POLITIE

Politieacademie

Informatiegestuurd politiewerk in de praktijk

Redactie:
Mariëlle den Hengst,
Tjeerd ten Brink
en Jan ter Mors

« waakzaam en dienstbaar »

Informatiegestuurd politiewerk in de praktijk

Informatiegestuurd politiewerk in de praktijk

Redactie:
Mariëlle den Hengst, Tjeerd ten Brink en Jan ter Mors

Vakmedianet, Deventer

Samensteller(s) en de uitgever zijn zich volledig bewust van hun taak een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kunnen zij geen aansprakelijkheid aanvaarden voor onjuistheden die eventueel in deze uitgave voorkomen.

De uitgever heeft getracht alle rechthebbenden op copyright van afbeeldingen en teksten te bereiken. Zij die desondanks menen aanspraak te kunnen maken op deze rechten, kunnen zich tot de uitgever wenden.

ISBN 978 94 6350 006 7
NUR 801

Eerste druk, eerste oplage 2017

Inhoud

Voorwoord

Mariëlle den Hengst, Tjeerd ten Brink en Jan ter Mors

In 2008 werd het *Nationaal Intelligence Model* 'Waakzaam van Wijk tot Wereld' door de toenmalige korpschefs vastgesteld. Tegelijkertijd verscheen het boek *Intelligencegestuurd politiewerk (IGP)* van Nicolien Kop en Peter Klerks met de uitgangspunten van IGP. Kop en Klerks schrijven in hun voorwoord dat 'IGP een manier van denken, van werken en van doen is. Het is belangrijk te beseffen dat IGP een van de grote ontwikkelingen is die binnen politieland gaande zijn. Een ontwikkeling met veel impact op de organisatie en sturing van én door de politie. Verdere ontwikkeling van het concept zal de komende jaren dan ook zeker plaats vinden'.

Deze voorspelling is zonder meer uitgekomen. Wie had in 2008 voor mogelijk gehouden wat we voor het politiewerk vandaag de dag allemaal tot onze beschikking hebben? Smartphones, tablets, big data, *data science, predictive* technieken... De afgelopen jaren is er veel tot ontwikkeling gekomen. Het was dan ook tijd om een nieuw en actueel IGP-boek te maken.

Als dit boek *Informatiegestuurd politiewerk in de praktijk* iets laat zien, dan is het wel dat de ontwikkelingen niet vanuit een ivoren toren plaats hebben gevonden, maar in de praktijk van het politiewerk tot wasdom zijn gekomen. Precies daarom hebben wij ervoor gekozen om dit boek een boek onder redactie te laten zijn. Het bevat de uiteenlopende bijdragen van een groot aantal mensen die informatiegestuurd politiewerk in de praktijk uitvoeren en ontwikkelen.

Wij hebben genoten van alle kennis, kunde en passie die de auteurs van dit boek laten zien. Dank en hulde voor de inzet van de auteurs om de inhoud te leveren. Tijdens het lezen en bespreken van de (concept)hoofdstukken hebben ook wij weer meer geleerd over het vak, vooral over alle mogelijke verbindingen die tussen onderwerpen uit de verschillende hoofdstukken te maken zijn.

Alles overziend hebben we ons afgevraagd of we als redactie nog een slimme analyse of een wijze beschouwing van het geheel zouden moeten meegeven. Dit doen we niet – in elk geval niet op papier. De lezer is veel beter in staat om dat zelf te doen. Door te lezen, te bladeren, te combineren en vanuit eigen vakmanschap en motivatie te leren. Het zou bovendien de indruk kunnen wekken dat we als redactie denken te gaan over IGP in de praktijk. En dat is natuurlijk niet zo. Uiteindelijk bepalen de vakmensen hoe het verder gaat met dit vak, met deze manier van denken, van werken en van doen. Dat het verder gaat met de ontwikkeling van IGP, daar zijn we van overtuigd.

Als redactie blijven we echter niet op onze handen zitten. Zoals gezegd, het vak ontwikkelt zich. Soms gaat dat best snel. Het boek is dus nooit af. Binnen het gegeven tijdsbestek is het bovendien niet gelukt om alle onderwerpen volledig af te dekken. Wij kunnen ons daarom goed voorstellen dat de professionals uit onze *intelligence community*

zich na het verschijnen van dit boek blijven inzetten om de verschillende onderwerpen inhoudelijk te verdiepen en ook onderwerpen aan het boek toe te voegen om anderen daar weer deelgenoot van te kunnen maken. Zo is er zeker nog meer te vertellen over internationale informatiecoördinatie, gaan de ontwikkelingen van sociale media en real-time intelligence ons nieuwe kansen en uitdagingen bieden en gaat business intelligence vast en zeker breder voet aan de grond krijgen.

Wat ons betreft mogen er nog veel meer praktijkvoorbeelden worden gedeeld, ter inspiratie en om lering uit te trekken. Om dit te ondersteunen, is er de Community of Intelligence.[1] Hier treft u niet alleen de volledige inhoud van dit boek, ook kunt u via deze site zelf bijdragen aan de inhoud en debat van het vak van informatiegestuurd politiewerk in de praktijk. Als redactie zullen wij op de community nieuwe bijdragen aan het IGP-boek en de discussies daarover actief volgen. We dagen de lezer uit met ons de werking van IGP in de politiepraktijk verder te brengen en het vakgebied verder te ontwikkelen. We hopen u daar te treffen!

Waarom dan toch een papieren boek, als alles ook digitaal beschikbaar is? Nadeel van een papieren boek in deze snel veranderende maatschappij is dat wat gisteren toekomst was, vandaag gewoon in werking is en morgen al aan de historie toegevoegd kan worden. Gelukkig gaan de veranderingen iets minder snel en is de houdbaarheid van het boek langer. Dit boek gaat bovendien voor een groot deel over achterliggende principes en uitgangspunten, die minder snel veranderen. Het IGP-concept is van alle tijden, de technologie om de principes in te vullen en de kennis die daarvoor nodig is, veranderen snel. Tegelijkertijd kunnen we niet ontkennen dat een papieren boek op gespannen voet staat met de veranderingen in de praktijk, daarom hebben we ook een dynamisch platform gekoppeld aan dit boek. En soms is het gewoon fijn om een boek in je handen te hebben of om er een in de handen te drukken van een leuke collega.

Het is een boek dat je niet per se van voor naar achter hoeft te lezen. De losse hoofdstukken zijn ook op zich te lezen. Immers, IGP raakt aan alles, maar dat betekent niet dat iedereen ook alles van IGP hoeft te weten. Gevolg is wel dat je af en toe herhaling aantreft. We hebben de hoofdstukken in dit boek in drie delen gegroepeerd. De ontwikkelingen in het vakgebied worden duidelijk in 'the future is now'; nieuwe loten ontwikkelen zich aan de boom: real-time informatie ondersteund politiewerk, vorderingen in predictive policing, opsporen met big data enzovoort. In de 'werking van IGP' zien we de diversiteit en brede verankering van IGP in het politiewerk terug. Het gaat om de dagelijkse briefing en debriefing van het werk, informatiecoördinatie op landelijk geprioriteerde thema's, samenwerking met partners, juridische en ethische kaders, analyse en inwinnen van informatie in het criminele milieu. Hieruit blijkt wel dat IGP in de praktijk soms ingewikkelder, soms diffuser is dan het in 2008 nog leek. En tegelijkertijd staan de fundamenten die in 2008 werden beschreven nog overeind. In 'IGP als politiestrategie' belichten we deze fundamenten.

---

1 De Community of Intelligence (CoI) is een platform voor intelligenceprofessionals om met elkaar kennis te delen over informatiegestuurd werken om zo het vakgebied verder te ontwikkelen. De CoI bestaat sinds 2011. De CoI is via internet te bereiken op het volgende adres: https://dw.politieacademie.nl/sites/coi. Via de politiewerkomgeving is het adres: http://dw.politieacademie.politie.nl/sites/coi.

We hopen dat het boek je helpt bij het informatiegestuurd werken. We schrijven niet over hoe IGP zou moeten zijn. Vanuit de bedoeling laten we zien hoe het in de praktijk werkt. We wensen je veel informatie en inspiratie toe!

Mariëlle den Hengst, Tjeerd ten Brink en Jan ter Mors

Deel I
IGP als politiestrategie

1 Van beheer(sing) naar flexibiliteit: in gesprek met politiechefs over IGP

Marjan Hanrath

Figuur 1.1 Peter Holla, Pieter-Jaap Aalbersberg en Paul van Musscher

Waar stonden we met het informatiegestuurd werken in 2009, waar staan we nu en wat is de rol van informatie in 2025?[1] Dat zijn de vragen die we voorleggen aan Pieter-Jaap Aalbersberg, Paul van Musscher en Peter Holla – drie politiechefs die vanuit verschillende invalshoeken bijdragen aan de ontwikkeling van het informatiegestuurd werken.

Paul trapt af: 'Van informatiegestuurd werken was in 2009 niet echt sprake, informatie kwam ongestructureerd binnen. We maakten niet echt onderscheid tussen operationele, tactische en strategische informatie. Inmiddels hebben we voorzichtig stappen voorwaarts gezet, maar we zijn er nog niet. Ik maak wel een verschil tussen het operationeel aansturen van het dagelijkse politiewerk met veredelde informatie, en het probleemgericht werken waarvoor – in het licht van de signalerende en adviserende taak van de politie – strategische en tactische informatieproducten worden gemaakt die leidend zijn in de aanpak van de veiligheidsproblemen samen met partners. We zijn wat dat betreft nog niet op het niveau dat we de informatie en analyses genereren waarmee we met partners "informatiegestuurde veiligheidszorg" kunnen bedrijven.

In de toekomst zullen we meer en meer informatie verzamelen, bewerken en analyseren vanuit de "1 overheid"-gedachte. We kunnen meer dan in 2009, maar het vraagt ook

1 In 2009 verscheen in opdracht van het toenmalige programma Intelligence de *Doctrine intelligencegestuurd politiewerk* van Nicolien Kop en Peter Klerks.

meer van onze systemen, de verwerking en opslag van informatie, de *awareness* voor privacy. We zijn nog te traditioneel in ons denken over wat het betekent om te werken met bijvoorbeeld open-sourcekennis, met partners, met geanalyseerde informatie ofwel intelligence, met big data. Wat doet dit voor onze financiering, voor onze informatievoorziening (IV)? We hebben nooit een nieuwe nulsituatie gemaakt met elkaar: wat betekent het een politie te zijn als informatieverwerkend bedrijf?'

Collectieve kwaliteit

Pieter-Jaap vult aan: 'We zijn tien jaar geleden begonnen en hebben veel bereikt, welk werkproces heeft in een zo korte tijd al een tweede boek opgeleverd over de ontwikkeling? Onze omgeving verandert snel, mensen werken nu anders met informatie dan tien jaar geleden. Onze informatieorganisatie als structuur is goed neergezet. We zijn hierin verder dan andere landen.

Ik zie nu drie grote bewegingen. Ten eerste: mensen zijn ons belangrijkste kapitaal, en data komen voor de politie op de tweede plaats. Dat zeggen we wel, maar dat zien we in de politiepraktijk nog onvoldoende. Want als dit waar is, is ook de kwaliteit van data van groot belang. Ten tweede: het waarnemen en vastleggen is een kerntaak van politiemensen, maar dat hebben we in de loop van de tijd wel laten verworden tot administratieve last. Toch is het een essentieel onderdeel van onze business die vraagt om hoge kwaliteit van handelen. Ten derde: het gebruik van de term informatiegestuurd politiewerk (IGP) maakt dat we de politie daarvan apart zetten en ik denk dat dit niet meer kan.

De nieuwe informatiesturing gaat nu naar een *next level*: sneller, beter, dynamischer en real-time. Het is nodig dat we data steeds meer als collectieve kwaliteit gaan zien. Mijn droom voor het derde boek is dat het dan realiteit is dat de wijkagent de noodhulpcollega's aanspreekt op eerdere mutaties, of andersom: dat de noodhulp de wijkagent aanspreekt op de opbouw van dossiers.'

Er ontstaat een discussie over het belang van de kwaliteit van informatie en de wijze waarop onze leidinggevenden en organisatie de medewerkers kunnen faciliteren om goed te muteren en informatie te verwerken. De politiechefs constateren dat het gaat om een andere manier van denken: als je de juiste boef vangt, vinden we dat allemaal belangrijk, als je op iets ingewikkelds beslag legt, vinden we dat al minder van belang, als jouw informatie gebruikt wordt in het oplossen van een zaak, dan hoor je dat niet terug.

Leiden we onze mensen voldoende op om professioneel informatie te verwerken? Weten zij welke consequenties het heeft als er niet goed of niet voldoende gemuteerd wordt? Is de ondersteuning door informatie- en communicatietechnologie (ICT) voldoende om medewerkers hun werk te laten doen?

Paul: 'We repareren ons suf. We moeten leren de dingen goed te doen.'

Peter: 'We accepteren nog steeds dat het niet goed loopt. De zorg is niet zozeer dat we geen nieuwe dingen kunnen bouwen, maar dat we de bestaande mogelijkheden onbenut laten.'

Pieter-Jaap: 'Weg van de zesjescultuur, waarnemen en vastleggen zijn een topprestatie in je vakmanschap.'

De politiechefs constateren dat de snelheid op de ontwikkeling van *business-intelligence*-voorzieningen 'buiten' hoger ligt dan bij de politie. Maar er komen veel jonge mensen onze organisatie binnen die goed om weten te gaan met de beschikbare technieken en informatie.

Wat is de huidige betekenis van IGP voor de opsporing? En hoe bepalend wordt het voor de toekomst?

Peter: 'Wat de bewijsvoering betreft zagen we dat we vroeger vooral steunden op kennis en ervaring in de tactische opsporing, in een volgende fase kwam forensisch onderzoek, en dan nu IGP.'

Pieter-Jaap wil loskomen van de kolommen van opsporing en handhaving: 'Informatie is er niet alleen voor de politie, maar ook van en voor haar partners. Ik verwacht dat we in de toekomst een geïntegreerde informatieomgeving hebben van politie met gemeenten, misschien enige private partijen en andere partners. De P van IGP valt weg, de informatie is van ons allemaal. Met de partners moeten we samen het risico- en veiligheidsdossier organiseren. Informatie en *intelligence* zijn geen proces "ernaast", het is het hart van het werk.

We zien bij de Raffinaderij (zie hoofdstuk 20 Big data) al dat opsporing en intelligence volledig samengaan, dat mensen die uit de informatieorganisatie komen samen met rechercheurs in de opsporing werken zonder dat die domeindiscussie er is.'

Paul: 'Sterker nog, deze domeinen worden elk voor zich informatiegenererende entiteiten. De informatie gaat booming worden door het kunnen koppelen van systemen en het hanteren van nieuwe technologieën die data vertalen naar informatie. We werken straks niet meer in een gebouw, we krijgen de informatie als we aanrijden en analyseren sporen op de PD. Veel tussenschakels zullen verdwijnen.'

Pieter-Jaap voegt toe: 'Een klassiek Team Grootschalige Opsporing hebben we dan niet meer. Belangrijk worden big data, met de goede mensen met de juiste kennis die informatie kunnen valideren en betekenis kunnen geven.'

Anders organiseren

Peter constateert nog een fundamenteel gevolg: 'Klassiek beschrijven wij de werkprocessen op basis waarvan we de opleidingen inrichten en mensen instrueren. We gaan ernaartoe dat de informatie- en communicatietechnologie onze werkprocessen stuurt. De informatie- en communicatietechnologie geeft de mogelijkheid altijd te zien waar onze mensen zijn, of hoe bijvoorbeeld de stressfactor is – dat zal de kennis bepalen die we onze collega's ter plaatse meegeven en hoe zij optreden.'

Paul ziet als belangrijke ontwikkeling dat burgers onze oren en ogen willen zijn en actief willen bijdragen aan de veiligheid. In de toekomst zal informatie dan ook niet slechts beschikbaar zijn voor politie en gemeenten, de informatie gaat de wijken en buurten in: 'Maar wij bouwen onze organisatie nog op beheer(sing) in plaats van kaderstelling, ruimte en flexibiliteit.'

Voor Peter liggen de geschetste ontwikkelingen gevoelsmatig niet ver weg: 'We zijn nu allemaal nog erg voorzichtig, laten ons remmen door mogelijke belemmeringen in wetgeving en structuren. Wat op straat normaal is, pakken wij bureaucratisch en gestandaardiseerd op.'

Toch zien de politiechefs ook de creatieve politiemensen die het werk anders organiseren. Teams beheren hun eigen Facebook-accounts, onder eigen verantwoordelijkheid. Dit gaat eigenlijk nooit mis. Mensen zien kansen en gaan deze benutten. Dit gaat zich verder ontwikkelen. Waar de politie nog niet goed in slaagt, is om iedereen op het juiste moment en de juiste plaats te voorzien van alle benodigde informatie. Dit vraagt om versnelling van de ontwikkeling die het korps nu doormaakt.

Hoe komen tot die versnelling?
Pieter-Jaap: 'Het is het informatiebewustzijn dat Paul eerder noemde, het bewustzijn van het belang van informatie voor de organisatie. We moeten daarbij onze politiemensen beter faciliteren, maar ook beter selecteren op ICT-vaardigheden. Weg van de bureaucratie en standaardisering moeten we naar een architectuur met meer kaders en ruimte voor politiemensen om zaken uit te proberen, en meer verbinding te zoeken met partners, ook op het gebied van ICT. Dit vraagt dat we in de business-intelligencestrategie (zie hoofdstuk 22 De business-intelligencestrategie in de politiepraktijk) niet alleen inzetten op beheersing, maar ook op vormen van flexibiliteit.'

Kent deze wijze van werken ook grenzen? Bijvoorbeeld bij de veelgenoemde privacyregelingen?
Pieter-Jaap: 'De politie moet ook de privacy van burgers beschermen. Privacy is geen grens, maar een waarde van het vak. Eigenlijk is het raar dat burgers de overheid verdenken van privacyschendingen.'

Peter: 'De politie als hoeder van de Wet politiegegevens (Wpg) (zie hoofdstuk 5 De Wpg). Maar de toegang tot alle informatie in de organisatie kan werken als bij het binnenkomen in een snoepjeswinkel: je gaat snoepen van al dat lekkers.'

Pieter-Jaap: 'Maar er staat in dit geval iemand aan de toonbank die dat controleert. Wij moeten met informatie net zo zorgvuldig omgaan als met geweld. Net zoals we bij het gebruik van predictive policing (zie hoofdstuk 21 Predictive policing) controleerbaar moeten zijn op de algoritmen die we gebruiken. De politie mag geen black box zijn, wij staan ook voor privacy.'

Paul: 'De begrenzing ligt bij de *rule of law* en de waarden van het vak. De waardendiscussie is complex, en het omgaan met informatie zal altijd om afwegingen vragen. Politiemensen wordt geleerd geweld proportioneel en subsidiair te gebruiken, zij worden daarin opgeleid en getraind. Hetzelfde geldt in feite voor het gebruik van informatie in de politiepraktijk.'

Vakmanschap

Paul: 'Het is, ook op het gebied van informatie, op de grens van je kunnen opereren, en vraagt het uiterste van je vakmanschap. Van ons allemaal.'

Pieter-Jaap als laatste: 'Daar kunnen we nog grote stappen in zetten, maar uiteindelijk is informatiesturing ook dat we onze collega's ter plaatse in staat stellen betere besluiten te nemen op basis van vakkennis en informatie.'

2 Informatiegestuurd werken en business intelligence

Tjeerd ten Brink, Jan ter Mors en Mariëlle den Hengst

De politie ontvangt, verwerkt en gebruikt informatie om haar werk te doen. Dat doet de politie altijd al en dat zal zij blijven doen: veiligheidsproblemen aanpakken op basis van correct ontsloten informatie, scherpe analyse en uitwisseling van gegevens met partners. Een politie die toegang heeft tot alle relevante data, en deze kan combineren, veredelen en analyseren, ziet beter wat er aan de hand is en is beter in staat om daarop in te spelen.

Dit hoofdstuk gaat over principes die aan de basis liggen van informatiegestuurd politiewerk (IGP). Daarbij wordt ook uitgebreid ingegaan op de rol van *business intelligence* (BI) in het politiewerk. IGP en BI zijn zijden van dezelfde medaille: hoe de politie met informatie werkt.

2.1 Informatiegestuurd politiewerk: wat is het?

Informatiegestuurd werken heeft een aantal basisprincipes, of het nu gaat om briefen, internationaal informatie uitwisselen of opschalen. Het kennen van deze principes stelt je in staat informatiegestuurd werken te herkennen, toe te passen en te verbeteren.

Het gebruiken van kennis en informatie bij besluitvorming is al eeuwenoud. Plato schreef al dat een goed besluit gebaseerd is op kennis, en niet op cijfers. De afgelopen decennia heeft informatiegestuurd werken een grote vlucht genomen. Een aantal technologische ontwikkelingen heeft daaraan flink bijgedragen. De ontwikkeling van de computer heeft daarvoor de basis gevormd. Het steeds goedkoper, kleiner en krachtiger worden van de computer en de introductie van de personal computer hebben in de jaren zeventig geleid tot de opkomst van informatiesystemen die besluitvormers ondersteunen. Meer recent is de explosie van de hoeveelheid data in onze informatiemaatschappij de belangrijkste ontwikkeling. De afgelopen jaren heeft de hoeveelheid gegevens zich per jaar verdubbeld en voor de komende jaren wordt daar geen verandering in verwacht. Sociale media, mobiele sensoren en zogenoemde *wearables* dragen allemaal bij aan die explosie van informatie. Hierdoor spreken we steeds vaker van big data.

Gepaard aan deze dataexplosie worden tools en technieken om deze data te analyseren steeds beter en met een hoge snelheid ontwikkeld. Met *datamining*, *data science* en *data analytics* kunnen tegenwoordig verbanden in de informatie verkend worden. Krachtige tools om deze verbanden te visualiseren maken ook dat deze inzicht en vooruitzicht bieden: hoe zit het vraagstuk in elkaar en wat kunnen we verwachten? Zie ook hoofdstuk 20 Big data.

Figuur 2.1 Informatiesamenleving

Dergelijke ontwikkelingen hebben gemaakt dat informatiegestuurd werken ook bij de politie is wat het nu is. Ontwikkelingen die ook in de toekomst in hoog tempo door zullen gaan en grote invloed zullen hebben op de manier van werken in het veiligheidsdomein en de positionering van de verschillende relevante instituties op dit gebied in de samenleving.

Maar of je nu met eenvoudige overzichten inzicht krijgt in een situatie, zoals een hotspot-kaart die aangeeft op welke plaatsen en tijden woninginbraken hebben plaatsgevonden, of geavanceerdere tools daarvoor tot je beschikking hebt, zoals het Criminaliteitsanticipatiesysteem (CAS) dat op basis van een scala aan factoren een verwachting geeft waar de komende diensten woninginbraken plaats gaan vinden: de basisprincipes van informatiegestuurd werken blijven hetzelfde (zie hoofdstuk 21 Predictive policing).

Definities van gegevens, informatie en kennis

Gegevens:	vastgelegde waarnemingen (menselijke en uit sensoren)
Informatie:	gegevens die betekenis hebben
Kennis:	inzichten door informatie te combineren, in context te plaatsen en eerdere ervaringen eraan te koppelen

In het bedrijfsleven staat het informatiegestuurd werken bekend als BI. Shell doet niet aan informatiegestuurd olieboren en Ford doet niet aan informatiegestuurd auto's produceren, maar zij doen beide wel aan BI (zie paragraaf 2.5 Informatiegestuurd politiewerk en business intelligence). Bij de politie kreeg dit begrip eerst als *intelligence-led policing* vorm, om te beginnen in Kent (Verenigd Koninkrijk) ongeveer twintig jaar geleden. En daarna ook

bij de politie in Nederland, eerst nog beperkt tot 'informatiegestuurde opsporing' (zie hoofdstuk 3 Kennis voor politiewerk: een blik vanuit het recente verleden).

In 2005 is in het rapport *Politie in ontwikkeling* door de Raad van Hoofdcommissarissen een visie neergelegd waarin wordt onderstreept dat informatiegestuurd werken niet beperkt moet blijven tot de opsporing, maar verder uitgebouwd moet worden naar politiezorg in de breedste zin van het woord.[1] Begin 2008 is intelligencegestuurd werken door de korpschefs tot strategisch beleid verheven, en zij werden daarin gesteund door de politieministers, het bestuur en het Openbaar Ministerie (OM). *Intelligence* is in 2008 in het *Nationaal Intelligence Model* (NIM) van de politie gedefinieerd als 'geanalyseerde informatie en kennis op grond waarvan beslissingen over de uitvoering van de politietaak worden genomen'.[2] Met de vorming van de nationale politie in 2013 is informatiegestuurd werken niet meer als aparte strategie benoemd, maar is IGP verweven in de hele organisatie en in alle processen. IGP zit als het ware in het DNA van het ontwerp en de inrichting van de politie. Hiermee is ook meteen duidelijk dat informatiegestuurd werken over het volledige spectrum van politiewerk gaat, en niet alleen over organisatieonderdelen zoals de informatieorganisatie of de IV-organisatie (informatievoorziening) zoals we die nu kennen.

Definitie van informatiegestuurd werken bij de politie
Informatie en kennis verzamelen en analyseren om op basis van overzicht, inzicht en vooruitzicht beslissingen te nemen over de aanpak van veiligheidsproblemen

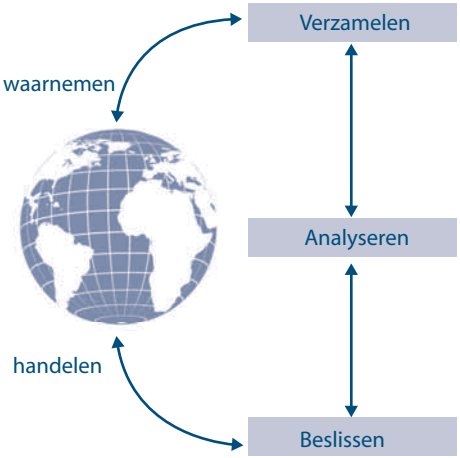
In de definitie van informatiegestuurd werken staan enkele begrippen centraal. Het gaat om het nemen van besluiten, het gaat om het analyseren en het gaat om het verzamelen en dus vastleggen van informatie. Na het verzamelen van gegevens en informatie kunnen deze geanalyseerd worden. Bij analyse worden verbanden gelegd tussen losse elementen om zo, aan de hand van informatie, overzicht, inzicht en vooruitzicht te creëren in de situatie of rond het vraagstuk dat speelt. De laatste stap is het op basis van de geanalyseerde informatie nemen van een beslissing, het door laten klinken van de informatie in de beslissing over de aanpak van een veiligheidsprobleem. Zonder het daadwerkelijk beïnvloeden van de besluitvorming zijn de processen verzamelen en analyseren voor niets geweest. Zonder de juiste analyses en duiding krijgt de informatie onvoldoende of misschien wel verkeerde betekenis. En zonder toegang tot de juiste informatie is de analyse onvoldoende effectief.

Alle drie de begrippen zijn dus belangrijk om van goed informatiegestuurd werken te kunnen spreken. In de volgende paragrafen worden deze afzonderlijk beschreven.

---

1 Projectgroep Visie op de politiefunctie, Raad van Hoofdcommissarissen, *Politie in ontwikkeling: visie op de politiefunctie*. NPI, Den Haag 2005.

2 Strategische beleidsgroep intelligence, *Waakzaam tussen wijk en wereld: Nationaal Intelligence Model Sturen op en met informatie*. 2008.



Figuur 2.2 Verzamelen, analyseren en beslissen in IGP

Paracetamol

Als de huisarts paracetamol voorschrijft, dan begint eigenlijk niemand de discussie of dit nu wel helpt. Het werkt gewoon. Voor informatiegestuurd werken geldt in grote lijn hetzelfde. Het is een bewezen effectieve, brede politiestrategie. Het werkt gewoon.

In de praktijk echter is ook te zien dat slim, informatiegestuurd werken soms lastig en weerbarstig is. En – net als het paracetamolletje – heeft het soms ook zijn bijwerkingen. Het in de praktijk werkend maken vraagt bewust bekwame toepassing van de basisprincipes van IGP en voortdurende bijstelling, oog voor kwaliteit en innovatie, een kritisch oog voor ongewenste effecten en daarop ook passende maatregelen nemen.

Informatiegestuurd werken is dus allang niet meer een aparte strategie, maar een manier van werken die andere belangrijke politiestrategieën zoals gebiedsgebonden werken en probleemgericht werken zeker niet uitsluit, maar juist versterkt en aanvult.[3]

2.2 Informatie verzamelen en delen

Informatie verzamelen en vastleggen, inclusief het hebben van toegang tot informatie bij anderen, vormen de kern van informatiegestuurd werken. Op verschillende manieren en met verschillende bronnen wordt de informatiepositie bij de politie opgebouwd (zie

3 Versteegh, P., T. van der Plas & H. Nieuwstraten, *The Best of Three Worlds: effectiever politiewerk door een probleemgerichte aanpak van hot crimes, hot spots, hot shots en hot groups*. Politieacademie, Apeldoorn 2010.

hoofdstuk 14 Inwinning en hoofdstuk 23 In gesprek met Ruud Staijen over informatievoorziening). Naast eigen bronnen gebruikt de politie bronnen bij andere overheden alsmede bedrijven en brancheorganisaties, en niet in de laatste plaats open bronnen. Zie ook hoofdstuk 13 Informatiegestuurd werken en samenwerkingsrelaties en hoofdstuk 15 Sociale media.

Deze bronnen zijn langs verschillende assen te classificeren. Een as is bijvoorbeeld de herkomst van de informatie. Een groot deel van de bronnen is gebaseerd op menselijke waarneming, *human intelligence*. Het aantal automatische waarnemingen door sensoren neemt echter snel toe. Het gebruik van ANPR-camera's (automatic number plate recognition) bijvoorbeeld is enorm gestegen. Maar ook het aantal sensoren dat mensen en apparaten zelf bij zich draagt, zoals een gps op de mobiele telefoon. Een derde belangrijke herkomst van informatie is die van open bronnen (zie hoofdstuk 15 Sociale media). Dit betreft vooral informatie die op internet en via sociale media te vinden is.

Een andere as is bijvoorbeeld wie de informatie invoert. Een aantal bronnen wordt door politiemensen gevuld, dit zijn de basisadministraties van de politie. Daarnaast worden bronnen gevuld door medewerkers van partnerorganisaties in het veiligheidsdomein, zoals gemeenten, het Openbaar Ministerie (OM) en het Centraal Justitieel Incassobureau (CJIB). De gemeentelijke basisadministratie persoonsgegevens (GBA) is een gemeentelijk systeem, Parket politiesysteem (PAPOS) wordt door het CJIB en de politie gebruikt om te communiceren over de executie van bepaalde maatregelen.

Een derde categorie op de as wie de informatie invoert, is de burger zelf. Via de internetaangifte bijvoorbeeld voeren mensen zelf het nodige in het systeem in. Maar ook de informatie die de politie via sociale media verkrijgt, is door de burgers zelf ingevoerd. Zeker bij deze laatste categorie moet de kwaliteit van de informatie vaak expliciet beoordeeld worden (zie hoofdstuk 9 Waar kwaliteit toe leidt). Immers, de bedoeling waarmee iemand informatie heeft gedeeld, kan bepalend zijn voor de waarde ervan. Zo kan iemand bewust misbruik maken door een valse melding te doen. Maar ook in het geval dat professionals de systemen vullen, is de kwaliteit niet altijd gegarandeerd. Niet omdat het misleidende informatie zou kunnen zijn, maar vooral omdat zij soms met een ander doel wordt ingevoerd en mede daardoor niet volledig is, of soms met fouten in de systemen ingevoerd wordt. Ook komt het regelmatig voor dat politiemensen informatie helemaal niet invoeren, bijvoorbeeld omdat men zich niet bewust is van de relevantie ervan.

Rapportage

Een belangrijk deel van de unieke informatiepositie van de politie is afhankelijk van de menselijke invoer in de eigen geautomatiseerde systemen. Dit wordt soms gezien als administratieve last van het politiewerk. Binnen de overheid wordt met administratieve last vaak gedoeld op (overbodige) handelingen die mensen in de organisatie moeten uitvoeren als gevolg van allerlei wettelijke verplichtingen, ongeacht of zij die handelingen ook zonder wettelijke verplichtingen zouden uitvoeren. Ze horen vaak niet tot het kernproces.

Maar het vastleggen van waarnemingen hoort bij de politie nu juist wel tot het kernproces. Het is het informatiedeel van het politiewerk. Het wordt door velen als last gezien: tijdens of aan het einde van de dienst nog het 'papierwerk' moeten doen, binnen zitten voor de administratie in plaats van zinvol op straat bezig (blijven) zijn,

niet-gebruiksvriendelijke systemen moeten vullen. En toch is goede rapportage over politiewerk een essentieel onderdeel van het werk. Als jouw collega dit nalaat, kun jij jouw werk ook niet goed doen. Er zijn uit de politiepraktijk talloze voorbeelden bekend waarbij het achterwege blijven van adequate rapportage over eigen waarnemingen of handelen geleid heeft tot grote missers; bijvoorbeeld het niet kunnen bewijzen van een relatie tussen crimineel A, B en C en daarmee een tenlastelegging 'criminele organisatie' (artikel 140 Wetboek van Strafrecht) niet rond kunnen krijgen. Of vuurwapengebruik tegen slecht geïnformeerde collega's door het onterecht ontbreken van de gevarenclassificatie 'vuurwapengevaarlijk' op een aan te houden verdachte. Zonder goede informatie onvoldoende inzicht, en zonder goed inzicht geen effectieve en efficiënte uitvoering van de politietaak.

Delen, tenzij

Het belang van informatie voor het goed kunnen uitvoeren van de politietaak wordt onderstreept door het principe 'delen, tenzij'. Voor de veiligheid is het belangrijk dat de informatie optimaal en op de juiste wijze wordt gedeeld binnen de politie en tussen de politie en haar omgeving. De cultuur daarin verandert: steeds minder vaak worden redenen als 'in het belang van het onderzoek, de getuigen en risico's voor de betrokkenen' genoemd om terughoudend te zijn in het vastleggen en delen van informatie. Ook de technologische mogelijkheden veranderen. Tot een paar jaar geleden was het niet eenvoudig om informatie te delen, bijvoorbeeld tussen 26 verschillende BasisVoorzieningen Handhaving (BVH's) Nu wordt informatie op landelijke schaal stap voor stap (bijna) real-time bij elkaar gebracht via de BasisVoorziening Informatie (BVI).

Maar natuurlijk is niet alle informatie bij de politie zomaar altijd voor iedereen toegankelijk. Het gaat er vooral om met welke professionele blik en grondhouding je kijkt naar je eigen verantwoordelijkheid als collega of partner in het veiligheidsdomein. Je deelt informatie en kennis waar mogelijk en waar nodig. Maar het gebruiken van informatie is in een 'delen, tenzij'-cultuur gebonden aan wettelijke kaders, de tenzij's. Deze wettelijke kaders worden besproken in hoofdstuk 5 De Wpg. Daar waar mogelijk zijn de wettelijke kaders in de informatiesystemen verweven door middel van het vastgestelde autorisatiemodel. Het autorisatiemodel bepaalt welke gegevens voor welke rollen en functies toegankelijk zijn. Dit wordt in hoofdstuk 6 Autorisatiemodel politie verder toegelicht. Ook kunnen ethische kwesties een tenzij opleveren (zie hoofdstuk 7 IGP en ethiek, ofwel: wat mag en wat mag niet? en hoofdstuk 8 In gesprek met Peter Holla over ethiek).

2.3 Analyseren van informatie

Politie, partners, betrokkenen, getuigen. Basisvoorzieningen, eigen beheerde omgevingen van politieonderdelen, zakboekjes, open bronnen, minder toegankelijke bronnen. Vaak beschikt de politie over veel informatie. Informatie die heel divers is en vaak niet compleet (veel verdachten hangen het 'delen, tenzij'-principe nog niet aan), laat staan volledig ontsloten en beschikbaar. Soms is de kennis en informatie die we hebben beperkt, niet meer dan een vermoeden. Soms zijn we kennisarm.[4] Soms ook niet.

4 Hengst-Bruggeling, M. den, *Informatierijk en toch kennisarm!?* Politieacademie, Apeldoorn 2010.

Informatiegestuurd werken komt tot leven – en wordt pas echt moeilijk – als we de beschikbare informatie gaan analyseren, combineren met wat we al weten en haar betekenis moeten geven voor bijvoorbeeld de aanpak van veiligheidsproblemen; het duiden van de informatie. Op welk moment en op welke wijze kunnen we op basis van beschikbare informatie stellen dat een zware crimineel een liquidatie gaat uitvoeren of dat een radicaliserende jongere als extreem gevaarlijk gezien moet worden en maatregelen vereist?

Analyseren gaat om het beantwoorden van de vragen die we hebben over het veiligheidsprobleem dat we willen aanpakken. Hoe groot is het probleem? Wie veroorzaakt het? Neemt het toe? Hoe zit het nu echt in elkaar? Is de aanpak effectief?

If you can't write the handbook of crime you are not in business

De opsporing kent al sinds jaar en dag de zeven gouden W's: wie, wat, waar, wanneer, waarmee, welke wijze, waarom? Enige tijd geleden opperde een recherchechef het idee dat het voor een goede analyse van een criminaliteitsprobleem goed zou zijn om elk van de zeven W's vooraf te laten gaan door de vraag waarom: Waarom wie (die)? Waarom wat (dat)? Waarom waar (daar)? Waarom wanneer (dan)? Enzovoort.

Bij het analyseren van informatie denken we al snel aan het bekende analyseproces dat vrij lang duurt, dat ingewikkelde technieken gebruikt zoals een sociale netwerkanalyse, en uitmondt in een zogenoemd analyseproduct: een dik pak papier met een kaft en de naam van de analist er op. Dat is inmiddels een te beperkte blik. De technologie maakt het steeds vaker mogelijk om snel en automatisch, zonder directe tussenkomst van een analist, gegevens te analyseren. Een voorbeeld hiervan is de BlueSpot Monitor (BSM), waarin je met een druk op de knop bijvoorbeeld alle woninginbraken in een bepaald gebied en een bepaalde periode in een tabel of op een zogenoemde *heat map* krijgt te zien.

Figuur 2.3 Snelle gebiedsanalyse met de BSM

Soms is de analist de medewerker van het Real-Time Intelligence Center (RTIC) die razendsnel besluit welke informatie bij een bepaalde melding moet meegaan, en welke niet. En iedere medewerker in de operatie analyseert voortdurend de informatie en kennis die op dat moment beschikbaar of nodig is. Wat is er aan de hand? Wat weet ik? Is het veilig? Is mijn collega veilig? Wat zijn mijn mogelijkheden? Met de lift of de trap? Waarmee moet ik rekening houden? Wat wil ik nog meer weten om adequaat te beslissen?

Vak

Alles bij elkaar is analyse daarmee een vak dat verschillende niveaus kent. In de basis is het voor iedereen te leren en te beheersen. Op een ander kennisniveau kent het vak een veelheid aan niches en specialiteiten, waarbij aanvullende en specialistische kennis en vaardigheden nodig zijn om het uit te oefenen.

Analyseren is vooral een vak omdat het niet zomaar gaat over het beantwoorden van een vraag. Analyseren is het beantwoorden van een vraag op basis van een paar strenge eisen. Dit zijn:

- *Op basis van informatie*. Analyses zijn gebaseerd op kennis en informatie. Speculatie, gevoel, *truthiness*, occultisme en dergelijke spelen daarin geen rol. Dat geldt ook voor puur rationalisme: op een werkelijkheid die alleen is gevormd door redeneringen zonder dat ze met gegevens is onderbouwd, kan geen analyse zijn gefundeerd.
- *Controleerbaar of herhaalbaar*. Het moet controleerbaar zijn hoe de analyse is uitgevoerd. In uitgebreide strategische analyses staat dat meestal in de methodeparagraaf. Maar die is er niet altijd. Een eenvoudige vuistregel is dat iemand anders met dezelfde kennis en informatie bij dezelfde vraag tot hetzelfde antwoord zou moeten komen.
- *Neutraal*. Analyseren zou zo vrij mogelijk moeten zijn van iemands eigen mening, overtuiging of vooringenomenheid. Helemaal waardenvrij, dat lukt eigenlijk niet. Een vuistregel kan zijn om je voor te stellen dat de conclusies van een analyse helemaal anders zijn dan je had verwacht, en hoe je je daarbij zou voelen. Je hebt bijvoorbeeld onderzocht of een nieuwe manier van aanpak van babbeltrucs beter werkt dan de oude. Je hebt enorm veel tijd besteed aan het invoeren van de aanpak in een basisteam en in het onderzoek of het werkt. Maar het werkt niet. Je eigen geesteskind heeft gefaald en toch moet je ook dan neutraal de resultaten accepteren en presenteren.
- *Antwoord op de vraag*. Tip voor beslissers. Hoe eigenaardig het ook klinkt. Een vuistregel is om steevast na te gaan wat de precieze vraag in een analyse nu is, en wat de conclusies zijn. Sluiten deze op elkaar aan? En sluit het aan bij wat de steller van de vraag ermee wil doen in de politiepraktijk?
- *Polsstok*. 'De wîder springen will, as sîn Kluwstock reckt, fallt in 'n Slot.' Enthousiasme, tijdsdruk of een dwingende afnemer kunnen leiden tot een conclusie die verder reikt dan alleen op basis van de beschikbare gegevens verantwoord is. 'Het loopt de spuigaten uit' en 'bij bosjes' zijn begrippen die opvallend gemakkelijk worden gebuikt nadat dertig mensen op één meetmoment is gevraagd naar hun ervaringen met een nieuw veiligheidsprobleem.
- *Zelfkritisch*. De beste analist is voor zichzelf een enorme zeurpiet. Klopt het wat ik heb gedaan? Maak ik denkfouten, is er een bias? Zitten er fouten in mijn data? Heb ik iets gemist? Heb ik mijn vraag helder gesteld? Heb ik onbevooroordeeld naar het antwoord geluisterd? Heb ik alle kritiek van anderen meegenomen?

