. Ook de infrastructurele positie van Nederland als internationaal doorvoercentrum tot Europa en haar centrale rol in internationale financiële netwerken zijn relevant voor een nodale aanpak. Onze onderzoeksvraag is dan ook: Wat zijn de consequenties van de nodale oriëntatie in de uitoefening van toezicht door de politie en andere toezichthouders in stromen en op infrastructurele knooppunten?

Dit artikel is gebaseerd op een onderzoeksrapport van Bekkers, Van Sluis, & Siep (2006) voor het onderzoeksprogramma van Politie & Wetenschap. Het empirisch materiaal van dit onderzoek is geactualiseerd door additioneel literatuuronderzoek, negen extra interviews en secundaire analyse van recent onderzoek naar de nodale oriëntatie bij de politie.[6]

In de volgende secties bespreken we eerst een aantal praktijkvoorbeelden van stromen en knooppunten waarin de nodale oriëntatie een rol speelt, namelijk de douane en de Rotterdamse haven, Schiphol en de nodale controle op verkeerstromen door de politie en anderen. Per praktijkvoorbeeld zal nadat de empirie en de technologische toepassingen beschreven zijn, worden ingegaan op de nodale strategieën die daar gespeeld hebben, de informatie-uitwisseling en samenwerking die heeft plaatsgevonden. In de daaropvolgende sectie zal geanalyseerd worden wat de implicaties zijn van de nodale oriëntatie op de uitoefening van toezicht op stromen en knooppunten. Conclusies zullen in de laatste sectie getrokken worden over de normatieve consequenties van de nodale oriëntatie zijn voor de politiek en de maatschappij.

Goederenstroom: De douane in de Rotterdamse haven

De Rotterdamse haven is direct gelegen aan de Noordzee met 24 uur per dag, 7 dagen in de week een optimale toegang. In de haven zijn veel verschillende ondernemingen actief variërend van opslag en overslag tot industriële verwerking. Daarnaast heeft de haven een heel groot en makkelijk bereikbaar (Europees) achterland met meer dan 500 miljoen consumenten. Er zijn vijf verschillende transportmodaliteiten in de haven aanwezig, te weten trein, binnenvaart, wegen, zeevaart en pijplijnen.[7] De haven is een zeer complexe en dynamische multi-nodale en Multi-infrastructurele knoop met wereldwijde vertakkingen.

Om een veiligere haven te creëren hebben belanghebbende (veiligheids)partijen in de haven van Rotterdam vijf stromen gedefinieerd: binnenvaart, goederen, zeevaart, havenveiligheid en grenstoezicht. In elke stroom zijn verschillende constellaties met daarin verschillende actoren actief in een geïntegreerde aanpak.[8] Dit initiatief past binnen het programma van vernieuwing toezicht uit 2009[9] dat probeert een effectievere toezichthouding met minder overlast voor ondernemingen te organiseren. Toezichthouders moeten meer samenwerken door middel van een betere uitwisseling van informatie, gecoördineerde inspectieprogramma's, gezamenlijke risicoanalyses en delen en overdracht van verantwoordelijkheden. Toezicht moet zich dan vooral richten op risicovolle organisaties. Organisaties die door het opbouwen van een 'track record' laten zien dat ze te vertrouwen zijn kunnen/moeten dan minder gecontroleerd worden zodat deze minder oponthoud kennen. Dit wordt ook wel horizontaal toezicht genoemd.

De douane houdt het toezicht op goederenstromen, in casus het grensoverschrijdende goederenverkeer, dus op de invoer, de doorvoer en de uitvoer van goederen. 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.

> De goederenstromen worden in de komende jaren zo gecontroleerd dat het bedrijfsleven zo min mogelijk oponthoud heeft. Dit gebeurt op basis van risico-informatie, die door de lidstaten onderling elektronisch wordt uitgewisseld. Hierdoor kan de Douane vooraf bepalen of goederen de grens mogen passeren. Het elektronisch uitwisselen van gegevens tussen de douanekantoren in de lidstaten van de Europese Unie én het bedrijfsleven, ondersteunt de uitvoering van de nieuwe wetgeving. Onder

de noemer Electronic Customs, of eCustoms, ontwikkelen de lidstaten alle nieuwe automatiseringssystemen die nodig zijn.[10]

De Rotterdamse haven was ook de eerste Europese haven die zich aansloot bij het Container Security Initiative (CSI) opgezet in 2002 door de U.S. Bureau of Customs and Border Protection (CBP).[11] Het doel van dit project was om de veiligheid van containerschepen naar de VS te vergroten. De douane van de VS wilde 24 uur voor vertrek naar een haven in de VS alle informatie van de containergoederen hebben, waarbij risicovolle ladingen in Rotterdam gescand of fysiek gecontroleerd moesten worden. Hiermee ontstonden zogenoemde ' fair-trade lanes', waarbij de douane uit de VS vertrouwt op de informatie van de Rotterdamse douane en vice versa. Deze methode is men in Rotterdam bezig ook te ontwikkelen met Shanghai (China) en men is in overleg getreden met de Japanse douane. De criteria voor de 'fair-trade lanes' worden gebaseerd op criteria afkomstig van de World Customs Organization (WCO).

De douane werkt momenteel met een systeem voor risicoselectie, PRISMA genaamd. Scheepvaartbedrijven zijn verplicht elektronisch informatie over ladingen toe te zenden. Elke lading krijgt een risicoprofiel op basis van een combinatie van variabelen: het type product, de verlader, land van herkomst, land van bestemming en de route. 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 en zijn vastgelegd in the Douanewet. Op grond van PRISMA wordt ongeveer 60% van alle zendingen als niet-risicovol beschouwd en de douane hoeft deze 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. Op deze manier wordt de inbreng van de menselijke factor in het proces van risicoanalyse en –selectie gewaarborgd. 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. Momenteel wordt PRISMA in heel Nederland uitgerold. De Europese lidstaten gebruiken echter allemaal een eigen systeem, maar men wil op korte termijn – ook door druk van de private sector – wel allemaal naar dezelfde indicatoren voor het maken van de risicoprofielen.

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 X-ray containerscan te halen. De douane beschikt over vaste, mobiele en een 'drive through' scans. Er worden jaarlijks ongeveer 50.000 foto's van ladingen van containers gemaakt, wat overeenkomt met ongeveer 2% van de niet-Europese stroom. 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 opengemaakt en vindt er een feitelijke inspectie plaats. Het percentage 'hits' en successen wordt niet publiekelijk bekend gemaakt. De verschillende douane-instellingen in Europa delen deze cijfers echter wel, gebaseerd op convenanten.

Binnen de Rotterdamse haven ontwikkelt de scantechniek zich vrij snel. Bij de ECT worden vanaf 2007 alle vrachtauto's door poortjes geloodst. Deze 40 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. Is er een gerede kans dat een container nucleair materiaal bevat, 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.

Analyse

Met andere diensten wordt informatie uitgewisseld, maar binnen de kaders én de beperkingen van de wettelijke grenzen. 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. 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.

Verkeersstromen: De Hoeksche Waard & Ochtendgloren

De Hoeksche Waard is een plattelandsgebied ingesloten tussen een paar snelwegen in de politieregio Zuid-Holland-Zuid. In een poging inbraken gepleegd door criminelen van buiten dit gebied tegen te gaan heeft het politiekorps besloten ANPR-apparatuur te installeren op de toegangswegen van het gebied. ANPR (Automatic Number Plate Recognition) is een systeem dat kentekens van voertuigen kan lezen en herkennen. Daarnaast is er gewerkt met een mobiele versie van het systeem. De monitoring heeft betrekking op alle passerende voertuigen maar slaat alleen aan 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. Het protocol geeft aan op grond van welke feiten het voertuig staande gehouden moet worden en welke actie ondernomen moeten worden.