Soorten analyse

Analyses leiden tot grofweg overzicht, inzicht en vooruitzicht.

- *Overzicht* leidt tot een beschrijving van een veiligheidsprobleem. Hoeveel woningovervallen zijn er in 2016 geweest? Zijn dat er meer of minder dan vorig jaar? Wat is de buit? Welke modus operandi (MO) wordt er gehanteerd? Wie zijn verdachten en daders? Leeftijd? Kenmerken?

- *Inzicht* leidt tot verklaring. Waarom neemt het aantal overvallen bijvoorbeeld af? Waarom gaat de buit omhoog? Waarom kiezen daders voor een bepaalde MO? Waarom zijn deze daders de daders?
- *Vooruitzicht* leidt tot verwachtingen voor de toekomst. Waar kunnen we woningovervallen verwachten? Leidt intensievere surveillance tot vermindering of verschuiving van het probleem? Wie ontwikkelt een criminele carrière en zal overvallen gaan plegen?

Het is niet zo dat een analyse die inzicht geeft beter is dan een analyse die overzicht biedt. (Vaak geeft de laatste wel minder werk dan de eerste.) De beste analyse is de analyse die het best aansluit bij de aanpak van het probleem en de 'behoeftesteller' goede aanknopingspunten biedt voor concreet beslissen over het handelen. Soms is een overzicht van hotspots in een wijk meer dan genoeg om overlast effectief aan te pakken. Soms kom je niet verder zonder inzicht: waarom gebruiken criminele organisaties in de cocaïnehandel sommige aanvoerroutes wel en andere niet?

Naast het voorgaande wordt ook gesproken van evaluatieonderzoek en prescriptieve analyse. Evaluatieonderzoek heeft doorgaans als doel vast te stellen of en in welke mate iets gelukt is en waarom. Het begrip is sterk verbonden met onderzoek naar beleid en wat minder met het dagelijkse informatiegestuurd politiewerk. Daarnaast lijkt het wat sterker gekoppeld aan verantwoorden dan aan sturing (zie hoofdstuk 4 De keerzijde van IGP: IGP en de metamorfose van politiebureaucratie). En toch leveren evaluatieonderzoeken zinvolle kennis en inzichten die gebruikt kunnen worden om gegeven een probleem de beste aanpak te bepalen.

Prescriptieve analyse heeft tot doel om te adviseren over de aanpak van het veiligheidsprobleem; evaluatieonderzoeken zijn daarvoor onmisbaar. Prescriptieve analyses vormen een onderdeel van vooruitzicht. Er zijn specifieke situaties waarin prescriptieve analyses hun nut hebben. Zo kan inzet van zichtbare mobiele eenheid (ME) op bepaalde supportersgroepen en onder bepaalde omstandigheden eerder een escalerend dan deescalerend effect hebben (zie voor veel meer informatie over analyse hoofdstuk 11 Analyse).

Opinion: 'Without data, you're just another person with an opinion.'[5]

2.4 Beslissen op basis van analyse

Een analyse biedt een handelingsperspectief voor degene die moet handelen of beslissen. Dit betekent overigens niet het klakkeloos opvolgen van dat wat er in de analyse staat. Het betekent dat je als beslisser betekenis geeft aan de analyse, dat je de resultaten van de analyse serieus afweegt en plaatst in de context van dat moment. Als beslisser moet je daarom de mogelijkheden van verschillende soorten analyses kennen en

5 Toegeschreven aan W.E. Deming.

begrijpen en deze mogelijkheden kunnen vertalen naar concrete toepassingen in de praktijk.

Dit geldt ook voor de analist. Soms wordt een eenvoudige vraag te zwaar ingeschat en wordt met een te lange doorlooptijd uiteindelijk veel ingewikkeld werk voor niets gedaan. Analyse is een vak. Beslissen ook. En net als bij analyse is beslissen een vak dat iedereen in de basis uitvoert, maar dat daarnaast een veelheid aan niches en specialiteiten kent waarbij aanvullende en diepgaande kennis en vaardigheden nodig zijn om het uit te oefenen. Vraag niet alle auteurs van dit boek om te beslissen over de juiste inzet van mobiele eenheid op basis van een risicoanalyse van een voetbalwedstrijd in de eredivisie voetbal.

Relaties op de werkvloer

De relatie tussen beslissers en analisten is bijzonder. In situaties waar beide functies naast elkaar bestaan, kun je verwachten dat men de basisvaardigheden van elkaars vak kent. Tegelijkertijd vraag je van beide vakmensen stevig vertrouwen in elkaars professionaliteit als het gaat om de specialistische kanten van het vak. Professioneel vertrouwen zorgt dat analisten niet hoeven uit te leggen dat Bonferroni geen pizza is.[6] Beslissers erkennen de professionaliteit van de analisten en nemen hun verantwoordelijkheid om met de resultaten vervolgstappen te nemen. En analisten kunnen met dit vertrouwen terughoudend zijn met de opmerking dat hun rapporten altijd in de la belanden.

Sturen op en sturen met informatie

Als je wilt beslissen op basis van informatie, dan dien je er ook voor te zorgen dat die informatie er is. Sturen *met* informatie kan daarom niet zonder sturen *op* informatie. Een recherchechef die voor een probleemgerichte aanpak wil weten waarom er voor de import van cocaïne in Europa bepaalde transportroutes wel en andere niet worden gebruikt, zal er samen met de collega's voor moeten zorgen dat de nodige informatie en kennis wordt verzameld en ontsloten. Ook moeten de verwachtingen over een op te leveren analyse helder zijn. In dit concrete geval kan het voor het beantwoorden van deze vraag bijvoorbeeld nodig zijn om informatieposities in het criminele milieu in te nemen door het runnen van voldoende betrouwbare informanten die weten hoe het echt zit (zie ook hoofdstuk 14 Inwinning).

Terug naar af

Beslissen is niet het einde van informatiegestuurd politiewerk. Beslissen hoe een veiligheidsprobleem aan te pakken, zorgt voor een verandering in het aan te pakken probleem, of niet. En dan begint alles weer opnieuw: hoe heeft de aanpak gewerkt? Wat is de omvang van het probleem nu, wat weten we ervan, wat betekent dit? Weten we wat helpt en wat niet? Wat moeten we doen? Kortom: evaluatie, overzicht, inzicht en vooruitzicht (zie ook hoofdstuk 16 In gesprek met Henk Bril over beslissen).

---

6 Bonferroni is een statistische methode om de kans te verkleinen dat je iets voor waar aanneemt waar dat feitelijk niet het geval is.

2.5 Informatiegestuurd politiewerk en business intelligence

IGP en BI zijn zijden van dezelfde medaille. Zij gaan over de manier waarop de politie in de operatie met informatie omgaat.

Definitie van business intelligence

Business intelligence is het geheel van processen, producten, hulpmiddelen en organisatorische inrichting ten behoeve van het geautomatiseerd verzamelen, integreren en veredelen van gegevens en het analyseerbaar maken, presenteren en distribueren van informatie.[7]

Informatiegestuurd werken is in deze tijd tot mislukken gedoemd als de BI-functie in de organisatie niet goed wordt ingepast. De politie moet net als vele andere bedrijven en instanties kunnen werken met de enorme hoeveelheid, snelheid en diversiteit van gegevens die erin omgaan en beschikbaar zijn. Ook hier weer voorbeelden te over. Hoeveel politiemensen zijn in plaats van ANPR nodig om alle kentekens te noteren en te controleren die in een bepaald uur over de A4 bij Schiphol gaan? Welke kentekens zijn daar eerder langsgekomen in vaste combinatie met een ander kenteken? Wat betekent dat? Zijn er van de vermoedelijke bestuurders van deze auto's foto's, tekst- of tapgegevens? Bestaat er vanuit een of meerdere rechercheteams op dit moment belangstelling voor de vermoedelijke bestuurder?

In het kader van dit soort vragen wordt ook bij de politie steeds meer gesproken van business intelligence. Dit is niet volstrekt anders dan informatiegestuurd werken. Het is eerder een begrip dat voortkomt uit brede ontwikkelingen in de informatiemaatschappij, informatie- en communicatietechnologie en bijvoorbeeld de gevolgen daarvan voor het organiseren van het werk en het snel kunnen realiseren van adequate informatievoorzieningen daarvoor.

De politie heeft sinds 2013 een eigen business-intelligencestrategie.[8] Ze beschrijft wat BI voor het politiewerk betekent en hoe daarmee om te gaan. De strategie past naadloos bij de begrippen en activiteiten waarmee we informatiegestuurd werken tot nu toe hebben beschreven.

Net als bij informatiegestuurd werken staat in de business-intelligencestrategie het verbeteren van de effectiviteit van het politiewerk met inzet van informatie en analyses centraal. De zes gebieden waar de BI-strategie zich in de operatie op richt, beschrijven we in de volgende paragraaf. Daarna gaan we in op wat dit voor de organisatie betekent.

2.5.1 Goed politiewerk staat centraal

In de BI-strategie gaat het om het operationele doel ten behoeve van het politiewerk: het verbeteren van beschikbaarheid en gebruik van informatie in het politiewerk. In de BI-strategie zijn zes gebieden onderscheiden:

---

7 Programma Intelligence Politie Nederland, *Business intelligence strategie*. 2012.

8 Programma Intelligence Politie Nederland, *Business intelligence strategie*. 2012.

Figuur 2.4 Informatie krijgt betekenis op straat

1 *Directe ondersteuning van de collega op straat met mobiele toepassingen.*
Bijvoorbeeld de ontwikkelingen van de integrale bevraging (BasisVoorziening Informatie voor Integrale Bevraging – BVI-IB) en de mobiele toepassingen daarvan door inzet van smartphones. Met de BVI-IB kan nu door iedere operationele politiemedewerker overal en in één keer een veelvoud van bronbestanden worden geraadpleegd, waardoor hij zelfstandiger en beter zijn werk kan doen. In 2016 werd de BVI-IB meer dan 50 miljoen keer bevraagd. Het aantal bevraagbare bronnen wordt gestaag uitgebreid. In Mobiel Effectiever Op Straat (MEOS) kan de politiemedewerker op straat bijvoorbeeld direct kentekens en identiteitsdocumenten controleren.

2 *Real-time ondersteuning van de collega door het RTIC.*
Directe informatievoorziening in de operatie is cruciaal voor politiepersoneel, burgers en partners. Daarom voorziet het RTIC de collega's die belast zijn met de afhandeling van meldingen steeds direct (in real-time) van extra informatie uit open en gesloten bronnen, waardoor zij beter voorbereid ter plaatse komen en veiliger kunnen werken. Zie ook hoofdstuk 19 Real-time intelligence (RTI).

3 *Gebiedsgebonden ondersteuning van de wijkagenten, wijkteams enzovoort.*
De BSM is hier een voorbeeld van. Collega's hebben inzicht welke incidenten zich in hun wijk hebben voorgedaan, welke personen zich daar ophouden enzovoort. Aanvullend kan het Business Intelligence Competency Center (BICC) in BlueSpot Report verschillende rapportages maken waarin gegevens uit andere bronnen worden meegenomen of specifiekere vragen worden beantwoord. Hiermee krijgen de wijkagenten, basisteamchefs en anderen een goed beeld over de situatie in hun wijk. Zo nodig op maat. Zie hoofdstuk 22 De business-intelligencestrategie in de politiepraktijk.

4 *Ondersteuning van analyse en onderzoek.*
De BVI wordt steeds beter geschikt als zoekmachine door veel bronbestanden. Het combineren en analyseerbaar maken van gegevens kost steeds minder tijd. Alle analisten binnen de politie werken binnenkort met vijf standaard analysetools. Er wordt inhoud gegeven aan *predictive policing*, waarbij trends en ontwikkelingen worden geanalyseerd en een verwachting wordt uitgesproken over mogelijke plaatsen en tijdstippen waar criminaliteit zich zal manifesteren. Teams als het Team High Tech Crime

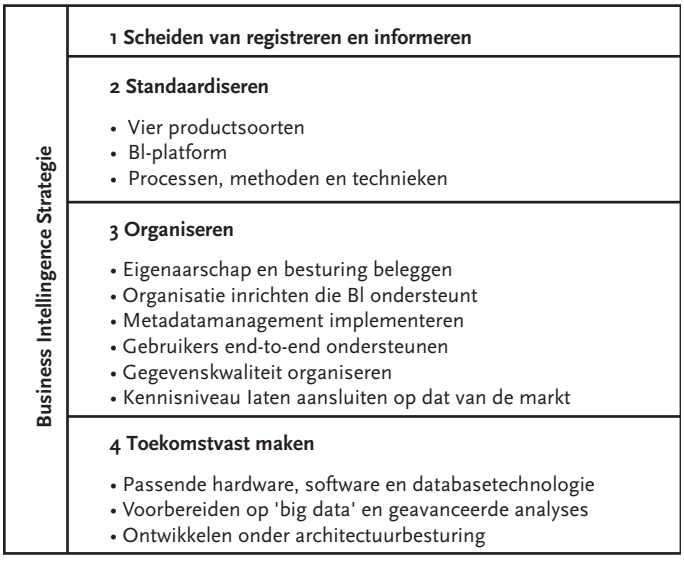
of de teams bestrijding van kinderporno werken al met analyse van big data. Hiervoor worden nieuwe zogenoemde schaalbare toepassingen ingezet die zeer grote hoeveelheden uiteenlopende gegevens razendsnel kunnen verwerken. Denk hierbij aan internetbestanden, maar dan in combinatie met vrije tekst, foto- en videobestanden, die direct gescand, automatisch getagd en geanalyseerd worden. Inzet van deze technologie heeft grote consequenties voor de technologische infrastructuur van de politie en de daartoe benodigde kennis, organisatie en budget. En niet in de laatste plaats voor hoe het politievak wordt uitgeoefend.

5 *Ondersteuning van sturing op de operatie.*
Briefing en debriefing waardoor collega's op straat bij aanvang van de dienst worden voorzien van de nodige informatie en werkinstructies. Operationele informatie wordt door de betrokken politiemensen verwerkt en daarmee direct weer ter beschikking gesteld aan de operatie (zie hoofdstuk 17 Briefen en debriefen: de wortels van IGP?). In de bedrijfsvoering worden toepassingen ontwikkeld die ook op het snijvlak van bedrijfsvoering en operatie voor verantwoordelijke beslissers met een druk op de knop actuele managementinformatie leveren.

6 *Informatie-uitwisseling tussen burgers, partners, internationaal.*
Denk bijvoorbeeld aan het gebruik van sociale media bij opsporingsonderzoeken; aan het combineren en ontsluiten van informatie van gemeenten en Openbaar Ministerie; en aan het (inter)nationaal uitwisselen van gegevens over bijvoorbeeld criminaliteit en terrorisme met inlichtingen- en veiligheidsdiensten (zie ook hoofdstuk 13 Informatiegestuurd werken en samenwerkingsrelaties).

2.5.2 BI onder de motorkap

Met de technologische kant van BI hebben we het over wat er onder de motorkap gebouwd en georganiseerd moet worden om als politie mee te kunnen komen in de informatiemaatschappij. Deze staan in figuur 2.5.



Figuur 2.5 BI onder de motorkap

Scheiden van registeren en informeren

Het belangrijkste principe onder de motorkap van BI is het scheiden van registreren en informeren in respectievelijk transactionele systemen (bijvoorbeeld de BasisVoorziening Handhaving – BVH) en informatieverstrekkende systemen (de BasisVoorziening Informatie – BVI).

Om besluiten te nemen, is het nodig zo goed mogelijk over alle beschikbare relevante informatie te beschikken. Informatieverstrekkende systemen bieden bijvoorbeeld inzicht in de ernst, aard of omvang van een veiligheidsprobleem. De focus in dergelijke systemen is op het bijeenkrijgen, integreren en veredelen van gegevens en het analyseerbaar maken, presenteren en verspreiden ervan.

Bij registratie is de focus eerder het ondersteunen van één proces, zoals het snel en goed opmaken van een proces-verbaal of het maken van een mutatie over de afhandeling van een incident. Een goede procesondersteuning is voor deze systemen van doorslaggevend belang. Een politiemedewerker wil namelijk zo snel en goed mogelijk een aangifte kunnen opnemen.

Standaardiseren

Standaarden in BI-systemen vergroten de flexibiliteit, toekomstvastheid en het vermogen om aan te sluiten bij gebruikerswensen. Sterke standaarden maken creativiteit mogelijk zonder afbreuk te doen aan uitwisselbaarheid en beheerbaarheid van informatie. Apple bijvoorbeeld hanteert zeer strikte standaarden voor het ontwikkelen van apps voor de iPhone. Binnen deze standaarden worden echter veel en uiteenlopende apps ontwikkeld die wereldwijd draaien, veilig en stabiel zijn en een eenvoudig onderhoudsmodel kennen. De politie wil graag innoveren en daarom zijn juist op BI-niveau standaarden nodig. Daarnaast heeft de politie ten opzichte van andere overheidsdiensten een extra grote verantwoordelijkheid om correct om te gaan met informatie.

Organiseren

Kwaliteit komt niet vanzelf. Om BI goed te laten werken, moet je het expliciet inrichten en organiseren. Bij de politie is gekozen voor een organisatievorm met maximale inbedding in de informatieorganisatie. Daarmee is de besturing van BI gepositioneerd bij de portefeuille Intelligence. De bedoeling is dat hierdoor voldoende samenhang ontstaat tussen de informatieorganisatie en de andere organisatieonderdelen waarin deze verankerd is. Zie ook hoofdstuk 22 De business-intelligencestrategie in de politiepraktijk.

Toekomstvast maken

Een BI-omgeving is niet iets wat je eenmalig op papier ontwerpt en dan invoert, maar net zo dynamisch als de politie zelf, zeker gezien de technologische ontwikkelingen. De gewenste organisatievorm en technische infrastructuur waarvan men in 2011 nog dacht dat deze jaren zouden kunnen voldoen, barsten nu al bijna uit hun voegen door de enorme toename van de hoeveelheid data en de grote vraag naar geautomatiseerde informatieproducten op zowel lokaal, nationaal als internationaal niveau. Voor BI zijn bovendien medewerkers nodig met andere kennis en vaardigheden om dit te kunnen leveren, bijvoorbeeld data science. De BI-strategie uit 2013 biedt de mogelijkheid om in de komende jaren mee

te groeien met deze ontwikkeling. Zie ook hoofdstuk 23 In gesprek met Ruud Staijen over informatievoorziening.

2.6 Informatiegestuurd politiewerk in een veranderende omgeving

Het is niet meer zo dat het bestaande werken ondersteund wordt door technologie, maar technologie maakt nieuwe manieren van werken mogelijk, zeker ook op het gebied van IGP. Daarvan zien we voorbeelden die we al weer heel gewoon vinden en niet meer opvallen. Denk aan het op een smartphone via een app een afspraak prikken, daarmee een hotelkamer boeken en de weg ernaartoe vinden. Andere voorbeelden vallen nog wél op, zoals het gebruik van *drones* of *bodycams*.

Hierna gaan we in op enkele veranderingen die wel te onderscheiden maar niet te scheiden zijn. De opsomming is niet compleet, maar biedt zicht op de kansen die nieuwe technologieën bieden om in het politiewerk effectief informatiegestuurd te blijven werken in samenwerking met partners en burgers. In alle gevallen geldt dat de principes die we in dit hoofdstuk hebben beschreven over verzamelen, analyseren en beslissen, blijven gelden, ook in deze veranderingen.

Integrale informatiepositie

Technologisch is het mogelijk met alle partners samen te werken op basis van toegang tot één gemeenschappelijk opgebouwde informatiepositie. De BVI is nu nog grotendeels van en voor de politie. Integraal werken aan veiligheidsproblemen betekent het in toenemende mate ontsluiten of beschikbaar stellen van de BVI voor de partners. Als informatie steeds sneller en beter op maat terechtkomt bij de professionals, dan zal de rol van de informatieorganisatie van de politie bovendien meer verbindend worden.

Werken vanuit de bedoeling

Nu we steeds beter informatie met elkaar kunnen delen, wordt de vraag steeds belangrijker: wie moet er wát mee? Als de wijkagent, de bijzonder opsporingsambtenaar van de gemeente en de politiechef allemaal toegang tot dezelfde informatie hebben, hoe weten we dan nog wie wat moet doen of doet? Domweg top-down instrueren werkt in dat geval lang niet altijd meer. Het wordt dan zaak van leidinggevenden om enerzijds glashelder aan te geven wat de bedoeling en prioriteiten van het politiewerk zijn, en anderzijds de voorwaarden te scheppen op basis waarvan de politiemedewerkers hun werk met voldoende professionele ruimte kunnen doen.

Power to the edge

Werken vanuit de bedoeling en een gedeeld, gemeenschappelijk kennis- en informatieplatform zijn belangrijke voorwaarden voor een slimme, snelle en geïntegreerde aanpak van veiligheidsproblemen. Het is dan nog wel nodig dat de professionals zelfstandig of in onderling overleg ‘ter plekke’ de juiste beslissingen kunnen en mogen nemen. Informatiegestuurd werken in het informatietijdperk blijft behelpen als medewerkers niet

empowered zijn om – vanuit de bedoeling – zelf te beslissen wat zij op basis van deze informatie doen in de context waarin zij werken. Dit vraagt niet alleen om formele verschuiving van beslisbevoegdheden, maar ook om georganiseerd vertrouwen in de professionaliteit van de medewerkers. En voldoende ruimte en faciliteiten om zich daarin verder te kunnen ontwikkelen.

Het vak van analyse verwetenschappelijkt

Het analyseren van informatie verwetenschappelijkt. Dit is niet alleen te zien aan het feit dat steeds hogere eisen worden gesteld aan analisten – *data scientists* doen aan analytics. Het is ook terug te zien in de toenemende eis om het politiewerk te baseren op empirisch onderbouwde resultaten. Welke interventie biedt onder welke omstandigheden de grootste kans van slagen? Risicotaxatie (zie hoofdstuk 12 Persoonsgerichte aanpak en risicotaxatie) en predictive policing (zie hoofdstuk 21 Predictive policing) zijn hier voorbeelden van.

Toenemende aandacht voor juridische vaardigheden, privacy en ethiek

De politie en partners kunnen en mogen veel met de informatie die zij hebben. Dit kan echter ook ongewenste effecten hebben. *Profiling* op etnische gronden is een voorbeeld, net als het veelvuldig, routinematig en lukraak bevragen van persoonsgegevens zonder operationele noodzaak en zonder dat dit tot zichtbare actie leidt. Aan het toenemend gebruik van automatische algoritmen kleven mogelijk nadelen als het (onbedoeld) vergroten van verschillen tussen groepen mensen, discriminatie en het lastiger maken van democratische controle.[9] De hoofdstukken 5 tot en met 9 gaan over de vraag: wat mag en wat niet?

9 Zie bijvoorbeeld O'Neil, C., *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Penguin Books, Londen 2016.

3 Kennis voor politiewerk: een blik vanuit het recente verleden

Guus Meershoek en Nicolien Kop

Nieuw in de huidige samenleving is de overvloed aan informatie. En meer nog dan andere organisaties dreigt de politie door allerlei soorten kennis te worden overspoeld. Deze situatie dwingt de politie hier nog veel selectiever dan in het verleden mee om te gaan. De juiste informatie op het juiste moment op de juiste plek in de juiste vorm beschikbaar te stellen is belangrijker dan ooit. Dat kan de politie alleen als zij goed beseft welk soorten kennis nodig zijn om haar doeleinden te bereiken en als zij waakt over de kwaliteit van de kennis. Dit hoofdstuk biedt een door kennis van het politieverleden geinspireerde reflectie op de betekenis van kennis in het huidige politiewerk, gevolgd door een beknopte beschrijving van de opkomst van informatiegestuurd politiewerk (IGP) in Nederland.

3.1 De betekenis van kennis

3.1.1 Een omslag in de structuur van kennis: het Interbellum

De opkomst van het informatiegestuurd politiewerk vindt plaats in een periode waarin de computer en het internet een omwenteling teweegbrengen in de manier waarop mensen informatie vergaren, gebruiken en delen; in de soort informatie die in de samenleving circuleert; en daarmee in het maatschappelijk leven en het openbaar bestuur. Die opkomst is daar niet los van te zien. Een publieke politiedienst die haar maatschappelijke functie wil blijven vervullen en positie wil blijven behouden, dient zich van die bredere context rekenschap te geven en op die veranderingen te anticiperen.

Hoewel het altijd lastig is om de historische betekenis van actuele veranderingen te beoordelen, lijkt de huidige omwenteling, veroorzaakt door de computer en het internet, even ingrijpend als die veroorzaakt door de uitvinding van de boekdrukkunst (rond 1450), van het register (eind achttiende eeuw) en van de kaartenbak (na de Eerste Wereldoorlog). Het betrof telkens radicale veranderingen in de vorm waarin kennis kon worden gegoten, en daarmee in de wijze waarop kennis kon worden opgeslagen, kon circuleren in de samenleving en beschikbaar kwam voor anderen. Die drie innovaties in de omgang met informatie gingen telkens gepaard met ingrijpende veranderingen in de identiteit van individuen, in de sociale omgangsvormen en in het openbaar bestuur, waaronder politie en justitie. Dat lijkt ook nu het geval met de intrede van de computer en het internet. De omslagen versterkten op de lange termijn de positie van politie en justitie maar op de korte termijn was telkens sprake van complexe, crisisachtige aanpassing. De veranderingen die zich na de Eerste Wereldoorlog in de politie voltrokken, kunnen dat duidelijk maken.

Aan het begin van de twintigste eeuw hadden politiekorpsen in de grotere steden in Nederland en elders een strakke, militaire hiërarchie. Opgetreden werd er slechts tegen een beperkt aantal overtredingen en misdrijven (dronkenschap, vernielingen, diefstal) en vrijwel alleen op heterdaad. De korpschef beschikte over enkele vertrouwde politieambtenaren die nasporing deden bij levensdelicten en inbraken: de recherche. Aangiftes werden aan het bureau opgeslagen in klappers (registers). Dit systeem bood de mogelijkheid om te controleren of een op heterdaad opgepakte verdachte recentelijk door een politiedienst elders werd gezocht, niet meer dan dat. Het leeuwendeel van de informatie die in de organisatie een weg naar boven vond, betrof de administratieve afhandeling van al dan niet correct gelopen rondes en van andere tekortkomingen en misdragingen van het eigen personeel. Managementinformatie, zouden we nu zeggen.

Professionalisering

Na de Eerste Wereldoorlog veranderde de politieorganisatie onder invloed van onder meer de introductie van de meldkamer en de telex en de aanwending van de dactyloscopie. De politie werd ontvankelijk voor het ideaal van professionalisering dat ook andere maatschappelijke organisaties in zijn greep kreeg. Zij ging zich zien als wetshandhaver. De hiërarchie en de territoriale distributie van het toezichthoudend personeel bleven in stand, maar de politieambtenaren op straat kregen meer bewegingsvrijheid, een ruimere taak, meer opleiding (vooral wetskennis) en de plicht bijzondere voorvallen te rapporteren. Een dagelijks verspreid gestencild overzicht van de voornaamste gesignaleerde delicten hield iedereen bij de les.

In dezelfde jaren vond, onder invloed van de instroom van geschoolde arbeiders in het criminele milieu, ook een professionalisering van de criminaliteit plaats. In het inbrekersgilde traden brandkastkrakers naar voren en in de prostitutie dwong het bordeelverbod souteneurs tot de exploitatie van horeca. De voornaamste criminelen hielden zich op in een ruimtelijk gesloten domein, het zogenoemde criminele milieu, veelal wat louche cafés in zogenoemde 'mindere' buurten. Buurtagenten kenden hun pappenheimers en lieten het een en ander oogluikend toe. Individueel opgebouwde ervaringskennis vormde de basis voor beperkt, proactief optreden. Mocht er sprake zijn van ernstigere zaken, wat veelal hoogstens werd vermoed, dan was dat een kwestie voor de recherche, de bevoorrechte collega's met wie weinig contact werd onderhouden. Ook deze rechercheurs verzamelden inlichtingen, veelal actuele informatie over de gewoontes van personen uit hun doelgroep, vaak ontleend aan persoonlijk contact met enkelen van hen, zogenoemde loodsmannetjes of informanten. Die informatie deelden zij niet met elkaar omdat zij er later persoonlijk beroepsmatig profijt van hoopten te trekken. Informatie delen werd van hen ook niet gevergd.

Nieuwe kennis: modus operandi

In de nieuwe politieorganisatie die na de Eerste Wereldoorlog ontstond, stroomde informatie niet meer alleen omhoog, maar kon opgeslagen informatie ook politie-interventies ondersteunen. Van centrale betekenis waren daarbij de kaartenbakken, die in

deze jaren de registers gingen vervangen. In die kaartenbakken werden persoonsgegevens, antecedenten, portretten en vingerafdrukken van eerder opgepakte criminelen opgeslagen. Hierdoor werd het mogelijk om nieuwe informatie over verdachten toe te voegen aan bestaande informatie over hen, om verdachten te categoriseren en om op basis van secundaire kenmerken vast te stellen welke eerder opgepakte personen mogelijk dader van een opgemerkt delict konden zijn. Aldus kon een deel van het speurwerk voortaan in het bureau worden verricht. Dat systeem van kaartenbakken werkte in de hand dat een aparte groep verdachten werd uitgeselecteerd: de beroeps- en gewoontemisdadigers. Zij werden geacht professionals in de criminaliteit te zijn en die kwalificatie te danken te hebben aan hun bijzondere, criminele vaardigheden: hun modus operandi (MO). Het herkennen van die modi operandi werd daarop de kern van het ambacht van de rechercheur.

Een fraaie illustratie van de kennis waardoor rechercheurs zich in het midden van de twintigste eeuw lieten leiden, is een tekening, gemaakt voor de Haagse brigadier van politie Jochem de Graaf, in de jaren dertig wachtcommandant bij de Centrale Opsporingsdienst.

Figuur 3.1 Tekening voor Haagse brigadier

Vermoedelijk kreeg hij het cadeau van zijn collega's bij zijn pensionering. De Graaf zelf is te zien linksonder in de tekening, steunend op een reeks wetboeken en processen-verbaal, de twee nieuwe 'wapens' van de politie. De overige personen zijn figuren uit de Haagse onderwereld. Voorop loopt Theo R., bijgenaamd De Stier, een beruchte inbreker en souteneur die bekendstond als de ongekroonde koning van het criminele milieu. Zijn vader, eveneens inbreker, duwt midden op de tekening een kinderwagen voort. Die kinderwagen is een verwijzing naar het feit dat hij een aantal jongeren wegwijs had gemaakt in het vak. De pronte dame rechtsonder die een dronken man meesleept, is een vermaarde prostituee die duidelijk de baas was over haar souteneur. Aldus is ook in het gedrag van alle andere personen op de tekening telkens iets eigenaardigs te onderkennen dat karakteristiek is voor hun wijze van optreden, en dat bij de ontvanger van het cadeau en zijn collega's onmiddellijk herkenning moet hebben opgeroepen. Op deze wijze illustreert de tekening dat

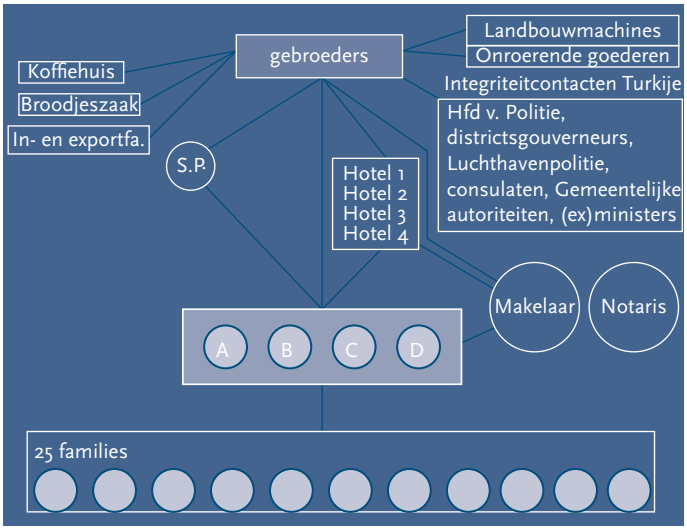
de nieuwe, vakmatige kennis van toenmalige rechercheurs was geordend volgens de structuur van de modi operandi.

3.1.2 Een hiërarchische politie in een netwerksamenleving

Vanaf het einde van de jaren zeventig veranderde de structuur van de politiële kennis. Ook ditmaal was de omslag deel van een samenstel van veranderingen in de samenleving en de politieorganisatie. De introductie van de computer in het maatschappelijk leven in de jaren tachtig, gevolgd door die van het internet in de jaren negentig, fungeerden daarbij als katalysator. Voor de politie was belangrijk dat de criminaliteit, de ordeverstoringen en veiligheidsbehoeften van burgers en overheid van karakter veranderden. In de criminaliteit maakte de penoze, die zich had toegelegd op prostitutie, inbreken en oplichting, plaats voor georganiseerde misdaad, die vooral in de drugshandel een lucratief operatieterrein vond, en voor junkies, die zorgden voor een explosie van zogenoemde kleine criminaliteit. Een justitiële aanpak, steunend op enkelvoudig rechercheren, was tegen deze twee nieuwe opgaven niet opgewassen. Ordeverstoringen werden niet langer veroorzaakt door oppositionele organisaties zoals een communistische partij of een radicale vakbond, maar door spontaan gevormde, losjes georganiseerde groepen die deelbelangen verdedigden, zoals krakers en voetbalhooligans. Een militair opererende Mobiele Eenheid kon tegen guerrilla-achtig optreden van ordeverstoorders weinig beginnen. Ten slotte werd onveiligheid een aantrekkelijk thema voor de media. De ophef die daarin ontstond, was met geruststellende verklaringen van autoriteiten niet meer te dempen.

Voor de politie vormde dit gewijzigde maatschappelijke veiligheidsvraagstuk een lastige opgave. Vanaf de jaren zeventig werd tegen de veranderende zware criminaliteit de telefoontap een veelgebruikt middel, gevolgd door gereglementeerde vormen van infiltratie zoals pseudokoop, het werken in teamverband en analyses van criminaliteit. In de aanpak van ordeverstoringen ging men over tot stafvorming, de oprichting van aanhoudingseenheden, het gebruik van draaiboeken en het verzamelen van *intelligence*. Om aan de geëxpliciteerde onveiligheidbeleving van burgers te voldoen werden buurtbewoners geënquêteerd, wijkteams gevormd en werd samengewerkt met gemeentelijke handhavers. Rode draad in het politiële aanpassingsproces was de introductie van de computer vanaf de jaren tachtig; een decennium later gevolgd door de personal computer. Vanaf dat moment maakte de kaartenbak plaats voor de digitale opslag van informatie, zoals tezelfdertijd in het openbaar bestuur de gemeentelijke basisadministratie persoonsgegevens (GBA) werd geïntroduceerd.

Al deze aanpassingen hadden tot gevolg dat ook de dominante structuur van de politiële kennis veranderde. Niet langer dicteerden de modi operandi het format, maar nu deden dat de onderlinge afhankelijkheidsrelaties tussen betrokken actoren. Het beeld van de criminaliteit werd niet meer gevormd door de eigenaardigheden van de individuele verdachten maar door hun onderlinge functionele banden, niet meer door beroepsmisdadigers en onverbeterlijke lastpakken maar door netwerken die de goede gang van zaken ondermijnen. Een analyseschema uit de opsporing in de jaren negentig maakt dat duidelijk.



Figuur 3.2 Analyseschema opsporing jaren negentig

Hierin staan niet meer de specifieke karaktertrekken van de criminelen centraal, maar hun onderlinge relaties, de bezittingen die hun misdrijven faciliteren en hun relaties met relevante instanties. Die wijziging in het administratieve beeld van de criminaliteit sluit aan bij de verandering in de dominante vorm van detecteren: niet meer individueel speurwerk naar opmerkelijke gedrag, maar ontrafeling van onderlinge hand- en spandiensten van personen in een netwerk. Het sluit ook aan bij een verandering van de dominante vorm van de politiële aanpak: niet meer het erop uit sturen van een ervaren rechercheur of een welbespraakte wijkagent, maar mobilisatie van een handhavingsapparaat dat volop relaties onderhoudt met instanties en organisaties in binnen- en buitenland.

3.2 De opkomst van informatiegestuurd politiewerk nader bekeken

3.2.1 Het concept informatiegestuurde opsporing[1]

Informatie verzamelen heeft altijd tot de kern van het politiewerk behoord. In de afgelopen eeuw onderging deze praktijk tweemaal een radicale verandering, die telkens samenhing met een verandering in de criminaliteit, in de politieorganisatie en in de technische uitrusting van de politie. Wat in deze gevallen oorzaak was en wat gevolg, is lastig vast te stellen. Zoals eerder aangegeven, vond de eerste verandering plaats na de Eerste Wereldoorlog en werden in de politiële informatievergaring de kaartenbak en het forensisch onderzoek geïntroduceerd. De politie ging zich richten op wetshandhaving, de recherche kreeg in de

1 De inhoud van deze paragrafen is grotendeels gebaseerd op Kop, N. & P. Klerks, *Doctrine intelligencegestuurd politiewerk*. Politieacademie, Apeldoorn 2009.

organisatie een prominentere plaats en de focus kwam te liggen op snelle reactie op meldingen van misdrijven. In de jaren zeventig bezweek deze reactieve aanpak onder de snel toenemende omvang van de criminaliteit. In de politiële informatievergaring deden de computer en de criminele inlichtingendiensten hun intrede. De politie ging zich richten op rechtshandhaving, wijkteams kregen in de organisatie een prominente plek en de focus kwam te liggen op verbetering van de veiligheidsbeleving van de bevolking.[2]

Probleemgericht werken

In de discussie over effectief politieoptreden in de nieuwe situatie had het idee van *problem-oriented policing* (POP), in 1979 gelanceerd door de Amerikaanse politiesocioloog Herbert Goldstein, een katalyserende werking. Kern van zijn boodschap was de gedachte dat de politie niet meer slechts moest reageren op meldingen van afzonderlijke misdrijven en overtredingen, maar daarnaast ook op zoek moest gaan naar hun sociale voedingsbodem, zoals conflicten in de buurt, onveilige verkeerssituaties of een gebrek aan toezicht. Telkens terugkerende incidenten zouden kunnen worden beschouwd als symptomen van dieper liggende, maatschappelijke problemen. Inzicht in en aanpak van die problemen, eventueel samen met andere instanties, zou de politie in staat stellen om meer resultaat te bereiken en wellicht zelfs criminaliteit en ordeverstoringen te voorkomen. Het is duidelijk dat probleemgericht werken, naast kennis van de samenleving afkomstig uit vakgebieden als de sociologie, criminologie en psychologie, ook adequate en actuele informatie van lokale situaties vergt.

Wijkgericht werken

De wijkteams, die in de jaren tachtig in de politie hun intrede deden, kregen bij het verzamelen van informatie een belangrijke taak. Zij moesten kennis van de buurt vergaren door nauwe banden aan te knopen met de bewoners. Om preventief te kunnen werken, moet de politie midden in de samenleving staan, in wijken zichtbaar aanwezig en aanspreekbaar zijn. De invoering van wijkteams en wijkagenten was erop gericht de politiezorg dicht bij de burger te brengen en zo ook de informatiepositie te versterken. Kennis van de buurt en haar problemen stond voorop.

In de jaren negentig was in Nederland en het Verenigd Koninkrijk het wijkgericht werken in de politie dominant geworden. Tegen de achtergrond van de nog steeds stijgende criminaliteitscijfers klonk in deze jaren vanuit de politiek en de samenleving kritiek op de effectiviteit van het gebiedsgebonden werken en de verwaarlozing van de recherche. In reactie op die kritiek lanceerde in Engeland de Kent Police een nieuwe manier van werken, waarbij politiepersoneel lokaal gericht werd ingezet op basis van analyses van hardnekkige criminaliteit.[3,4] In plaats van reactief misdrijven op te helderen, ging de politie zich richten op buurten en personen die geassocieerd werden met criminaliteit, daarbij gebruikmakend van informanten en analyses.

---

2 Voor een overzicht van de veranderingen in de Nederlandse politieorganisatie in de twintigste eeuw: Meershoek, G., *De Gemeentepolitie in een veranderende samenleving*. Boom, Amsterdam 2007.

3 Gill, P., *Rounding up the Usual Suspects? Developments in Contemporary Law Enforcement Intelligence*. Ashgate, Aldershot 2000.

4 Ratcliffe, J.H., *Intelligence-Led Policing*. Willan Publishing, Cullompton (Devon) 2008.

ABRIO[5]

In Nederland introduceerde het korps Rotterdam-Rijnmond met hulp van Kent Police midden jaren negentig informatiegestuurde opsporing (IGO).[6] Vervolgens werd het concept met hulp van het programma Accacia, later gevolgd door het programma ABRIO, over de Nederlandse politie verbreid.

Het doel van ABRIO was leidinggevenden een format te verstrekken waarmee de opsporing, vertrekkend vanuit op intelligence gestoelde, afgewogen keuzes, procesmatig kon worden aangestuurd. De focus was aanvankelijk gericht op de aanpak van georganiseerde misdaad door de kernteams en op een vermindering van zogenoemde veelvoorkomende criminaliteit. In overeenstemming met het POP-concept meende men dat niet incidentgericht moest worden opgetreden, maar aan de hand van criminaliteitsclusters zoals seriedelicten, dadergroepen en voor criminaliteit kwetsbare omgevingen als parkeergarages en uitgaansgebieden. Hiertoe moest gericht actuele, betrouwbare informatie over criminaliteit worden ingewonnen en geanalyseerd. De analyses konden worden gebruikt om leidinggevenden te ondersteunen. Naast projectmatige opsporing stond een op de buitenwereld gerichte, proactieve houding centraal. Het management diende in plaats van een actief afwachtende, een actief aansturende opstelling aan te nemen.

3.2.2 Naar een informatiegestuurde politie

De projectgroep ABRIO drong er bij de korpsen op aan om op strategisch niveau met de implementatie van IGO te starten. De politieleiding wilde de aanpak echter niet tot de opsporing beperken, maar het concept ook introduceren in andere bedrijfsprocessen zoals de noodhulp, het wijkgerichte werken en de intake en service. In plaats van informatiegestuurde opsporing werd daarom voortaan gesproken van IGP.[7] De implementatie van het IGP-concept stuitte evenwel op forse moeilijkheden. De verwachting dat de nieuwe aanpak zou leiden tot een verbetering van de kwaliteit van de politieleiding, het politiewerk en de samenwerking met derden werd niet snel bewaarheid. Aangedrongen werd op verandering van de bedrijfscultuur en meer aandacht voor de operationele processen.

In 2005 publiceerde de Raad van Hoofdcommissarissen het rapport *Politie in ontwikkeling* waarin een visie op de toekomst van politiewerk werd geformuleerd en het belang van informatiegestuurd optreden opnieuw werd onderstreept. Analyse van gegevens en informatie zou het hart moeten gaan vormen van de strategische en tactische besluitvorming. Informatiegestuurd werken op basis van veredelde en geanalyseerde informatie werd voor een kennisintensieve uitvoeringsorganisatie als de politie een voorwaarde geacht om verantwoorde keuzes te kunnen maken: 'informatie gestuurde politiezorg brengt relaties aan tussen voorheen gescheiden informatiebronnen en besluitvormingslijnen. (...)

---

5 Aanpak Bedrijfsvoering Recherche, Informatiehuishouding en Opleiding.

6 Jansen, H., 'Informatiegestuurde politie. Van actief afwachten, naar actief aansturen.' In: Broeck, T. van den et al. (red.), *Intelligence Led Policing*. Politeia, Brussel 2005, pp. 34-35.

7 Raad van Hoofdcommissarissen, *Informatie-Gestuurde Politie: sturen op resultaat*. ABRIO, Houten 2005.

Informatie moet binnen de eigen organisatie zo veel mogelijk een neutraal productiegoed worden ten gunste van de effectiviteit van het gehele primaire proces.'[8]

In het rapport werd ook gesteld dat met partners in het veiligheidsdomein op basis van gelijkwaardigheid informatie diende te worden uitgewisseld onder het motto 'van *need to know* naar *need to share and need to show*'.[9] Met het oog op een integrale aanpak van criminaliteit en onveiligheid diende de politie een goed functionerende, nationale informatiearchitectuur te vormen, steunend op steunpunten in de regionale korpsen.[10] Dit streven sloot aan bij het concept *business intelligence* (BI) in de marktsector.

In de volgende jaren trachtten de regionale politiekorpsen hun werkprocessen te verbinden met die van partners binnen en buiten de overheid, veelal op basis van integrale veiligheidsplannen, in de verwachting gebruik te kunnen gaan maken van informatie afkomstig van die partners. Peter Versteegh, hoofd van de onderzoeksafdeling van de toenmalige regiopolitie Haaglanden, sprak daarop de verwachting uit dat het IGP-concept steeds meer zou leiden tot een concept intelligencegestuurde veiligheidszorg (IGV). Deze zou garant staan voor een steeds effectievere aanpak van de onveiligheid.[11] Een parallelle ontwikkeling vond plaats in het openbaar bestuur. Daar werden in 2007 Regionale Informatie- en Expertisecentra (RIEC) opgericht, met het oog op versterking van de bestuurlijke aanpak van georganiseerde criminaliteit.

In 2008 gaf de Strategische Beleidsgroep Intelligence van de Raad van Hoofdcommissarissen een nieuwe impuls aan de verbetering van de informatiehuishouding met het opstellen naar Brits voorbeeld van het *Nationaal Intelligence Model* (NIM). Het NIM formuleerde hoe de politie zich door informatie dient te laten leiden en hoe leiding moet worden gegeven aan de verzameling, bewerking en distributie van kennis op basis waarvan de uitvoering gestuurd kan worden. Het aan het model verbonden programma Intelligence moest zorgen voor de verwezenlijking van het model in de regionale korpsen. Het formuleerde daartoe richtlijnen en zeven doeleinden:

1 een samenhangend stelsel van stuurploegen;
2 veiligheidsproducten verschijnen op basis van de intelligenceagenda;
3 een samenwerkend stelsel van informatieknooppunten;
4 IGP is de manier van werken voor alle politiemensen;
5 de politie innoveert en verbetert voortdurend de intelligencegestuurde organisatie;
6 de politie wisselt informatie en kennis uit met overheidsinstanties;
7 de politie wisselt informatie en kennis uit met instellingen buiten de overheid.

---

8 Raad van Hoofdcommissarissen, *Politie in ontwikkeling*. Nederlands Politie Instituut, Den Haag 2005, pp. 91-93.

9 Raad van Hoofdcommissarissen, *Politie in ontwikkeling*. Nederlands Politie Instituut, Den Haag 2005, p. 94.

10 Raad van Hoofdcommissarissen, *Politie in ontwikkeling*. Nederlands Politie Instituut, Den Haag 2005, p. 95.

11 Versteegh, P., *Informatiegestuurde veiligheidszorg*. Dordrecht: SMVP Producties 2005.

Opsporing of informatie?

Rond 2010 werd in de politieleiding gediscussieerd over de vraag waar het Team Criminele Inlichtingen (TCI), toen nog Criminele Inlichtingeneenheid (CIE) geheten, in de organisatie onder te brengen: bij de informatieorganisatie of bij de opsporing. Hoewel beide varianten voor- en nadelen kennen, werd besloten het TCI in de informatieorganisatie te plaatsen. Dat is nog steeds het geval. Het TCI kwam aldus mentaal verder van de opsporing af te staan. Aanhangers van de opsporingsvariant vonden dat ook het grootste bezwaar van deze keuze. Het belangrijkste argument om het TCI onder te brengen bij de informatieorganisatie was dat het zo informatie breder beschikbaar kon stellen.[12]

In de jaren daarna spanden de regionale korpsen, de Voorziening tot Samenwerking Politie Nederland (VtSPN) en de Politieacademie zich in om het informatiegestuurd werken bij de politie verder in werking te brengen. Zo werd in alle korpsen een informatieorganisatie op afdelings- of regionaal niveau ingericht en zetten de VtSPN en de korpsen de BasisVoorziening Informatie (BVI) op. Voor de politiemensen op de werkvloer en de docenten in het politieonderwijs werd de *Doctrine intelligencegestuurd politiewerk* geschreven.[13] Het aanbod aan opleidingen Intelligence werd uitgebreid en aan de Politieacademie werd een lectoraat Intelligence verbonden. In alle korpsen werd in de informatieorganisatie de nieuwe functie van analist veiligheidsinformatie geïntroduceerd. Zie hoofdstuk 11 Analyse.

3.2.3 Informatiegestuurde politie in ontwikkeling

Drie nieuwe initiatieven trokken de afgelopen jaren de aandacht. In de nieuwe nationale politie kreeg het informatiegestuurd werken een belangrijke plaats, getuige de aandacht in het Ontwerpplan, het Inrichtingsplan en het Realisatieplan. Zo is aan alle tien geografische eenheden en de landelijke eenheid een Real-Time Intelligence Center (RTIC) toebedeeld van waaruit 24 uur per dag, zeven dagen in de week politiepersoneel op straat bij meldingen actief wordt ondersteund met up-to-date informatie, onttrokken aan politiesystemen, gesloten (zoals RDW-Rijksdienst voor het wegverkeer) en openbare bronnen (zoals websites en sociale media). Doel is de kans op een arrestatie op heterdaad en de veiligheid van politiemensen en burgers te vergroten. Tot op heden kost het grote moeite dat doel te bereiken.[14] Voorts wordt er periodiek een nationale intelligenceagenda

12 Kop, N., 'Criminele Inlichtingen Eenheden: dilemma's en kansen.' In: *het Tijdschrift voor de Politie* 74 (2012), nr. 1, pp. 6-10.

13 Kop, N. & P. Klerks, *Doctrine intelligencegestuurd politiewerk*. Politieacademie, Apeldoorn 2009.

14 Scholtens, A., M. den Hengst & R. Waterreus, *Het real-time informeren van noodhulpeenheden: een onderzoek naar de RTI-functie om frontlijnpolitiefunctionarissen snel te voorzien van relevante informatie*. Reeks Politiekunde nr. 77. Reed Business Information, Amsterdam 2016.

Figuur 3.3 Doctrine intelligencegestuurd politiewerk

opgesteld, op basis van het vierjaarlijks opgemaakte Nationaal Dreigingsbeeld (NDB). De briefing wordt bovendien in de vorming van de nationale politie als een van de strategische thema's benoemd.

Ten tweede is een digitale 'Community of Intelligence' opgericht (zie hoofdstuk 18 Community of Intelligence), waarin kennis over intelligencegerelateerde zaken wordt gedeeld en de vakbekwaamheid wordt bevorderd. Er worden bijeenkomsten en workshops georganiseerd, maar ook wordt er virtueel gediscussieerd over delicten, analyse- en onderzoeksmethoden, partners en internationale ontwikkelingen op intelligencegebied.

Ten slotte is de politie aan haar personeel op straat smartphones gaan uitreiken met de applicatie BasisVoorziening Informatie voor Integrale Bevraging (BVI-IB). Met één zoekslag kan informatie uit twintig verschillende (inter)nationale en regionale registers worden opgevraagd. Het nieuwe instrument ondersteunt vooral het toezicht, de handhaving en de noodhulp. In de opsporing is het van minder waarde. Wel draagt BVI-IB daar bij aan een efficiënter werkproces doordat verschillende systemen niet meer apart hoeven te worden geraadpleegd.[15]

15 AEF, *Onderzoek naar de betekenis van integrale bevraging voor het operationele politiewerk*. Wetenschappelijk Onderzoek- en Documentatie Centrum/Ministerie van Veiligheid & Justitie, Den Haag 2014.

Figuur 3.4 MEOS

2015: Politie krijgt app voor identiteitscontroles en boetes

Straatagenten krijgen een speciaal mobieltje met de app, waardoor ze meer tijd aan andere zaken kunnen besteden. De politie heeft een app ontwikkeld waarmee agenten op hun telefoon de identiteit van mensen en paspoorten en rijbewijzen kunnen scannen. Ook kunnen er digitale boetes mee worden uitgeschreven en verwerkt. Dat meldt de politie naar aanleiding van berichtgeving van ANP. De app, MEOS (Mobiel Effectiever Op Straat) genaamd, staat op een speciaal dienstmobieltje die bij wijze van proef al is uitgedeeld aan 10.000 agenten. Een agent met app heeft genoeg aan een naam en geboortedatum om de betreffende persoon met pasfoto op te vragen. De app maakt daarbij gebruik van zowel interne als externe systemen om bijvoorbeeld te kijken of iemand gezocht wordt of gevaarlijk is. Ook openstaande boetes worden vermeld. De politie hoopt dat agenten zo veiliger hun werk kunnen doen en minder onnodige handelingen op straat nodig hebben. Zo kunnen ze hun aandacht aan andere zaken besteden. Het wordt bijvoorbeeld moeilijker een verkeerde identiteit op te geven en er wordt tijd bespaard omdat mensen zonder identiteitsbewijs niet meer meegenomen hoeven te worden naar het politiebureau. Ook wordt de dienstverlening naar burgers toe verbeterd door 'kortere wachttijden en betere informatieverstrekking', aldus de politie. [....][16]

16 *NRC Next* 30 oktober 2015.

3.3 Vooruitzicht

Kennis in de politie is als geld in de economie. Zij is verbonden met alle interne transacties. Zij is een middel om werkelijk belangrijke zaken te bereiken, niet meer dan dat, niet het doel van politieoptreden, maar zij is wel onmisbaar. Kennis kan de politie een strategisch voordeel geven op opponenten en dat is niet onbelangrijk voor een soepele uitvoering van de politietaak. Kennis is begeerlijk, zozeer dat zij soms het belangrijkste lijkt. Dan ontstaat de misvatting dat kennis macht is. Kennis alleen is echter machteloos. Pas als zij op het juiste moment bij de juiste persoon voorhanden is en wordt geaccepteerd, kan zij helpen resultaat te bereiken. Evenals geld berust kennis namelijk onder meer op vertrouwen, vertrouwen in de verifieerbaarheid. En zoals verlies van vertrouwen in de waarde van een munt tot inflatie leidt, zo krijgt een politieorganisatie die steunt op onbetrouwbare kennis, te kampen met gefrustreerde medewerkers en na verloop van tijd met verlies van gezag bij de rechter, bij het bevoegd gezag en uiteindelijk ook bij het publiek.

Sinds enkele decennia ondergaan samenleving en bestuur onder invloed van de personal computer en het mobiele internet ingrijpende veranderingen. De politie probeert hier aansluiting bij te houden en laat zich daarbij leiden door de doctrine *intelligence-led policing* of informatiegestuurd politiewerk. Het is niet vreemd dat een hiërarchische organisatie als de politie meer dan individuele burgers en commerciële ondernemingen moeite heeft om nieuwe technologieën te incorporeren. Hoeveel er ook is veranderd in de politie, als haar optreden wordt afgezet tegen de maatschappelijke behoefte aan veiligheidszorg is het nog onvoldoende. De politie is bijvoorbeeld nog nauwelijks in staat om substantieel weerwerk te bieden aan criminaliteit op internet. In deze bijdrage betoogden wij dat het belangrijk is dat de politie op de ingeslagen weg voortgaat en daarbij, meer dan tot nu toe het geval is, onderkent welke nieuwe structuur de in de samenleving circulerende kennis heeft, welke vormen van kennis de eigen organisatie nodig heeft om te blijven voorzien in de maatschappelijke behoefte aan politiezorg, en last but not least, dat kennis niet leidend maar ondersteunend moet zijn. Miskenning van die gedifferentieerde, eigen behoefte aan kennis leidt algauw tot een eenzijdige versterking van de interne hiërarchie en daarmee tot een verdere afkalving van de eigen positie in de netwerksamenleving.

4 De keerzijde van IGP: IGP en de metamorfose van politiebureaucratie

Ries Straver en Peter van Os

De titel 'De keerzijde van IGP' die wij van de samenstellers van dit boek aangereikt kregen, doet vermoeden dat wij tegenstanders van informatiegestuurd politiewerk (IGP) zijn. Dat is geenszins het geval. Wij vinden dat IGP een waardevol instrument is om beslissingen in het politiewerk, van strategische beleidsvorming tot en met de uitvoering, te ondersteunen, en elders in dit boek is uitgebreid beschreven hoe sophisticated het zich in de afgelopen vijftien jaar ontwikkeld heeft.

Als er een keerzijde is van IGP – een op zich neutrale managementtool – zit hem die vooral in hoe IGP feitelijk wordt ingevuld en gebruikt. Dat is afhankelijk van de visie op organiseren en sturing van het politiewerk in een korps, en hoe die op zijn beurt weer wordt ingekleurd door de visie op de functie van de politie in de samenleving.

Dat behandelen wij in dit artikel. En omdat politie nu eenmaal een frontlijnorganisatie is, kijken we daarbij ook naar de vraag in hoeverre IGP niet alleen de organisatie als geheel helpt, maar vooral ook de politiemens in de uitvoering, in het bijzonder in de basispolitiezorg. Daar immers worden de meeste feitelijke beslissingen genomen.

4.1 Bureaucratie

Sedert ruim vijftien jaar is informatiegestuurd politiewerk een hulpmiddel om politiewerk, dat intrinsiek bureaucratisch is, te sturen. We gebruiken bureaucratie hier in haar neutrale betekenis; een organisatievorm die gekenmerkt wordt door aan regels gebonden procedures, verdeling van verantwoordelijkheid, hiërarchie en onpersoonlijke relaties, en scheiding tussen (politieke) beleidsvorming en ambtelijke uitvoering. Bij de overheid moet dat bijdragen aan gelijke behandeling van burgers en het uitbannen van willekeur. Gebondenheid aan regels is niet alleen belangrijk vanwege de machtsmiddelen die de politie heeft, maar ook omdat de politiemens deel uitmaakt van de (straf) rechtsketen en er scherp op moet zijn dat wat hij vastlegt, bijdraagt aan de toepassing van het recht. Dat vraagt precisie in waarneming van feiten en de taal waarmee die feiten worden vastgelegd. Het gebruik van bevoegdheden is scherp gereguleerd en iedere politiemedewerker moet leren omgaan met een duale rolinvulling; enerzijds de professional als vertegenwoordiger van de rechtsstaat en anderzijds de mens, die heeft gekozen voor dit vak, maar die ook eigen ideeën heeft over wat nodig is voor het goede samenleven.

Politiemensen kunnen dus vanuit twee verschillende oriëntaties gebeurtenissen waarnemen: een oriëntatie op regels en protocollen, de legaal-rationele kant met onvermijdelijk bureaucratische trekken, naast een sociale oriëntatie, waarin waardering vanuit de 'menskant' met persoonlijke trekken, ideeën en voorkeuren. Totaal verschillende brillen van

waaruit totaal verschillende betekenissen kunnen worden verbonden aan wat we waarnemen. Ter illustratie:

> Kort na de vorige reorganisatie in 1994 werden de 47 wijkagenten in Arnhem in het kader van een driedaagse opleiding en bij wijze van experiment, een voor een geïnterviewd over hun wijk.
> Het waren open, niet-gestructureerde gesprekken waarin wijkagenten werden bevraagd over de positieve en minder positieve eigenschappen van hun wijk, ontwikkelingen over een reeks van jaren, de aard van de bewoners, wie de criminelen zijn, probleemveroorzakers of -plekken. Het waren totaal van elkaar verschillende, geanimeerde gesprekken met veelkleurige uitkomsten.
> Enkele maanden later kregen de wijkagenten ieder een A4 waarop cijfermatig de criminaliteitsontwikkelingen van de wijk werden geschetst. Kale cijfers, zonder nadere toelichting. Bij een volgende reeks interviews, die op dezelfde manier werden afgenomen, verhaalden de wijkagenten vooral over deze cijfermatige ontwikkelingen. Kennelijk had het appel dat van het A4'tje uitging het gewonnen van het appel dat tijdens de driedaagse op ze was gedaan. Of was het A4'tje makkelijker te behappen dan de wijk waarin ze werkten?

Al in die tijd, toen IGP binnen de politie nog nauwelijks gestalte kreeg, was dus al zichtbaar hoe makkelijk rationele betekenisgeving (in dit geval het aantal aangiften over een bepaalde periode) de sociale betekenisgeving (hoe ontwikkelt de wijk zich en wat zijn de problemen) kan verdringen. Alleen het eerste – aantallen – is in systemen te vangen, dat kun je bekijken. Sociale betekenisgeving vanuit het politiewerk buiten wordt pas waarneembaar als je er middenin staat.

Twee vormen

In hoeverre die sociale betekenisgeving naast rationele betekenisgeving wordt of mag worden benut, hangt ook af van het type bureaucratie dat de politie is. René ten Bos[1] wijst erop dat in Nederland momenteel twee vormen van bureaucratie zich lijken te vermengen. De Europese (Frans/Duitse) bureaucratie, ook wel aangeduid als het Rijnlandmodel, stoelend op denkers als Goethe en Montesquieu, oorspronkelijk bedoeld om bestuurlijke macht te kanaliseren en gericht op de mainstream of middelmaat, met conflict als intern model. Van een opdracht kan in dat model gemotiveerd worden afgeweken. Regels en voorschriften worden naar de geest nageleefd en niet naar de letter. Anderzijds is er in toenemende mate de Angelsaksische bureaucratie, stoelend op het Amerikaanse tayloriaanse denken. Met interne harmonie als model, te realiseren via hiërarchische verhoudingen en taakverdeling, en gericht op excellentie, standaardisatie en uniformiteit van producten en centralisatie van beheerstaken. Vooral voor overheidsinstellingen lijkt dat problematisch, want een product is wat anders dan dienstverlening of cocreatie. Welke vorm van bureaucratie het best past bij de politieorganisatie is afhankelijk van hoe haar functie wordt benaderd.

1 Bos, R. ten, *Bureaucratie is een inktvis*. Boom, Amsterdam 2015.

4.2 Politiefunctie en politiebureaucratie; een terugblik

In de traditionele visie op de maatschappelijke functie van de politie stond de wettelijke taak 'handhaving van de rechtsorde' en vooral wetshandhaving als doel op zich centraal. Niet als een eigen zelfstandige aan de wet ontleende opdracht, maar in strikte ondergeschiktheid aan het bevoegd gezag. Rechtsorde werd daarbij gelijkgesteld aan wettelijke orde en de vraag wat met wetshandhaving in de samenleving moest worden bereikt behoorde – in elk geval door de politie zelf – niet te worden gesteld. Een instrumentele functiebenadering waarbij, om de uitvoering van de politietaak conform de wet en voorschriften van het bevoegde gezag te waarborgen, de politie werd georganiseerd met de beheersingsmechanismen van de bureaucratie en wel, volgens de typering van René ten Bos, naar het Angelsaksische model.

Veranderend denken

Na het rapport *Politie in Verandering* (PiV) veranderde het denken over de functie van de politie. Orde en wetshandhaving zijn geen doel op zich meer, maar moeten bijdragen aan een democratische, veilige, ordelijke en vreedzame samenleving. Symptoomgericht werken, waartoe instrumentele wetshandhaving leidt, heeft plaats moeten maken voor probleemgericht werken, ook samen met anderen. Verder is het voor de legitimiteit van de politie niet meer voldoende om conform de wet te werken; het werk van de politie moet daarnaast als redelijk, juist en zinvol worden ervaren. Daarvoor is integratie van de politie in de gemeenschap waar zij werkt essentieel als basis voor 'maatwerk': door duurzame relaties en kennis van mensen, problemen en achtergronden hoeft ook minder te worden teruggegrepen op het gebruik van machtsmiddelen.

Verder werd met PiV op de kaart gezet dat de discretionaire bevoegdheid zowel de facto als de jure een kenmerk van de politiefunctie is en dat die discretionaire ruimte op elk niveau bestaat, óók in de uitvoering. Deze discretionaire bevoegdheid is uiteraard niet onbeperkt, maar wordt begrensd door:

a *Het recht:* het handelen van de politie moet niet alleen in overeenstemming zijn met de wet. Ook binnen de ruimte die de wet laat, moeten de maatstaven van het recht in acht worden genomen: rechtsbeginselen, mensenrechten, grondrechten, beginselen van behoorlijk bestuur en van subsidiariteit en proportionaliteit. Dat raakt aan het 'moreel kompas' en ethische grenzen die leidend moeten zijn; wat binnen de grenzen van de wet mag, behoeft of behoort niet altijd te gebeuren. Dat moet het vertrouwen bieden dat de politie – naar iedereen – rechtmatig en rechtvaardig optreedt. Het is een voorwaarde voor de legitimiteit van de politie.

b *Het beleid van het bevoegde gezag en de politieorganisatie zelf*: het moge duidelijk zijn dat een sterke beleidsmatige inperking van de discretionaire ruimte van basisteams en politiemensen de mogelijkheid tot maatwerk en contextgedreven werken vermindert.[2]

2 Musscher, P. van & R. Straver, 'Basisteams inrichten in roerige tijden; over principes waaraan we vast moeten houden.' In: *het Tijdschrift voor de Politie* 78 (2016), nr. 2, pp. 6-12.

Het Rijnlandmodel past hier beter bij dan het Angelsaksische, omdat het de individuele politieman meer ruimte geeft om vanuit de sociale betekenisgeving te opereren. Deze visie vraagt immers dat hij niet alleen wetmatig maar ook rechtvaardig handelt, dat hij probleemgericht probeert te werken, dat hij er oog voor heeft dat zijn optreden gegeven de omstandigheden als redelijk, juist en zinvol moet worden ervaren in de gemeenschap waarin hij werkt.

We zijn nu veertig jaar verder. De visie op de maatschappelijke functie van de politie uit PiV is deel gaan uitmaken van het denken en de waarden van de Nederlandse politie en leidde ook tot anders organiseren. Bij de vorming van de regionale korpsen begin jaren negentig werd gebiedsgebonden politie (GGP) leidend, maar de invulling daarvan was zeer divers.[3]

De ontwikkeling bij de politie sloot aan bij het andere denken in de samenleving over het criminaliteitsvraagstuk dat in 1984 op de kaart werd gezet door de commissie-Roethof.[4] Daarin werd onderkend dat strafrecht en repressie niet de enige oplossing waren maar dat die gezocht moest worden in het aanpakken van de achterliggende oorzaken van veiligheidsproblemen waarin de politie probleemgericht samen gaat werken met bestuur, ondernemingen, instanties en burgers. Daarmee werd de basis gelegd voor wat het integrale veiligheidsbeleid ofwel de gemeenschappelijke veiligheidsaanpak is geworden.

Werken aan resultaten

Toch kwam er rond de eeuwwisseling zowel ten aanzien van het integrale veiligheidsbeleid als de functie van de politie daarin weer een kentering. De onvrede in de samenleving over het gebrek aan succesvolle aanpak van het probleem van criminaliteit en onveiligheid leidde tot politisering van het veiligheidsvraagstuk, tot een roep om *law and order*. Er werd een tekort aan rechtshandhaving geconstateerd. In 2002 leidde dat tot het beleidsplan *Naar een veiliger samenleving* van het kabinet-Balkenende, dat weliswaar de integrale aanpak handhaaft, maar met een zwaar accent op de versterking van de strafrechtelijke rechtshandhaving.[5]

Bij de politie betekende dat een kerntakendiscussie met, als het op integrale veiligheid aankwam, meer kijken naar wat anderen moeten doen. Daarnaast leidde de met het New Public Management overgewaaide nadruk op meetbare resultaten en prestaties tot meer focus op opsporing en handhaving dan op preventie en investeren in relaties en samenwerking. En in het verlengde daarvan de tendens tot meer sturing en beheersing van de uitvoering om de opgelegde of afgesproken resultaten te bereiken. Dat staat op gespannen voet met de discretionaire ruimte die gebiedsgebonden werken vraagt om maatwerk te kunnen leveren. Het was zoeken naar balans.

---

3 Straver, M.A., R. Ulrich & I. van Duijneveldt, *Gebiedsgebonden politie: maatschappelijke integratie en het organiseren van politiewerk*. Politieacademie, Apeldoorn 2010.

4 Commissie Kleine Criminaliteit, *Interimrapport van de Commissie Kleine Criminaliteit*. Commissie Kleine Criminaliteit, Den Haag 1984.

5 Ook in *Politie in ontwikkeling: visie op de politiefunctie* klinkt dat door: de visie op de politiefunctie uit PiV werd in essentie onderschreven, maar veiligheid kreeg ook daar een zwaarder accent; legitimiteit en maatschappelijke integratie werden meer gezien als voorwaarden om resultaatgericht aan een veilige samenleving te werken.

De gangbare strategie die de politie volgde om te werken aan veiligheidsresultaten is het in samenhang hanteren van drie beproefde benaderingen waaraan de politie Haaglanden als treffend motto[6] 'best of three worlds' meegaf; een combinatie van *problem-oriented policing, intelligence-led policing* en *community policing*.

Community policing of gebiedsgebonden politie zorgt voor kennis van de wijk, de mensen en de problemen, de opbouw van relaties met partners en burgerparticipatie en legt daarmee de basis voor problem-oriented policing – probleemgericht werken.

Met problem-oriented policing worden de belangrijkste orde- en veiligheidsproblemen zorgvuldig in beeld gebracht, wordt geanalyseerd wat de oorzaken zijn, wordt nagegaan wat de beïnvloedbare factoren zijn en wat politie, Openbaar Ministerie (OM), bestuur, partnerorganisaties, bewoners en bedrijfsleven daaraan kunnen doen. Daarna wordt onder regie van de gemeente in nauwe samenwerking tussen alle betrokken partijen, organisaties en ook burgers, een op de problematiek afgestemde mix van preventieve, strafrechtelijke en bestuurlijke maatregelen uitgevoerd. De politie opereert dus in het kader van een brede integrale aanpak en draagt daaraan bij door gerichte toezicht- en opsporingsactiviteiten. De aanpak wordt geëvalueerd en draagt bij tot kennis van wat werkt en wat niet werkt.

Randvoorwaarde voor probleemgericht werken is ook intelligence-led policing ofwel informatiegestuurd politiewerk, waarbij de strategische, tactische en operationele sturing en uitvoering permanent moeten worden ondersteund met relevante en actuele informatie en kennis. Vooral voor het lokale veiligheidsbeleid was daarbij de informatie vanuit het gebiedsgebonden werken van groot belang.

Het *Referentiekader gebiedsgebonden politie* (2006)[7] gaf handvatten voor de vormgeving van GGP en voor de gemeenschappelijke veiligheidsaanpak via probleemgericht werken en partnerschap. De vormgeving van IGP (waarvan de ontwikkeling uitgebreid beschreven is in hoofdstuk 3 Kennis voor politiewerk: een blik vanuit het recente verleden) werd beschreven in het *Nationaal Intelligence Model* (NIM) (2008)[8] en hoe IGP en met name analyse kan worden ingezet voor probleemgericht werken in onder andere *Probleemgericht werken in 60 kleine stappen*.[9]

Hoe korpsen feitelijk deze strategieën toepasten, vertoonde een divers beeld zoals blijkt uit meerdere onderzoeken.[10] Hoe je ze invult, heeft namelijk ook te maken met visies op sturing en organiseren van politiewerk; is het Rijnlandse of het Angelsaksische bureaucratiemodel dominant?

---

6 Versteegh, P., Th. van der Plas & H. Nieuwstraten, *The Best of Three Worlds: effectiever politiewerk door een probleemgerichte aanpak van hot crimes, hot spots, hot shots en hot groups*. Politieacademie, Apeldoorn 2010.

7 *Referentiekader gebiedsgebonden politie*. Politieacademie, Apeldoorn 2006.

8 Strategische Beleidsgroep Intelligence, *Waakzaam tussen wijk en wereld: Nationaal Intelligence Model*. 2008.

9 Eysink Smeets, M. & P. van Os, *Probleemgericht werken in 60 kleine stappen*. Politieacademie, Apeldoorn 2010.

10 Zie voor wat betreft GGP: *Gebiedsgebonden politie: maatschappelijke integratie en het organiseren van politiewerk*. Politieacademie, Apeldoorn, en voor IGP: Inspectie OOV, *Informatiegestuurde Politie*. 2009.

4.3 Politiebureaucratie en de vorming van de nationale politie

Verwacht mocht worden dat de komst van de nationale politie tot meer *unité de doctrine* zou leiden, en het heeft er alle schijn van dat bij de inrichting van de nationale politie de Angelsaksische benadering feitelijk de overhand heeft gekregen.[11] De start, met het *Ontwerpplan Nationale Politie* (2011), was nog ambivalent; in de inrichtingsprincipes is er enerzijds nadruk op uniformiteit, centrale sturing, scheiding van beleid en uitvoering en gestandaardiseerde processen, maar anderzijds vind je er ook intenties terug als 'een stevige lokale verankering (p. 7), spreiding van verantwoordelijkheden[12] (p. 7) en vergroting van de professionele ruimte van politiemedewerkers[13] (p. 9)'. In de praktijk van vier jaar reorganiseren zijn die intenties ondergesneeuwd in een inrichtingsproces waarbij zowel de veranderingsaanpak als de situatie waar die toe moest leiden, centraal werd bepaald en detaillistisch werd aangestuurd. Het korps is daardoor vooral zelfreferentieel aan het worden; gericht op de eigen positie, de eigen resultaten. De burger staat alleen op papier centraal.

Hoe dat uitgepakt heeft, blijkt uit meerdere onderzoeken. Wij beperken ons hier tot de basispolitiezorg waarover het recente rapport *Basisteams in de Nationale Politie* een ronduit alarmerend beeld schetst en onder meer constateert:

- Het van bovenaf opleggen van rigide schema's zonder ruimte voor lokale invulling staat op gespannen voet met de telkens weer herhaalde oproep tot professionele ruimte en sturing op vertrouwen.
- De gebiedsgebonden benadering en het probleemgerichte, informatiegestuurde en contextgedreven werken zijn nog ver weg en er zijn ontwikkelingen op gang gekomen die hier belemmerend kunnen werken.
- De wijkagent neemt in het team een te geïsoleerde plaats in.
- De afstand tot de burger is toegenomen en de relatie tussen burgers en politie is verder geformaliseerd en onpersoonlijker geworden.[14]

4.4 De opgave nu: van systeemgedreven naar contextgedreven organiseren in de basisteams

We zien het gebeuren, wellicht ongewild, maar in elk geval ongewenst. Er is wel hoop op een kentering. De nieuwe korpschef Erik Akerboom constateert in *het Tijdschrift voor de*

11 Schouten, I., 'Gebiedsgebonden politiezorg: te simpel voor Den Haag'. In: *het Tijdschrift voor de Politie* 79 (2017), nr. 1.

12 Verantwoordelijkheden en bevoegdheden worden daar belegd waar de aanpak van de veiligheidsproblematiek plaatsvindt.

13 De professionele ruimte van de politiemedewerkers wordt vergroot, zodat zij binnen hun verantwoordelijkheden naar 'bevind van zaken' kunnen handelen.

14 Terpstra, J. et al., *Basisteams in de Nationale Politie: organisatie, taakuitvoering en gebiedsgebonden werk*. Reeks Politiewetenschap nr. 88. Reed Business Information, Amsterdam 2016.

Politie onbalans tussen wat er centraal en decentraal gebeurt en stelt: 'Mensen in de teams en de wijk moeten voelen dat ze zelf hun werk kunnen beïnvloeden, zelf hun keuzes kunnen maken.'[15]

Het moet anders. In het belangwekkende rapport *Omdat de samenleving er aan toe is*[16] uit 2011 werd het verschil tussen de visies op politiebureaucratie op een andere manier weergegeven en de gewenste ontwikkelingsrichting voor de nationale politie aangegeven: een verschuiving van systeemgedreven naar contextgedreven organiseren. Bij systeemgedreven organiseren zijn de interne oriëntatie op het realiseren van top-down vastgestelde doelstellingen en interne normen voor deskundigheid leidend. Bij het contextgedreven organiseren staan burgers en de orde- en veiligheidsproblemen in hun omgeving centraal en richten teams en medewerkers hun activiteiten, resultaten en werkwijzen hierop. Dat geldt met name voor de basispolitiezorg. Voor de specialistische diensten geldt dat de context bepalend is voor het beleid (welke veiligheidsvraagstukken krijgen prioriteit?), maar zijn normen ontleend aan expertise bepalend voor hoe het werk wordt gedaan.

Figuur 4.1 Wijkagenten te midden van burgers

Contextgedreven organiseren zou je kunnen beschouwen als een eigentijdse benadering van het Rijnlandse bureaucratiemodel voor de politie. Het veronderstelt voor de basispolitiezorg wel andere uitgangspunten voor de sturing:

- beleids- en professionele ruimte voor de verschillende organisatorische niveaus en de uitvoering binnen de kaders van eenheids- en landelijk beleid (vrijheid in gebondenheid);

15 Verhagen, C. & M. Hogendoorn, 'Interview Erik Akerboom'. In: *het Tijdschrift voor de Politie* 78 (2016), nr. 6, pp. 12-17.

16 Dinten, W.L. van et al., *Omdat de samenleving er aan toe is*. Stichting Sezen en Bascole, Wijk bij Duurstede 2011.

- de schaal van veiligheidsproblematiek is bepalend voor waar de verantwoordelijkheid ligt; veelal dus het lokale niveau, het teamniveau;
- het eenheidsbeleid beperkt zich tot sturen op hoofdlijnen.[17]

Tegen deze sturingsprincipes wordt in theorie al snel ja gezegd, maar de praktijk van de sturing van het werk is weerbarstig. Geconstateerd kan worden dat de interne logica van moderne sturingsconcepten en managementbenaderingen rondom Planning en Control, procesgericht werken, kwaliteitszorg en ook informatiegestuurd politiewerk het risico inhouden van een systeemgedreven invulling en dan feitelijk meer benut worden voor centrale beheersing van de uitvoering dan ter ondersteuning van decentrale sturing en uitvoering. Laten we kijken hoe dat met IGP uitpakt.

4.5 Contextgedreven werken en informatiegestuurd politiewerk

IGP veronderstelt dat informatie volledig, snel, flexibel en efficiënt wordt vergaard, verwerkt en geanalyseerd. Zo kan een permanente en actuele ondersteuning met informatie- en analyseproducten gerealiseerd worden voor de beslismomenten in het politiewerk op strategisch, tactisch en operationeel sturingsniveau en in de uitvoering.

Prima, maar ondersteunt de wijze waarop IGP nu feitelijk is ingevuld het contextgedreven werken in de basispolitiezorg voldoende? Met andere woorden, bevordert IGP in de basisteams en districten dat daar het werk zó gestuurd en door politiemensen uitgevoerd kan worden, dat ze gelet op de specifieke problematiek in hun gebied het maatwerk leveren dat daar optimaal bijdraagt aan veiligheid, orde en vrede, en dat leidt tot waardering en vertrouwen? En aan de andere kant, bevordert IGP voldoende dat de waarnemingen in de uitvoering, die zo belangrijk zijn voor het vroegtijdig onderkennen van veiligheidsproblemen of spanningen in de gemeenschap, ook meegenomen worden in de informatie waarmee het beleid wordt ondersteund? Met andere woorden, wordt de politieman of -vrouw voldoende benut als bron van informatie?

Op dat gebied is nog een wereld te winnen, want geconstateerd kan worden dat naarmate de beslissingen die door de informatieorganisatie moeten worden ondersteund, dichter bij de uitvoering en de dagelijkse sturing van het politiewerk op straat komen, de kloof tussen idee en werkelijkheid van IGP toeneemt.[18] Het hiervoor geschetste risico van een systeemgedreven en top-down invulling lijkt dit in de hand te werken.

Waarom slagen instellingen als Buurtzorg, die ook contextgedreven verondersteld worden te werken, er eigenlijk wel in om hun informatieondersteuning daarop te

17 Zie voor een verdere uitwerking: Musscher, P. van & R. Straver, 'Basisteams inrichten in roerige tijden; over principes waaraan we vast moeten houden.' In: *het Tijdschrift voor de Politie* 78 (2016), nr. 2, pp. 6-12.

18 Zie bijvoorbeeld Duijneveldt, I. van, P.M.A. Meesters & M.A. Straver, *Dit helpt ons echt!* Politieacademie, Apeldoorn 2012, hoofdstuk 3.

organiseren met een minimale overhead (minder dan 10 procent) en moderne informatiesystemen? Het verschil zit hem in onze ogen in de oriëntatie die daarbij wordt gehanteerd. Bij Buurtzorg is de dominante oriëntatie 'de professional in de uitvoering', de professionaliteit wordt benaderd vanuit de mensen; medewerkers zijn vakmensen en de organisatie is een organisatie van professionals, en informatiesystemen ondersteunen de sociale oriëntatie waarbinnen deze medewerkers samenwerken. Bij de politie is de dominante oriëntatie het bedrijfsmatige (Angelsaksische) model. De basis voor professionaliteit zijn niet de *mensen,* maar de organisatie die de professionele uitvoering door mensen bewerkstelligt door het hanteren van bedrijfsmatige instrumenten waaronder informatiesystemen. Niet de individuele politiemens als bron en eindgebruiker van informatie staat centraal, maar het systeem: het sturingssysteem en de op uniformiteit en producten ontworpen informatiesystemen.

Om de gememoreerde kloof van IGP op papier en in de werkelijkheid te illustreren, zoomen we in op de (de)briefing.

Een voorbeeld: (de)briefing

In de *Doctrine intelligencegestuurd politiewerk*[19] wordt de briefing een cruciaal onderdeel in het sturings- en informatieproces genoemd. Met als doel het verstrekken van informatie en het uitzetten van werkopdrachten. De doctrine werkt dat verder uit evenals de debriefing, die als doel heeft de check of de werkopdrachten zijn uitgevoerd, het 'aftappen' van informatie en ten slotte coachen en leren.

Maar de negatieve evaluaties over hoe dit alles in de praktijk werkt, hebben zich in de loop der jaren opgestapeld.

In een recent onderzoek[20] naar de werking van briefings formuleren de onderzoekers het genuanceerder: 'Wil de briefing voor operationele medewerkers meer betekenis en operationele waarde krijgen, dan zal de briefing an sich, en ook de in de briefing gepresenteerde informatie, moeten voldoen aan de vier effecten alertheid, sturing, teambuilding en leren.' Een pleidooi dus voor een oriëntatie op de wereld van de professional, zodat IGP iets van hen wordt.

- *Alertheid* gaat over het herkennen van situaties op straat en daar juist naar kunnen handelen. In de briefing wordt wel veel gedeeld, maar behalve bij informatie die raakt aan eigen veiligheid leidt dit niet altijd tot het gewenste effect, namelijk informatie die betekenis krijgt in het werk op straat.
- *Sturing.* Het daadwerkelijk aansturen van politiemedewerkers door ze op basis van informatie opdrachten te geven, blijft precair; slechts een ruime helft van de deelnemers geeft aan sturing te ervaren. De cruciale rol van de leidinggevenden >>

19 Kop, N. & P. Klerks, *Doctrine intelligencegestuurd politiewerk*. Politieacademie, Apeldoorn 2009.

20 Hengst, M. den & M. In 't Veld, *Briefen voor en door basisteams*. Politieacademie, Apeldoorn 2014, p. 30 e.v.

>> kan beter. Vaak besteden zij hun rol uit aan anderen of verzorgen zij een briefing met inhoudelijk materiaal dat anderen (dikwijls buiten het team) hebben voorbereid. Veel leidinggevenden zien de briefing niet als het sturingsmoment.