Gedurende de testperiode werden 3507 hits gegenereerd op de vast opstelling en 211 op de mobiele opstelling van de ANPR: in beide gevallen ging het om minder dan 1 % van het totaal aantal passanten. Tijdens de proefperiode zijn de regels met betrekking tot privacy geformuleerd. Het OM geeft aan dat de inzet van ANPR ter uitvoering van de Wegenverkeerswetgeving is toegestaan en mag dienen als selectiemiddel in relatie tot geregistreerde veelplegers en dat de registratie van reguliere bewegingen is toegestaan. Of deze gegevens kunnen en mogen worden gebruikt als een systematische bron voor ondersteuning van de informatiepositie van de politie is nog een vraag die openstaat, gelet op de vigerende privacywetgeving en de standpunten van het College Bescherming Persoonsgegevens.

De aanleiding voor 'Ochtendgloren' lag in de toenemende criminaliteit op en rond autosnelwegen in het Oost-Nederland. Er werden in toenemende mate roofovervallen op geparkeerde vrachtwagens gepleegd. Deze vorm van mobiel banditisme werd voornamelijk uitgevoerd door criminele organisaties uit voorheen Oost-Europese landen die in Nederland criminele activiteiten plegen om vervolgens tegen het 'ochtendgloren' huiswaarts te keren. De KLPD is samen met de betrokken korpsen Twente, IJsselland en Gelderland gemeenschappelijke controles in gaan stellen. Deze controles zijn gericht op de criminaliteitsbestrijding op en rond de snelwegen waarbij geïntervenieerd wordt binnen de verkeersstroom. Bovendien is Ochtendgloren interessant omdat nadrukkelijk wordt samengewerkt met andere opsporingsdiensten, zoals overheidsinspectiediensten, Vreemdelingendienst en het Openbaar Ministerie, maar ook de Duitse politie, onder andere om een gemeenschappelijke informatiepositie op te bouwen.

Tijdens Ochtendgloren worden alle voertuigen gecontroleerd in het kader de Wegenverkeerswet (100% controle). Het bepalen of voertuigen al dan niet bijzondere aandacht verdienen gebeurd op basis van informatie uit verschillende databases van aanwezige opsporingsdiensten maar ook op basis van intuïtie en kennis van de politieagent en inspectiemedewerker. Tegelijkertijd wordt een mobiele versie van het ANPR ter plaatste ingezet waarbij aanvullende selectie plaatsvindt op basis van informatie uit andere databases. 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.

De locatie waarop de operatie Ochtendgloren gericht is, wordt ook gebruikt om de inzet van moderne technologieën zoals de mobiele scanmobiel 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" 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.

Analyse

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.

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.

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.

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

Schiphol: knooppunt van infrastructuren en stromen[12]

Schiphol is een knooppunt dat verschillende soorten infrastructuren met elkaar verbindt (lucht, weg, rail) en waarbinnen zich in ieder geval personen en goederenstromen bewegen. Schiphol is ook een knooppunt van activiteiten van uiteenlopende private en publieke organisaties. Het is behalve een efficiënt en multinodaal 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. De Schiphol Group is eigenaar en exploiteert Amsterdam Airport Schiphol volgens het concept van de 'Airport City', een dynamische omgeving waar mensen en bedrijven, logistiek en winkels, informatie en entertainment samenkomen en elkaar versterken.

Het instapproces voor passagiers wordt verregaand geautomatiseerd. In plaats van incheckbalies en -zuiltjes komen er 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 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. In 2015 moet 90% van de passagiers gebruikmaken van de selfserviceapparatuur.

Op Schiphol werken alle zestien toezichthouders samen in het Front Office Schiphol, dat vanaf juli 2008 operationeel is, als onderdeel van het rijksprogramma Vernieuwing Toezicht. Het is een coördinatie- en afstemmingsverband om de inspectielast te verminderen en de kwaliteit van het toezicht te verbeteren. Het motto is: 'Meer effect, minder last'. Er is één aanspreekpunt voor bedrijven op Schiphol, het toezicht wordt zo duidelijker. Het streven is dat bedrijven in de toekomst slechts eenmaal hun gegevens hoeven aan te leveren. Daarnaast worden gezamenlijke risicoanalyses gemaakt en er wordt een geïntegreerd toezichtprogramma opgesteld. In het Veiligheidsplatform Schiphol (VPS) werken alle bedrijven op Schiphol samen aan veiligheid. Het VPS is het aanspreekpunt voor het Front Office, mede vanwege veiligheidsrisico's die ontstaan op de raakvlakken tussen de verschillende afzonderlijke veiligheidsmanagementsystemen van bedrijven.[13]