- Bij *teambuilding* wordt onderkend dat veel *intelligence* inmiddels real-time beschikbaar is. Samenkomen om informatie uit te wisselen, wordt minder nodig. Die tijd kan beter besteed worden om de interne sociale banden tussen collega's en de leidinggevende te versterken.
- Tot slot *leren*, in onze ogen een cruciaal aspect. Ervaringen gedurende de laatste jaren met initiatieven als Blauw Vakmanschap en duurzaam verbeteren, die gericht zijn op het ondersteunen van intercollegiaal leren op de werkvloer, wijzen uit dat de behoefte eraan bij politiemensen enorm is, maar dat ze daar echt hulp bij nodig hebben.[21]

De onderzoekers spreken vervolgens over de vijf briefingmythen[22]: onderliggende bedoelingen van de briefings, die door de ontwerpers steeds maar weer in de lucht worden gehouden ('gij zult…'), maar die eigenlijk niet realistisch of achterhaald zijn. We noemen ze en voegen daar een eigen kleur aan toe.

1 *Politiemedewerkers mogen geen informatie mislopen.*
Uit onderzoeken blijkt echter dat veelal meer informatie wordt aangeboden dan mensen kunnen onthouden en dat het dan 'essentieel' is voor het werken op straat. Briefen met een overload aan intern van belang gevonden informatie zorgt ervoor dat de politieman op straat minder openstaat voor zijn omgeving.

2 *De briefing is het moment voor het operationeel leiderschap en de verdeling van operationele opdrachten per persoon.*
Feitelijk wordt dat niet gerealiseerd. De operationeel leidinggevende voelt zich in veel gevallen geen eigenaar van de briefing, of wordt door allerlei andere taken zo van het werk gehouden, dat diegene er niet aan toe komt. Vaak besteedt hij de briefing aan anderen uit, of is de inhoud niet door hem of haar voorbereid. Het wrange is dat dat in veel gevallen ook voor de niet-operationeel leidinggevende niveaus geldt.

3 *De briefing is een integraal product waaraan alle disciplines zichtbaar een bijdrage leveren.*
Dit is in de praktijk hoogst zelden het geval. Verschillende disciplines voeden de briefing op verschillende manieren met informatie, prioriteiten worden vanuit hogere managementlagen ingebracht en de informatieafdeling zit meestal op afstand. Interne scheiding tussen processen en afdelingen belemmeren sturing en ondersteuning vanuit complete, consistente, actuele en contextrelevante informatie. >>

21 Maas, H. et al., *Blauw Vakmanschap laten werken*. Politieacademie, Apeldoorn 2016.

22 Hengst, M. den & M. In 't Veld, *Briefen voor en door basisteams*. Politieacademie, Apeldoorn 2014, p. 129 e.v.

>>

4 *De briefing is een plek voor procedures, protocollen of persoonlijke aangelegenheden.*
Hoewel er andere kanalen (Intranet, Politiekennisnet (PKN) en dergelijke) zijn om deze informatie te delen, komen er te veel randzaken aan de orde die de aandacht van de sturingsinformatie afleiden.

5 *Iedere leidinggevende binnen de politie bezit vaardigheden om een adequate briefing te verzorgen.*
In de praktijk moet de leidinggevende het over het algemeen doen met de eigen praktijkervaring en zijn de vaardigheden niet altijd aanwezig.

Waartoe dat leidt, is ook terug te vinden in het eerdergenoemde rapport *Basisteams in de Nationale Politie: 'De* verwachtingen hierover (briefing) zijn weliswaar hoog, maar het informatiegehalte, de betrokkenheid en de mate waarin gericht werkopdrachten worden verstrekt, zijn in de praktijk vaak teleurstellend. Het maakt eerder de indruk van een routinematige voorbereiding en van een sterk ritualistische uitvoering.'
Veelzeggend is dat in de basisteams de debriefing nog steeds nagenoeg ontbreekt. Al met al lukt het in de basisteams nauwelijks via gerichte sturing tot een minder reactieve en incidentgedreven invulling van het werk te komen.

4.6 IGP dienstbaar maken aan contextgedreven basispolitiezorg

IGP is geen panacee voor alle kwalen. Het voorbeeld maakt duidelijk dat de invulling beter kan, maar wij zijn van mening dat het *Kurieren am Symptom* blijft als binnen de politie de organisatie en sturingsprincipes niet verschuiven naar het Rijnlandmodel en richting contextgedreven organiseren.

Een verschuiving dus naar een organisatie die de politiemedewerker en de wijze waarop de professionele ruimte wordt benut, centraal stelt, niet door die te beheersen maar door die te ondersteunen. Zelfs voor de kanjers komt er zoveel 'organisatorische ruis' op de lijn, dat een 'contextgedreven oriëntatie' wordt bemoeilijkt of zelfs onmogelijk wordt gemaakt. Hoe complexer, inconsequenter en veeleisender het systeem wordt waarin je werkt, hoe moeilijker het wordt om 'buiten-gewoon' je werk te doen. De centrale vraag is dus niet: 'Hoe stop ik de professional vol met sturingsinformatie?', maar in de eerste plaats: 'Hoe help ik hem of haar bij dit moeilijke werk?', en in de tweede plaats: 'Hoe kan de organisatie hier wijzer van worden?' Van een informatie*gestuurde* naar een informatie*gebruikende* organisatie.

Daarbij willen we het echter niet laten. Hierna geven we een aantal aangrijpingspunten om IGP voor de basispolitiezorg meer contextgedreven in te vullen. We gaan daarbij niet in op de technologische aspecten en de organisatie van de informatieorganisatie, maar vooral op de sturingsaspecten.

Balans

Er moet meer balans komen tussen bottom-up en top-down invulling van IGP, en tussen de ondersteuning met informatie, analyse, veiligheidsdeskundigheid en kennis die nu vooral de sturing op eenheidsniveau en districtsniveau bedient, en de sturing op teamniveau. Voor het overgrote deel van het politiewerk en de orde- en veiligheidsproblemen is de sturing op teamniveau van de uitvoering bepalend voor de effectiviteit. Probleemgericht werken vraagt sturing dicht bij de betrokken orde- en veiligheidsproblemen, en ondersteuning daarvan met decentrale analyse en kennis.

Protocollering

De protocollering van de sturingsoverleggen en briefing en debriefing is op papier een sluitend systeem, maar moet zowel wat betreft het proces als ten aanzien van de te gebruiken informatieproducten meer rekening houden en ruimte bieden aan de behoefte op teamniveau. Zo niet dan is 'rituele' sturing het gevolg, sturing die voldoet aan de regels maar niet is toegesneden op de specifieke problematiek in het teamgebied, en die derhalve minder effectief is.

Sturen en verantwoorden scheiden

Mede onder invloed van het Amerikaanse CompStat-systeem heeft het verantwoorden van resultaten de afgelopen tien jaar steeds meer aandacht gekregen. Planning en control en managementinformatiesystemen werden er op aangepast, en de methodiek van het in managementteams verantwoorden van resultaten van districten c.q. teams heeft ook in Nederland veel navolging gekregen en is vaak het belangrijkste sturingsmoment, waarbij echter de verantwoording van prestaties en resultaten centraal staat. Daarbij zijn wel een paar kanttekeningen te plaatsen.

1 Sturing en verantwoording zijn niet synoniem; sturen is vooruitkijken, verantwoorden is terugkijken en maakt hooguit bijsturing mogelijk.
2 Verantwoording van resultaten leidt tot aandacht op wat meetbaar is, op input en output. Preventie en proactie laten zich daar maar slecht in vatten en de orde, vrede en veiligheidssituatie in de wijken staan daarbij niet vanzelfsprekend centraal.
3 Sturing via verantwoording kan leiden tot een verkeerde dynamiek. Benchmarking en ranking kunnen hulpmiddelen zijn om van elkaar te leren, maar ook ervaren worden als *blaming and shaming* en dan de voorbereiding en praktijk van het sturingsoverleg negatief beïnvloeden en de kwaliteit van de sturing schaden.

Relatie basisteams – informatieorganisatie

Een hechtere relatie tussen de basisteams en de informatieorganisatie is gewenst. De informatieorganisatie moet 'dichtbij' zijn. Vanuit de districtelijke informatieknooppunten (DIK) moeten 'liaisonofficieren' die de veiligheidsproblematiek in het team kennen en op de hoogte zijn van de actuele veiligheidsitems, het sturingsoverleg en de briefings permanent ondersteunen. Teams hebben voor de tactische en vooral de operationele en dagelijkse sturing een schreeuwende behoefte aan meer snelle, actuele en contextspecifieke informatieondersteuning op basis van permanente monitoring; het doorlopend veredelen en analyseren van de meest actuele (politie)gegevens.

Die nabijheid en betrokkenheid van de informatieorganisatie moet ook tot meer wisselwerking leiden; dat er ook meer informatie vanuit het dagelijks werk in het gebied

wordt gegenereerd en doorgeleid naar (de systemen van) de informatieorganisatie, ten behoeve van betere informatie en analyse ter ondersteuning van de politieorganisatie en de netwerken met partners.

Spilfunctie wijkagenten

Belemmeringen die verhinderen dat de wijkagenten een spilfunctie vervullen in IGP moeten worden weggenomen. Zij kunnen de wijk of het dorp 'lezen', onder andere door de contacten in de wijk of het dorp met de sleutelfiguren daar – de mensen die door hun positie, functie of achterban niet alleen een positie hebben om een positieve invloed te hebben in een gemeenschappelijke veiligheidsaanpak of het voorkomen van maatschappelijke onrust, maar ook een bron zijn van voor het politievak zo belangrijke informatie. Het vergaren en inbrengen van die kennis over, en zicht op, het veiligheidsbeeld in de wijk, moeten stelselmatiger gestimuleerd worden en veel meer ingezet kunnen worden als input voor de veiligheidssturing op teamniveau en de briefings en de analyses op thema's.

Dat vraagt, gelet op de actuele stand van zaken rond de rol van de wijkagent[23], vooral veranderingen in de basisteams, maar dat neemt niet weg dat ook de relatie met de informatieorganisatie moet worden versterkt via de DIK's. Die moeten de wijkagenten actief voorzien van informatie en benaderen met informatievragen, en hun informatie als een essentiële verrijking en verdieping van het veiligheidsbeeld gebruiken.

Figuur 4.2 Wijkagent bezoekt moskee

Burgerparticipatie

Ten slotte: IGP moet bijdragen aan een probleemgerichte aanpak in nauwe samenwerking met anderen. Met name de actieve betrokkenheid van burgers speelt daarbij een doorslaggevende rol. Burgers en ondernemers zijn op allerlei manieren actief in het verbeteren van

23 Terpstra, J. et al., *Basisteams in de Nationale Politie: organisatie, taakuitvoering en gebiedsgebonden werk*. Reeks Politiewetenschap nr. 88. Reed Business Information, Amsterdam 2016.

de leefomstandigheden in hun omgeving. Veiligheid is daarbij altijd een dominant thema. De politie is er om dat soort processen te ondersteunen. Voor een effectieve informatie-uitwisseling in het kader van samenwerking met externe partners én met burgers, is actieve wederkerigheid de sleutel. Dat houdt in dat de politie niet alleen informatie uit het veld ontvangt, maar ook informatie verstrekt en rekening houdt met de wensen van de burger. Dat vraagt actieve uitwisseling met burgers die betrokken worden bij het vinden van oplossingen voor veiligheidsproblemen in de wijk. Daarbij kunnen zij informatie verschaffen over locaties, delicten, overlast, daders en slachtoffers, en over sterke en zwakke punten in de aanpak. Dat is in het kader van de gebiedsgebonden veiligheidsaanpak een onmisbare aanvulling op de traditionele informatiebronnen.

4.7 Tot slot

Onze bijdrage begon ermee dat wij ondanks de titel van deze bijdrage geenszins tegenstanders van IGP zijn. De 'keerzijde van IGP' die wij beschreven, is meer de keerzijde van het rationele en systeemgedreven organiseren van de politie, dat de laatste jaren alleen maar lijkt te zijn versterkt. Daar ligt het echte probleem! Een riskant probleem in een periode van turbulentie, van snelle en ingrijpende veranderingen waaronder de toenemende polarisatie die ook op straat soms heftig ontspoort, en die onze relatie met een deel van de bevolking onder druk zet. Die werkelijkheid is alleen te begrijpen als de sociale oriëntatie van het politievak weer de volle ruimte krijgt die het verdient.

Deel II
De werking van IGP: wat mag en wat niet?

5 De Wpg[1]

Suzanne Franken

5.1 Inleiding

Hoewel het begrip informatiegestuurd politiewerk (IGP) als zodanig niet wordt genoemd in de Wet politiegegevens (Wpg) of de memorie van toelichting van de Wpg, is de wet van groot belang voor het IGP-gedachtegoed. Het Wetboek van Strafvordering (Sv) geeft de voorschriften voor het verzamelen van gegevens, maar de Wpg geeft de voorschriften voor het verwerken ervan. Aangezien gegevens de kern vormen van het primaire politieproces en duizenden collega's dagelijks gebruikmaken van de gegevens die door hun collega's zijn verzameld, is de Wpg voor het politiewerk even belangrijk als het Wetboek van Strafvordering.

Figuur 5.1 Politiemedewerker die op de computer werkt

1 Delen uit dit hoofdstuk zijn afkomstig uit *Privacy by design*, het *Praktijkhandboek Wpg* en de *Handreiking verwerken van politiegegevens*. Als je goed op de hoogte bent van de Wpg, kun je direct naar paragraaf 5.4; daar gaan we dieper in op bepaalde IGP-elementen van de wet.

5.1.1 Context van de Wet politiegegevens (Wpg)

De Wpg beschrijft op welke wijze gegevens mogen worden verwerkt voor de politietaak en voor welke doeleinden ze mogen worden gebruikt.[2] De wetgever heeft deze wet opgesteld met als doelen:

- betere opsporing door meer gegevens met elkaar te delen in het hele land;
- beter gegevens delen door zorgvuldig autorisatiebeheer en gegevens beschikbaar te stellen, met name via de informatieorganisatie;
- de privacy waarborgen van personen over wie wij gegevens vastleggen;
- gebruikmaken van technologische ontwikkelingen zoals *datamining*. Dit maakt slim opsporen en informatiegestuurd politiewerk mogelijk;
- meer lokale samenwerking en politiegegevens delen met publieke en particuliere organisaties, omdat ook zij een taak kunnen hebben bij de integrale veiligheidsaanpak;
- internationale informatieverstrekking stimuleren om criminaliteit te bestrijden.

De 'grote broer' van de Wpg is de Wet bescherming persoonsgegevens (Wbp). Die geldt voor de meeste instanties en bedrijven. Voor het verwerken van persoonsgegevens voor de politietaak is er specifieke wetgeving in de vorm van de Wpg omdat:

- de politie gegevens over burgers registreert zonder dat zij daar vooraf toestemming voor geven;
- waarheidsvinding het risico met zich meebrengt dat politiegegevens onjuist, zeer gevoelig en onvolledig zijn[3];
- de politie een bijzondere rol in de maatschappij heeft in de verhouding tussen overheid en burger. De wet reguleert het informatieproces, waardoor dit transparant en controleerbaar is.

5.1.2 Reikwijdte van de Wpg

De Wpg is van toepassing op de verwerking van persoonsgegevens die in het kader van de politietaak worden verwerkt. De Wpg is niet van toepassing bij:

1 toezichthoudende taken van de politie die niet behoren tot de taken ten dienste van justitie (art. 1 lid 1 onder i Politiewet 2012). Bijvoorbeeld het uitvoeren van prostitutiecontroles ('burgemeesterstaken'); deze gegevens vallen onder de Wbp. De wapenvergunningenadministratie wordt uitgevoerd onder de Wpg;
2 gegevens met betrekking tot een rechtspersoon die niet herleidbaar zijn tot een natuurlijke persoon;
3 gegevens bedoeld voor persoonlijke doeleinden van de politiefunctionaris;
4 gegevens bedoeld voor interne bedrijfsvoering van de politie;
5 gegevens die de politie verwerkt over bezoekers en bijvoorbeeld leveranciers (daarop is de Wbp van toepassing).

---

2 De Wpg regelt niet de bevoegdheid om gegevens te verkrijgen. Dat gebeurt vooral in het Wetboek van Strafvordering, de Politiewet 2012 en bijzondere wetten.

3 Politiegegevens kunnen weliswaar correct zijn verwerkt, maar de gegevens zelf kunnen onjuist zijn. Het strafbare feit is, anders dan bij justitiële gegevens, nog niet bewezen verklaard door de rechter.

Een twitterende wijkagent hoort dat een burger een filmpje op YouTube heeft geplaatst. Je ziet hoe twee 'flipperende' dames zich toegang tot een woning verschaffen. Eindelijk zijn ze in beeld! Wat mag hij hiermee doen?

Het plaatsen van een tweet naar het filmpje is op de grens. De beelden zijn (nog) geen politiegegevens. Let op dat je niet meewerkt aan particuliere opsporing en volg de Aanwijzing Opsporingsberichtgeving en de richtlijnen van het landelijk programma Social Media.[4] *Deze schrijven waarschijnlijk voor dat er eerst aangifte gedaan dient te worden.*

5.2 Begrippen

De volgende begrippen zijn van belang om de betekenis van de Wpg goed te kunnen begrijpen. In paragraaf 5.4 Belangrijke onderdelen van de Wpg voor IGP komen nog meer begrippen en concepten aan de orde die speciaal voor IGP van belang zijn.

5.2.1 Politiegegeven

Een politiegegeven is een gegeven dat te herleiden is tot een geïdentificeerd of identificeerbaar natuurlijk persoon en dat in het kader van de politietaak wordt verwerkt, bijvoorbeeld in een (geautomatiseerd) systeem. Denk aan een naam, adres, kenteken, mutatie of procesverbaal. Ook signalementgegevens, een uitgelezen telefoon, foto of vingerafdrukken kunnen tot identificatie leiden en zijn daarom politiegegevens. Ook al weet je nu (nog) niet om wie het precies gaat.

5.2.2 Verwerken

Elke handeling die je verricht met politiegegevens, is voor de wet een verwerking. Dus het vastleggen, raadplegen, vergelijken, wijzigen, tonen en verstrekken zijn allemaal vormen van verwerken. Als de wet zegt dat gegevens vijf jaar mogen worden verwerkt, betekent dit dus ook dat je ze na die tijd niet meer mag raadplegen.

5.2.3 Verwerkingsgrondslag

Het doel waarvoor politiegegevens worden verwerkt, bepaalt op welke wijze ze mogen worden gebruikt en onder welke voorwaarden. Zo hebben bijvoorbeeld meer medewerkers toegang tot gegevens die verwerkt zijn voor de dagelijkse politietaak (artikel 8) dan tot gegevens die worden verwerkt door het Team Criminele Inlichtingen (TCI) (artikel 10). Paragraaf 5.3 Voor welke doeleinden mag de politie gegevens verstrekken? beschrijft alle verwerkingsgrondslagen.

4 http://intranet.politie.local/algemenedocumenten/1315/wie-wat-waar-social-media.html.

Bij de judovereniging is er acht jaar geleden een zedenschandaal geweest. Het nieuwe bestuur wil de trainers en medewerkers bij de politie laten screenen. Wat zijn daartoe de mogelijkheden?

Het is geen onderdeel van de politietaak om te screenen. Een Verklaring Omtrent het Gedrag (VOG) is hiervoor het aangewezen middel (subsidiariteitstoets). Een veroordeling staat vast, maar politie-informatie is zachter. Het verstrekken van politiegegevens voor het screenen van betrokkenen zou alleen kunnen als de ontvanger een eigen rechtsgrond heeft in een wet om dergelijke besluiten te nemen. Ook moeten alle waarborgen met betrekking tot kenbaarheid en transparantie zijn betracht evenals het recht op bezwaar en beroep. We leven in een rechtsstaat: een keer verdacht of veroordeeld wil niet zeggen dat je daar je leven lang last van hebt in het normale maatschappelijke verkeer.

5.2.4 Delen van politiegegevens

Voor effectief informatiegestuurd politiewerk is het cruciaal dat gegevens daadwerkelijk gedeeld worden. De Wpg stimuleert dit doordat er een plicht is opgenomen om informatie ter beschikking te stellen.[5] Het motto binnen de Wpg is 'delen, tenzij'; er bestaat een *free flow of information* binnen het volledige Wpg-domein. Dit geldt naast de politie ook voor de Koninklijke Marechaussee, Rijksrecherche en opsporingsambtenaren van de bijzondere opsporingsdiensten (BOD'en). De BOD'en zijn de Fiscale Inlichtingen- en Opsporingsdienst - Economische Controledienst (FIOD-ECD), de Inspectie Sociale Zaken en Werkgelegenheid (ISZW) (voorheen Sociale Inlichtingen- en Opsporingsdienst: SIOD), de Nederlandse Voedsel- en Warenautoriteit - Inlichtingen- en Opsporingsdienst (NVWA-IOD) en de Inspectie Leefomgeving en Transport/Inlichtingen- en Opsporingsdienst (ILT/IOD). Door deze plicht om te delen, maakt de wetgever beter informatiegestuurd werken mogelijk. Zo kunnen politiegegevens die bijvoorbeeld verkregen zijn bij een verkeerscontrole (artikel 8-gegevens) verder worden verwerkt in een drugsonderzoek (artikel 9-gegevens). Alleen op deze wijze voorkom je dat er bijvoorbeeld twee observatieteams hetzelfde subject volgen zonder dat van elkaar te weten.

Een groot deel van deze terbeschikkingstellingen verloopt geautomatiseerd, bijvoorbeeld doordat de gegevens uit de BasisVoorzieningen Handhaving (BVH) landelijk kunnen worden bevraagd met integrale bevraging (BasisVoorziening Informatie voor Integrale Bevraging – BVI-IB) of Mobiel Effectiever Op Straat (MEOS). Of door autorisatiemechanismen in Summ-IT zodat opsporingsinformatie wordt gedeeld met eenieder die dat nodig heeft voor zijn werk. Dit werkt vooral binnen het politiedomein, en nog niet binnen het volledige Wpg-domein zoals met de BOD'en.

Voor het ter beschikking stellen, gelden de volgende voorwaarden:

1 Er wordt gedeeld met een collega binnen het Wpg-domein die geautoriseerd is.
2 Deze medewerker heeft het gegeven nodig voor een goede uitvoering van de politietaak.

5 Artikel 15 lid 1 Wpg.

3 Die (verdere) verwerking is expliciet toegestaan door de wetgever.
4 Als het gaat om artikel 9- of artikel 10-gegevens: er is instemming van de bevoegd functionaris en er is geen weigeringsgrond van toepassing (artikel 2:13 Besluit politiegegevens (Bpg).[6]

Een tweede manier van delen, is met organisaties buiten het Wpg-domein en met burgers. Dit kan alleen als de Wpg het expliciet mogelijk maakt. Denk aan gemeenten, de Belastingdienst, de Stichting Processen Verbaal en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). In een samenwerkingsverband kan onder voorwaarden ook verstrekt worden aan partners zoals een woningbouwvereniging en winkeliers. In de Verstrekkingenwijzer vind je het totaaloverzicht van instanties met de daarbij behorende voorwaarden. Deze instanties kunnen politiegegevens nodig hebben voor het verrichten van hun eigen taken, maar ze kunnen ook bijdragen aan de politietaak. Zij kunnen bijvoorbeeld hulp verlenen of strafbare feiten voorkomen doordat ze beschikken over politiegegevens. Het gaat hier om elke vorm van bekendmaken: zowel mondeling als schriftelijk meedelen, maar ook online toegang tot systemen, het geven van een printuitdraai, het laten meekijken op een beeldscherm of bevestigend antwoorden op een vraag.

Check bij het verstrekken de identiteit en de functie van een partner. En realiseer je dat partners zich vaak niet bewust zijn van het wettelijk kader waar de politie zich aan te houden heeft. Soms moet je dus uitleggen waarom gegevens niet verstrekt kunnen worden.

5.3 Voor welke doeleinden mag de politie gegevens verwerken?

5.3.1 Overzicht van de verwerkingsgrondslagen

De wet formuleert verschillende doelen waarvoor politiegegevens mogen worden verwerkt: de verwerkingsgrondslagen. In figuur 5.3 zie je hoe deze zich tot elkaar verhouden. Van belang is dat je je ervan bewust bent onder welk regime gegevens thuishoren. Alleen dan kun je beoordelen hoe je de gegevens mag gebruiken, of je ze mag verstrekken en of er speciale voorwaarden van toepassing zijn. Voor elk regime gelden andere regels. De wet onderkent de volgende verwerkingsgrondslagen, die we in de volgende paragrafen nader toelichten:

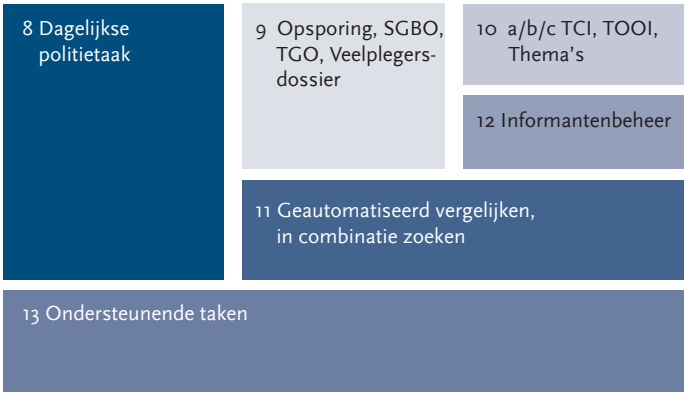
- dagelijkse politietaak inclusief eenvoudige opsporingsonderzoeken (artikel 8);
- uitgebreidere opsporingsonderzoeken en veelplegersdossiers (artikel 9);
- opbouwen informatiepositie door het TCI, Team Openbare Orde Inlichtingen (TOOI) en themaverwerking (artikel 10);
- de mogelijkheid om verbanden te leggen tussen gegevens (artikel 11);
- beheer en controle van informanten (artikel 12);
- de ondersteuning van de politietaak (artikel 13);
- het bewaren van verwijderde politiegegevens (artikel 14).

6 Zie voor aanwijzing van de bevoegd functionarissen artikel 2:10 Bpg. Hierbij speelt ook de zaaksofficier een rol.

Personen en instanties	Welke politiegegevens	Speciale aandachtspunten	Wordt verstrekt door (KMar)	Wordt verstrekt door (politie)
Autoriteit Financiële Markten (AFM) *art. 18 Wpg en art. 4:3 tweede lid, onder c Bpg*	Alle politiegegevens	Nodig voor een betrouwbaarheidsonderzoek in het kader van: • de Wet financieel toezicht; • de Wet toezicht accountantsorganisaties. De verstrekking wordt eerst afgestemd met het OM.	Infodesk	Teammedewerker, DRIO/DLIO
Belastingdienst *art. 18 Wpg en art. 4:2 derde lid Bpg*	Art. 8 en art. 13 eerste lid	1 Nodig voor het inschatten van de veiligheidsrisico's (agressie & geweld) met betrekking tot het toezicht houden op naleving van: • Invorderingswet 1990; • Algemene wet inzake rijksbelastingen; • Wet arbeid vreemdelingen.	OIM	Teammedewerker Teammedewerker Teammedewerker AVIM
art. 20 Wpg	Art. 8 en art. 13 eerste lid	2 Voor andere doeleinden dan bij 1, zoals samen structureel fraude voorkomen of de 'patseraanpak', moet er sprake zijn van een samenwerkingsverband/convenant (art. 20 Wpg).	Medewerker genoemd in convenant/OIM	Medewerker genoemd in convenant
art. 16 eerste lid, onder a Wpg	Alle politiegegevens	3 Bij een opsporingsonderzoek van de Belastingdienst kan de BOA politiegegevens verstrekt krijgen. Voor haar toezichtstaken kan ze gegevens ontvangen via de FIOD (artikel 15).	OIM/Infodesk	Teammedewerker, DRIO/DLIO
Benadeelden van strafbare feiten of schendingen van de openbare orde of de verzekeraar die optreedt namens de benadeelde. Denk aan zorgverzekeraars, maar ook advocaten en rechtsbijstandsverzekeraars. *art. 18 Wpg en art. 4:2 eerste lid, onder n Bpg*	Art. 8 en art. 13 eerste lid	1 Noodzakelijk om in rechte voor hun belangen op te kunnen komen. 2 Om een civiele procedure te starten voor het regelen van schade. In verband met de uitvoering van de Wet versterking positie van het slachtoffer: neem altijd contact op met het Slachtofferloket. 3 Maak altijd een proportionaliteits- en subsidiariteitsafweging. Als je kunt volstaan met het doorgeven van een kenteken (zodat de verzekeraar met de tegenpartij contact zoekt), doe dit dan en verstrek geen adresgegevens indien dit niet hoeft.	OIM/Infodesk	Teammedewerker, DRIO/DLIO

Figuur 5.2 Fragment uit de Verstrekkingenwijzer Wpg

Er is altijd ten minste een verwerkingsgrondslag.[7] De artikelen 8, 9, 10 en 12 zijn de initiële verwerkingsgrondslagen. Daarnaast mogen gegevens verder worden verwerkt voor een ander doel dan waarvoor ze oorspronkelijk verkregen zijn. Dit mag alleen indien de Wpg daar uitdrukkelijk in voorziet. Dat doet de wet in de artikelen 11, 13 en 14.



Figuur 5.3 Verwerkingsgrondslagen

5.3.2 Dagelijkse politietaak inclusief eenvoudige opsporingsonderzoeken (artikel 8)

De dagelijkse politietaak bestaat onder andere uit handhaving van wetten en regels, hulpverlening, surveillance, verkeerszaken en eenvoudige opsporingsonderzoeken. Dit wordt ook wel de oog- en oorfunctie van de politie genoemd.[8] De dagelijkse politietaak is dus een onderdeel van de politietaak zoals die staat omschreven in artikel 3 van de Politiewet 2012. Het merendeel van de BVH-gegevens zijn artikel 8-gegevens. Het kan zowel om verdachte als onverdachte personen gaan; de wet maakt daar geen onderscheid in. Het eerste jaar mag je van alles met deze gegevens doen; je kunt er ook doorheen bladeren op zoek naar patronen. Na dit eerste jaar mogen de gegevens nog vier jaar met een gerichte zoekvraag worden benaderd. Bijvoorbeeld via (een deel van) een kenteken, adres, straat of naam. Na vijf jaar worden ze achter een virtueel schot geplaatst. Ze zijn dan 'verwijderd' en alleen te benaderen via een poortwachter.[9] Elke eenheid heeft een aantal medewerkers binnen de informatieorganisatie aangewezen en opgeleid als poortwachter.

Omdat het merendeel van de uitgevoerde zoekvragen en raadplegingen gericht zijn, kun je als vuistregel aanhouden dat artikel 8-gegevens vijf jaar verwerkt mogen worden.[10]

---

7 In *Privacy by design* is beschreven dat gegevens ook meerdere grondslagen kunnen hebben. De initiële blijft in elk geval altijd behouden.

8 Zie pagina 38 van de memorie van toelichting bij de Wpg.

9 Hier lees je wat er besloten is rondom de poortwachtersorganisatie: https://agora.portal.politie.local/sites/staven/150311105/Onze%20documenten/Inrichting%20poortwachtersorganistie%20nav%20Wpg-schoning%20BVH.pdf#search=poortwachter.

10 Dit is zo vastgelegd in *Privacy by design*.

Bestanden die niet in BVH kunnen worden opgenomen – denk aan gescande documenten of afbeeldingen – mogen niet in een groepsmap, eigen map of mailbox worden opgeslagen. Dit doe je – bij de politie – op de daarvoor ingerichte O-schijf. Alleen zo voldoe je aan de plicht tot het delen van de gegevens met collega's (artikel 15 Wpg).

Figuur 5.4 Termijnen artikel 8-gegevens

5.3.3 Uitgebreidere opsporingsonderzoeken en veelplegersdossiers (artikel 9)

Worden er grote hoeveelheden gegevens verzameld gericht op bepaalde personen of een specifieke gebeurtenis, dan is er sprake van een artikel 9-verwerking. Dan gaat het dus niet meer over de dagelijkse politietaak zoals bedoeld in artikel 8, en wordt de inbreuk op de privacy langzaamaan groter. Dit zijn bijvoorbeeld onderzoeken waarbij bijzondere opsporingsbevoegdheden worden ingezet, zoals tappen of stelselmatige observatie. Vaak gaat het om MRO[11]-waardige onderzoeken. Wat dit betekent (en meer informatie over de grens tussen artikel 8 en 9) vind je op PKN/Kompol.[12] Ook een gericht onderzoek naar overlast in een woonwijk, verstoringen van de openbare orde of dossieropbouw over een veelpleger vallen onder artikel 9. Het doel van het onderzoek moet binnen een week worden vastgelegd. De bevoegd functionaris, de leider van het onderzoek, kan gegevens ter beschikking stellen voor een van de andere verwerkingsdoelen. Bijvoorbeeld als informatie uit een onderzoek noodzakelijk is voor de briefing van een basisteam.

Het ontsluiten van de whatsappgroep van een *outlaw motor gang* (OMG) levert veel data op: ook foto's en gesproken berichten. Die worden in een aparte omgeving opgeslagen. Vallen deze gegevens onder de Wpg, en zo ja, onder welk regime en hoe zorg je dat regels over delen, autoriseren en termijnen worden nageleefd? >>

11 Melding Recherche Onderzoek.

12 http://kompol.politieacademie.politie.nl/ccms/documenten/Vragen_Wpg_2010_onderscheid_artikel_8_en_9.pdf.

>> *Ja, deze gegevens worden onder artikel 9 verwerkt. Als gegevens in de geijkte systemen als Summ-IT worden opgeslagen, wordt een aantal regels geautomatiseerd ondersteund. Als je gegevens op netwerkschijven als de O-schijf opslaat, dan moet de bevoegd functionaris hier maatregelen voor treffen. Denk aan afschermen, schonen, delen met iedereen die de gegevens nodig heeft enzovoort. Gebruik de richtlijnen van het project Mappen en Schijven. Hiermee wordt uitvoering gegeven aan het uitgangspunt 'delen, tenzij'*[13]

Artikel 9-gegevens dienen alleen beschikbaar te zijn voor collega's die een rol hebben in het betreffende onderzoek en voor informatiemedewerkers. Dit geldt zowel bij de eerste verwerking in het bronsysteem (Summ-IT, maar ook in BVH komen artikel 9-gegevens voor), als voor de verdere verwerking in bijvoorbeeld BasisVoorziening Informatie (BVI). Bij het maken van rapportages waar artikel 9-gegevens in zitten, is het dus van belang dat de autorisaties goed gecontroleerd worden. De autorisatie dient als het ware 'aan de data te hangen' en het moet niet uitmaken of een gebruiker toegang heeft tot deze data via het bronsysteem, via BVI of via een Cognos-rapportage.[14,15] Ditzelfde geldt voor de termijnbewaking en toestemming van de bevoegd functionaris om gegevens verder te verwerken voor een ander doel dan waarvoor ze verzameld waren: als gegevens in informatieproducten en rapportages te herleiden zijn tot personen, dient er altijd handmatig gecontroleerd te worden of deze gegevens wel beschikbaar gesteld mogen worden.

Figuur 5.5 Termijnen artikel 9-gegevens

Na een onherroepelijke uitspraak of na het verstrijken van de verjaringstermijn mag je artikel 9-gegevens niet meer gebruiken voor het dagelijks politiewerk (tijdstip x in het schema). JustID houdt de volledige registratie van afdoeningen bij en in de praktijk is bij de politie niet altijd bekend wanneer een onherroepelijke uitspraak heeft plaatsgevonden.

---

13 *Privacy by design*, februari 2015: http://intranet.politie.local/nieuws/0000/2015/maart/10/boekje-open-over-privacy.html.

14 Cognos is een business-intelligencesysteem waarmee informatierapporten kunnen worden gemaakt.

15 Zie ook BVI Inrichting voor Security en Wpg-compliancy v1.02.

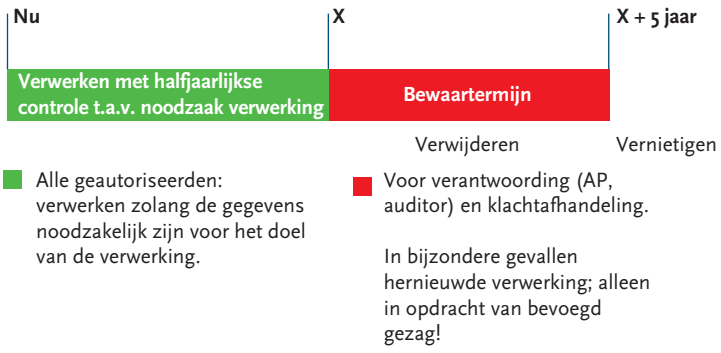
Er wordt aan gewerkt om afloopberichten van het Openbaar Ministerie (OM) direct in de politiesystemen te verwerken zodat gegevens aangepast en verwijderd kunnen worden. Zolang dat nog niet goed verloopt, moet je er dus zelf goed rekening mee houden! Deze regel negeren kan leiden tot bewijsuitsluiting. In de praktijk is bij artikel 9 de verwerkingstermijn van gegevens langer dan bij artikel 8.

5.3.4 Opbouwen informatiepositie (artikel 10)

Artikel 10 is de enige categorie waarbinnen je een informatiepositie over mensen mag opbouwen die losstaat van concrete handhavings- of opsporingsacties. Gegevens die verwerkt worden door het TCI en het TOOI en de themaverwerkingen (terrorisme, mensenhandel en mensensmokkel) vallen hieronder. Deze gegevens kunnen eerst onder artikel 8, 9 of 12 verwerkt zijn. Ze kunnen onder artikel 13 lid 2 verder worden verwerkt voor zover ze relevant zijn voor landelijk inzicht op het betreffende specialistische onderwerp zoals terrorisme.

Om zicht te krijgen op verschijnselen die een ernstige bedreiging van de rechtsorde kunnen vormen, is het nodig gegevens te verwerken over – ook onverdachte – personen. Artikel 10 biedt de mogelijkheid om daartoe een informatiepositie op te bouwen. Denk aan zware criminaliteit, terrorisme en ernstige verstoringen van de openbare orde door bijvoorbeeld voetbalvandalen of activisten. Door middel van omvangrijke en op bepaalde personen gerichte gegevensverzameling wordt geprobeerd een beeld te krijgen van de betrokkenheid van die personen bij handelingen of misdrijven. Dit gebeurt in een permanent analyseproces, dat leidt tot het vastleggen van gegevens over veelal nog onverdachte personen. Op basis van de informatiepositie kan worden besloten tot een opsporingsonderzoek (een artikel 9-verwerking) of bijvoorbeeld operationele maatregelen in de sfeer van de openbare orde.

Wat betreft de verwerkingstermijnen geldt dat ten minste elk halfjaar gecontroleerd moet worden wat de laatste zwacri-waardige (zware criminaliteit in georganiseerd verband) mutatie is (de verwerking die blijk geeft van de noodzaak tot het verwerken van gegevens over deze betrokkene).



Figuur 5.6 Termijnen artikel 10-gegevens

5.3.5 De mogelijkheid om verbanden te leggen tussen gegevens (artikel 11)

Bij het (actief) ter beschikking stellen van politiegegevens is verdere verwerking voor andere doelen afhankelijk van degene die de gegevens oorspronkelijk verwerkt. Alleen als hij weet dat deze nodig zijn voor een ander doel, zal hij de gegevens daarvoor ter beschikking stellen. Dit brengt het risico met zich mee dat gegevens die wel voor een ander doel van belang zijn, daarvoor niet beschikbaar komen. De Wpg bevat daarom nog twee zoekmogelijkheden. Daarmee kan rechtstreeks worden gezocht in politiegegevens die voor andere doeleinden zijn verwerkt: geautomatiseerd vergelijken en in combinatie verwerken. Hierbij maakt niet degene die de gegevens oorspronkelijk verwerkt ze voor andere doeleinden beschikbaar. Maar het is degene die voor dat andere doel gegevens nodig heeft, die zoekt in gegevens die voor andere doeleinden zijn verwerkt.

Geautomatiseerd vergelijken is de meest toegepaste vorm van zoeken in gegevens. Je wilt vaststellen of bepaalde gegevens uit de ene gegevensverzameling ook voorkomen in andere gegevensverzamelingen binnen het Wpg-domein. Alleen gegevens die al beschikbaar zijn voor het doel van je huidige verwerking, mogen daarvoor gebruikt worden.[16] Het Bpg regelt in de artikelen 2:11 en 2:12 hoe de resultaten van een geautomatiseerde vergelijking zichtbaar worden.

Politiegegevens mogen ook geautomatiseerd worden vergeleken met andere persoonsgegevens dan politiegegevens. Dit is uitgewerkt in artikel 11 lid 5. Dit kan alleen ten behoeve van een artikel 9- en 10-verwerking. Het is daarbij van belang of gegevens zijn binnengehaald (bijvoorbeeld na vordering door de officier) of niet. Zijn de gegevens het politiedomein binnengehaald, dan is er géén sprake van een artikel 11 lid 5-verwerking. De gevorderde of op andere wijze (bijvoorbeeld van internet of andere openbare bronnen) verkregen gegevens worden dan gewoon verwerkt op basis van artikel 8, 9, 10 of 13. Blijft het gegevensbestand extern (buiten de gegevensverzameling die valt onder de Wpg), dan vindt er een vergelijking plaats zoals dit bedoeld is in artikel 11 lid 5 Wpg. De vergelijking wordt dus extern, door of onder toezicht van de politie en op haar verzoek uitgevoerd. De politie ontvangt en verwerkt vervolgens de resultaten in de bestaande gegevensverwerking.

Je bent bezig met een artikel 9-analyse rondom woonfraude. Daarbij combineer je een extract uit het Kadaster met gegevens uit BVH. Is dat toegestaan?

Artikel 11 lid 5 biedt de mogelijkheid om politiebestanden te vergelijken met bestanden van partners. De bevoegd functionaris, leider van het onderzoek, zorgt ervoor dat aan de voorwaarden wordt voldaan.

16 Memorie van toelichting bij de Wpg, pp. 52-53.

Alle artikel 11-verwerkingen moeten conform de protocolplicht schriftelijk worden vastgelegd. Dit betekent dat de privacyfunctionaris een overzicht dient te hebben dat beschrijft welke gegevens gebruikt zijn in de zoekvraag en welke gegevens verder worden verwerkt. Een deel hiervan wordt automatisch ingevuld door loggingsfunctionaliteit.

In combinatie verwerken

Wat onder in combinatie verwerken van politiegegevens dient te worden verstaan is niet in de Wpg gedefinieerd. Het is ruimer dan geautomatiseerd vergelijken, want alle beschikbare politiegegevens kunnen worden geraadpleegd, doorzocht en gecombineerd, bijvoorbeeld door het stellen van samengestelde zoekvragen of analyse aan de hand van bepaalde profielen van daders, slachtoffers of feiten. Dit is een verstrekkende bevoegdheid waarbij onbeperkt geanalyseerd wordt en zeer geavanceerde zoekmethoden kunnen worden toegepast, bijvoorbeeld zoals in Raffinaderij (zie hoofdstuk 20 Big data). Grote hoeveelheden gegevens, ook van onverdachte burgers (aangevers, getuigen, slachtoffers) die in een ander verband zijn verzameld, kunnen worden gebruikt en op basis van patronen of profielen worden onderzocht en inzichtelijk worden gemaakt. Daarom is dit alleen toegestaan door daartoe aangewezen informatiemedewerkers. Het mag alleen in bijzondere gevallen en in opdracht van het bevoegd gezag (de officier van justitie of de burgemeester).[17]

5.3.6 Beheer en controle van informanten (artikel 12)

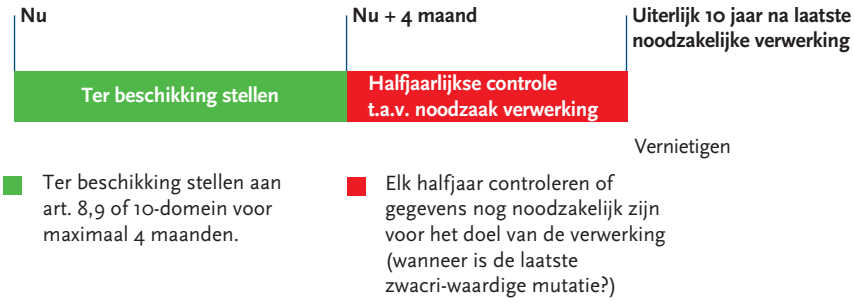
Artikel 12-gegevens zijn onder andere gespreksverslagen met informanten en gegevens die door runners van het TCI of het TOOI worden vastgelegd. Deze worden uit dit domein overgeheveld naar artikel 10, 9 of 8. Artikel 12 kent eigen verwerkingstermijnen en autorisatieregels.

Een informant is een persoon die heimelijk aan een opsporingsambtenaar informatie verstrekt omtrent (vermoedens van) strafbare feiten of ernstige schendingen van de openbare orde die door anderen worden gepleegd of verricht. Omdat hierover praten gevaar voor deze persoon of voor derden oplevert, kenmerkt de informantenverwerking zich door een grote mate van afscherming. Het gaat hier om meer gegevens dan wat de informant verstrekt; namelijk ook de beschikbare informatie over diens betrouwbaarheid en de integrale verslagen van de gesprekken met een informant (de zogenoemde brutoverslagen).

Informanten zijn in de eerste plaats van belang voor het verkrijgen van inzicht in de betrokkenheid van personen bij ernstige schendingen van de rechtsorde. Informantgegevens worden dan ook verwerkt bij de eenheden waar de TCI-TOOI- en themaverwerkingen worden gevoerd.

Gedurende vier maanden mogen deze gegevens gebruikt worden. Meestal worden de gegevens dan verder verwerkt binnen een artikel 10-verwerking, maar dat kan ook direct verder gebeuren binnen een artikel 8- of 9-verwerking. Zie voor meer over TCI en TOOI hoofdstuk 14 Inwinning.

17 Zie ook de *Aanwijzing Wet politiegegevens en de rol van de officier van justitie*.



Figuur 5.7 Termijnen artikel 12-gegevens

5.3.7 Ter ondersteuning van de politietaak (artikel 13)

Dit artikel biedt de mogelijkheid om gegevens die oorspronkelijk zijn verwerkt op basis van artikel 8, 9 of 10, verder te verwerken ter ondersteuning van de politietaak. Bijvoorbeeld om personen of goederen te signaleren (opsporingssysteem – OPS, Nationaal Schengen Informatiesysteem – NSIS). Andere mogelijkheden zijn identificatie, verificatie en bejegening van personen (Het Automatisch Vinger Afdrukkensysteem Nederlandse Kollektie – HAVANK), fotoconfrontatiemodule (FCM) en het centraal raadplegen van antecedenten. De bron voor antecedenten (het Herkenningssysteem – HKS), is niet meer in gebruik. Deze gegevens zijn voortaan via BVI te raadplegen, bijvoorbeeld met BVI-IB. Zo verandert er meer op dit gebied: het Landelijk Overvallen Registratiesysteem (LORS) is een rapportage die voortaan wordt gegenereerd uit BVI.

De centrale registratie rond wapenvergunningen (Verona) valt ook onder artikel 13, net als PSH-V voor de vreemdelingenregistratie. Artikel 13-gegevens worden vaak landelijk raadpleegbaar gesteld. Hoelang je deze gegevens mag gebruiken, staat in het daarbij behorende reglement of protocol. Sommige gegevens mogen bijvoorbeeld vijftien jaar beschikbaar blijven, andere dertig jaar. Dit reglement is een belangrijke waarborg voor artikel 13-verwerkingen. De korpschef moet van tevoren een artikel 13-reglement ondertekenen waarin beschreven is voor welk doel deze gegevens verder verwerkt worden, om wat voor gegevens het gaat en hoelang de gegevens verwerkt mogen worden.[18] Er is landelijk nog geen overzicht van alle bestaande artikel 13-reglementen. Let dus goed op als je in het informatieproces gebruikmaakt van dit soort gegevens. Als vuistregel geldt dat artikel 13 lid 1-gegevens langer verwerkt mogen worden dan artikel 8-gegevens.

Artikel 13-gegevens worden opgesplitst in een categorie die de hele politie mag raadplegen, en een categorie alleen bestemd voor bepaalde functionarissen. Artikel 13 lid 2 en 3 gaan over die laatste categorie. Deze gegevens worden centraal verwerkt om inzicht te krijgen in specialistische onderwerpen als moord, kinderporno, voetbalvandalisme en overvallen. Dit gebeurt door de Landelijke Eenheid of speciaal daartoe aangewezen teams.

---

18 Zie artikel 13 lid 4 Wpg en artikel 6:2 Bpg voor een exacte omschrijving van de vereiste gegevens.

Het eerdergenoemde LORS is een voorbeeld. VROS-gegevens (Verwijzingsindex Rechercheonderzoeksysteem), die inzichtelijk maken of een subject of locatie ook in andere opsporingsonderzoeken voorkomt, vallen onder artikel 13 lid 3.

Als gevolg van de nationalisering van de politie worden steeds meer applicaties geïntegreerd in het landelijk applicatielandschap. Daarmee komen oude 'artikel 13-systemen' te vervallen of ze worden vervangen door een rapportage op BVI. Dat verbalisanten in BVH gevarenclassificaties invoeren, laat zien dat ook in BVH artikel 13-gegevens voorkomen.

5.3.8 Het bewaren van verwijderde politiegegevens (artikel 14)

Artikel 8-, 9- en 10-gegevens die verwijderd zijn, worden nog vijf jaar bewaard. Ze mogen in die periode alleen gebruikt worden voor klachtafhandeling, toezicht en audits. Ze mogen dus niet verstrekt worden. In bijzondere gevallen kunnen gegevens hernieuwd verwerkt worden. Dat kan alleen na een zorgvuldige afweging, in opdracht van het bevoegd gezag en ten behoeve van een artikel 9- of 10-verwerking.[19] Alleen de poortwachter heeft binnen de politie toegang tot deze verwijderde gegevens.

Na deze vijfjarige bewaartermijn worden de gegevens vernietigd. Er wordt echter afgezien van vernietiging 'voor zover de waarde van de archiefbescheiden als bestanddeel van het cultureel erfgoed of voor historisch onderzoek zich daartegen verzet'. De gegevens die uitgezonderd worden van vernietiging, blijven onder de Archiefwet nog langer bewaard en worden op den duur openbaar. Ze worden overgedragen aan het Nationaal Archief of een stadsarchief.

5.4 Belangrijke onderdelen van de Wpg voor IGP

In deze paragraaf worden de belangrijkste Wpg-elementen uitgewerkt die een rol spelen bij een juiste uitwerking en toepassing van het IGP-gedachtegoed.

Noodzaak, proportionaliteit en subsidiariteit

Het IGP-gedachtegoed wordt nog weleens uitgelegd als 'leg alles maar vast, want je weet nooit waar het goed voor is'. Dit is niet alleen een onjuiste samenvatting, het gaat regelrecht in tegen het wettelijk kader. Gegevens mogen namelijk alleen worden vastgelegd voor zover dat noodzakelijk is, ze moeten ter zake dienend zijn en niet bovenmatig.[20] Uiteraard is dat een lastige afweging, want het is inherent aan het politiewerk, zeker aan het opsporingsproces, dat van tevoren nog niet altijd helder is of gegevens relevant zullen zijn. Dit ontslaat de politie echter niet van de verplichting om deze afweging te maken. En niet alleen de politieman op straat dient dat te doen, maar ook de beleidsmakers, ICT-medewerkers enzovoort. De politie dient een werkomgeving te creëren waarbij men zich ervan bewust is, dat het niet is toegestaan gegevens vast te leggen onder het motto 'je weet maar nooit'.

---

19 Zie ook de *Aanwijzing Wet politiegegevens en de rol van de officier van justitie*.

20 Zie artikel 3 lid 1 en 2 Wpg.


Tegen twee uur 's ochtends sluiten de twee politiepaarden plotseling de Varkensstraat af. Een paar tieners, eerder op de avond al danig onder invloed van drank, wordt ingesloten door zes agenten. Een agent: „Je noteert hun naam. Daarmee trek je ze uit de anonimiteit. De kans is dan klein dat er later op de avond nog iets gebeurt."

Het is de rest van de avond rustig geweest. De politieambtenaar komt na afloop van zijn dienst op het bureau. Mag hij de namen van de tieners die hij genoteerd heeft vastleggen in BVH?

We dienen gegevens te vernietigen zodra ze niet (meer) noodzakelijk zijn voor het doel waarvoor we ze verzameld hadden. In dit geval kun je discussiëren of dat punt bereikt is: hij heeft ze uit de anonimiteit gehaald en het is de rest van de avond rustig gebleven.

Wat betreft proportionaliteit en subsidiariteit geldt dat het gebruik van gegevens altijd in verhouding moet staan tot het doel: gegevens uit een moordzaak mag je niet gebruiken om een winkeldiefstal op te lossen. En als je een gedupeerde kunt helpen door gegevens te verstrekken aan zijn verzekeringsmaatschappij in plaats van aan hemzelf, heeft dat de voorkeur. Er vindt dan minder inbreuk op de privacy plaats en het doel is wel bereikt. Hetzelfde geldt voor een verstrekking aan de gemeente: niet per definitie een heel proces-verbaal verstrekken, maar alleen de gegevens die noodzakelijk zijn voor bijvoorbeeld de sluiting van een café.

Voor de zoekmogelijkheden verlangt het subsidiariteitsbeginsel dat de politie eerst zoekt in de gegevens die zij zelf tot haar beschikking heeft, te beginnen met artikel 13 lid 1-gegevens. Ook kan voor een artikel 8-verwerking het gecombineerd verwerken zoals beschreven in artikel 8 lid 3, worden toegepast. Is er sprake van een artikel 9- of 10-verwerking, dan zijn artikel 11 lid 1 en 2 de grondslagen voor het zoeken. Het een na laatste middel dat ingezet kan worden, zijn de mogelijkheden die artikel 11 lid 4 biedt. Hier worden artikel 8-, 9- en 10-gegevens in combinatie met elkaar verwerkt. Tot slot biedt artikel 11 lid 5 de mogelijkheid om politiegegevens met grote hoeveelheden externe gegevens te vergelijken.

Bovenmatigheid en dataminimalisatie

De Wpg schrijft in artikel 3 lid 2 voor dat gegevens niet bovenmatig mogen zijn; er mogen dus niet 'te veel' gegevens verwerkt worden. Dataminimalisatie betekent dat er zo min mogelijk persoonsgegevens verwerkt moeten worden; alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking.[21]

Het gemak van digitale communicatie en de grote hoeveelheden gegevens die we als politie voorhanden hebben, maakt niet dat we alles klakkeloos kunnen gebruiken en delen. Zo zijn het berekenen en opslaan van een geweldsindicator voor alle personen die

21 De Autoriteit Persoonsgegevens beschouwt dataminimalisatie als een belangrijk concept voor *privacy by design*.

in BVI voorkomen, een bovenmatige verwerking. Het doet er niet aan af dat een persoon een score 'niets aan de hand' krijgt. Voor personen die aangehouden zijn geweest, verdachten en veroordeelden, is het uit te leggen dat we een dergelijke indicator standaard berekenen. Dat is noodzakelijke informatie voor een juiste bejegening bij een toekomstig contact. Voor een aangever of getuige is dit echter niet goed uit te leggen. Dus mag een dergelijke indicator niet voor iedere persoon die in BVI voorkomt, standaard berekend worden.

Is het toegestaan dat hotels dagelijks gegevens over hun gasten aan de politie verstrekken voor goede uitvoering van de politietaak?

Nee, hier is geen noodzaak of grondslag voor. Dit werd in het verleden wel gedaan. Hotels zijn verplicht een nachtregistratie bij te houden. De politie mag deze overnachtingsgegevens alleen opvragen ter voorkoming van gevaar, ten behoeve van opsporingsonderzoek of bij vermiste personen. Er mag dus geen structurele geautomatiseerde verstrekking plaatsvinden door de hoteleigenaar. Meer informatie op politie-intranet en op de site van de Autoriteit Persoonsgegevens.[22]

Doelbinding en verder verwerken

Doelbinding is een Europees privacyconcept dat inhoudt dat gegevens alleen worden gebruikt voor het doel waarvoor ze verzameld zijn. In de Wpg is dit uitgewerkt in de verwerkingsgrondslagen. Als de Wpg daarin uitdrukkelijk voorziet, mogen zij ook worden verwerkt voor een ander doel ('verder verwerkt'). Zoals eerder benoemd, voorziet onder andere artikel 13 daarin. Deze structuur impliceert dat van tevoren bekend is waarom gegevens verwerkt worden. Binnen IGP-ontwikkelingen is dit niet altijd het geval: er wordt allerlei informatie vergaard en via (geautomatiseerde) redenering worden hier signalen uit gehaald waarop de politie haar activiteiten baseert.

Met het oog op moderne manieren van informatie verwerken, is het wenselijk dat bij het ontwikkelen van een nieuwe Wpg rekening gehouden wordt met deze discrepantie. Zoals in het rapport van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) over big data in een veilige samenleving is aangemerkt, is het nodig dat er niet alleen regels zijn over de eerste verwerking, maar vooral ook over de analysewerkzaamheden en gebruikstoepassingen.[23]

Autoriseren

De politie is verplicht om passende technische en organisatorische maatregelen te treffen om politiegegevens te beveiligen tegen verlies of vormen van onrechtmatige verwerking (artikel 4 lid 3 Wpg). Een van die maatregelen is vooraf bepalen wie welke gegevens mag

22 https://autoriteitpersoonsgegevens.nl/nl/nieuws/politie-vraagt-nachtregisters-hotels-niet-meer-standaard-op.

23 Hirsch Ballin, E., D. Broeders & E. Schrijvers, *Big data in een vrije en veilige samenleving*. Wetenschappelijke Raad voor het Regeringsbeleid, Den Haag 2016.

verwerken, oftewel het autoriseren. Bij het invullen van het autorisatieregime heeft de politie een zekere vrijheid, maar de hoofdregel is dat naarmate de politiegegevens 'gevoeliger' worden en specialistisch, er minder geautoriseerden mogen zijn. In artikel 6 Wpg staan de algemene eisen opgesomd waaraan autorisaties moeten voldoen.

Politiemedewerkers moeten gericht geautoriseerd worden om politiegegevens te mogen verwerken.[24] Ook moet de autorisatie expliciet maken voor welke taken de autorisatie geldt en voor welke handelingen er precies geautoriseerd wordt. Een algemene bevoegdheid tot 'het verrichten van handelingen' is onvoldoende specifiek. Zie voor meer over het autorisatiemodel hoofdstuk 6 Autorisatiemodel politie.

Artikel 6 lid 4 biedt de mogelijkheid om ook personen te autoriseren die niet onder het beheer van de korpschef staan en geen ambtenaar van politie zijn. Dit betekent dus dat onder bepaalde voorwaarden ook ingehuurde medewerkers, onderzoekers of stagiairs met politiegegevens mogen werken.[25]

Figuur 5.8 Verwerking van gegevens

In combinatie verwerken

In de artikelen 8 lid 2 en 3 en artikel 11 komen de begrippen 'geautomatiseerd vergelijken' en 'in combinatie verwerken' voor. Geautomatiseerd vergelijken is het invoeren van één of meer (delen van) zoeksleutels uit de eigen gegevensverwerking in de politiesystemen om te zien of er overeenkomsten zijn in andere verwerkingen. De gerelateerde gegevens kunnen verder verwerkt worden in de eigen verwerking voor zover deze noodzakelijk zijn. Denk aan hits na een bevraging in BVI-IB, BVH, Summ-IT of BlueSpot Monitor (BSM).

---

24 In het Bpg zijn nadere regels opgenomen over specifieke categorieën van personen en gegevensverwerkingen die vanwege hun karakter beperkt moeten worden tot daartoe gespecialiseerde personen (met soms specifieke deskundigheidseisen).

25 Dit is uitgewerkt in onder andere het beleidskader autorisatie externen voor gebruik politiegegevens, 25-05-2016.

Na diverse liquidaties, onder andere in Amsterdam-West op 29-12-2012, wil men inzicht krijgen in dwarsverbanden tussen zaken. Ervaring uit het verleden laat zien dat sleutelpersonen vaak buiten schot blijven doordat ze in individuele onderzoeken een te geringe rol spelen. Echter, als er meer overzicht verkregen wordt, wordt wel inzichtelijk wat zij voor rol hebben en kunnen ze aangepakt worden. Bijvoorbeeld een wapenhandelaar die al sinds 2002 criminele organisaties van wapens voorziet. Het onderzoeksteam wil twaalf onderzoeken samenvoegen waarvan het op basis van tactische informatie of TCI-informatie weet dat er verbanden zijn. Het doel is om met 'slimme' zoekvragen, zoals profielen (mannen ouder dan 35 die in een leaseauto rijden) of significante afwijkingen (personen die vaak worden genoemd in verklaringen, erg veel vermogen bezitten of vaak naar Zuid-Amerika reizen) te achterhalen of er personen in de bestanden voorkomen die als verdachte kunnen worden aangemerkt of op andere wijze als sleutelpersoon fungeren. Wat voor soort verwerking is dit en wat zijn de voorwaarden?

Dit is een artikel 11 lid 4-verwerking. Dit omdat bestanden worden samengevoegd en in combinatie worden verwerkt. Hiervoor geldt dat dit alleen mag 'in bijzondere gevallen', door daartoe bevoegde informatiemedewerkers. Het bevoegd gezag toetst van tevoren de aanvraag voor deze verwerking.

Gecombineerd verwerken is het daadwerkelijk samenvoegen van (delen van) bestaande gegevensverwerkingen (bestanden) met de eigen onderzoeksgegevens, om met analysetechnieken verbanden te kunnen leggen tussen deze gegevens. Bijvoorbeeld patronen herkennen of profielen samenstellen. Als dit gebeurt in het kader van een artikel 9- of 10-verwerking, zijn daar voorwaarden aan verbonden: het mag alleen worden gedaan door daartoe aangewezen en opgeleide informatiemedewerkers, er moet sprake zijn van een bijzonder geval en het bevoegd gezag moet er opdracht voor geven. Verder geldt dat – als er verbanden blijken te bestaan – de bevoegd functionaris van het oorspronkelijke onderzoek instemming moet verlenen om de gerelateerde gegevens verder te verwerken.

Bij een gewelddadige verkrachting van een 63-jarige vrouw vermoedt het opsporingsteam dat de dader een band heeft met de buurt waar het misdrijf gepleegd is. Er wordt een extract uit de Basisregistratie Personen opgevraagd met speciale aandacht voor alleenstaande mannen, mannen met antecedenten zeden en geweld en aandachtsvestigingen. Het Team Grootschalige Opsporing doet een integrale bevraging op deze 1427 personen. Er blijven er 150 over. Van 11 daarvan is het DNA-profiel bekend bij het Nederlands Forensisch Instituut (NFI). Hoe maakt de Wpg zo'n vergelijking mogelijk en welke voorwaarden zijn daaraan gebonden?

Artikel 11 lid 5 biedt de mogelijkheid om politiebestanden te vergelijken met bestanden van partners. De bevoegd functionaris zorgt ervoor dat aan de voorwaarden wordt voldaan. De vergelijking moet in elk geval schriftelijk worden vastgelegd. Dit betekent dat een aanmeldformulier verstuurd moet worden naar de privacyfunctionaris met daarin beschreven welke gegevens gebruikt zijn in de zoekvraag en welke gegevens verder worden verwerkt.

Verwerkingstermijnen

Voor elke verwerkingsgrondslag heeft de wetgever bepaald wanneer een gegeven verwijderd en vernietigd moet worden. Verwerkingen na deze termijnen zijn per definitie onrechtmatig. Wanneer gegevens verstrekt worden aan een partner, dan komen deze gegevens onder het gegevensbeschermingsregime te vallen van de desbetreffende partner. Vaak is dit de Wet bescherming persoonsgegevens (Wbp). Die termijnen kunnen anders zijn dan die in de Wpg. Het is dus mogelijk dat bepaalde gegevens nog wel bij partners verwerkt mogen worden maar niet meer bij de politie (en andersom).

Voor sommige processen biedt de wetgever een ander kader. Regels uit het Wetboek van Strafvordering bepalen bijvoorbeeld wanneer gegevens die verkregen zijn met bijzondere opsporingsmiddelen vernietigd moeten worden. En ANPR-gegevens (automatic number plate recognition) mogen vier weken bewaard worden.[26] Het gaat dan om locatie, tijdstip en de foto van een voertuig die gebruikt mogen worden bij de opsporing van een specifiek misdrijf en voor de aanhouding van voortvluchtige personen. Hier is dus al een proportionaliteits- en subsidiariteitstoets gemaakt en besloten dat vier weken acceptabel is, ook voor de zogenoemde no-hits.

Ook de politie kan beleid opstellen waarbij het wettelijk kader nader wordt ingevuld. Op Agora, een communicatiemiddel, worden politiegegevens op de tijdlijn automatisch na twee weken verwijderd. Dit is een invulling van 'verwijderen zodra ze niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verwerkt'.[27]

Toezicht en verantwoording

Een belangrijk beginsel van gegevensbescherming is transparantie. De politie moet zich kunnen verantwoorden voor al haar handelingen: vooraf bijvoorbeeld door een zorgvuldige autorisatieregistratie, achteraf doordat handelingen inzichtelijk en controleerbaar zijn. In de Wpg is op verschillende manieren voorzien in toezicht op de naleving van de wet. Zo moeten diverse verwerkingen geprotocolleerd worden, moeten er periodiek audits worden uitgevoerd en is voorzien in intern en extern toezicht.[28]

Protocolplicht

De Wpg verplicht in artikel 32 tot de schriftelijke vastlegging van een aantal zaken. Door dit te doen, wordt het mogelijk na te gaan of de politie zich aan de spelregels houdt. Zo moeten de doelomschrijvingen van de artikel 9-verwerkingen worden vastgelegd, maar ook de autorisaties die zijn toegekend. Ook de geautomatiseerde vergelijkingen en gecombineerde verwerkingen moeten worden vastgelegd. Met de omzetting van de Europese Richtlijn naar de nieuwe Wpg verandert de protocolplicht, vooral met betrekking tot de *logging*-bepalingen.[29]

---

26 Wijziging van het Wetboek van Strafvordering in verband met de regeling van het vastleggen en bewaren van kentekengegevens door de politie: https://www.eerstekamer.nl/wetsvoorstel/33542_vastleggen_en_bewaren.

27 Zie artikel 4 lid 2 en artikel 8 lid 6.

28 In paragraaf 5 van de Wpg zijn deze maatregelen uitgewerkt.

29 De laatste paragraaf van dit hoofdstuk bevat een beschrijving van de Europese ontwikkelingen rondom de gegevensbeschermingswetgeving.

Herkomst en wijze van verkrijging

In verband met de vereiste juistheid en nauwkeurigheid van politiegegevens verplicht de Wpg (art. 3 lid 4) dat voor artikel 9-, 10- en 12-gegevens de herkomst en wijze van verkrijging worden vastgelegd. Dit gebeurt onder andere in Summ-IT. Mocht een rechter of advocaat verzoeken om duidelijkheid hierover, dan moet de politie in staat zijn die meteen te verschaffen. Ook bij analyses en gebruikmaking van bigdata-technieken is het van belang dat deze metadata 'meereizen' met de gegevens (zie ook hoofdstuk 9 Waar kwaliteit toe leidt over de kwaliteit van gegevens).

Rechten betrokkene

Personen die in de politiesystemen staan, hebben het recht om deze gegevens in te zien. Ook mogen ze weten welke gegevens de afgelopen vier jaar verstrekt zijn. Als deze onjuist blijken, kunnen ze een verzoek indienen om gegevens te laten corrigeren. Aan een verzoek om kennisneming hoeft niet altijd voldaan te worden. Een verzoek kan worden afgewezen als dat noodzakelijk is in het belang van de goede uitvoering van de politietaak, de bescherming van de rechten van de betrokkene of van de rechten en vrijheden van derden, of in het belang van de veiligheid van de staat (artikel 25 lid 1, artikel 27 Wpg).

5.5 Relevante overige wetgeving

De Wpg is niet de enige wet die relevant is binnen het IGP-gedachtegoed. De Archiefwet en de Wbp zijn eveneens van belang. De Wbp kwam al in de paragrafen 5.1.1. en 5.1.2 aan bod. Daar is onder andere te lezen dat gegevens rondom wapenvergunningen en prostitutiecontroles onder de Wbp vallen. Om goed gegevensbeheer uit te voeren en ons aan de wet te houden, is het verstandig deze gegevens niet te vermengen met politiegegevens.

De Archiefwet heeft als doel om documenten een tijd netjes te bewaren en vindbaar te maken. Het achterliggende doel is een overheid die handelingen voor langere tijd kan reconstrueren en verantwoorden. De Wpg en Wbp hebben juist als doel gegevens niet langer te bewaren dan noodzakelijk. De Archiefwet vereist dat overheidsorganen een selectielijst opstellen waarin ze beschrijven welke gegevens na hoeveel tijd vernietigd worden. Bij het opstellen van die selectielijst is rekening gehouden met de Wpg, maar ook met het Wetboek van Strafrecht (Sr) en dat van Strafvordering (Sv) en de Wbp. De selectielijst beschrijft hoelang gegevens bewaard moeten blijven: voor artikel 8 geldt in de Wpg vijf jaar verwerken, dan vijf jaar bewaren en dan vernietigen. Voor artikel 9 eist de Wpg dat gegevens zolang verwerkt worden als voor het doel noodzakelijk is. Dit is in de selectielijst verder uitgewerkt op basis van de verjaringstermijnen uit het Wetboek van Strafrecht.

Het is mogelijk dat gegevens uitgezonderd worden van vernietiging. Dit is beschreven in artikel 14 lid 4 Wpg.[30]

30 Zie paragraaf 5.3.8.

5.6 Toekomstige ontwikkelingen

In mei 2016 zijn in de Europese Unie de algemene verordening gegevensbescherming (AVG) en de Richtlijn gegevensbescherming opsporing en vervolging in werking getreden. Deze regels zullen vanaf 25 mei 2018 in de gehele Europese Unie van toepassing zijn. De AVG is rechtstreeks werkend en vervangt de Wbp. Daarnaast zal de AVG van toepassing zijn op de verwerking van persoonsgegevens in het kader van de Vreemdelingenwet. De richtlijn zal voorafgaand aan de toepassingsdatum moeten zijn omgezet in nationale wet- en regelgeving. Dit betekent een wijziging van de Wpg en de Wet justitiële en strafvorderlijke gegevens (Wjsg). Deze nieuwe Europese regels leiden onder meer tot een versterking van de rechten van de betrokkene, een zwaardere loggingsverplichting en een verplichte interne toezichthouder (functionaris voor gegevensbescherming) naast de Autoriteit Persoonsgegevens.

In 2018 zal de Wpg er dus anders uitzien. Zo zal een aantal elementen uit de protocolplicht[31] vervangen worden door een registratieplicht en loggingsverplichtingen. Het is nog niet duidelijk hoe de gegevensverwerking voor de vreemdelingentaak er zal uitzien.

Na 2018 zal de Wpg nog een keer worden aangepast en mogelijk worden samengevoegd met de Wjsg. Dan zullen ook zaken aangepast worden die uit bijvoorbeeld het knelpuntenonderzoek naar voren zijn gekomen of uit wensen vanuit de politieorganisatie.[32]

31 Artikel 32 Wpg.

32 Zie het door het WODC uitgevoerde onderzoeksrapport van Smits, J. et al., *Glazen privacy: knelpuntenonderzoek uitvoering Wet politiegegevens (Wpg)*. WODC, Den Haag 2013.

6 Autorisatiemodel politie

Jan Mellema

In artikel 6 van de Wet politiegegevens (Wpg) staat beschreven hoe politiemensen en andere partijen geautoriseerd worden om met (politie)gegevens te werken. Het beschrijft de plichten die de verantwoordelijke (korpschef) heeft op het gebied van autorisaties en het bijbehorende autorisatieproces. Een belangrijk aspect daarin is dat de verantwoordelijke zorgvuldig moet zijn bij het verlenen en intrekken van autorisaties, en dat verleende autorisaties ook proportioneel moeten zijn. Dit zijn twee onderwerpen die de afgelopen periode veel in de publiciteit zijn geweest, bijvoorbeeld over politiemol Mark M. in december 2015, omdat hier onvoldoende sprake van was.

6.1 Waar we vandaan komen

De oorzaak van dat probleem ligt deels in onze historie. De regionale korpsen waaruit de nationale politie is ontstaan, waren zeer verschillend georganiseerd en ingericht. De informatievoorziening was zo mogelijk nog complexer ingericht, er was meestal sprake van een systeembenadering in plaats van autorisaties gericht op gegevens. Binnen het ene korps had je bijvoorbeeld in de BasisVoorziening Opsporing (BVO) de rol van 'rechercheur' en kon je alleen in je eigen onderzoek kijken. Binnen een ander korps kreeg je de rol van 'informatierechercheur' en kon je in alle drugsonderzoeken van het korps kijken. Er was vaak sprake van meer dan één persoonlijk inlogaccount. Collega's hadden meerdere identiteiten omdat ze in verschillende rollen en/of in meerdere korpsen werkzaam waren. Dit alles zorgde ervoor dat de verantwoordelijke niet aan de autorisatievereisten uit de Wpg kon voldoen.

Naast het wettelijke kader van de Wpg werd vanaf het begin van deze eeuw de noodzaak om meer informatie (landelijk) met elkaar te delen steeds groter. In het land zijn de afgelopen decennia verschillende initiatieven[1] geweest om tot een beter autorisatiebeleid, -beheer en -management te komen, rekening houdend met de eisen vanuit de Wpg. Kenmerkend was echter dat de initiatieven vooral op eigen regionaal niveau werden ontwikkeld. Er waren nauwelijks een gezamenlijke visie en strategie, en de versnippering bleef. De focus van de initiatieven lag op het hier en nu en op het verbeteren en beheersen van het bestaande.

---

1 Onder andere de korpsen Noord- en Oost-Gelderland, Hollands-Midden en Rotterdam hebben begin deze eeuw een poging gedaan een Autorisatiebeheersserver (ABS) of Nieuwe Autorisatiestructuur (NAS-tool) te implementeren.

Er was binnen de politie dus nog geen gemeenschappelijke, landelijke visie en gezamenlijk beleefde urgentie met betrekking tot het eenduidig delen van politie-informatie. In 2010 concludeerde de Inspectie Openbare Orde en Veiligheid[2] niet voor niets dat landelijke eenduidigheid, inzicht, transparantie én toezicht ten aanzien van het delen van politie-informatie, alsmede een landelijk autorisatiebeleid, essentiële voorwaarden zijn op weg naar een informatiecultuur en -professionaliteit, die uitgaat van het 'delen, tenzij'-principe.

Tussen 2011 en 2013 werd in opdracht van de Raad van Korpschefs (RKC), en vervolgens de nieuwe korpsleiding, het eerste landelijke autorisatiemodel politie uitgewerkt. Dit is het fundament voor alle autorisatievraagstukken. Gelijktijdig is de ontwikkeling gestart van een landelijke visie op delen van informatie.[3] De visie en het autorisatiemodel zijn ook door zowel de RKC als de nieuwe korpsleiding goedgekeurd. De leidende principes van deze visie zijn:

- landelijk 'delen, tenzij';
- eenvoudig en transparant;
- uitgaan van de professionaliteit van de medewerkers;
- rol gebaseerd;
  - wie ben ik? Landelijke Functiehuis Nederlandse Politie (LFNP) als fundament (uitvoering, leiding, ondersteuning);
  - waar werk ik? Procesgericht (dagelijkse politiezorg, opsporing, intelligence);
  - wat mag ik? Volgens het boekje, Wpg-ruimte en -rollen leidend;
- gegevensgericht, in plaats van applicatiegericht;
- gedragscomponent in het model.

6.2 De kern van het autorisatiemodel

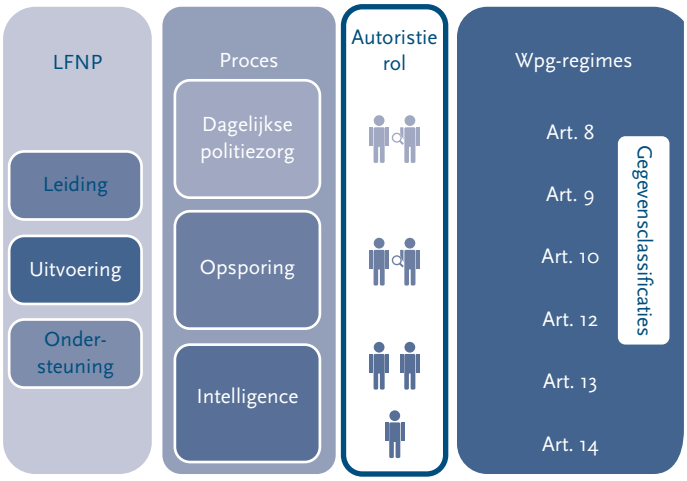
De verschillende in gebruik zijnde politietoepassingen kennen of kenden zeer uiteenlopende rollen. De BasisVoorziening Handhaving (BVH) bijvoorbeeld kent negen rollen, Summ-IT kent er veertien en Betere Opsporing door Sturing op Zaken (BOSZ) negentien. Om de complexiteit terug te dringen, is er in het autorisatiemodel voor gekozen het aantal autorisatierollen te beperken. Deze rollen en de bijbehorende rechten (zie figuur 6.1) zijn vastgesteld op basis van:

- iemands functie in het landelijk functiehuis Nederlandse politie: leiding, uitvoering of ondersteuning;
- het proces waarin iemand werkt: dagelijkse politiezorg, opsporing of intelligence.

---

2 Inspectie Openbare Orde en Veiligheid, *Onderzoek Samenwerkingsafspraken politie 2008*. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag 2010.

3 *'Autoriseren: zo doen we dat hier!': visie op een landelijk autorisatiemodel voor de Nederlandse politie*. Juli 2011.



Figuur 6.1 Basis autorisatiemodel politie

Raadplegen			Medewerker dagelijkse politietaak	Informatiecoördinator dagelijkse politietaak	Medewerker rechtsorde	Informatiecoördinator rechtsorde	Medewerker CIE/RID/Thema	Informatiecoördinator CIE/RID/Thema
Dagelijkse politietaak	Art. 8 WPG	Binnen 1 jaar	√	√	√	√	√	√
		2- 5 jaar	hit/no hit	√	hit/no hit	√	√	√
Onderzoek bepaald geval	Art. 9 WPG	Eigen onderzoek			√	√	√	√
		Afhandelcode Bruikbaar		hit/no hit	hit/no hit	√	√	√
		Afhandelcode For Intell Only				√	√	√
		Afhandelcode Embargo	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.
Inzicht dreiging rechtsorde	Art. 10 WPG	Alle verwerkingen					√	√
		Afhandelcode Bruikbaar			hit/no hit	√	√	√
		Afhandelcode For Intell. Only Hit/no hit				hit/no hit	√	√
		Afhandelcode Embargo	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.
Onder-ste-unende taken	Art. 13 WPG	'Art. 8' basis	hit/no hit	√	hit/no hit	√	√	√
		'Art. 9' basis			hit/no hit	√	√	√

√ = Vrij doorzoeken: dit is het doorzoeken van grote hoeveelheden politie- gegevens met uitgebreide zoeksleutels en het leggen van complexe verbanden. Wie vrij mag doorzoeken, mag ook hit/no hit zoeken.

Hit/no hit = Hit/no hit zoeken: zoeken door middel van een beperkte zoeksleutel/vaste kenmerken (zoals op naam, kenosleutel, postcode of kenteken).

Signaal = Deze gegevens worden niet getoond aan degene die raadpleegt, maar de bevoegd functionaris krijgt een signaal dat iemand naar die informatie heeft gezocht.

Figuur 6.2 De basis van het Landelijk Autorisatiemodel Politie

Dagelijkse politiezorg en opsporing

Voor beide bedrijfsonderdelen dagelijkse politiezorg en opsporing is één autorisatierol beschikbaar. Je kunt dus als medewerker van een basisteam in Groningen bij dezelfde informatie als iemand van een basisteam in Oost-Brabant. En als medewerker opsporing kun je in alle eenheden bij dezelfde informatie.

Intelligence

Voor het bedrijfsonderdeel *intelligence* zijn meerdere rollen beschikbaar. Hierbij zit het verschil vooral in de zoekmogelijkheden door de verschillende informatie in de BasisVoorziening Informatie (BVI). De informatiecoördinator dagelijkse politiezorg, die bijvoorbeeld de briefing op een basisteam voorbereidt, kan alle artikel 8 Wpg-registraties geautomatiseerd doorzoeken en mag ook alle deelbare informatie binnen artikel 9 Wpg zien.[4] De informatiecoördinator rechtsorde plus, bijvoorbeeld een informatiecoördinator binnen een Team Grootschalige Opsporing (TGO) of Staf Grootschalig en Bijzonder Optreden (SGBO), kan naast artikel 8 en 9 Wpg-informatie ook artikel 10 Wpg-informatie zien met de afhandelingscode 11, zie ook figuur 6.3.[5] Als hij voldoet aan zeer strikte voorwaarden[6] kan deze informatiecoördinator ook informatie met de afhandelingscode 01 bekijken. Aan de twee genoemde autorisatierollen zijn op basis van artikel 6 Wpg strikte deskundigheidseisen verbonden over de plaats in de organisatie, screening en bewezen competenties.

Afhandelingscodes	
11	Operationaal te gebruiken
01	Alleen te gebruiken na overleg met de afzender
00	Informatie met zware beperkingen voor gebruik
200	Kan niet operationeel gebruikt worden, maar kan onder bepaalde voorwaarden wel voor coördinatie- en analyse doeleinden worden gebruikt + informatie met verhoogd afbreukrisico
300	Kan niet operationeel gebruikt worden, maar kan onder bepaalde voorwaarden wel voor coördinatie- en analyse doeleinden worden gebruikt + informatie met bronbescherming

Figuur 6.3 Afhandelingscode Besluit Verplichte Politiegegevens

De termen 'deelbare informatie', '11' en '01' zijn voorbeelden van gegevensclassificatie die op basis van bedrijfsafspraken en/of wettelijke kaders aan informatie kan worden toegevoegd. Een voorbeeld hiervan is de Wet bijzondere opsporingsbevoegdheden (Wet BOB), waarin beschreven staat dat teamleiders (in hun procesrol als bevoegd functionaris) en de officier van justitie toestemming moeten geven om de informatie in andere onderzoeken te mogen gebruiken. Ook kan informatie op basis van de artikelen 2:12 en 2:13 van het Besluit politiegegevens (Bpg) worden voorzien van een dergelijke classificatie. In het politiejargon is er dan vaak sprake van wat men noemt 'embargo-informatie', hoewel dit niet overeenkomt met de definitie in de Wpg.[7] Binnen de opsporing is dit begrip ook nog in gebruik voor veel gegevens uit rechercheonderzoek.