Bij de bescherming tegen moedwillig gevaar, beveiliging en publieke veiligheid zijn politiek en bestuur nauw betrokken. Schiphol is sinds de wijziging van de Luchtvaartwet in 2003 wettelijk verantwoordelijk voor de uitvoering van preventieve beveiligingstaken op de luchthaven, maar onder controle van de overheid.[14] Particuliere beveiligingsbedrijven voeren de werkzaamheden uit. De Koninklijke Marechaussee controleert de naleving van de wetgeving en houdt toezicht op de uitvoering van de beveiligingsmaatregelen door de particuliere sector, vooral Amsterdam Airport Schiphol, luchtvaartmaatschappijen en luchtvrachtbedrijven. De Nationaal

Coördinator Terrorismebestrijding (NCTb) draagt onder meer zorg voor een adequate beveiliging van de burgerluchtvaart in Nederland en is tevens verantwoordelijk voor de systematische kwaliteitstoetsing van deze beveiliging.

Betrokken publieke en private partijen werken samen in het Platform Beveiliging en Publieke Veiligheid Schipol (opgericht op 25 januari 2005) om veiligheid en beveiliging in samenhang op te pakken. Een betere informatiepositie, ondersteund door techniek en integratie van activiteiten, maakt een gezamenlijke risicoanalyse mogelijk. Zo worden de gezamenlijke risico's in de beveiliging/veiligheid beter beheersbaar, worden doublures vermeden en kunnen partijen hun processen beter stroomlijnen. Het platform slecht grenzen tussen bedrijfsleven en overheid en maakt onderwerpen bespreekbaar. Win-winsituaties treden steeds gemakkelijker op, waardoor gezamenlijke initiatieven eerder van de grond komen. Voorbeelden zijn de inzet van camera's en de gezamenlijke controlekamer. De kosten worden gelijkelijk gedeeld met de overheid. 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 korte lijnen gecreëerd met 'Den Haag', waardoor politieke steun kan worden gemobiliseerd als dat nodig is.

Op Schiphol zelf is een netwerk van camera's operationeel. Deze camera's dienen voor een gezamenlijk gebruik van beveiligingsbeelden. 'A network is being set up in which all parties involved can track, register and reconstruct their security processes via cameras. Public and private partners can each use visual materials for observation, identification and investigation, each for its own specific purposes and responsibilities.'[15] Schiphol wil meer toezicht uitoefenen met behulp van camera's en wil minder personeel inzetten. 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. Dat maakt in principe een proactief gebruik mogelijk.

De maatregelen die in Nederland worden genomen ter beveiliging van de luchtvaart, zijn bijna allemaal gebaseerd op EU-beleid, via rechtstreekse verordeningen. Dit zijn de zogenoemde regels voor de beveiliging van luchthavens, die gelden voor alle lidstaten. Schiphol heeft een reeks van maatregelen genomen op het gebied van beveiliging van stromen. Enkele daarvan zijn geïmplementeerd, andere zijn nog in ontwikkeling.

Handbagage gaat bij de toegang door de röntgenapparatuur. Ruimbagage wordt automatisch gecontroleerd op explosieve en gevaarlijke stoffen en voorwerpen met een volautomatisch systeem dat vanaf 2002 in de EU wordt toegepast. Voordien werden koffers niet bekeken. Thans is er 100% bagagecontrole, een controle die sinds 2006 wereldwijd plaatsvindt.

Er wordt ook gebruikgemaakt van bodyscans, die gebruikmaken van röntgenstralen die door de huid gaan om ingeslikte goederen te traceren. De security scan wordt ingezet bij de security-en douanecontrole van passagiers. De security scan maakt op basis van weerkaatsing een beeld van de contouren van het lichaam. Zo wordt gezien of een passagier verboden voorwerpen op zijn of haar lichaam draagt, of dat er goederen gesmokkeld worden in of onder de kleding. Voorlopig mag de passagier kiezen of hij of zij gebruik wil maken van de security scan. Wil hij dat niet, dan doorloopt hij de gebruikelijke controle. Het Europees Parlement verklaarde zich begin december 2008 overigens tegen een verplichte invoering, vanwege de privacyaspecten en mogelijke risico's voor de gezondheid. De discussie over de bodyscans is weer opgelaaid naar aanleiding van de veredelde bomaanslag op eerste kerstdag 2009. Tijdens een vlucht van Schiphol naar Detroit probeerde een Keniaanse jongeman een bom tot ontploffing te laten komen die

door de detectiepoortjes van Schiphol was gekomen, maar die in een bodyscan wel gesignaleerd zou zijn.

De meeste personeelsdoorgangen zijn voorzien van apparatuur waarmee deze biometrische gegevens van de Schipholpas gecontroleerd kunnen worden. Op personeelspasjes staat een digitale afbeelding van de iris. Ook wordt gewerkt aan software die het mogelijk maakt om verdachte passagiers sneller en gemakkelijker op te merken, waardoor de betreffende persoon ook eerder en effectiever kan worden gevolgd. Er is een 100% controle op personeel.

Behalve voor passagiers en goederen is er op Schiphol ook aandacht voor stromen via het spoor en de weg. Met de Nederlandse Spoorwegen zijn proeven gedaan met gericht cameratoezicht op de treinperrons onder de terminal. Op die manier kan onbeheerde bagage tijdig worden gesignaleerd. 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. Er waren veel 'hits'. Parkeerterreinen worden bijvoorbeeld door criminelen gebruikt om gestolen auto's een tijdje weg te zetten. Vanaf 1 juli 2008 worden ook alle voertuigen die het platform van de luchthaven Schiphol betreden, onderworpen aan een beveiligingscontrole.

Analyse

De casus Schiphol laat zien dat een nodale oriëntatie leunt op de kwaliteit van de samenwerking en de afstemming tussen een veelheid van publieke en private actoren in netwerkachtige structuren, die deels nieuwe horizontale sturingsarrangementen vergen. Dat geldt ook voor internationale partijen, juist vanwege het landsgrensoverstijgende karakter van veel personen en goederenstromen en de internationale positie van Schiphol.

Publiek-private samenwerking op het bedrijventerrein Schiphol is een belangrijke succesfactor. Er is immers een samenloop van belangen en er zijn gemeenschappelijke belangen. Initiatieven van het platform hebben ook betrekking op een betere informatiepositie. Alle informatie van Vreemdelingenzaken, justitie, douane, rechtshandhaving, marechaussee, Defensie en KLM wordt in een servicebus opgeslagen en op basis van autorisatie kan iedereen de informatie eruit halen die hij nodig heeft, op basis van getekende contracten. Informatie kan immers voor meerdere doelen worden gebruikt. Het platform biedt een forum voor moeilijke onderwerpen, zoals de privacyproblematiek bij cameratoezicht en de kwaliteit van de informatie-uitwisseling. Het College bescherming persoonsgegevens is bij deze discussie betrokken.

Implicaties van de nodale oriëntatie

Technologische implicaties

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- en 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. In 'Politie in Ontwikkeling' wordt verwezen naar zogenaamde catch-ken of catch-scantechnieken, 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.

De nodale oriëntatie is sterk informatiegedreven. 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 hoeven te zijn. Er kan een kloof zijn tussen de theoretische en feitelijke kenmerken. Een verdenking betekent in dat geval dat aan bepaalde profielkenmerken wordt voldaan, maar nog niet tot een gerede verdenking hoeft te leiden. 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 van belang omdat 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.