4 Zie hoofdstuk 5 De Wpg voor een toelichting op de Wpg en de artikelen.

5 Afhandelingscodes zijn classificaties van gegevens die het mogelijk maken bepaalde informatie adequaat te beschermen.

6 Om 01 te mogen zien, is een A-screening verplicht en voor 11-informatie is dat een P-screening.

7 Artikel 2:13 Bpg onder f: 'van een verwerking voor een door het College van procureurs-generaal als embargo-onderzoek aangemerkt onderzoek met een zeer groot belang van afscherming vanwege afbreukrisico's, levensbedreigende risico's, politieke gevoeligheid of publiciteitsgevoeligheid van het onderzoek'.

CIE/RID/Thema

Voor medewerkers en informatiecoördinatoren werkzaam binnen de criminele en openbare inlichtingen zijn ook de aparte autorisatierollen uit figuur 6.2 in gebruik.

6.3 De veranderopgave

De implementatie van het autorisatiemodel zou altijd al een ingewikkelde veranderopgave zijn geweest. Maar ten tijde van een organisatorische verandering én een personele reorganisatie van de politie een autorisatiemodel invoeren dat gebaseerd is op nieuwe functies en rollen, is pas echt een grote uitdaging. Het op orde hebben van de basisadministratie van het personeel is daarvoor noodzakelijk. Als die administratie actuele medewerkersgegevens kan leveren zoals de functie, formele en/of informele plaats in de organisatie, screeningsniveau en verworven competenties, kunnen de randvoorwaarden voor (geautomatiseerde) autorisatie-uitgifte worden ingevuld.

Daarnaast zijn er allerlei technische issues om de informatievoorziening aan te passen aan het autorisatiemodel of de uitgangspunten. De systeemoriëntatie loslaten en overgaan naar een gegevensautorisatie is een complex traject. Nieuwe systemen kunnen conform het autorisatiemodel gebouwd worden; de oude systemen vergen aanpassingen die tijd en geld kosten. Het hebben van een BasisVoorziening Informatie (BVI), waarop verschillende systemen gebouwd worden zoals BlueSpot Monitor (BSM) en BasisVoorziening Informatie voor Integrale Bevraging (BVI-IB), laat zien dat het landelijk informatie delen conform het autorisatiemodel mogelijk is, en dat het de efficiëntie en effectiviteit verhoogt.

Figuur 6.4 Politiemedewerker aan het werk met systemen

De volgende fase van deze veranderopgave is de culturele verandering binnen de gehele politie en specifiek binnen de opsporing. Er zijn veel cultuurbepaalde factoren die een

weergave zijn van het gebrek aan onderling vertrouwen bij informatiedeling: afbreukrisico's die mensen in de opsporing zien, het delen van niet gevalideerde informatie, interpretatievrijheid, 'het zijn mijn gegevens' enzovoort.

Het zal waarschijnlijk nog enkele jaren duren voordat autoriseren conform het vastgestelde autorisatiemodel en autorisatiebeleid bij de politie in alle systemen en organisatieonderdelen volledig in werking is.

7 IGP en ethiek, ofwel: wat mag en wat mag niet?

Peter Tazelaar

Ethiek, een tak van de filosofie, is de studie naar de moraal, ofwel naar hetgeen we als de juiste manier van handelen beschouwen of zouden moeten beschouwen. Een beschouwing over ethiek met betrekking tot een zeer breed onderwerp als informatiegestuurd politiewerk (IGP) kan slechts een door de tijdgeest bepaalde visie opleveren, niet eens op wat al dan niet toelaatbaar wordt geacht, maar hooguit een visie waarin aandachtspunten worden benoemd die in de discussie hierover zouden kunnen worden betrokken.

Hoewel formeel onjuist, worden in de praktijk de begrippen 'ethiek' en 'moraal' door elkaar gebruikt, en ook ik zal me daar in het onderstaande aan bezondigen wanneer ik me de vraag stel of bepaalde vormen van handelen ethisch verantwoord zijn.

Bij ethiek in relatie tot IGP gaat het dus om de vraag wat onze normen en waarden ten aanzien daarvan zouden moeten zijn en hoe tot de vaststelling daarvan te komen. En daarmee wordt al meteen opgeworpen hoe glad het ijs is waarop we ons daarbij begeven. Immers er is niet alleen sprake van collectieve normen en waarden in onze samenleving die, als het om politieel optreden gaat, veelal zijn neergelegd in wet- en regelgeving (gij zult niet... of gij dient...), maar ook ontwikkelen individuen hun eigen normen en waarden op basis van persoonlijke overtuigingen. Wat voor de een ethisch verantwoord handelen is, is dat voor de ander niet.

7.1 Vroeger en nu

Vroeger zat de rijksveldwachter – naast af en toe een ommetje door het dorp – achter zijn bureau en wachtte hij op een telefoontje waaruit hem bleek dat er iets was gebeurd, als gevolg waarvan hij in actie moest komen (reactief optreden). Vandaag de dag zijn grote delen van de politie proactief bezig met het verzamelen en analyseren van informatie. Dit teneinde niet alleen een zo goed mogelijk beeld te krijgen van een bepaalde situatie (*descriptive policing*) maar ook om zo veel mogelijk aan de voorkant te komen van hetgeen er staat te gebeuren (*predictive policing*) en dat zo mogelijk te voorkomen. En zeker bij blauw op straat wordt dit vaak dan ook nog gekoppeld aan instructies en toe te passen procedures indien de informatie tot een zekere conclusie leidt (*prescriptive policing*).

Nu deed de veldwachter weliswaar op zeer kleine schaal hetzelfde, immers hij kende zijn pappenheimers in zijn dorp, had dus informatie over hen, vormde zich daar een beeld bij en wist door bepaalde personen tijdig aan te spreken, onprettige zaken te voorkomen. Ziedaar het beeld (van een deel van de taak) van de tegenwoordige wijkagent.

Het verschil met vroeger echter ligt in het feit dat al die data van de verschillende wijkagenten en andere politieambtenaren, gecombineerd met informatie uit opsporingsonderzoeken, uit andere private of overheidsdatabases en uit open bronnen, bij de tot één

korps omgesmede politie samenkomen in één grote informatiefabriek. Dat is ook nodig, zo betogen velen terecht, want de criminaliteit speelt zich niet meer af in het dorp, maar is regio- en grensoverschrijdend. Maar waar je dan vroeger slechts gekend werd door die ene veldwachter in jouw dorp, ben je tegenwoordig – als er informatie over je wordt vastgelegd – bekend bij de politie in heel Nederland, en als gevolg van de toegenomen Europese samenwerking in heel Europa of zelfs nog daarbuiten.

En dat de rest van de wereld nog geheel andere opvattingen heeft over hetgeen in de richting van de burger wel of niet verantwoord is, bleek onder meer uit de discussie tussen Europol en de Russische Federatie over een mogelijke operationele samenwerkingsovereenkomst. Toen daarbij het onderwerp 'rechten betrokkene' ter sprake kwam, moesten de Russische delegatieleden smakelijk lachen over de Europese opvatting dat een burger in beginsel het recht op kennisneming moet kunnen uitoefenen. Het kon toch niet zo zijn dat je de criminelen ging vertellen welke informatie je over hen had?

7.2 Privacy

Figuur 7.1 Privacy

Een ander aspect dat van invloed is op de schaalgrootte van de informatieverwerking is de toenemende afhankelijkheid van de burger (waaronder ook de politieambtenaar en de crimineel zijn te rekenen) van de hedendaagse zich snel ontwikkelende informatie- en communicatietechnologie, waarbij de gemiddelde burger lijkt te vergeten dat (of lijkt te wennen aan het feit dat) de overheid steeds meer over hem weet en daarmee zijn persoonlijke levenssfeer steeds meer aantast.

Hoe ver mag je als overheid, als politie daarin gaan? Volgens sommigen zeer ver, zolang dit de veiligheid ten goede komt. Velen, onder wie ook opmerkelijk veel politieambtenaren, stellen dat wanneer je niets op je geweten hebt, je ook niets hebt te verbergen. Je mag alles van me weten, behalve mijn pincode, grappen ze dan. Toen ik nog lesgaf op de

Rechercheschool over privacywetgeving ('die leidt er toch alleen toe dat criminelen worden beschermd?'), werd ik regelmatig door rechercheurs geconfronteerd met die stelling dat zij echt helemaal niets te verbergen hadden. 'Dus als jouw vriendin jou een liefdesbrief schrijft, mag iedereen die lezen?' vroeg ik dan. 'Eh... nou nee, dat zou ik nu echt niet prettig vinden', was dan altijd het antwoord. En dat is nu precies waar het om gaat bij de bescherming van de persoonlijke levenssfeer. Privacy is namelijk het recht dat anderen – en zeker de overheid – zich niet met je bemoeien, tenzij er een duidelijke en legitieme noodzaak en wettelijke grondslag is waarom ze dat wel (mogen) doen. *The right to be left alone*, zoals dat zo treffend wordt aangeduid.

De mate waarin iemand op dat recht een beroep wil doen, is een puur persoonlijke aangelegenheid, maar ook culturele verschillen in waar je geheimzinnig over wilt doen of niet, spelen een rol. In de Verenigde Staten pronken mensen met de hoogte van hun inkomen, want hoe meer je verdient, hoe meer status je verwerft in je omgeving en dat mag, nee, dat móét iedereen weten. Maar in Nederland bestaat er een tendens om zo weinig mogelijk inzicht te geven in wat je verdient – het zal wel iets te maken hebben met onze calvinistische achtergrond –, al wordt die tendens doorbroken door de tegenwoordige roep om transparantie en de mogelijkheden die, voor zover het de overheid betreft, de Wet openbaarheid van bestuur aan burgers biedt om toch dat inzicht te verkrijgen. Culturele verschillen zijn dus medebepalend ten aanzien van de vraag waar de grenzen liggen.

Waar vroeger door politie en justitie (en andere overheden) alleen gegevens werden vastgelegd over personen die (vermoedelijk) iets hadden gedaan of waarmee anderszins bemoeienis was gerechtvaardigd, worden tegenwoordig gegevens vastgelegd over iedereen, ook over onverdachte personen.

Voorbeelden daarvan zijn de dataretentie van communicatiegegevens, het onlangs door de Tweede Kamer geaccordeerde wetsvoorstel tot vastlegging van alle passagegegevens voor een periode van 28 dagen teneinde deze te kunnen gebruiken als zich een strafbaar feit heeft voorgedaan, maar ook de beelden van de gemeentelijke toezichtcamera's die voor eenzelfde periode kunnen worden bewaard. En dan hebben we het nog niet over de in opkomst zijnde drones en de vele satellieten die ons dagelijks vanuit de lucht bespieden en waarvoor ook de politie zich opmaakt om die middelen op korte termijn (drones) of lange termijn (satellieten) in te gaan zetten ter vergroting van de veiligheid.

Het vraagstuk van de gegevensopslag over onverdachte personen door de politie beheerste jarenlang in de Wet politieregisters de discussie. In beginsel mocht de politie slechts de gegevens opslaan van verdachten (personen ten aanzien van wie uit feiten of omstandigheden een vermoeden van schuld aan een strafbaar feit voortvloeide). Over onverdachte personen mocht de politie slechts gedurende vier maanden de gegevens bewaren en als deze niet binnen de gegeven periode leidden tot een verdenking, dienden de gegevens te worden verwijderd. Dat criterium is allang losgelaten en ook het verdenkingsbegrip is opgerekt in die zin, dat als het gaat om zware criminaliteit in georganiseerd verband of om terrorisme, aanwijzingen van betrokkenheid bij strafbare feiten al voldoende zijn om niet alleen gegevensverwerking maar ook de inzet van strafvorderlijke bevoegdheden te rechtvaardigen. We zijn dus als politie veel meer aan de voorkant gaan zitten.

7.3 Vermenging

En daarmee doemt nog een ander gevaar op, met name waar het de bestrijding van terrorisme betreft, namelijk de scheiding van taken en verantwoordelijkheden tussen enerzijds de politie en anderzijds de inlichtingen- en veiligheidsdiensten.

Ter bescherming van de democratische rechtsorde en de veiligheid van de staat mogen laatstgenoemde diensten al in een zeer vroeg stadium personen op de korrel nemen van wie men vermoedt dat deze een gevaar voor de democratische rechtsstaat zouden kunnen vormen. En die diensten mogen daarover (met inzet van vergaande bevoegdheden) gegevens vergaren en vastleggen, waarna – als blijkt dat er sprake is van een verdenking van (of in bepaalde gevallen: aanwijzingen van betrokkenheid bij) strafbare feiten – dit door middel van een ambtsbericht aan de politie ter kennis kan worden gebracht, die dan de verdere opsporing ter hand neemt.

Althans, zo is de klassieke onderverdeling. Maar de praktijk wijst uit dat waar het om terrorisme gaat, de politie steeds meer aan de voorkant is gaan zitten en zelf steeds meer als een inlichtingendienst is gaan opereren, waarbij uitvoerig gegevens worden vastgelegd over personen ten aanzien van wie er nog slechts heel zwakke signalen bestaan inzake mogelijke betrokkenheid bij terrorisme (Themaregister Terrorisme).

Natuurlijk is de samenwerking inzake de bestrijding van terrorisme een goede zaak, maar is zo'n sluipende vermenging van werkwijzen nu wel hetgeen we echt willen, en wie bewaakt dan de grenzen van ons opschuiven naar de voorkant?

Wie de debatten in de Tweede Kamer over dit onderwerp heeft gevolgd, kan constateren dat de Tweede Kamer nog weleens tegenstrijdige meningen uitdraagt. In het ene debat wordt met kracht gehamerd op het belang van de persoonlijke levenssfeer en in een volgend debat, meestal na een plaatsgevonden aanslag, wordt de minister van Veiligheid en Justitie verweten dat hij niet méér informatie in relatie tot betrokkene heeft vastgelegd en daarop actie heeft ondernomen, ook al stelt de minister dat de wettelijke mogelijkheden hiertoe niet toereikend waren.

Als het de bedoeling is dat de grenzen van hetgeen ethisch verantwoord en dus acceptabel is ten aanzien van de inmenging in de persoonlijke levenssfeer van de burger, door ons in gezamenlijkheid worden vastgesteld en zo veel mogelijk in wetgeving worden verankerd, dan maken dergelijke uiteenlopende standpunten waarbij te veel op 'dossierniveau' wordt geoordeeld zonder de grotere verbanden en onderlinge verhoudingen in het oog te houden, de discussie er niet gemakkelijker op.

Dat de regelgeving op dit terrein en het denken daarover zich in rap tempo hebben ontwikkeld, blijkt ook uit het feit dat er in de eerste privacywetgeving voor de politie nog sprake was van een verbod op het koppelen van bestanden. Dit verbod gold slechts dan niet wanneer het desbetreffende privacyreglement – dat vooraf moest worden goedgekeurd door de Registratiekamer (de tegenwoordige Autoriteit Persoonsgegevens) – precies omschreef voor welk doel en met welk bestand een koppeling van het in het reglement beschreven bestand mocht plaatsvinden. En als zo'n koppeling niet van tevoren was beschreven, toegelicht en goedgekeurd, mocht die in ad-hocgevallen alleen plaatsvinden met toestemming van de Registratiekamer.

Het behoeft geen vermelding dat de politie in die tijd deze regel regelmatig schond omdat immers al snel duidelijk werd dat je door de vergelijking van verschillende

bestanden aan heel nuttige opsporingsinformatie kon komen. Een dergelijk koppelingsverbod is heden ten dage niet meer denkbaar, zelfs niet meer werkbaar, al wordt door middel van het beginsel van de doelbinding (met alle daarop van toepassing zijnde uitzonderingen) nog wel getracht om enigszins paal en perk te stellen aan willekeur bij de onderlinge vergelijking van databestanden.

7.4 Ontwikkeling opvattingen

Behalve dus het opschuiven in ons denken met betrekking tot hetgeen acceptabel is onder invloed van bijvoorbeeld terrorisme, is ons normbesef ook onderhevig aan het beschikbaar komen van steeds effectievere technologisch geavanceerde middelen. Ze zijn er, en waarom zou je ze dan niet inzetten om Nederland of de wereld veiliger te maken? De ontwikkelingen gaan door, ze zijn niet meer te stoppen en ze gaan steeds sneller. En onze tegenstanders gebruiken ze ook en we willen onszelf toch niet op achterstand zetten? Sterker nog, indien de politie wel over informatie kan beschikken maar deze niet gebruikt, lopen we nog tegen het verwijt aan dat we willens en weten een onveilige situatie hebben laten ontstaan die we met gebruik van beschikbare informatie en technologie hadden kunnen voorkomen.

De ontwikkeling van onze normen en waarden en hetgeen wij acceptabel achten als het gaat om de door sommigen als ongebreideld aangemerkte informatiebehoefte van de overheid, is in de historie verlopen met horten en stoten. Het verzet tegen de volkstelling van 1971 – die onder meer herinneringen opriep aan de Duitse bezetter tijdens de Tweede Wereldoorlog die zo efficiënt gebruik wist te maken van onze met veel precisie bijgehouden bevolkingsboekhouding – leidde in Nederland tot aandacht voor privacy, tot het ontstaan van de eerste privacywetgeving rond 1990 en tot de oprichting van de eerste onafhankelijke toezichthouder voor privacy, de Registratiekamer. Maar ook bij de opname van vingerafdrukken in het paspoort, de invoering van de Wet op de identificatieplicht en de Wet bevoegdheden vorderen gegevens was er rumoer. En zo ook bij vele andere wetsvoorstellen die de bevoegdheden van de overheid zouden vergroten met het oog op een efficiënter overheidsoptreden, zoals recentelijk het genoemde wetsvoorstel inzake automatic number plate recognition (ANPR), met betrekking waartoe de Stichting Privacy First al heeft aangekondigd, na aanname van het wetsvoorstel door de Eerste Kamer, een geding te zullen starten om deze wet ongeldig te doen verklaren.

En toch worden vrijwel al deze wetsvoorstellen – soms met aanpassingen of extra ingebouwde waarborgen – uiteindelijk doorgevoerd. En het rumoer verstomt en we gaan op naar de volgende inbreuk makende wet. We accepteren als burger het onvermijdelijke en schikken ons in ons lot, zozeer zelfs dat de jongere generaties zich over het algemeen niet eens meer bewust zijn van de gevaren die aan de grote informatiedeling kunnen kleven en achteloos hun hele 'hebben en houden' op het internet etaleren met soms grote negatieve gevolgen voor hun persoonlijke leven.

Onze eigen opvattingen als burger zijn in deze informatiemaatschappij dus aan sterke verandering onderhevig. Werden jaren geleden burgers boos omdat er een camera in hun straat werd geplaatst die ook zicht op hun voordeur had, tegenwoordig zijn velen er juist

blij mee omdat het hun gevoel van veiligheid vergroot. Als burgers vragen we (via de gemeenteraad) soms zelfs om toezichtcamera's in de gemeente, omdat we inmiddels aan veiligheid een grotere waarde toekennen dan aan de bescherming van onze persoonlijke levenssfeer, en de overheid en politie haken daarop in.

Uiteindelijk gaat het steeds om de verhouding tussen de toenemende roep om veiligheid en de steeds meer naar de achtergrond gedrongen wens om in alle vrijheid en onbespied zichzelf te kunnen zijn. De instelling van de Patriot Act in de Verenigde Staten bracht sommige tegenstanders daarvan ertoe om te stellen dat het behoud van individuele vrijheden dan helaas maar gepaard moest gaan met menselijke offers. Of, om het anders te stellen, het omkomen van tientallen of honderden mensen als gevolg van zo af en toe een terroristische aanslag, was de prijs die we maar moesten betalen voor het behoud van onze vrijheden tegenover een al te bemoeizuchtige overheid.

Dat een dergelijke stellingname op steun van weinigen kon en kan rekenen en ook zeker niet een beleid is dat enig kabinet durft voor te stellen, is bekend, maar de openbaringen van WikiLeaks en Edward Snowden tonen aan dat in elk geval de Amerikaanse overheid lang niet altijd in staat is gebleken zichzelf te begrenzen en haar eigen regels na te leven of ten minste transparant te zijn over haar gedrag. En zou dat in andere landen heel anders zijn?

7.5 Vooruitzichten

Terugkerend naar het ethische vraagstuk, kunnen we nog slechts constateren dat de vraag waar de grenzen liggen van hetgeen nog acceptabel en ethisch verantwoord is, niet zozeer bepaald wordt door absolute normen, als wel door de schuivende panelen die door de technologische ontwikkelingen in gang worden gezet. En door de vraag wat wij zelf nu eigenlijk willen, waarbij de grote invloed van het opgekomen terrorisme zeker niet moet worden onderschat.

Wat wij zelf willen en acceptabel achten, leggen wij gezamenlijk vast in regels over hoe wij willen omgaan met informatie. Wat vroeger volstrekt onacceptabel was, is vandaag de dag de normaalste zaak van de wereld. De beelden van sommige Hollywoodfilms tonen ons hoe de wereld er in de toekomst uit zou kunnen zien, en sommige jaren geleden nog vrij futuristische technieken, zoals automatische gelaatsherkenning, beginnen op dit moment steeds meer bewaarheid te worden. Die techniek kan nu nog slechts met succes worden toegepast wanneer er een helder van voren getoond gezicht kan worden vergeleken met de foto's in de database. Maar op termijn zal eenieder die op straat het zich nog steeds uitbreidende cameranetwerk passeert, continu kunnen worden vergeleken met de database waarin afbeeldingen zijn opgeslagen over personen die bijzondere aandacht behoeven.

En als je dan toch graag 'alleen wil worden gelaten' door de overheid, maar de overheid denkt – terecht of onterecht – daar anders over, dan is het als hedendaagse burger vrijwel onmogelijk je te onttrekken aan niet gewenst 'toezicht'. Dit bleek maar weer eens duidelijk uit het onlangs uitgezonden programma *Hunted*, waarbij >>

>> een aantal burgers de opdracht kreeg zich drie weken onvindbaar te maken voor een (zogenaamd) rechercheteam dat alle mogelijkheden van onze tegenwoordige informatiemaatschappij toepaste om hen op te sporen. Er bleek wel uit dat het je alleen nog redt om onopgemerkt voor die overheid te blijven indien je – zo mogelijk vermomd en voorzien van voldoende cash geld – bereid bent afstand te doen van al die technologische verworvenheden die tegenwoordig zo deel uitmaken van ons dagelijks leven. Geen telefoon of internet gebruiken, bereid zijn om in een tentje in het bos te leven en je slechts laten vervoeren in de kofferbak van hopelijk betrouwbare personen die daarover dan op hún beurt niet reppen via hun telefoon of op hun eigen sociale media.

Big brother is watching you lijkt een cliché, maar is intussen sluipend werkelijkheid geworden. Je kunt alleen nog hopen dat de zoekende ogen en oren niet op jou gericht zijn omdat je toch immers niets hebt misdaan, en dat de zoekende overheid misschien door de brij aan informatie jou per ongeluk over het hoofd ziet. Maar zelfs die kans wordt steeds kleiner met de opkomst van zelflerende computersystemen, kunstmatige intelligentie, steeds betere analysesystemen die verbanden aantonen waarnaar men zelfs niet op zoek was en steeds meer data ter beschikking om te vergelijken of om profielen mee te vervaardigen.

7.6 Bewustwording

De toegenomen mogelijkheden en bevoegdheden om gegevens te verzamelen, vast te leggen en met elkaar te vergelijken, leggen met name op de overheid en in het bijzonder de politie een zware verplichting om ervoor te zorgen dat er voldoende waarborgen worden ingebouwd en nageleefd om een verkeerd gebruik tegen te gaan; de burger zelf heeft daarop immers nauwelijks invloed meer.

Is de overheid in het algemeen en de politie in het bijzonder altijd te vertrouwen in het gebruik van en de omgang met onze persoonlijke gegevens? Er zijn, behalve de hiervoor weergegeven voorbeelden uit Amerika, ook in Nederland gevallen bekend waarin is gebleken dat de overheid niet goed met onze gegevens is omgegaan. Niet alleen beveiligen we ze soms onvoldoende waardoor ze gehackt worden, maar soms ook zijn er helaas collega's die ze lekken naar de verkeerde mensen. En dan hebben we het nog niet over collega's die onbewust (vanwege een gebrek aan kennis) of bewust (het is toch immers voor de goede zaak!) de regels met betrekking tot de omgang met die informatie aan hun laars lappen.

Toegegeven, de privacy- en andere regels zijn vaak lastig te interpreteren en moeilijk toe te passen in onze bedrijfsinformatiestructuur en in onze cultuur die sterk is gericht op het behalen van (opsporings)resultaat. Het feit dat we inmiddels bezig zijn aan het zoveelste verbeterplan voor een betere implementatie van de Wet politiegegevens (Wpg) toont aan dat de omgang met, en correcte naleving van, deze regels een weerbarstige materie is die we wel nooit voor 100 procent onder de knie zullen krijgen; het blijft uiteindelijk mensenwerk. En dus bieden regels alleen niet een sluitende oplossing en zijn beter toezicht, meer transparantie en interne bewustwording van de risico's bij de omgang met informatie over anderen een absolute must.

Gelukkig wordt ook de overheid zich steeds meer bewust van de risico's die verbonden zijn aan grootschalige informatieverwerking. Zo schrijven de in Brussel tot stand gekomen algemene verordening gegevensbescherming (AVG) en de Richtlijn Opsporing en vervolging, die in 2018 in werking zullen treden, onder meer voor dat privacy by design[1] en *privacy by default* een grotere rol dienen te gaan spelen bij de inrichting van informatiesystemen, zodat er minder valt af te wegen door de individuele ambtenaar en deze dus minder fouten kan maken. Voorts dient de overheid aanmerkelijk transparanter te worden in de richting van de burger waar het betreft inzicht geven in de dataprocessen binnen de overheid en de doelen waarvoor deze plaatsvinden.

Bovendien schrijven de Brusselse regels voor dat een persoon niet mag worden onderworpen aan een besluit met voor hem negatieve rechtsgevolgen of dat hem in aanmerkelijke mate treft indien dat besluit alleen wordt genomen op grond van een geautomatiseerde verwerking die bedoeld is om een beeld te krijgen van bepaalde persoonlijke aspecten. Voor zo'n verwerking dienen passende waarborgen te worden geboden, waaronder specifieke voorlichting aan betrokkene en het recht op menselijke tussenkomst.

Er zijn verschillende gevallen bekend waarbij dergelijke 'geautomatiseerde besluiten' totaal verkeerd uitwerkten. Zo werden in de Verenigde Staten honderden leraren ontslagen nadat op basis van een wiskundig model was aangetoond dat deze leraren laag scoorden in hun geschiktheid als leraar. De door een privaat bedrijf ontwikkelde algoritmes werden geheim gehouden en later bleek dat het model was gebaseerd op een testcode van slechts 25 kinderen. Het departement van Onderwijs begreep zelf het model niet, de leraar wist niet waar zijn score vandaan kwam of hoe hij deze kon verbeteren, maar de leraren werden er wel om ontslagen, want de computer vertelde dat ze ongeschikt waren.[2]

Die beoordelingsmodellen worden gebouwd door mensen. En mensen kunnen fouten maken in hun beoordeling of onbewust daarin hun eigen vooroordelen inbouwen. Dat is ook bij de politieambtenaar op straat het geval, wanneer hij de neiging heeft om meer dan gemiddeld personen van een bepaalde bevolkingsgroep staande te houden en daardoor ook meer dan gemiddeld bij die bevolkingsgroep onregelmatigheden constateert en aldus wordt bevestigd in zijn mening dat er met die personen ook altijd iets aan de hand is. Dat gevaar van discriminatie en stigmatisering ligt zoveel te meer op de loer bij grootschalige geautomatiseerde gegevensverwerkingen en de daarop losgelaten analysemethoden voor profilering van verdachte gedragspatronen. Bovendien leidt een en ander tot omkering van de bewijslast, want de burger die aan het profiel voldoet, zal dienen uit te leggen waarom hij toch echt niets kwaads in de zin heeft; en daarmee vormt dat ook nog eens een aantasting van de onschuldpresumptie.

---

1 Zie ook: Brussaart, P. et al., *Nieuwe Operationele Informatievoorziening Nationale Politie: Privacy by Design*. Politie, Den Haag 2015.

2 Janssen, G., 'Wiskunde is mooi, maar de wereld is wispelturig'. In: *Vrij Nederland*, 19 november 2016, pp. 45-49.

7.7 Permanente discussie

Het in april 2016 door de Wetenschappelijke Raad voor het Regeringsbeleid aan het kabinet aangeboden rapport *Big data in een vrije en veilige samenleving* constateert dat big data in belangrijke mate aan veiligheid kunnen bijdragen, maar ook risico's kunnen opleveren die met bigdata-toepassingen gepaard gaan. Het rapport bepleit daarom een versteviging van het toezicht, de transparantie (ook van de gebruikte analysemethoden en -grondslagen) en het rechterlijk toezicht met betrekking tot big data en het gebruik ervan. De reactie van het kabinet hierop toont aan dat het kabinet zich zeer bewust is, niet alleen van de mogelijkheden die big data bieden om de veiligheid in Nederland te vergroten, maar ook van de risico's die hiermee gepaard gaan.

De term IGP of informatiegestuurd politiewerk suggereert dat de politie, met inachtneming van collectieve of persoonlijke normen en waarden, niet zozeer zichzelf stuurt op basis van beschikbare informatie, maar daarentegen wórdt gestuurd door de aanwezige informatie. En dat de individuele politieambtenaar dus over de juistheid van die informatie en over het daarop te baseren handelen niet zelf meer hoeft na te denken.

Nu zal dat laatste niet zo scherp zijn bedoeld, maar het toont wel aan dat wanneer we een zo grote rol toekennen aan de informatie die het handelen van de politie aanstuurt, er een verschuiving plaatsvindt van het persoonlijk nadenken over de normen en waarden die bij een bepaald politieoptreden van toepassing zijn, naar een normen- en waardesysteem dat deel moet uitmaken van en ingebouwd dient te zijn in het informatiekader zelf, in de vergaring en in het gebruik van die informatie.

Dat betekent dat we als individuele politieambtenaar het denken over de normen en waarden van hetgeen acceptabel is, in toenemende mate overlaten aan de juristen die de regels stellen en aan de techneuten die, in een poging de soms weinig transparante regels zo goed mogelijk te interpreteren, de knoppen van de systemen zo instellen dat bepaalde handelingen en vergelijkingen wel of niet plaats kunnen vinden. En dat zou een gemis zijn, want de discussie over hetgeen toelaatbaar is of niet, dient continu op alle niveaus te worden gevoerd, niet alleen in het parlement en op de departementen, maar ook bij de politiemanagers en vooral ook op de werkvloer van de politie.

Want juist daarvandaan komen veel van de innovatieve gedachten voor weer nieuwe vormen van op de persoonlijke levenssfeer van burgers diep ingrijpende informatieverwerking, waarover ik nog wel eens pleeg te zeggen: 'Nog los van de nog uit te zoeken vraag of dit juridisch misschien kan, moet je dit gewoon niet willen, want dit gaat ook over jou en jouw familieleden.' En de politieambtenaar in de operatie die gebruiker van al die voorhanden zijnde informatie is, zal zich steeds bewust moeten zijn van de gevolgen die dit gebruik kan opleveren voor de burger die wellicht volkomen onschuldig is.

Met de oproep aan alle politiecollega's om vooral ook zelf, als burger en als onderdeel van deze samenleving, voortdurend te blijven nadenken over de ethische grenzen die aan onze informatieverwerking zouden moeten worden gesteld – en de juristen en privacyadviseurs zullen graag willen meedenken – beëindig ik deze beschouwing over IGP en ethiek, in de hoop dat deze stemt tot nadenken en aldus een bijdrage levert aan de bewustwording van onze verantwoordelijkheid als politie ten opzichte van de samenleving.

8 In gesprek met Peter Holla over ethiek

Figuur 8.1 Peter Holla

Peter Holla: 'Toen ik begin jaren tachtig bij de politie startte, werd een proces-verbaal getypt op een typemachine met een carbonpapiertje ertussen. De doorslag was voor de administratie. Om informatie te delen met collega's was er niets! Hooguit de administratie handmatig doorzoeken en aangiften eruit vissen die enige vergelijking hadden: kortom monnikenwerk. Het Herkenningssysteem (HKS) was het enige om gegevens over de modus operandi (MO) en signalement te vergelijken. Dertig jaar later is het HKS niet meer in gebruik en zoeken we kriskras door alle systemen van de politie. Op dit moment al meer dan vijftig miljoen keer per jaar door middel van BVI-IB, waarbij in één keer al meerder gegevensbestanden bevraagd kunnen worden. Een megaverandering in slechts één loopbaan.'

Figuur 8.2 Administratie politie

Dat laat zien: wettelijk mogen er veel dingen, technisch kunnen er steeds meer dingen. Niet alle wetten en regels zijn technisch te garanderen en bovendien zit er 'interpretatieruimte' in de wetten en regels zoals de Wet politiegegevens (Wpg). Welke ethische vraagstukken kun je bij deze ruimere mogelijkheden en interpretatie stellen?

'Het is geen wonder dat de vraag naar voren komt waar de grens ligt. Ten eerste: we weten al veel meer dan wat we er nu mee doen. Dat betekent dat er niet sprake moet zijn van een afbakening, maar van een verdere ontwikkeling. Wat bedoel ik hiermee? Als een rechercheur van een basisteam met onderzoek aan een net aangehouden verdachte begint, bevraagt hij, als hij goed zijn werk doet, minimaal BVI-IB (integrale bevraging) om een goed beeld te krijgen van diegene die voor hem zit. Soms vraagt hij aan het districtelijk informatieknooppunt (DIK) een nadere duiding.

Maar veelal gebeurt dit niet door gebrek aan tijd. Het beeld dat de rechercheur hierdoor krijgt van wat er echt bekend is over deze verdachte, is verre van volledig. Alleen overzichten van antecedenten en BVH-mutaties zijn onvoldoende voor een compleet beeld van diegene die voor hem zit. De rechercheur begint als het ware op nul. Als er een bredere analyse getoond zou worden over zijn achtergrond, motieven, MO's, verklaringen, netwerk enzovoort zou hij of zij veel sneller gefocust aan de gang kunnen gaan en zou ook de afhandeling bij de zogenoemde ZSM-aanpak[1] waarschijnlijk betekenisvoller kunnen gebeuren. Om dit enigszins mogelijk te maken in de toekomst wordt het digitale persoonsdossier gemaakt dat veel van deze vragen wel beantwoordt. Je hele (criminele) doopceel op een paar A4'tjes, en daarna beschikbaar voor de hele strafrechtsketen. De informatie is er al en de techniek om het te bevragen en te presenteren ook.'

Moet dit begrensd worden?

'Welnee! De burger verwacht niets anders dan dat we dit allang doen. Maar het dient wel te voldoen aan het wettelijk kader dat door onder andere de Wet politiegegevens (Wpg) wordt geboden. En door de snelle ontwikkeling van alle datasystemen en bijbehorende regelgeving staat het goede gebruik ervan onder druk.

Sinds de samenvoeging van veel data in een database als BVI is er heel veel mogelijk geworden qua bevraging en analyse. Het is voor de eindgebruiker steeds moeilijker om dit bij te houden en de nieuwe mogelijkheden onder de knie te krijgen. Het is absoluut te overwegen een periode niet te veel effort te steken in nog meer nieuwe mogelijkheden, maar meer in opleiding. Een programma zoals de integrale beroepsvaardighedentraining (IBT) gericht op systeem- en gegevensgebruik. Rechtmatig benutten wat er mogelijk is. Hierin zou dan ook aandacht besteed kunnen worden aan de vraag waar de grens van bevragen ligt.'

Dat leidt naar de vraag met welk doel je een systeem mag bevragen

'Zelf ben ik in mijn eenheid verantwoordelijk voor de beslissingen over alle disciplinaire zaken. Met een grote frequentie zitten daar onderzoeken tussen met betrekking tot foutief gebruik van de systemen. Uiteraard kennen we de voorbeelden van de politiemol. Hierover

1 ZSM staat voor zorgvuldig, snel en op maat met betrekking tot het afdoeningstraject. Binnen ZSM wordt door OM, politie, reclassering, kinderbescherming, slachtofferhulp en hulpverlening nauw samengewerkt.

is weinig discussie. Willens en wetens wordt er dan informatie uit de politiesystemen verkocht aan criminelen.

Veel moeilijker zijn de bevragingen met een onjuist doel. Iedereen die BVI-IB bevraagt, moet invullen wat de reden van de bevraging is: dagelijkse politietaak (artikel 8 Wpg) of onderzoek bepaald geval (artikel 9 Wpg) of opbouwen informatiepositie (artikel 10 Wpg). Ik ben ervan overtuigd dat dit zonder diep na te denken aangeklikt wordt, en dan veelal de eerste mogelijkheid. Net zoals dat je inlogt op je werkcomputer en de "default" mededeling ziet dat je in een politiesysteem komt en dat misbruik strafbaar is. Dat soort meldingen hebben na verloop van tijd geen impact meer.

Maar wat is nou de essentie van deze vraag? Zijn de jaarlijks vijftig miljoen bevragingen van BVI-IB allemaal geoorloofd? Voor mijn beoordeling zijn je politietaak en je ambtseed hierin steeds bepalend. Vraag ik deze informatie op om mijn werk goed te kunnen doen en gebruik ik het zoals het een goed politieambtenaar betaamt?'

Laten we daarbij eens een paar praktijkvoorbeelden aan je voorleggen. Voorbeeld 1: een collega die in de top 10 van bevragers staat, verklaart dat hij bij het invullen van zijn kerstkaarten altijd BVI-IB gebruikt om de postcode te vinden.

'Een interessante casus. Op zich benadeelt hij niemand, dus waarom niet. Maar wel een simpel antwoord: deze bevraging heeft niets met zijn werk te maken, en mag dus niet.'

Voorbeeld 2: een collega bevraagt de nieuwe vriend van zijn dochter.

'Die verleiding kan er natuurlijk zijn. Ook dit mag in principe niet omdat het niets met je werk te maken heeft. Maar er is wel een nuance. Door informatie van je dochter of van anderen kun je twijfelen aan de achtergrond van de nieuwe vriend. Als hij bijvoorbeeld deel uitmaakt van een criminele groepering, kan dat jouw werk gaan raken. Na overleg met je chef kan een bevraging dan wel degelijk toegestaan zijn. Zo zijn er meerdere privébevragingen te bedenken die in principe niet onder de politietaak vallen, maar door omstandigheden wel relevant kunnen worden. Overleg met de leidinggevende moet dan uitkomst bieden.'

Voorbeeld 3: collega's treffen een vrouw aan die dronken is. Ze regelen voor haar een taxi en geven aan de taxichauffeur haar adres door.

'Een complexer geval. Op zich ben je bezig met hulpverlening, en je doel is erger te voorkomen. Aan de andere kant geef je aan een taxichauffeur zonder toestemming privégegevens door. En wat nou als dat adres niet klopt en ze wordt afgezet bij haar ex-vriend tegen wie ze aangifte gedaan heeft? Meestal gaat het goed, maar willen we het risico lopen dat het fout gaat?'

Voorbeeld 4: de bevraging van een kenteken van een auto waar je achter rijdt, zonder dat de bestuurder van de auto iets fout gedaan heeft.

'Dat mag volgens de Wegenverkeerswet. Maar dit is ook erg interessant in het kader van de discussie rondom etnisch profileren, namelijk als deze bevraging kan helpen om de bestuurder van de auto niet te gaan controleren. Als we het zo kunnen regelen dat je kunt zien dat deze auto al gecontroleerd is en, door middel van een foto, dat de chauffeur dezelfde is, dan voorkomt dit het te vaak aan de kant zetten van eenzelfde auto en bestuurder.

Goed, je ziet wel dat het bij veel van dit soort kwesties niet altijd zwart of wit is, maar dat het vraagt om het systematisch beantwoorden van een aantal relevante vragen.'

Hoe controleren we het juiste gebruik?
'Hierbij zijn meerdere manieren mogelijk. Vanuit professioneel vakmanschap past het principe *high trust, high penalty* het best. Veel vertrouwen in de gebruiker, hem/haar daar ook goed over instrueren, maar bij misbruik fors straffen. Hetzelfde doen we immers bij het uitreiken van het dienstwapen.

Aan een goede instructie schort het nog weleens. Bij beëdigingen is het vaak een vast punt, maar daarna is het niet structureel ingebed om dit soort thema's op werkbijeenkomsten te bespreken. Medewerkers die onderwerp van onderzoek zijn klagen daarover. Goed gebruik van informatiesystemen en zorgvuldig gebruik van politiegegevens moeten vaste onderwerpen zijn van opleidingen, bijscholingen en werkoverleggen. We hebben met onze informatie goud in handen, maar privacyvoorvechters willen daaraan graag beperkingen opleggen. Wij zijn het zelf die moeten bewijzen dat we er zorgvuldig mee omgaan.'

Hoe zal dit alles zich volgens jou ontwikkelen?
'De mogelijkheden gaan toenemen, maar mogen we er ook meer gebruik van gaan maken? In 2016 was het programma *Hunted* op tv, waarin een zogenaamd rechercheteam mensen opspoort die zich "verstoppen". Aan het brede publiek wordt getoond hoe makkelijk het is om mensen te traceren door middel van telefoon, pingedrag of camerabeelden. Door deze al relatief oude technieken te laten zien wordt het Nederlandse publiek zich bewust van de eigen zichtbaarheid. Wat is hiervan de consequentie? Gaat de politiek dit omarmen en de mogelijkheden verruimen om mensen die zich niet aan de wet houden op te sporen? Of is tijdelijk de grens bereikt en worden de regels strenger?

Ik verwacht zelf het eerste. Het gebruik van de techniek en de informatie is onomkeerbaar en de mogelijkheden zullen gebruikt mogen worden. Veel minder vanaf de straat, maar veel meer vanuit boardrooms zullen we netwerken volgen en informatie koppelen.'