Implicaties voor informatiepositie

De aanwezigheid van betrouwbare en geldige informatie is een belangrijke succesfactor in een nodale oriëntatie. Dat vereist op zijn beurt weer verbindingen voor het uitwisselen van informatie en het koppelen van databases, dus een betrouwbare infrastructuur. Onder voorwaarden moeten kennis en informatie worden gedeeld en uitgewisseld op basis van onderkenning van wederzijdse afhankelijkheid en onderling vertrouwen tussen partijen. Hiervoor kunnen protocollen worden ontwikkeld.

Een nodale oriëntatie veronderstelt een gedetailleerd beeld van kwetsbaarheden en een proactieve stijl van werken, waarin de verzameling en interpretatie van informatie – afkomstig vanuit verschillende bronnen – leidt tot het ontdekken van specifieke verbanden die als risicovol kunnen worden aangemerkt. Daarvoor is het opbouwen van een strategische informatiepositie noodzakelijk, gericht op het zoeken naar verbanden die risicovol zijn. Hiervoor moeten diverse informatiebronnen worden aangeboord en gekoppeld, zodat 'intelligence' ontstaat die proactief gebruikt kan worden voor het maken van risicoprofielen.

'Intelligence' ontstaat door de interpretatie van bestaande data door ze op een bepaalde manier met elkaar in verband te brengen. Intelligence verwijst naar informatie 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. Daarnaast moet meer met risicoprofielen worden gewerkt om te bepalen welk soort gedrag binnen een stroom of van bepaalde soorten van bewegingen binnen een knooppunt als verdacht moet worden beschouwd.

Implicaties voor de inzet van 'high tech'

De inzet van geavanceerde detectietechnologie (zoals intelligente camera's) is onontbeerlijk in een nodale oriëntatie. Hiermee verbonden is het gevaar van naïef instrumentalisme en een onvoorwaardelijk vertrouwen in de mogelijkheden en de zegeningen van de techniek. De feitelijke lekken in de beveiliging op Schiphol zijn een goed bewijs van de beperkingen van de techniek. Intelligent cameratoezicht kan een 'privacy enhancing technology' zijn, met een positief effect op de privacy, omdat alleen beelden worden opgenomen als dat nodig is op basis van detectie van bewegingen. Maar in het algemeen – en Schiphol is geen uitzondering – staat de proactieve aanwending van technologie nog in de kinderschoenen, ondanks alle ambities in deze richting.

Voor risicoprofilering is de kwaliteit van risicodefinitie, risicoanalyse en risico-evaluatie van belang. Het vereist ook kennis en vaardigheden om bepaalde patronen te zien, te herkennen, maar deze ook te relativeren (een statistisch verband hoeft nog geen 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 ook om vakinhoudelijke kennis van het reilen en zeilen binnen een stroom of binnen een knooppunt. Aan een aantal van deze voorwaarden wordt feitelijk nog (lang) niet voldaan.

Implicaties voor samenwerking en governance

Kenmerkend voor knooppunten en stromen is dat zij meerdere 'eigenaren' hebben, met soms uiteenlopende belangen. Een nodale oriëntatie veronderstelt samenwerking met andere publieke en private partijen. In een netwerksamenleving betekent de focus op knooppunten, infrastructuren en stromen per definitie dat ook een goede internationale samenwerking uiterst belangrijk is. Een goede samenwerking, gebaseerd op het onderkennen van wederzijdse afhankelijkheid en vertrouwen, is een van de meest vitale factoren. Een adequate aanpak van veiligheid vereisen coproductie en van 'security governance', binnen veiligheidsnetwerken van publieke en private actoren. Per stroom, knooppunt of infrastructuur wordt de vraag relevant waar het primaat van de opsporing ligt en wat dit betekent voor de rol van de politie. Dat veronderstelt een gezamenlijke probleemdefinitie en -oplossing evenals coproductie met burgers en andere instellingen. Op het niveau van stromen is het moeilijk verbindingen te leggen met de burgers. Dat is anders als het hun directe leefomgeving betreft. Een nodale oriëntatie impliceert bij uitstek het accepteren dat de politie (slechts) een van de actoren is op het gebied van veiligheid en niet noodzakelijkerwijs de dominante actor.[16]