Dit brengt ons op een ander oud vraagstuk. Hoe betrouwbaar is onze informatie?
'Bij een toenemend gebruik van de informatie in onze systemen is het van essentieel belang dat deze ook klopt. Dat is een achilleshiel van onze organisatie, waar mensen werken die elke administratieve handeling al snel als een last ervaren. Het goed vastleggen van de juiste en volledige gegevens en het gebruik van bijvoorbeeld juiste metagegevens wordt de enige garantie naar onze toezichthouders dat het veelvuldig gebruik ervan gerechtvaardigd is!

En nogmaals, we staan nog maar aan het begin van een informatiegedreven samenleving. We ervaren het als normaal dat we via Google in milliseconden informatie van de hele wereld gepresenteerd krijgen. Dezelfde techniek wordt ontwikkeld voor de politiesystemen. Razendsnel kunnen we verbanden leggen tussen alle data over personen, locaties en gebeurtenissen. Niet onlogisch dus om je nu al af te vragen hoe misbruik voorkomen kan worden en professioneel gebruik van de bevoegdheid gestimuleerd kan worden.

Bij etnisch profileren werd gedacht aan stopformulieren die vanwege administratieve lastenverzwaring van de hand zijn gewezen. Maar het moment zal naderen dat logging van bevragingen gemeengoed gaat worden om achteraf verantwoording af te kunnen leggen over het correcte gebruik van de informatie uit onze immense mondiale databank! Dit blijkt ook uit de nieuwe Europese privacywetgeving – de algemene verordening gegevensbescherming – AVG – en de nieuwe Wpg, die beide vanaf 2018 van kracht zullen zijn.'

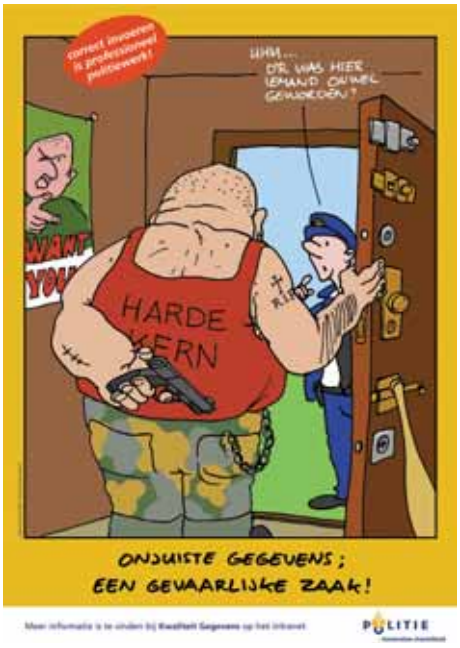
9 Waar kwaliteit toe leidt

Gerbrand Mijzen

9.1 Inleiding

In informatiegestuurd politiewerk (IGP), of welke informatiegestuurde organisatie dan ook, moet kwaliteit van gegevens voortdurend aandacht krijgen. We bekijken dan waar (gebrek aan) kwaliteit toe kan leiden, welke uiteenlopende kwaliteitsaspecten en -kenmerken er zijn en hoe we kwaliteit objectief kunnen maken. We beantwoorden de vraag wie nu eigenlijk bepaalt wat kwaliteit is. Ook gaan we in op de veranderende rol van gegevens voor de informatiegestuurde organisatie. Wordt kwaliteit nu gewoon weer (nog) iets belangrijker dan die al was, of is er meer aan de hand?

In informatiegestuurd politiewerk wordt een (groot) deel van het politioneel handelen gebaseerd op kennis, die uit informatie (en op haar beurt uit gegevens) wordt opgebouwd. Het is daarom belangrijk dat de politie zich om de kwaliteit van de informatie bekommert. Immers, hoe beter de informatie, hoe beter het handelen op basis daarvan kan zijn. Welke doelen bereiken we bij de politie met goede kwaliteit van informatie?



Figuur 9.1 Onjuiste gegevens

- Kwaliteit van informatie betekent veiligheid voor de collega's op straat. Weten wat voor pand je betreedt, welke mensen er mogelijk verblijven met wat voor antecedenten, maakt dat je je kunt voorbereiden op situaties en adequaat kunt handelen.
- Kwaliteit van informatie betekent effectief politieoptreden: informatie wijst ons op verdachte situaties, sporen en aanwijzingen. Zonder informatie werkt de politie in het donker en is een resultaat meer het resultaat van persoonlijke kennis en ervaring.
- Kwaliteit van informatie betekent ook effectiviteit van de politie in de keten. Het Openbaar Ministerie (OM) krijgt zaken alleen rond als de politiedossiers van goede kwaliteit zijn.

'Goede informatie is nodig om te weten waar iemand is, hoe het met hem is en of hij gevaarlijk is.'
– Michèle Blom, directeur-generaal Straffen en Beschermen, ministerie van Veiligheid en Justitie

---

Voorbeeld

Tijdens een surveillance krijgt een wagen een oproep voor een woninginbraak buiten heterdaad. Ter plaatse ontmoeten de twee politiemedewerkers van het basisteam de kennelijke bewoner, van wie zij de identiteit vaststellen op basis van de Wet op de identificatieplicht (WID), de persoon zelf en wat controlevragen. De politiemedewerkers stellen braaksporen vast en leggen dat samen met de vermoedelijke modus operandi (MO), in dit geval de kerntrekmethode[1], vast in een procesverbaal.
De politiemedewerker legt ook een signaal vast voor het team woninginbraak, omdat de kans op herhaling van deze MO in deze nieuwbouwwijk – met overal hetzelfde type slot op de voordeur – aanzienlijk is.

Wat valt hier op? Ten eerste, dat de politieman of -vrouw zich realiseert dat opsporing en handhaving eisen stelt aan de kwaliteit van de gegevens over bijvoorbeeld de aangever, diens identiteit en de vastgestelde feiten. Ten tweede, dat de politieman of -vrouw een link legt naar het thema woninginbraak, waarmee deze de gegevens ook waarde geeft voor het team woninginbraak. Informatiegestuurd politiewerk (IGP) vergt dus een constante focus op het politiewerk als geheel: besef dat gegevens ook waarde hebben na en naast de directe aanleiding waarvoor ze worden vastgelegd.

Als het belang van kwaliteit van informatie zo hoog is, kunnen we zeggen dat de gegevens kennelijk een essentieel bedrijfsmiddel (asset) zijn voor de organisatie. We zeggen ook wel: gegevens zijn de kern. De kwaliteit van de gegevens heeft de constante aandacht van

---

1 De kerntrekmethode is sinds een aantal jaren een populaire methode onder inbrekers. Een inbreker schroeft een zogenoemde 'trekschroef' in de cilinder op de plek waar men normaal de sleutel insteekt. Met een 'cilindertrekker' breekt de cilinder af en kan uit het slot getrokken worden. Hierna kan het slot van buitenaf eenvoudig opengedraaid worden met een universele bouwsleutel.

informatiegestuurd politiewerk, omdat de kwaliteit van de gegevens voorwaardelijk is voor de kwaliteit van het politiewerk zelf. Maar waaruit moet die zorg dan bestaan? Het is nodig dat informatiegestuurd politiewerk:

1 de *benodigde* kwaliteit van gegevens kent: verschillende doelen vereisen verschillende kwaliteit – kwaliteit is dus telkens maatwerk;
2 de *werkelijke* kwaliteit van gegevens kent – meten is weten om erachter te komen waar de kwaliteit voldoende is en waar niet;
3 de kwaliteit van gegevens en de processen waarin deze worden verwerkt continu *verbetert*; zoals we ook voortdurend investeren in mensen en in veiligheid;
4 zich bewust is van wat er fout gaat als de kwaliteit onvoldoende is, dus bewust risico's neemt of ze vermijdt.

Het begrip kwaliteit

Kwaliteit van informatie is dus van groot belang voor informatiegestuurd politiewerk. Maar wat is nu kwaliteit? Om kwaliteit te managen, is het nodig beter naar het begrip te kijken.

Ten eerste is er de definitie. Er zijn veel definities van kwaliteit in gebruik, die bijna allemaal het afnemerperspectief gemeenschappelijk hebben. Dit geldt ook voor de definitie van gegevenskwaliteit die bij de politie wordt gebruikt:

> 'Gegevenskwaliteit is de mate waarin politiegegevens in diverse bronsystemen voldoen aan de eisen en verwachtingen die behaald moeten worden om producten en diensten te kunnen realiseren die het dagelijkse politiewerk ondersteunen.'[2]

Deze definitie benadrukt dat kwaliteit de match is tussen verwachtingen van de afnemer of gebruiker of klant, en de realiteit. Kwaliteit is dus een relatieve maat (relatief aan de verwachting) en geen absolute. Daarnaast valt het klantperspectief op: gegevens zijn nooit in zichzelf van voldoende kwaliteit, maar alleen vanuit het perspectief van het doel – ondersteunen van politiewerk.

IGP zet hierin een stap verder; de producten en diensten vormen de informatie die sturend is voor het politiewerk. Dat verandert niet het 'klantperspectief' – immers we beoordelen nog steeds vanuit het doel. Het benadrukt wel het essentiële belang van goede gegevens voor de politie. Een beter bruikbare definitie is dan:

> 'Gegevenskwaliteit is de mate waarin politiegegevens voldoen aan de eisen en verwachtingen die behaald moeten worden om – door middel van producten en diensten – de intelligence op te bouwen die het dagelijks politiewerk aanstuurt.'

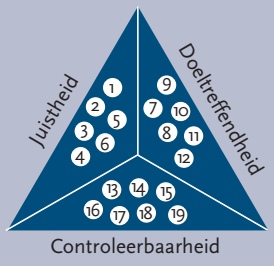
Tot zover de definitie van het begrip gegevenskwaliteit. Dan zijn er de kwaliteitsaspecten, ofwel die eisen en verwachtingen uit de definitie, waaraan moet zijn voldaan. Ook hierover

2 Visie op Kwaliteit. Business Intelligence Competency Center, Nationale Politie 2013.

zijn in de loop der tijd veel opvattingen ontstaan. We gaan hier uit van de kwaliteitskenmerken zoals die in de strafrechtketen worden gehanteerd.[3]

Raamwerk gegevenskwaliteit strafrechtketen

Dit raamwerk is opgesteld door het ministerie van Veiligheid en Justitie ten behoeve van de strafrechtketen en is ook bruikbaar in de vreemdelingenketen. Hierin is een aantal kaders, waaronder de Information Data Quality en de Dienst Justitiële Inrichtingen-variant van het *Datamanagement body of knowledge*-raamwerk, verenigd in een model dat bruikbaar is voor de strafrechtketen en als een checklist voor gegevenskwaliteit kan dienen. Gegevenskwaliteit wordt hier uitgesplitst naar drie hoofdaspecten: juistheid, doeltreffendheid en controleerbaarheid.



1 Correctheid
2 Referentiële integriteit
3 Volledigheid
4 Nauwkeurigheid
5 Aannemelijkheid
6 Validiteit
7 Relevantie
8 Universaliteit
9 Legaliteit
10 Beschikbaarheid
11 Tijdigheid
12 Actualiteit
13 Beheerbaarheid
14 Consistentie
15 Eenduidigheid
16 Uniciteit
17 Traceerbaarheid naar bron
18 Traceerbaarheid naar gebruiker
19 Exclusiviteit

Figuur 9.2 Raamwerk gegevenskwaliteit

De kenmerken die hieronder vallen, staan echter min of meer met elkaar op gespannen voet. Want tref je veel maatregelen ten behoeve van doeltreffendheid, dan zie je dat de juistheid afneemt. Tenzij je daar ook maatregelen voor neemt, maar dan daalt weer de controleerbaarheid enzovoort. Gegevens kunnen bijvoorbeeld niet helemaal (12) actueel en (10) beschikbaar zijn, en tegelijkertijd (1) correct (want controle kost tijd) en (19) exclusief (want dan is het niet meer openbaar). Je doet het kortom nooit goed: kwaliteit is een optimum – geen maximum – van kenmerken waar in bepaalde mate aan is voldaan.

Bij een aantal kenmerken van juistheid (correctheid, volledigheid, nauwkeurigheid enzovoort) moet niet uit het oog worden verloren dat deze in het kader van waarheidsvinding een tweede betekenis hebben. Is bijvoorbeeld een valse aangifte die netjes is opgetekend in de betekenis van dit raamwerk correct (want goed opgetekend) of niet (want moedwillig van valse informatie voorzien)? Is een gedeeltelijk signalement wel 'volledig' te noemen? Voor de eenvoud: de kwaliteitskenmerken in dit kader gaan over de kwaliteit van gegevens *zoals de politie die waarneemt*. Een gedeeltelijk signalement is dus 'volledig' als het volledig is overgenomen van de getuigenverklaring. Dat daarna een onderzoek start naar de werkelijke toedracht, doet aan de kwaliteit van de gegevensvastlegging niets af.

3 Ministerie van Veiligheid en Justitie, *Raamwerk gegevenskwaliteit strafrechtketen*. Ministerie van Veiligheid en Justitie, Den Haag 2016.

Sturen op kwaliteit

Het gaat dus om optimale kwaliteit en niet om maximale kwaliteit. Wanneer hebben gegevens dan de 'optimale' kwaliteit om te voldoen aan de eisen van intelligence? Wie spreekt die eisen uit? Bij het sturen op kwaliteit van gegevens is dat de gebruiker, ofwel de persoon die verantwoordelijk is voor het politiewerk dat met de *intelligence* wordt gestuurd.

Figuur 9.3 Wel scannen, niet typen

Voorbeeld: door administratieve fout verdacht van vuurwapenbezit[4]

De politie heeft vrijdagavond drie onschuldige personen aangehouden op de A16. Het drietal werd met getrokken pistolen gedwongen om op de grond te gaan liggen. Het bleek om een administratieve fout van de politie te gaan.
De politie scande de nummerplaten van auto's om te zien of er mensen over de A16 reden met openstaande boetes, gevangenisstraffen of betalingsachterstanden. Volgens het computersysteem werd de eigenaar van de auto gezocht en was hij vuurwapengevaarlijk. De snelweg werd afgezet en ter hoogte van Hendrik-Ido-Ambacht werd de automobilist gemaand om te stoppen. Onder dreiging van getrokken pistolen moest het drietal uitstappen en op de weg gaan liggen. Korte tijd later bleek het om een administratieve fout te gaan. Volgens de politie is er iets misgegaan bij de invoer van de nummerplaten. De politie heeft haar excuses aangeboden.

Hoe hoog mag het percentage fouten in de automatic number plate recognition (ANPR) liggen? Is 99 procent juistheid voldoende? Of 99,99 procent? Het antwoord op die vraag kan het best worden beantwoord door de collega die zijn werk door die informatie laat

4 http://www.rijnmond.nl/nieuws/113294/Door-administratieve-fout-verdacht-van-vuurwapenbezit.

sturen. De collega, de teamchef of wie dan ook die verantwoordelijk is voor het politiewerk dat volgt, beoordeelt ook welke (kwaliteit van) informatie nodig is.

Soms is het even zoeken naar de kwaliteitsverantwoordelijke binnen de politie. Omdat informatie wordt verrijkt, gedeeld, gecombineerd met andere gegevens voor diverse analyses en producten, zijn er achtereenvolgens meerdere personen die politiewerk met die informatie sturen.

Voorbeeld

In een aantal registratiesystemen zoals BasisVoorzieningen Handhaving (BVH) en Summ-IT is de tabel verzorgingsgebieden (VG) beschikbaar. Hierin zijn politieregio's opgedeeld in kleinere gebieden (VG's) ten behoeve van operationele sturing en intelligence. Basisteams hebben daarnaast ook de mogelijkheid zelf een eigen gebied te definiëren, als zij dat handig vinden voor registratie rondom bijvoorbeeld een straat of een gebouw.

Het Business Intelligence Competency Center (BICC) van Midden-Nederland gebruikt de VG-indeling voor het 'stapelen' van informatie voor diverse rapportages ten behoeve van opsporingsteams. Zij willen af van de eigen gebiedsindeling, zodat zij voortaan op wijkniveau rapportages kunnen opstellen die vergelijkbaar zijn met de cijfers van het Centraal Bureau voor de Statistiek (CBS), die op de VG-indeling gebaseerd zijn.

Wie is in dit voorbeeld nu de verantwoordelijke voor de gegevens? Het lijkt erop dat er twee eigenaren zijn: de politiechefs die de indeling gebruiken voor operationele sturing en business-intelligence-afdelingen die informatieproducten willen standaardiseren.

Soms zijn de wensen verenigbaar, soms moeten we voor meerdere doelen meerdere indelingen (referentietabellen) creëren, bij voorkeur zonder gegevens dubbel op te slaan. De verantwoordelijke moet in elk geval oog hebben voor de belangen van iedereen die de gegevens verder verwerkt. Ook moet hij oog hebben voor het belang van de persoon wiens gegevens het betreft, de betrokkene.

Kwaliteit in relatie tot privacy

De belangen van de betrokkenen zijn vastgelegd in privacywetgeving zoals de Wet politiegegevens (Wpg) en Wet bescherming persoonsgegevens (Wbp) (zie ook hoofdstuk 5 De Wpg). Deze wetgeving stelt eisen aan de mate waarin voldaan moet zijn aan kwaliteitskenmerken zoals toegankelijkheid, volledigheid en correctheid. Gegevensbescherming in het kader van informationele privacy wordt dus gedeeltelijk bereikt door op bepaalde kenmerken van gegevenskwaliteit te sturen. Er zijn ook privacyaspecten zoals grondslag, doelbinding, proportionaliteit en subsidiariteit die meestal tot de rechtsbeginselen worden gerekend en niet tot kenmerken van gegevenskwaliteit.

Gegevensbescherming is een belangrijk aandachtspunt bij informatiegestuurd werken, omdat de wet de voorwaarden stelt aan het inbreuk maken op de privacy door het verwerken van gegevens. Een van die voorwaarden is een duidelijke (helder omschreven) en concrete (naar een zaak toe leidende) grond voor het verwerken. Terwijl de doctrine van

IGP nu juist is dat we zuinig zijn op alle gegevens en deze ook verwerken (bewaren) in de hoop er in een later stadium gebruik van te kunnen maken, als een dergelijke verwerkingsgrond zich alsnog aandient.

In hoofdstuk 5 De Wpg is meer te lezen over de verwerkingsgronden in relatie tot informatiegestuurd politiewerk.

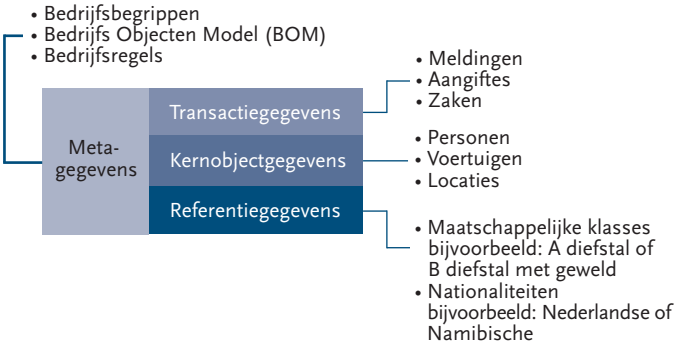
9.2 Welke dimensies heeft kwaliteit?

Kwaliteit is maatwerk

Kwaliteit van gegevens is dus een verzamelbegrip voor diverse kenmerken van kwaliteit. Welke kenmerken (op het gebied van juistheid, correctheid en doelmatigheid) in welke mate moeten worden vervuld, wordt bepaald door de persoon die verantwoordelijk is voor het politiewerk. Wat goed is voor een rechtszaak, is weer anders dan wat goed is voor een fenomeenanalyse, en wéér anders dan wat goed is voor hotspotanalyse. Het is bijvoorbeeld voorstelbaar dat informatie in de briefing voor een wijkteam vooral actueel, relevant en beschikbaar moet zijn. De politieman of -vrouw moet er zogezegd 'wat aan hebben', en het zal minder van belang zijn of de informatie in alle gevallen helemaal juist is. Liever een keer te veel gewaarschuwd voor een agressieve of verwarde persoon dan te weinig.

Kwaliteit van operationele gegevens, referentiegegevens en metagegevens

Gegevens worden geleverd door de operatie vóór de operatie: gegevens over zaken, aangiftes en ook over voertuigen, wapens, hotspots en hotshots. Er zitten ook gegevens in het systeem voordat de operatie ze gebruikt. Deze gegevens bepalen het 'gedrag' van het systeem en maken dat het te gebruiken is voor het politiewerk: als we een burgerservicenummer (BSN) in een systeem invoeren, krijgen we een naam en adres terug. Als we op een kleur willen zoeken (voertuig, kleding), krijgen we een lijst met van te voren gedefinieerde waardes. Wanneer we inloggen, is ergens vastgelegd wat ons wachtwoord is, wat we mogen in het systeem en wat niet, hoelang gegevens bewaard mogen blijven enzovoort. Ook deze gegevens 'onder de motorkap' hebben een bepaalde kwaliteit. En ook hier geldt weer: kwaliteit is maatwerk.



Figuur 9.4 Verschillende soorten gegevens

Voor referentiegegevens gelden andere eisen en andere accenten dan voor transactiegegevens. In het beleidsstuk *Verantwoordelijkheid van gegevens* wordt onderscheid gemaakt tussen verantwoordelijkheid voor beleid over gegevens en voor de inhoud van gegevens. De operatie is bijvoorbeeld wel verantwoordelijk voor het noteren van de juiste geweldsindicatie van een verdachte, maar niet voor de volledigheid van de tabel met alle geweldsindicaties.[5]

Tabel 9.1 Schematische weergave van soorten gegevens, kwaliteitsaspecten en verantwoordelijke

	Transactie-gegevens	Kernobject-gegevens	Referentie gegevens	Meta-gegevens
Definitie	Beschrijven het handelen	Beschrijven de objecten	Sorteren en categoriseren andere gegevens	Definiëren de betekenis en het gebruik van gegevens
Voorbeelden	Meldingen, aangiftes, zaken	Voertuigen, gebouwen, wapens, personen	Soort voertuig, kleur, maatschappelijke klasse	Definitie, datum van invoer, toegang
Belangrijkste kwaliteitsaspecten	Juistheid en Doeltreffendheid	Juistheid en Doeltreffendheid	Controleerbaarheid	Juistheid en Controleerbaarheid
				
Inhoudsverantwoordelijke voor gegevens	Operatie	Operatie	Informatiemanagement (IM)/gegevensgebruik en -beheer (GGB)	IM/gegevensgebruik en -beheer (GGB)
Beleidsverantwoordelijke voor gegevens	Portefeuillehouder namens de operatie	Portefeuillehouder namens de operatie	Directie Informatievoorziening (IV)/Gegevensautoriteit	Directie IV/ Gegevensautoriteit

Voorbeeld van de begrippen in de praktijk

Iemand doet aangifte van een diefstal. De aangifte is een 'transactie' en de gegevens vallen daarom in de categorie 'transactiegegevens'. De aangever, het object dat is gestolen, de verdachte enzovoort zijn kernobjecten en gegevens daarover dus 'kernobjectgegevens'. Bij het beschrijven van het signalement (zwart haar, sportschoenen, spijkerbroek) wordt gekozen uit een referentietabel met haarkleuren respectievelijk kleding. Dit zijn 'referentiegegevens'. Als de mutatie klaar is, hangt het systeem er automatisch een datum aan vast. Dat is een 'metagegeven'.

5 Beleid voor Verantwoordelijkheid voor Gegevens, Gegevensautoriteit (eind 2016).

Kwaliteit en structuur van gegevens

Een andere dimensie in gegevens is die van de mate waarin ze zijn geformaliseerd. Dit is de mate waarin gegevens voldoen aan een model, of zijn georganiseerd op een manier die we (van tevoren) kennen. Dus een lijst met inkomende en uitgaande telefoongesprekken is gestructureerd als we de telefoonnummers zelf, de duur van het gesprek, caller-ID enzovoort kunnen herkennen uit de cijfers en letters die op de lijst staan. Afbeeldingen zijn minder geformaliseerd, omdat we ze niet makkelijk (automatisch) kunnen sorteren, rubriceren enzovoort. We hebben wel (meta)gegevens óver afbeeldingen, zoals de datum waarop de foto is genomen en de resolutie, maar we kunnen de foto's niet op inhoud sorteren. Er is dus wel structuur, maar minder.

De geformaliseerdheid is belangrijk voor kwaliteit omdat we aspecten van kwaliteit baseren op de structuur die we erin zien. Van een gestructureerd gegeven als BSN of strafrechtketennummer (SKN) kunnen we vaststellen dat het beschikbaar is, valide, uniek, en correct verwijst naar de basisregistratie. Van een minder geformaliseerd gegeven als een geluidsopname kunnen we vaststellen dát het er is, maar niet of het relevant, correct, volledig is, of voldoet aan de wet. Hoe kunnen we toch de kwaliteit bewaken?

- Door minder geformaliseerde gegevens handmatig van kenmerken te voorzien, formaliseren we de gegevens alsnog en is een kwaliteitsbeoordeling ook makkelijker. Bijvoorbeeld foto's kunnen we handmatig laten beoordelen en sorteren op elk kwaliteitskenmerk dat we relevant achten. Daarna is het vaststellen van 'de' kwaliteit een kwestie van optellen.
- Gegevens die volledig ongeformaliseerd zijn, die zeer groot in omvang zijn en/of waar steeds nieuwe gegevens bijkomen, zijn veel lastiger handmatig te beoordelen. Bijvoorbeeld alle getapte telefoongesprekken in een bepaalde periode, alle foto's op harddisks die onderschept zijn in een netwerk. Dit soort gegevens beschouwen we als big data. Bigdata-analyse is de laatste jaren sterk in ontwikkeling en heeft geleid tot de eerste succesvolle toepassingen van (zelflerende) algoritmes. Deze herkennen bijvoorbeeld afbeeldingen van een mens automatisch door kennis van (heel) veel andere afbeeldingen van een mens. Dit algoritme herkent dus niet volgens een procedure die we er – met kennis van een of ander gegevensmodel – in hebben gestopt, maar op basis van overeenkomsten die het zelf heeft geleerd en herkend. Ondanks de succesvolle toepassingen staan bigdata-technieken zoals zelflerende algoritmes nog in de kinderschoenen. Als deze straks breder worden toegepast, schuift de grens van big data ook weer op. Gegevens die big data waren, kunnen dan worden herkend en gerubriceerd en gestructureerd. We kunnen dan ook de kwaliteitsaspecten vaststellen. Over big data is meer geschreven in hoofdstuk 20 Big data.

9.3 Wat is er al in werking om kwaliteit te borgen?

9.3.1 Organisatorisch

De verantwoordelijkheid voor kwaliteit van gegevens is op diverse plaatsen in de organisatie belegd. Vóór de vorming van de nationale politie was de regio als korps

eindverantwoordelijk. Kwaliteit was geregeld per korps en er werd dus per regio bepaald wie verantwoordelijk voor de gegevens was en wie controleerde. Er konden per regio daarom ook verschillen ontstaan. Met de vorming van de nationale politie is de eindverantwoordelijkheid voor kwaliteit van gegevens nationaal komen te liggen. Maar, niet in alle gevallen is controle ook echt ingericht. Borging van kwaliteit, vooral aan de invoerkant, is bij de operatie in de eenheden zelf belegd.

9.3.2 Procedures

Er zijn veel procedures in het politiewerk die de kwaliteit van gegevens borgen. Vaak hebben ze betrekking op de veiligheid en doelmatigheid van de taakuitvoering, soms op de rechtmatigheid van het handelen en veel minder vaak op het bevorderen van de juistheid van gegevens. We investeren dus vooral in doelmatig gebruik en controleerbaarheid en minder in juistheid. Procedures die we op dat vlak kennen zijn bijvoorbeeld:

- Procedure voor terugmelding van zaken vanuit het OM aan de politie. Dossiers die op vorm (bijvoorbeeld ontbreken van een SKN) of inhoud (bijvoorbeeld onvoldoende heldere omschrijving in het proces-verbaal) onvoldoende van kwaliteit zijn, worden retour gezonden naar de politie om te worden verbeterd. Dit leidt tot *double loop learning*: we leren het dossier beter op te maken en leren welke zaken verbetering behoeven om dossiers in het vervolg beter op te maken.
- Eind 2016 is er door informatiemanagement een leidraad ontwikkeld om de kwaliteit van begripsdefinities en bedrijfsregels te verbeteren. Dat is van belang voor de kwaliteit van kernregisters en tabellen met referentiegegevens. Begrippen als antecedent en moord krijgen daarmee een betere omschrijving en komen dus ook eenduidig terug in de rapportages en systemen. Ook de kwaliteit van de kennisregels in het kwaliteitssysteem TrueBlue kan hierdoor verbeteren, met weer betere kwaliteitscontroles tot gevolg.

9.3.3 Systemen

Systemen en koppelingen met referentiegegevens en kernregisters vormen de belangrijkste pijler onder gegevenskwaliteit. Veel registratieve systemen hebben ook eigen invoercontroles voor juistheid van het ingevoerde BSN, SKN of bijvoorbeeld IBAN (*international bank account number*). Ingevoerde gegevens die niet aan bepaalde kennisregels voldoen, worden met een toepassing als TrueBlue gesignaleerd. Bijvoorbeeld de invoer van rijbewijsgegevens van iemand die jonger is dan zeventien jaar.

Beschikbaarheid van systemen bepaalt natuurlijk ook de beschikbaarheid (als aspect van kwaliteit) van gegevens. Eisen aan beschikbaarheid worden vertaald in functionele eisen en overeenkomsten voor beheer (*service level agreements* – SLA's).

9.3.4 Kennis en cultuur

IGP kenmerkt ook een cultuuromslag in denken over de waarde van informatie voor de politie. Informatie is niet meer dienend aan het organisatiebelang maar ís het organisatiebelang. Kennis van het politiewerk alleen is niet meer voldoende; informatiekennis en vaardigheden op het gebied van privacywetgeving, bewaartermijnen, ketensamenwerking enzovoort zijn onmisbaar om de politietaken goed uit te kunnen voeren.

Voorbeeld

Collega's in de noodhulp krijgen 's avonds een oproep over een verward persoon, mogelijk suïcidaal op het Amstelstation in Amsterdam-Oost. De persoon wordt zittend op de trap naar het perron aangetroffen en is moeilijk aanspreekbaar. Ze heeft geen identificatiebewijs, noemt niet haar naam maar kan wel melden in welke straat ze woont. Een collega ziet via de BasisVoorziening Informatie voor Integrale Bevraging (BVI-IB) dat op dat adres een persoon woont die suïcidale klachten heeft. Hij noteert de naam en het BSN van deze persoon en geeft het op een briefje aan de ambulancemedewerkers mee, die zijn gearriveerd: 'Hier heb je vast een BSN', zegt de collega. De ambulance vertrekt met de persoon richting ziekenhuis.

De politieambtenaar moet kennis en ervaring van het politiewerk combineren met informatievaardigheden. Dat betekent in het hiervoor genoemde voorbeeld: begrijpen wat een geverifieerde identiteit betekent, welke controles je uit moet voeren voordat je een gegeven (BSN) doorgeeft aan een andere organisatie binnen of buiten de keten en wat de gevolgen kunnen zijn als dat niet gebeurt.

Als we deze kennis missen, opereren we als politie op een eiland in de strafrechtketen en in de maatschappij. Het huidige cultuuraspect zit er in, dat een collega met onvoldoende informatievaardigheden in de ogen van collega's nog steeds een professional is: iemand met veel ervaring in de opsporing en/of handhaving, iemand van wie je het werk kunt leren. Het is moeilijk te onderkennen dat veel kennis en ervaring in het politiewerk gepaard kunnen gaan met onvoldoende informatievaardigheden of informatiediscipline. Er zijn soms moed en 'oncollegiale' feedback nodig om elkaar scherp te houden hoe we met informatie omgaan. Dat is moeilijk omdat het politiewerk van oorsprong juist onvoorwaardelijke steun vereist. Fouten lossen we op, je collega val je niet af. De volgende keer is hij er voor jou. Reflectie, feedback, achteraf praten, zit velen (gelukkig?) niet in het bloed. Voor de informatiegestuurde organisatie hebben die cultuurwaarden wel een keerzijde als we ze toepassen in de manier waarop we met informatie omgaan. Dan is het juist nodig te bezinnen eer we beginnen; mag ik deze gegevens verstrekken, heb ik alles goed opgeschreven, zal ik het nog even laten lezen aan een collega? Stel ik hier nu aan de orde of dit wel mag wat we doen? Van de collega wordt in het informatietijdperk gevraagd dat hij schakelt tussen deze twee manieren van werken; solidair voor elkaar in acute situaties en kritisch reflecterend als het om de omgang met informatie gaat. Als een collega een dergelijke kritische houding aanneemt, dient hij te kunnen vertrouwen op onvoorwaardelijke steun van zijn leidinggevende. Dit is een belangrijke voorwaarde om met het hele korps succesvoller informatiegestuurd te kunnen werken.

9.4 Kwaliteit wordt aan de voorkant geregeld: dus als je invoert

Gegevens zijn een waardevol bezit, een asset geworden. Mensen zijn (het) waardevol(st), geld is waardevol, gegevens zijn ook waardevol – en ook nog eens waardevast. Gegevens

zorgvuldig verwerken, is een vorm van sparen. Het is een investering in tijd en aandacht die zich op een later moment uitbetaalt. Als collega in de keten betracht je die zorgvuldigheid zodat de collega's verderop in de keten er rendement van hebben. Dat doe je als je politiewerk verricht, of vanuit de ondersteunende diensten met gegevens van welke soort dan ook werkt. Kwaliteit van gegevens maken we samen. Wat kun je er zelf aan doen?

De politie geeft een op de vier aangiftes niet goed door aan Slachtofferhulp. Tienduizenden slachtoffers wachten daarom nog op hulp.[6] Dat meldt De Persdienst, de landelijke redactie van regionale kranten. De politie krijgt jaarlijks zo'n 225.000 aangiftes binnen van verschillende categorieën misdrijven. Afspraak is dat Slachtofferhulp al die aangiftes inclusief contactgegevens krijgt.
Maar dat gaat vaak mis. Er wordt vergeten aan te vinken of er een 'benadeelde partij' is. Daardoor komen er jaarlijks maar 195.000 aangiftes bij Slachtofferhulp binnen. Daarvan is in eerste instantie een kwart ook nog onbruikbaar, omdat gegevens niet kloppen. Uiteindelijk weten 180.000 slachtoffers hulp te krijgen.
De organisatie wil nu inzage in politiesystemen. De politie erkent in de krant dat het doorgeven van slachtoffergegevens niet optimaal verloopt.

Maak het belangrijk

Het werken met informatie is geen bijzaak meer, maar politiewerk zelf. Prioriteer het en waardeer het als manager, politiechef of coördinator. Maak er als collega werk van, op de volgende manier.

- *Koppel gegevens*
  Gegevens stijgen in waarde als ze gekoppeld zijn aan andere gegevens. Leg verbanden vast waar je die ziet of vermoedt dat ze er zijn. Vermeld referentienummers, leg een relatie naar een thema, een ander proces-verbaal, of een andere verdachte.
- *Deel gegevens*
  Gegevens zijn minder waard als ze alleen in jouw boekje staan. Deel gegevens, want voor een andere collega kan gedeelde informatie het ontbrekende puzzelstukje zijn. De Wpg vereist ook dat gegevens gedeeld worden.
- *Toets bij het doorgeven*
  Toets de kwaliteit nog een keer als je gegevens doorgeeft. Gegevens die zijn gecontroleerd, zijn meer waard. Als die extra controle even niet lukt, geef het dan zelf aan. Jouw collega weet dan de waarde van de gegevens en handelt daarnaar. Zo vergroot je de betrouwbaarheid van informatie in de keten.

6 http://www.rtlnieuws.nl/nieuws/binnenland/slachtoffers-de-kou-door-registratiefouten-politie (2015).

Voorbeeld

Voor het afgeven van Verklaringen Omtrent het Gedrag (VOG) is de Dienst Justis afhankelijk van de registratie van veroordelingen. Kwaliteit van de doorgegeven gegevens is op sommige punten echter onvoldoende structureel geborgd. Geschat is dat het handmatig navragen bij alle betrokken organisaties veel onnodige tijd vraagt.[7]

- *Koppel terug*
  Koppel de kwaliteit van gegevens terug aan de bron. Zo investeer je in de kwaliteit zelf en in de persoon/het systeem dat verantwoordelijk is voor die kwaliteit. Koppel ook eens terug als het wel goed is: 'Dankzij deze gegevens hebben we een goede analyse, aanhouding, inval... kunnen doen!' Van terugkoppeling worden we allemaal beter.

7 Uit: Werkgroep gegevenskwaliteit, *De strafrechtketen werkt met goede gegevens*. Ministerie van Veiligheid en Justitie, Den Haag 2016.

Deel III
De werking van IGP: het informatieproces

10 Informatiecoördinatie

Harold van Voornveld, Karin van Baarle en Bert Voerman

10.1 Inleiding

Dat we als politie beter informatiegestuurd moeten werken, is een adagium dat nog steeds van toepassing is. Er worden nog steeds beslissingen genomen op basis van halve informatie. Soms kan dat niet anders, maar niet altijd wordt de voor een beslissing noodzakelijke informatie gevraagd of afgewacht.

Informatiecoördinatie is het werkingsprincipe voor het gecontroleerd opbouwen van een informatiepositie. Informatiecoördinatie gaat over het monitoren van de wereld 'buiten' (incidenten, trends, veiligheidsthema's) met een proactief doel: tijdig signaleren en adequaat vertalen van informatie naar advies over interventies. Het is gericht op het sturen en uitvoeren van het politiewerk. Informatiecoördinatie betekent ook: de juiste informatie, op het juiste moment en op de juiste plaats krijgen. Essentieel daarvoor is afstemming binnen de informatieorganisatie en tussen de informatieorganisatie en de onderdelen in de operatie die informatie leveren en informatie gebruiken. De coördinatie van het opbouwen van informatieposities ligt bij de informatieorganisatie, maar het opbouwen van informatieposities is een gezamenlijke verantwoordelijkheid van de gehele organisatie: politie en partners. Zo kunnen bijvoorbeeld briefen en debriefen een belangrijke rol spelen bij het inwinnen van informatie, naast het open en heimelijk inwinnen door de informatieorganisatie (zie bijvoorbeeld ook hoofdstuk 14 Inwinning).

Informatiecoördinatie staat aan de basis van de hoofdtaken van de informatieorganisatie: beeldvorming en duiding, opwerken van signalen en ondersteunen van en participeren in de uitvoering van politiewerk. Goede informatieposities zijn daarvoor essentieel. Om die informatieposities in te kunnen nemen moet nagedacht zijn over de te kiezen informatiestrategie en de wijze van informatie-inwinning. De informatiestrategie betreft de wat-vraag van het onderwerp waarop een informatiepositie nodig is en de te behalen resultaten en effecten in de operatie. Informatie-inwinning gaat over de hoe-vraag: welke informatie is nodig om de vereiste informatiepositie in te nemen en hoe kan die verkregen worden? In de praktijk worden de stappen van informatiestrategie en -inwinning nog weleens overgeslagen. Dit leidt tot onduidelijkheden in het gehele informatieproces, omdat men bijvoorbeeld onvoldoende scherp heeft wat de bedoeling is en wie de verkregen informatie waarvoor gaat gebruiken.

Een gedegen intake van de opdracht en een concrete probleemomschrijving zijn noodzakelijk om de eigen organisatie te richten, maar vormen ook de basis voor samenwerking met partners. Politie-informatie is niet de enige bron voor informatiecoördinatie; informatie van zowel publieke als private partners is een niet te verwaarlozen onderdeel in het proces, zie ook hoofdstuk 13 Informatiegestuurd werken en samenwerkingsrelaties. Een

integrale aanpak van een probleem begint bij een gezamenlijke probleemanalyse. Daarnaast maakt in steeds meer zaken internationale informatie-uitwisseling onderdeel uit van succesvolle informatiecoördinatie. Informatie van partners, nationaal en internationaal, is nodig voor de effectieve aanpak van onze veiligheidsproblemen.

Op basis van een goede informatiepositie kunnen de noodzakelijke of gewenste producten gemaakt worden. De informatiebehoefte van de gebruiker van de informatie staat daarbij centraal: voor wie is de informatie bedoeld, waar heeft deze de informatie voor nodig, wat wil deze er mee doen? Met dezelfde informatiepositie kunnen verschillende producten worden gemaakt: bijvoorbeeld periodieke situatierapporten (sitraps), briefings of overzichten van hot times, hotshots en hotspots. En hoewel daar overlap tussen zit, speelt ook mee dat op basis van een en dezelfde informatiepositie verschillende groepen bediend kunnen worden:

- operationeel: straatinformatie in de actualiteit voor noodhulp, toezicht/handhaving, bewaken/beveiligen en ten behoeve van interventies;
- tactisch: zaaksinformatie voor lopende rechercheonderzoeken en thematisch overzicht/inzicht;
- strategisch: sturingsinformatie voor lijnchefs over incidenten of thema's.

Een informatiepositie op outlaw motor gangs (OMG's) bijvoorbeeld kan gebruikt worden voor alle drie genoemde groepen, mits bij het opstellen van de informatiestrategie en -inwinning daarmee nadrukkelijk vooraf rekening gehouden is.

Informatiecoördinatie heeft tevens een vaste plek verworven in gevestigde structuren als de Teams Grootschalige Opsporing (TGO's) en de (Nationale) Staven Grootschalig Bijzonder Optreden (NSGBO's en SGBO's). Binnen deze samenwerkingsvormen zijn vaste informatiecoördinatierollen ingericht. De functie van informatiecoördinatie is hetzelfde: beeldvorming, duiding en advisering op basis van verzamelde, gecombineerde en geanalyseerde informatie met het doel om gecoördineerde en geverifieerde informatie en een eventueel advies tijdig bij de juiste medewerkers en beslissers te brengen. De inrichting van het werk verschilt tussen TGO en (N)SGBO. Hiervoor vinden dan ook aparte opleiding en training plaats.