Conclusies

Politieke en maatschappelijke effecten

De inzet van technologie en de ontwikkeling van de informatiestrategie heeft politieke en maatschappelijke effecten. Technologie is een politiek instrument 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.[17] Technologie is daardoor ook een kneedbaar.[18] Ten tweede wijzen anderen erop dat technologie per definitie gericht is op controle en disciplinering. Bij ICT wordt het inherente controlepotentieel nog eens versterkt, omdat het gebruik van ICT overal digitale sporen achter laat, waardoor het gedrag van mensen veel gemakkelijker kan worden gereconstrueerd of worden gevolgd.[19] 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.

Normatieve aspecten

Een belangrijk aandachtspunt in de normatieve discussie over de nodale oriëntatie is de mate waarin de concentratie van informatiemacht 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?[20] Binnen deze normatieve discussie moet dan een aantal afwegingen gemaakt worden.

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. De persoonlijke levenssfeer kan worden aangetast door het volgen van personen c.q. het monitoren van het gedrag van personen met camera's, door het ontsluiten van data in publieke en private databestanden en door de interpretatie van bestaande databestanden die met elkaar in verband worden gebracht of geaggregeerd.

Een tweede afweging betreft de afweging tussen vrijheid en efficiency. De kosten die moeten worden gemaakt om het gedrag van bepaalde personen transparant te maken moeten 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. Dit betekent in veel gevallen dat er niet op voorhand sprake is van een bepaalde verdachte. In veel gevallen gaat het om het volgen en/of ontanonimiseren van grote groepen van niet-verdachte personen die echter als 'verdachte' worden aangemerkt. Verdachten en niet-verdachten worden dan als gelijk behandeld omdat zij zich binnen een bepaalde stroom of knooppunt bewegen. 'Gelijke behandeling' is verdedigbaar op grond van de in het geding zijnde risico's: een afweging die echter alleen maar inhoud krijgt wanneer ze geconcretiseerd wordt 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.

Belangrijk is dat in nieuwe arrangementen die ontstaan rondom de nodale oriëntatie aandacht is voor de gezaghebbende toebedeling van waarden die daarin plaatsvindt om een bepaald veiligheidsniveau te kunnen garanderen. De vraag is of er een balans bestaat tussen de bijdrage van technologietoepassingen aan het opsporen van bedreigingen van de veiligheid, en rechten en plichten ten aanzien van de bescherming van de persoonlijke levenssfeer. Essentieel is dat transparant is wie de afweging maakt, wie hiervoor verantwoordelijk is, hoe deze afwegingen worden gemaakt, en hoe zij getoetst worden.

De concentratie van informatiemacht die ontstaat wanneer bestanden aan elkaar worden gekoppeld en het gedrag van personen wordt gevolgd, vereist daarnaast een systeem van controle en verantwoording, van 'checks and balances', om de kans op machtsmisbruik te voorkomen.[21] Tevens dient te worden gewaakt voor de onbedoelde gevolgen van de inzet van technologie. Technologie is een kneedbaar instrument dat bepaalde belangen en waarden belichaamt, een eigen dynamiek genereert en daarmee ook onbedoelde effecten. Ook hier is de normatieve vraag gerechtigd: wie controleert de inzet van technologie en hoe?

Over het privacyvraagstuk dient een intensieve publieke en politieke dialoog te worden gevoerd, gelet op de grote verschillen van inzicht die er bestaan tussen verschillende partijen. Het is te belangrijk om uitsluitend over te laten aan opsporingsinstanties. Deze discussie wordt bij

voorkeur niet gevoerd in termen van 'wij' en 'zij', waarbij technologische mogelijkheden, het maatschappelijke probleem of de privacybescherming verabsoluteerd dan wel gebagatelliseerd worden. Van belang is een zakelijke discussie te voeren en nadrukkelijk afweging tussen politieke waarden te laten plaatsvinden 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.

Bibliografie

Bannister, F. (2005). The panoptic state: Privacy, surveillance and the balance of risk. *Information Polity , 10* (1-2), 65-80.

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

Bekkers, V. (1998). *Grenzeloze overheid.* ALphen aan de Rijn: Samson.

Bekkers, V., van Sluis, A., & Siep, P. (2006). *De Nodale Oriëntatie van de Nederlandse Politie: over ciminaliteitsbestrijding in de netwerksamenleving.* Rotterdam: Center for Public Innovation.

Bijker, W. E., Hughes, T. P., & Pinch, T. (1987). *The social construction of technological systems: New Directions in the Sociology and History of Technology.* Cambridge: Cambridge University Press.

Bruul, v. I., Damkat, P., Dijk, v. W., Frenken, W., & Haasteren, v. P. (2008). *Leiderschap als knooppunt. Een studie naar de rol van leiderschap in de diffusie van nodale oriëntatie binnen de Nederlandse politie.* Warnsveld: School voor Politie Leiderschap.

Castells, M. (1995). *The rise of the netwerk society.* Oxford: Blackwell.

Duivenboden, v. H. (1999). *Koppeling in uitvoering.* Delft: Eburon.

Ferwerda, H., & Adang, O. (2005). *Hooligans in beeld.* Apeldoorn/Arnhem: Advies- en onderzoeksgroep Beke.

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

Havenbedrijf Rotterdam,. (2009, september). Opgehaald van Over het havenbedrijf: http://www.portofrotterdam.com/nl/home/

Inspectie Verkeer en Waterstaat. (2009). *Vernieuwing toezicht: Toezichtplan Vervoer over Water 2009.* Den Haag: Koninklijke De Swart.

Inspectieloket. (2009, september). *Vernieuwing Toezicht*. Opgehaald van Inspectieloket: inzicht in inspectiewerk: http://www.inspectieloket.nl/vernieuwing_toezicht/

Kerckhove, d. D. (1996). *Gekoppelde intelligentie.* Ede: SMO.

Mul, d. J. (2002). ICT de baas? In P. Frissen, *Internet en openbaar bestuur.* Tilburg.

PIO. (2005). *Politie in ontwikkeling. Visie op de politiefunctie.* Den Haag: NPI.

Schiphol. (2008). *Eenduidig Toezicht Schiphol.* Hoofddorp: Amsterdam Airport Schiphol.

Schiphol Group. (2006). *Corporate responsibility in 2006*. Amsterdam: Amsterdam Airport Schiphol.

Schiphol Group. (2009). *Verantwoord ondernemen op Schiphol.* Amsterdam: Amsterdam Airport Schiphol.

Shearing, C. (2005). Nodal security. *Police Quarterly , 8* (1), 57-63.

Sluis, v. A., & Bekkers, V. (2009). De ontknoping van de nodale oriëntatie: op zoek naar randvoorwaarden en kritische factoren. *Justiële verkenningen , 35* (1), 78-92.

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

Tilley, N. (2003). Community policing, problem-oriented policing and intelligence-led policing. In T. Newborn, *Handbook of Policing.* Devon: Willan Publishing.

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

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

---

[1] PIO (2005)

[2] PIO (2005: 87)

[3] PIO (2005)

[4] Castells (1995)

[5] Beck (1999)

[6] Ferwerda & Adang (2005)

[7] Havenbedrijf Rotterdam (2009)

[8] Inspectie Verkeer en Waterstaat (2009)

[9] Inspectieloket (2009)

[10] http://www.douane.nl/zakelijk/ecustoms/ (januari 2010)

[11] www.cpb.gov 2002 (september 2009)

[12] Voor deze casus is intensief gebruik gemaakt van Van Sluis & Bekkers (2009)

[13] Schiphol (2008)

[14] Schiphol Group (2009)

[15] Schiphol Group (2006)

[16] Shearing, (2005): 58.

[17] Bijker, Hughes, & Pinch (1987)

[18] Winner (1988)

[19] Frissen (1989)

[20] Mul (2002)

[21] Bekkers (1998)