10.2 Sturen op informatie om te kunnen sturen met informatie

De kern van informatiegestuurd werken is de beschikbaarheid van de juiste informatie, op de juiste plaats, op het juiste moment om goed te kunnen beslissen in het politiewerk. Om dat te bereiken moet ook gestuurd worden op het informatieproces, in casu op het hebben van de noodzakelijke informatieposities. Bij informatiecoördinatie in de actualiteit lijkt dat – op het moment dat de situatie of het incident zich voordoet - lastiger dan bij thematische informatiecoördinatie. Informatiecoördinatie in de actualiteit gaat over het (ad hoc) inwinnen van situationele informatie en de directe duiding daarvan aan de hand van bekende beelden. Thematische informatiecoördinatie kan, omdat er meer tijd beschikbaar is, gedegen worden voorbereid en uitgevoerd aan de hand van bijvoorbeeld de keuzes die gemaakt zijn in het nationale of regionale beleid. De operationele prioriteiten worden opgenomen

in de intelligenceagenda van de eenheden en vertaald naar het aanbod van de informatieorganisatie, de in te nemen informatiepositie. Dan is er tijd om de informatiestrategie en -inwinning te bepalen, af te stemmen en uit te voeren. De volgende paragrafen beschrijven beide vormen van informatiecoördinatie in meer detail.

Voordat er met informatie gestuurd kan worden, moet de informatiepositie idealiter dus eerst opgebouwd zijn. Zowel bij informatiecoördinatie in de actualiteit als bij thematische informatiecoördinatie is de wisselwerking tussen de informatieorganisatie en de andere collega's en partners in de operatie cruciaal. Zonder informatie over een incident of zonder vastgelegde rest- en zijtakinformatie uit een rechercheonderzoek kan geen goede informatiepositie worden opgebouwd. De kost gaat voor de baat uit, oftewel: we moeten eerst op de informatie-inwinning sturen om vervolgens de informatie te kunnen gebruiken.

Sitraps kunnen gebruikt worden bij het sturen op en het sturen met informatie. Primair geven sitraps periodiek de situatie over een incident of thema weer op basis van de opgebouwde informatiepositie. Ook kan worden aangegeven welke informatie (algemeen of specifiek) nog nodig is om de informatiepositie te verbeteren. Dit kan ook in de briefing worden meegegeven.

10.3 Informatiecoördinatie in de actualiteit

Informatiegestuurd werken is bij de afhandeling van incidenten van groot belang. De informatie die voorhanden is - voor zowel de uitvoerende politiemedewerker als voor degene die stuurt op de operatie - bepaalt mede hoe effectief het politieoptreden bij incidenten en crises is. Informatie biedt niet alleen inhoudelijke context bij wat je ter plaatse aantreft, maar draagt ook bij aan een veilige afhandeling. Beide elementen zijn van invloed op het handelingsperspectief van de politiemedewerker.

Informatiecoördinatie in de actualiteit is het voorzien van beslissers en uitvoerders van actuele, geverifieerde, op de situatie toegesneden informatie op basis van wat er nú gebeurt. Omdat incidenten en crises zich op elk moment kunnen voordoen, is voor deze vorm van informatiecoördinatie dan ook een 24-uursvoorziening beschikbaar: het Real-Time Intelligence Center (RTIC) met de sturende rol van de officier van dienst-informatie (OvD-I).

Het RTIC

Het RTIC is een belangrijke component van de real-time-intelligencefunctie, zoals deze beschreven wordt in hoofdstuk 19 Real-time intelligence (RTI). Het RTIC als onderdeel van de informatieorganisatie is in elke eenheid 24/7 operationeel gekoppeld aan het Operationeel Centrum. Het RTIC veredelt informatie rond spoedeisende meldingen (streeftijd binnen 0-5 minuten). Deze informatie wordt meegegeven aan de eenheid die ter plaatse gaat of al ter plaatse is. Voor grotere incidenten breidt deze dienstverlening zich

uit tot het gouden uur (het eerste uur nadat een incident zich heeft voorgedaan), waarin relevante informatie veredeld en geduid wordt voor zowel de uitvoerder op straat als degene die beslist over de operatie. De OvD-I stuurt het actuele informatieproces.

OvD-I

De OvD-I is een medewerkersrol die gedurende een dienst vanuit de informatieorganisatie voor de gehele eenheid wordt uitgevoerd. De OvD-I voorziet de andere operationeel verantwoordelijke rollen van contextinformatie en advies voor de aanpak van het incident of de crisis.[1] De OvD-I is in de actualiteit ook het aanspreekpunt voor de leidinggevenden van de diensten en districten binnen de eenheid.

De OvD-I kan capaciteit van alle informatieafdelingen regionaal of landelijk bijschakelen (opschalen) en deelt waar nodig informatie met de OvD-I van andere eenheden. Zo vormen de elf OvD-I'en met elkaar een nationaal netwerk en de link naar internationaal: bij sommige incidenten (terrorisme en kinderontvoeringen) kan directe informatiedeling met het buitenland cruciaal zijn.

Overdracht en opschaling

Ook na het gouden uur blijft coördinatie op het informatieproces van belang. Afhankelijk van de situatie zal de aanpak van het incident in opgeschaalde vorm (TGO of SGBO) kunnen worden voortgezet.

Figuur 10.1 TGO

Maar ook als niet voor deze opschaling wordt gekozen, is het informatieproces nog niet ten einde. Om de RTIC-capaciteit weer beschikbaar te maken voor het reguliere werk of nieuwe incidenten zorgt de OvD-I voor overdracht naar de reguliere lijn: informatiecoördinatoren binnen de informatieknooppunten, of indien van toepassing binnen al

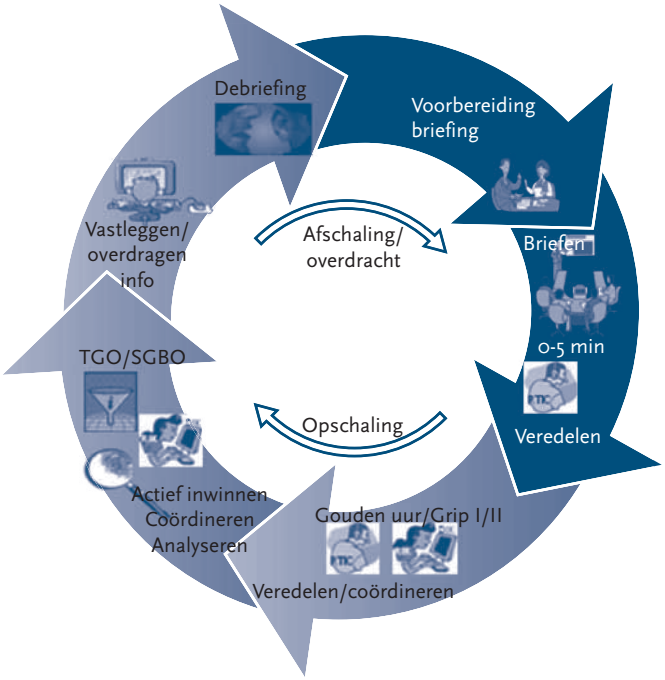
1 Dit zijn de officier van dienst voor de recherche (OvD-R), die voor het operationeel centrum en de hoofdofficier van dienst (HOvD).

bestaande structuren, zoals informatiecellen contraterrorisme, extremisme en radicalisering (CTER) en OMG's.

De overdracht door de OvD-I valt samen met de overdracht van de operationele behandeling van het incident door de hoofdofficier van dienst (HOvD) aan de reguliere lijn (bijvoorbeeld een opsporingsteam of afhandelunit) of tijdelijke hulpstructuur (TGO of SGBO).

In voorkomende gevallen zal de OvD-I een debriefing organiseren, waarmee belangrijke informatie beschikbaar komt voor collega's die de opvolging ter hand nemen en voor de briefing van volgende dienstverbanden.

Het gehele verloop informatiecoördinatie in de actualiteit – van eerste incidentmelding, gouden uur, opschaling en afschaling, tot overdracht – staat in figuur 10.2.



Figuur 10.2 Informatiecoördinatie in de actualiteit bij op- en afschaling

Signaleringsfunctie: proactief delen

De informatieorganisatie vervult een permanente radarfunctie op veiligheidsontwikkelingen. Deze signaleringsfunctie vereist dat afwijkingen van het normale patroon (bijzondere incidenten, trends en fenomenen) actief worden gedeeld binnen de eenheid en tussen de eenheden. Elk thema is ooit zo begonnen, dus 'is geen geprioriteerd thema' is geen reden om iets terzijde te schuiven. Via rapportage aan het informatieknooppunt landelijke eenheid wordt detectie van nieuwe, eenheidsoverstijgende, veiligheidsproblemen mogelijk. Afstemming hierover binnen de politie en met gezag en partners kan leiden tot verdere informatiecoördinatie op basis waarvan besluiten genomen kunnen worden.

10.4 Thematische informatiecoördinatie

Dit betreft het proces van het opbouwen van informatieposities op veiligheidsthema's die binnen de politie geprioriteerd zijn. Deze informatieposities vormen de basis voor specifieke informatieproducten die overzicht, inzicht en vooruitzicht bieden om de politie of partners in staat te stellen de juiste operationele, tactische en strategische keuzes te maken voor het effectief beïnvloeden van de veiligheid. Thema's kunnen ontstaan uit een enkel (groot) incident (bijvoorbeeld spanningen tussen Turken in Nederland na een coup-poging in Turkije), maar meestal uit een trend, een reeks gebeurtenissen die wijzen op een groeiend belang van het thema voor de veiligheid. Dergelijke thema's kunnen het karakter van doelgroepen hebben, maar ook van bredere fenomenen. Bekende thema's in de afgelopen jaren zijn CTER, OMG's, *high impact crime* (woninginbraken, overvallen, ram- en plofkraken), ondermijning, vuurwapens, asielstromen & mensensmokkel en mobiel banditisme.

Thema's die voorzienbaar het hele jaar worden gevolgd door de politie, staan in de intelligenceagenda. Dat geldt bijvoorbeeld voor de thema's waarover de politie internationale afspraken maakt, zoals die in EU-verband binnen het EMPACT-programma (European multidisciplinary platform against criminal threats). Ook vanuit portefeuilles zoals ondermijning en cybercrime worden thema's toegevoegd. Op regionaal niveau kunnen gebiedsscans en de evenementenkalender leiden tot extra thema's. Daarnaast vereist de actualiteit soms het volgen van nieuwe thema's. Nationale vragen vanuit het ministerie of portefeuillehouders (politiechefs) kunnen leiden tot tussentijdse herprioritering in de te volgen thema's. Ditzelfde kan binnen een regionale eenheid gebeuren.

Figuur 10.3 Politietoezicht bij voetbalwedstrijd

Sturing op thematische informatiecoördinatie

Sturen op en met informatie is een belangrijke basisfunctie in de informatieorganisatie. De capaciteit van de informatieorganisatie is beperkt, dus het is nodig om scherp te kiezen

waarop de capaciteit wordt ingezet. Thematische informatiecoördinatie vraagt toegewezen capaciteit gedurende langere tijd (maanden tot jaren). Dat impliceert dat beslissingen hierover door de leiding van de informatieorganisatie worden genomen in samenspraak met het bevoegd gezag. Vooral hier geldt dat de informatiestrategie (wat-vraag) helder moet zijn: zonder duidelijke (beleids)doelstellingen op het thema is het lastig te bepalen welke informatieposities met welke diepgang op te bouwen.

De intensiteit waarmee thema's gevolgd worden, kan in de loop van de tijd verschillen: sommige thema's worden gemonitord, sommige thema's worden zeer actief gevolgd, waarbij ook actief informatie ingewonnen wordt, bijvoorbeeld via heimelijke inwinning door de teams criminele inlichtingen en openbare-orde-inlichtingen (zie hoofdstuk 14 Inwinning). Voor sommige thema's is het houden van overzicht voldoende, bij andere thema's is daarnaast inzicht gewenst, wat meer inspanning vergt. Op basis van de actualiteit, de ervaren lacunes in de informatiepositie (witte vlekken en *dark numbers*[2]) en soms ook de beschikbare capaciteit beslist de leiding van de informatieorganisatie of geïntensiveerd of juist afgeschaald wordt. Hiermee wordt dus ook gestuurd over de verschillende thema's heen.

Intelligenceagenda

Voor thema's en onderwerpen die geprioriteerd zijn, staat in de intelligenceagenda wat de informatieorganisatie doet op het betreffende thema. De intelligenceagenda wordt jaarlijks vastgesteld door het bevoegd gezag en is daarom de leidraad voor de informatieorganisatie voor zover het deze thema's betreft. Daar zit vooral het verschil met de informatiecoördinatie in de actualiteit; die is veelal niet te voorzien.

De intelligenceagenda's van de elf eenheden en de nationale intelligenceagenda zijn nauw met elkaar verbonden: voor veel onderwerpen worden nationale informatiebeelden gemaakt, waarbij de bijdragen van de eenheden daaraan in de intelligenceagenda's van de eenheden worden afgesproken. Voorbeelden hiervan zijn het Nationaal Ondermijningsbeeld, het Nationaal Dreigingsbeeld en de Nederlandse bijdrage aan internationale informatieproducten, zoals de SOCTA (Serious and Organised Crime Threat Assessment) en de bijdragen aan EMPACT-thema's. Zo draagt de intelligenceagenda niet alleen bij aan thematische informatiecoördinatie, maar ook aan landelijke informatiecoördinatie.

Uitvoering thematische informatiecoördinatie

Als de wat- en waartoe-vraag helder zijn, moet ten behoeve van de uitvoering de hoe-vraag beantwoord worden. Dit gebeurt in samenwerking tussen leiding (teamchefs), coördinatoren en experts van de informatieorganisatie. Het gaat hierbij om vragen als:

- Welke inwinstrategie (bijvoorbeeld inwinplannen) hanteren we?
- Welke (nieuwe) bronnen willen we ontsluiten voor dit thema?
- Welke partners moeten we betrekken?
- Welke andere onderdelen binnen de politie laten we gericht informatie inwinnen?
- Gaan we ook via heimelijke inwinning investeren op dit thema?

2 Een deel van de criminaliteit wordt, om verschillende redenen, niet gemeld of niet geregistreerd. Dit deel wordt geduid met de term dark number.

- Welke capaciteit en middelen moeten we inzetten?
- Hoe organiseren we dat intern, hoe en waar leggen we de informatie vast?

Thematische informatiecoördinatie is in principe een reguliere activiteit, die onder operationele aansturing van coördinatoren binnen de informatieknooppunten van de regionale en landelijke informatieorganisaties belegd kan worden. Situatieafhankelijk kan ook worden gekozen voor inrichting van een tijdelijke infocel en/of het benoemen van een themacoördinator.

Landelijke informatiecoördinatie

Voor veel thema's geldt dat enkel het opbouwen van informatieposities binnen de eenheid niet volstaat. Het opbouwen van landelijke veiligheidsbeelden op thema's vereist horizontale en verticale samenwerking bij het opbouwen van de informatieposities: tussen de regionale eenheden, tussen het regionale en het nationale niveau en soms ook in samenwerking met partners zoals bijzondere opsporingsdiensten, Koninklijke Marechaussee (KMar), onderzoeksinstellingen en zusterdiensten in het buitenland of het bedrijfsleven.

Daartoe worden binnen de politie afspraken gemaakt over de bijdragen van alle eenheden om tot landelijke beelden te komen, zoals dat bijvoorbeeld voor het Nationaal Dreigingsbeeld en het Nationaal Ondermijningsbeeld al enkele jaren gebeurt. We spreken in dat geval over landelijke informatiecoördinatie. De hierna geschetste werkingsafspraken zijn in ontwikkeling en worden in de praktijk beproefd en eventueel bijgeslepen.

De elf diensten informatieorganisatie van de politie werken als één informatieorganisatie, waardoor het mogelijk wordt om de regie op de informatiecoördinatie op thema's over de elf diensthoofden te verdelen, veelal in lijn met de portefeuilleverdeling over de elf politiechefs. Het regisserende diensthoofd is, samen met de teamchefs, verantwoordelijk voor het tot stand komen van de informatiestrategie en de inwinstrategie, zoals hiervoor omschreven. Dat begint met het aanbodgesprek met de landelijk portefeuillehouder om de beleidsdoelen operationeel te vertalen naar de informatiebehoeften. Daarna moet een passende inwinstrategie worden bepaald, in afstemming met alle eenheden. De beschikbare expertise, bronnen en capaciteit van de verschillende disciplines in de informatieorganisatie (zoals business intelligence (BI) en analyse) zijn hiervoor medebepalend. Door de BI-discipline al aan de voorkant te betrekken, kan maximaal gebruikgemaakt worden van de mogelijkheden die BI biedt en kan voorkomen worden dat energie verspild wordt aan handmatige dataverzameling en -bewerking. De concrete vertaling naar geoperationaliseerde vraagstellingen, informatieproducten, werkverdeling en tijdlijnen wordt vastgelegd in een landelijk inwinplan voor het betreffende thema, dat vervolgens – na vaststelling – wordt uitgevoerd.

Het regisserende diensthoofd is verantwoordelijk voor de totstandkoming en oplevering van de landelijke beelden door de informatieorganisatie als geheel, de evaluatie met de portefeuillehouder en het proces van bijstellen van landelijke informatiecoördinatie. Beslissingen tot opschaling of juist beëindiging van landelijke informatiecoördinatie zal hij samen met de collega-diensthoofden in gezamenlijkheid nemen.

De inrichting van de uitvoering van het afgesproken werk is aan de eenheden zelf en is ook afhankelijk van welke bijdrage gevraagd wordt; die hoeft niet voor alle elf eenheden gelijk te zijn. Wel is minimaal één aanspreekpunt per eenheid noodzakelijk om goed te kunnen sturen op landelijke informatiecoördinatie.

Om te zorgen dat de informatieposities en -producten van lokaal en regionaal niveau stapelbaar zijn naar het landelijke niveau worden gezamenlijke afspraken gemaakt over onder meer (data)definities, wijze van vastleggen en tooling. Dat is overigens van belang voor alle thema's, ook die waarvoor geen landelijke informatiecoördinatie wordt gevoerd.

11 Analyse

Ronald Reijneveld

Het analyseren van politiële informatie is sinds lange tijd onderdeel van het politiewerk. Zo heeft een aantal ontwikkelingen en programma's in de jaren tachtig en negentig erin geresulteerd dat korpsen zogenoemde bureaus misdaadanalyse inrichtten. Het afgelopen decennium hebben twee programma's in belangrijke mate bepaald wat de taak en het werk van analyse zijn binnen het intelligenceproces. Dit is het Programma Versterking Opsporing en Vervolging (PVOV) en het Programma Intelligence. PVOV richtte zich op de verbetering van, onder andere, de rol van analyse binnen rechercheonderzoeken. Het Programma Intelligence concentreerde zich op de bijdrage van analyse aan de sturing op veiligheidsvraagstukken.

Waar het voorheen, vooral binnen kleine korpsen, lastig was om aan beide taakgebieden een goede en permanente invulling te geven (een nieuw TGO-onderzoek – Team Grootschalige Opsporing – resulteerde in het on hold zetten van veiligheidsanalyses), heeft de reorganisatie tot de nationale politie er in geresulteerd dat elke eenheid een afdeling Analyse & Onderzoek heeft ingericht binnen de Dienst Regionale Informatieorganisatie (DRIO) en de Dienst Landelijke Informatieorganisatie (DLIO). Elke afdeling heeft de taakstelling zowel zaaksanalyses als veiligheidsanalyses uit te voeren. De samenvoeging van 26 bureaus analyse tot elf afdelingen Analyse & Onderzoek heeft de formatieve ruimte geboden om beide taakgebieden in alle eenheden permanent beschikbaar te hebben.

In de volgende paragrafen worden beide vormen van analyse nader beschreven. Daarbij gaan we vooral in op dat wat de analyses behelzen en waartoe ze dienen. Het analyseproces, de stappen die je moet zetten om zo'n analyse dan te maken, beschrijven we in de derde paragraaf. Dit hoofdstuk wordt afgesloten met een bespiegeling over toekomstige ontwikkelingen binnen het analysevak.

11.1 Zaaksanalyse: analyseren en adviseren binnen onderzoeken

Het vak van zaaksanalyse richt zich op de ondersteuning van de uitvoering van de operationele politietaak. Dit type analysevraagstukken heeft betrekking op het ondersteunen van onderzoeken die zich primair richten op:

- het vermoeden dan wel een concrete aanwijzing van strafbaar handelen, onderzocht onder verantwoordelijkheid van een leider onderzoek en het Openbaar Ministerie (OM);
- persoonsgerichte benadering (subject of groepering);
- via overwegend strafrechtelijke waarheidsvinding het aanhouden van mogelijke verdachte(n) dan wel het doen stoppen van het strafbaar handelen.

Zaaksanalisten worden vaak ingezet bij de uitvoering van rechercheonderzoeken. Deze vorm van analyse is echter tevens van waarde in andere contexten waarbij waarheidsvinding een belangrijke onderzoeksdoelstelling is. Zo wordt zaaksanalyse ook ingezet in de informatieorganisatie ten behoeve van intelligencebeelden of bij de uitvoering van integriteitsonderzoeken.

Er zijn twee vormen van zaaksanalyse: operationele zaaksanalyse en tactische zaaksanalyse. Operationele zaaksanalyse richt zich op het structureren en analyseren van de beschikbare zaaksinformatie op basis van, met name, de leidende onderzoeksrichting. Tactische zaaksanalyse richt zich, vanuit een brede oriëntatie op het gehele onderzoek, op het ontwikkelen van hypothesen en scenario's die leiden tot het identificeren van alternatieve kansrijke onderzoeksrichtingen.

11.1.1 Operationele zaaksanalyse

De operationeel zaaksanalist is verantwoordelijk voor het analyseren en interpreteren van de verkregen onderzoeksinformatie. De kracht van operationele zaaksanalyse schuilt in het combineren van deze informatie. Belangrijke analyseproducten zijn onder andere relatieschema's (wie kent wie?), tijdlijnen (wat is wanneer gebeurd?) en telecomanalyses (wie heeft met wie contact?). Het combineren van beschikbare opsporingsinformatie kan tot nieuwe inzichten leiden in relatie tot de kennis zoals deze binnen het onderzoeksteam bekend is. Zo kunnen verklaringen geverifieerd of gefalsificeerd worden.

Effe checken

Ergens in Nederland heeft een ernstige woningoverval plaatsgevonden door twee overvallers. Tijdens de overval zijn bewoners gekneveld en is gedreigd met geweld. De districtsrecherche start hierop een onderzoek en een operationeel zaaksanalist wordt aan het team toegevoegd.

De eerste vraag aan de analist is om een tijdlijn van gebeurtenissen op te stellen. Tegelijkertijd komen via verklaringen van de slachtoffers twee verdachten in beeld. De verdachten zijn bekenden van de politie en we weten dus hoe ze te werk gaan. Er is veel informatie over ze bekend en de analist maakt op basis hiervan een relatieschema van de verdachten en hun criminele contacten.

De twee verdachten worden al snel aangehouden en geconfronteerd met de verklaringen. Een van de verdachten begint deels te verklaren en geeft aan dat er een derde persoon bij betrokken was. Deze persoon is niet in de woning geweest, maar stond buiten op de uitkijk.

Deze persoon was al door het rechercheteam aangemerkt als interessante persoon aangezien deze vanuit het relatieschema van de analist nadrukkelijk naar boven kwam vanwege zijn antecedenten en de relatie met de andere twee verdachten bij dit soort strafbare feiten. Hierop wordt deze persoon gehoord. Hij ontkent echter elke betrokkenheid en verklaart op dat tijdstip ergens anders te zijn geweest. Om deze persoon aan het praten te krijgen en als verdachte aan te merken, is er meer nodig. >>

>> Hierop gaat de analist aan de slag om te bekijken of de onderzoeksinformatie tot een andere conclusie zou kunnen leiden. Een belangrijke bron is in zo'n situatie de telecominformatie. Aangezien het telefoonnummer van de verdachte bekend is, kan informatie behorend bij dit nummer gekoppeld worden aan de tijdlijn van de gebeurtenissen. De analist onderzoekt of de telefoon van de derde verdachte rondom het tijdstip van de overval de dichtstbijzijnde zendmast heeft aangestraald. Het blijkt dat dit nummer ongeveer een minuut heeft aangestraald op de betreffende mast.
De verdachte wordt wederom uitgenodigd op het bureau en met deze informatie geconfronteerd. Op basis hiervan breekt de verdachte en begint te verklaren. Hij verklaart dat hij zijn telefoon uit had staan en dat dit ook een afspraak was tussen de drie verdachten, omdat ze wisten dat dit uitgepeild kon worden. Hij verveelde zich echter terwijl hij op de uitkijk stond dus hij heeft even zijn telefoon aangedaan om te checken of hij nog voicemailberichten had.

11.1.2 Tactische zaaksanalyse

Het Programma Versterking Opsporing en Vervolging (2006-2010) heeft het vakgebied van tactische criminaliteitsanalyse vormgegeven. Bij de evaluatie (2005) van de Schiedammer parkmoord (2000) is gekeken naar de rol die analyse had binnen het onderzoek en welke vooral ook niet. Zo deed de onderzoekscommissie-Posthumus onder andere de volgende bevindingen:

'Juist het hoge emotionele gehalte van deze zaak kan gemakkelijk leiden tot al te simplistische verklaringen voor de onterechte veroordeling van Kees B.' (p. 167)

'Niemand heeft voorgesteld of opdracht gegeven om een koppel rechercheurs of de analisten te belasten met de taak de hypothese dat Kees B. de dader was te ontkrachten of om een overzicht van zwakke punten te maken. (...) Er is geen opdracht gegeven overige onderzoeksrichtingen goed in kaart te brengen.' (p. 26)

'De analisten hebben geen presentatie hoeven te geven aan het team of teamleiding van de stand van zaken op een bepaald moment in het onderzoek.' (p. 74)

Deze constateringen hebben ertoe geleid dat het vak van tactische zaaksanalist binnen het Programma Versterking Opsporing en Vervolging geformaliseerd is, inclusief het vaststellen van de benodigde opleidingseisen. In de Regeling Team Grootschalige Opsporing is vastgelegd dat een tactisch zaaksanalist een recherchekundige is.

Tactische zaaksanalyse richt zich op het aan de hand van hypothesen en scenario's in- en uitsluiten van alternatieve onderzoeksrichtingen. Hypothesen en scenario's dragen bij aan een voortdurende kritische reflectie van het hele onderzoeksteam op de gekozen onderzoeksrichting. De tactisch analist is verantwoordelijk voor het opstellen en

permanent actualiseren van hypothesen en scenario's. Een hypothese gaat in op de watvraag. Een scenario verdiept de hypothese door middel van het beantwoorden van de hoevraag.

De klusjesman

Ergens in Nederland.
In haar woning wordt een bejaarde vrouw vastgebonden en nagenoeg naakt aangetroffen. Het was bekend dat het slachtoffer zeer vermogend was en dat zij geld in huis bewaarde. Ze was niet aanspreekbaar en werd met spoed naar het ziekenhuis vervoerd. Het slachtoffer heeft nadien niet meer gesproken en is uiteindelijk overleden. Voor deze zaak werd een TGO gestart.
Bij het onderzoeksteam is de afdeling Analyse & Onderzoek aangesloten voor zaaksanalyse, zowel operationeel als tactisch. Op tactisch gebied werd een aanvang gemaakt met het samenstellen van hypothesen en scenario's. Bij de hypothesen was het vanaf het eerste moment duidelijk dat het om een misdrijf ging. Bij de scenario's waren er diverse mogelijkheden: roof, wraak, zedendelict.
Gezien het feit dat het slachtoffer nagenoeg naakt werd aangetroffen, was een zedendelict zeer aannemelijk. Voor wraak leek er geen aanleiding en doordat de woning netjes werd achtergelaten, was roof eveneens niet logisch. Het scenario zedendelict was leidend.
Gedurende het uitrechercheren van de onderzoeksrichting kwamen drie personen in beeld:

- de zoon van het slachtoffer;
- een ex-vriend van het slachtoffer;
- een klusjesman die kort voor het misdrijf werkzaamheden bij de woning van het slachtoffer had uitgevoerd en vreemde opmerkingen bij een buurvrouw had gemaakt.

Door het team werd primair ingezet op de zoon en de zoektocht naar de ex-vriend, van wie de identiteit niet bekend was. Vanuit het heersende scenario werd de klusjesman ook onder de loep genomen. Gaande het onderzoek kwamen rondom diens persoon feitelijkheden naar voren die nader onderzoek zouden kunnen rechtvaardigen. Deze feitelijkheden sloten echter niet aan bij het heersende scenario zedendelict. Aangezien de tactisch analist alle feitelijkheden beoordeelt op de drie scenario's, stelde de analist voor om het heersende scenario los te laten en een focus te leggen op de klusjesman. Met het kantelen van het onderzoek in de focus op de persoon werd de beschikbare zaaksinformatie opnieuw beoordeeld. De operationeel zaaksanalist voerde een telecomanalyse uit op de telefoon van de klusjesman. Tevens werd het relatieschema rondom deze klusjesman gedetailleerd uitgewerkt. In de combinatie van de telecomanalyse en het relatieschema werden belangrijke lijnen ontdekt tussen het slachtoffer, de klusjesman en een persoon uit het netwerk van de klusjesman. Dit tweetal is uiteindelijk voor dit ernstige misdrijf veroordeeld. Roof was het motief.

Ook nadat de valide overtuiging is ontstaan dat het dominante scenario tot oplossing van de zaak leidt, is de tactische analysevraag niet afgerond. Voor de zaaksofficier is het belangrijk om alternatieve scenario's uit te sluiten die de verdachte een mogelijke *escape* bieden tijdens de behandeling van de rechtszaak. Ook dit vraagt om operationele informatie te beoordelen in relatie tot openstaande hypothesen en scenario's. Er is dan ook niet voor niets in de TGO-regeling vastgelegd dat uiteindelijk de zaaksofficier bepaalt of de inzet van een tactisch analist niet meer nodig is om de zaak succesvol ter zitting te verdedigen.

11.1.3 Samenwerking

De kracht van analyse is om bij de teamleiding van een onderzoek constant die spiegel voor te houden en hierbij tegelijk te adviseren over mogelijkheden tot aanpak. Een team dat informatiegestuurd de juiste onderzoeksrichting uitloopt, zal worden geprezen om zijn focus. Een team dat emotiegestuurd investeert in de verkeerde onderzoeksrichting is ten prooi gevallen aan tunnelvisie. Een belangrijke taak voor analisten is om enerzijds mee te kunnen bewegen met het team en anderzijds kritisch te zijn op vooringenomen meningen en aannames. Het analysevak vraagt, naast stevige discussies op de inhoud, ook om onderhandelings- en relationele vaardigheden om het momentum van het team vast te houden. Momentum binnen een team én het voorbereiden van de teamleiding op inzet op alternatieve onderzoeksrichtingen kunnen naast elkaar bestaan als de analist beide belangen voor ogen houdt.

Ondanks het feit dat een operationeel en een tactisch zaaksanalist verschillende taken en verantwoordelijkheden hebben, is samenwerking tussen deze twee analisten onontbeerlijk. Een tactische analyse zonder goede operationele onderbouwing is onvoldoende geloofwaardig. Kleine stukken informatie kunnen een kanteling in het hele onderzoek betekenen. Operationele en tactische analyse gaan hand in hand. Intensieve samenwerking tussen beide analisten is een vereiste.

Figuur 11.1 Samenwerking

11.2 Veiligheidsanalyse: analyseren en adviseren op veiligheidsvraagstukken

Het Programma Intelligence (2008-2012) heeft het vakgebied van veiligheidsanalyse ontwikkeld tot zijn huidige vorm. Met de introductie en het formatief inrichten van de analist veiligheidsinformatie (AVI) heeft dit programma invulling gegeven aan het analysevak dat zich richt op het vervaardigen van analyseproducten ten behoeve van de sturing op integrale veiligheidsvraagstukken. Waar het vak van zaaksanalyse zich in de politieoperaties afspeelt, spitst de analyse- en adviseringstaak van de veiligheidsanalist zich toe op sturingsvraagstukken op lokaal, regionaal, en nationaal niveau. Veiligheidsanalyses steunen deze sturingsprocessen op operationeel, tactisch en strategisch niveau. Deze analysevorm heeft op deze sturingsniveaus verschillende functies.

- *Strategisch*
  Veiligheidsanalyses en -onderzoeken die het doel hebben om stuur- en weegploegen onderbouwde keuzes te laten maken welke veiligheidsvraagstukken prioriteit genieten.
- *Tactisch*
  Veiligheidsanalyses die het doel hebben om stuur- en weegploegen keuzes te laten maken in mogelijke interventies op basis van actuele trends en ontwikkelingen in specifieke veiligheidsthema's.
- *Operationeel*
  Veiligheidsanalyses die het doel hebben om stuur- en weegploegen keuzes te laten maken in de aanpak van concrete personen of groeperingen.

Waar de termen strategisch, tactisch en operationeel voorheen meer een indicatie waren van de hiërarchie van de organisatie, geeft het nu de type sturing aan. Deze type sturing kan op meerdere niveaus plaatsvinden. Zo wordt er zowel op lokaal, eenheids-, als nationaal niveau strategisch gestuurd en kan er op nationaal niveau ook zeer operationeel gestuurd worden.

11.2.1 Strategische veiligheidsanalyse

Bij strategische sturing worden de prioriteiten van een politieorganisatie bepaald, veelal voor meerdere jaren. Een strategische veiligheidsanalyse kan bij uitstek dit besluitvormingsproces informatiegestuurd laten verlopen.

Figuur 11.2 Misdaadstatistiek

Regionale veiligheidsstrategie

Ergens in Nederland.

Om de collectieve krachten te bundelen en te richten, wordt in gezamenlijkheid tussen politie, bestuur en OM in een regionale veiligheidsstrategie bepaald welke veiligheidsthema's de komende jaren prioriteit dienen te krijgen. Aan de afdeling Analyse & Onderzoek wordt de opdracht gegeven om samen met veiligheidsspecialisten van de partners een richtinggevend veiligheidsbeeld te maken.

Men kiest ervoor via een SWOT-analyse[1] inzicht te krijgen in de sterke en zwakke punten van de huidige aanpak, en in de resultaten binnen elk van de geprioriteerde veiligheidsthema's. Daarnaast wordt bekeken welke kansen en bedreigingen zichtbaar zijn die invloed hebben op de aanpak van de bestaande thema's.

Input komt uit groepssessies en interviews met vertegenwoordigers van allerlei veiligheidspartners, waardoor een rijk informatiebeeld ontstaat en de bevindingen een groot draagvlak kennen. De SWOT's worden gepresenteerd aan de eenheidsleiding, het OM en het regionaal college.

De collectieve reactie van de beslissers is dat ze zowel de bevindingen als de vorm waarin het gepresenteerd wordt 'waanzinnig interessant' vinden. Het vaststellen van de prioriteiten en de aanpak is vervolgens snel gerealiseerd.

11.2.2 Tactische veiligheidsanalyse

Bij tactische sturing worden actuele trends en ontwikkelingen op geprioriteerde thema's inzichtelijk gemaakt. De vraag naar veiligheidsanalyse ontstaat vooral op het moment dat het gevoel bestaat dat men de controle op een bepaald thema aan het verliezen is. Er wordt wel op ingezet, maar uit de cijfers valt op te maken dat het probleem niet verdwijnt. Een goede veiligheidsanalyse geeft inzicht in het verhaal achter de cijfers en biedt concrete handelingsperspectieven.

Coldspot

Ergens in Nederland.

In basisteam X was sprake van een enorme stijging van de woninginbraken. Dit stond haaks op de ontwikkeling in de rest van de eenheid, waarbij juist sprake was van een daling. Het basisteam had al veel maatregelen genomen, onder andere door het formeren van een woninginbrakenteam. Het lukte desondanks niet om het aantal inbraken omlaag te brengen. Daarom werd de hulp van analyse ingeroepen.

De dadergerichte informatiepositie was in het lokale informatieknooppunt al goed georganiseerd ten behoeve van de recherche. Een daderanalyse zou weinig toegevoegde waarde hebben. Daarom is er voor gekozen om een geografische analyse toe te passen. Daaruit bleek dat naast een aantal prominente hotspots (waar de focus van >>

1 Strengths, weaknesses, opportunities and threats.

>> het basisteam deels al op gericht was) er ook sprake was van een aantal opvallende coldspots in de betreffende stad. Dit waren plekken waar ook veel woningen stonden, maar waar nagenoeg niet werd ingebroken.
De aanbeveling van de analist was om de aandacht meer op deze coldspots te richten (in plaats van alleen op de hotspots zoals gebruikelijk is). Welke kenmerken hadden deze coldspots die mogelijk verklaarden waarom daar niet werd ingebroken, en was het vervolgens mogelijk om deze kenmerken ook toe te gaan passen op de hotspots? In plaats van het versterken van de repressieve aanpak zijn concrete acties voorgesteld ten behoeve van preventieve maatregelen. Zowel de basisteamchef als de burgemeester vond deze suggestie erg verfrissend en ze zijn de aanbevelingen in gang gaan zetten.

11.2.3 Operationele veiligheidsanalyse

Bij operationele sturing wordt, op basis van inzicht in de meest actieve criminele personen en groeperingen, een beargumenteerde keuze gemaakt voor een specifieke aanpak. De reden om dit via een veiligheidsanalyse uit te laten voeren, is dat de informatieorganisatie permanente monitoring organiseert op hoog geprioriteerde veiligheidsproblemen. Vanuit deze monitoring kan relatief eenvoudig ingezoomd worden op subjecten of groeperingen die verantwoordelijk zijn voor een toename aan signalen van criminele activiteiten.

Serie

Ergens in Nederland.
In basisteam Y was sprake van een aantal aanrandingen waarbij zowel bij de (onbekende) dader als bij de slachtoffers sprake was van een jeugdige leeftijd. Vanwege de jonge leeftijd van de slachtoffers lagen de zaken erg onder een vergrootglas van bewoners, politiek en media. Er werd gesproken van een serieaanrander en allerlei zaken werden door de media aan elkaar gelinkt.
Het basisteam was op zoek naar in- en overzicht en wilde uiteraard geen fouten maken, al helemaal niet nu de politiek hen zo kritisch op de vingers keek. Daarom werd de hulp ingeroepen van de afdeling Analyse & Onderzoek.
De analist heeft allereerst het fenomeen breed in kaart gebracht en alle aanrandingen van de afgelopen anderhalf jaar bekeken. Het doel was tweeledig: enerzijds een algemeen beeld geven van de aanrandingen in het desbetreffende gebied, en anderzijds vaststellen of er nog meer aanrandingen waren die mogelijk in de serie pasten, en of er nog meer series vielen te ontdekken. Vervolgens is ingezoomd op de zaken die mogelijk binnen de serie van de jeugdige aanrander pasten. Deze zijn nauwkeurig geanalyseerd. Tot slot werden praktische en snel toepasbare aanbevelingen gedaan.
Naast het schriftelijke verslag is de analyse mondeling gepresenteerd aan het basisteam en de afdeling Zeden. Het team had nu goed zicht op de aanrandingen, kreeg handvatten voor een betere aanpak en het verbeteren van de informatiepositie. Tevens bood de analyse veel nieuwe aanknopingspunten voor het lopende onderzoek.

11.2.4 Samenwerking

Strategische, tactische en operationele sturing zijn geen strikt gescheiden processen. Dit geldt tevens voor de veiligheidsanalyses. Om tactische sturingsvraagstukken goed te kunnen beantwoorden, zijn strategische inzichten nodig. Om goed operationeel te kunnen adviseren, biedt een overzicht van trends en ontwikkelingen een belangrijke context om de juiste keuzes te kunnen maken.

Tevens is de scheiding tussen het vakgebied zaaksanalyse en veiligheidsanalyse bij bepaalde analysevraagstukken niet strikt. Een vergelijkende zaaksanalyse kan zowel aan een rechercheteam, zoals een woninginbrakenteam, worden gepresenteerd als aan een districtelijk managementteam. Het verschil is dat er binnen het rechercheteam persoonsgericht wordt gewerkt en dat er dus dadergericht wordt beslist. Binnen een districtelijk managementteam kan zo'n vergelijkende zaaksanalyse tot een andere benadering leiden, bijvoorbeeld het starten van een campagne om het keurmerk veilig wonen in een bepaald gebied te promoten.

Een analist dient zich daarom terdege bewust te zijn in welke context hij aan het werken is, en wat de consequenties hiervan zijn voor het uitvoeren van een analyseopdracht en het presenteren van de bevindingen en aanbevelingen. De competentie van de analist wordt, behalve door het vakmanschap, in toenemende mate bepaald door de manier waarop hij weet om te gaan met de verschillende contexten in het werk. Deze contexten zijn niet beperkt tot de politieprocessen. Naarmate een integrale aanpak de sleutel is tot het oplossen van hardnekkige veiligheidsproblemen (zie ook hoofdstuk 13 Informatiegestuurd werken en samenwerkingsrelaties), wordt meer van de analist gevraagd om zich beter te kunnen verplaatsen in het werkveld van andere veiligheidspartners en het advies hierop af te stemmen. De zwaarte en daarmee ook de waardering van analysewerk wordt in toenemende mate bepaald door de senioriteit die nodig is om een specifieke analyseopdracht uit te voeren. De voorheen gehanteerde termen strategisch, tactisch of operationeel analist zijn losgelaten ten behoeve van dat senioriteitsbeginsel. Het uitvoeren van een complexe operationele zaaksanalyse onder hoge politieke druk vraagt meer van een analist dan een eenvoudige beschrijvende tactische veiligheidsanalyse.

11.3 Het analyseproces

Het analyseproces bestaat globaal uit drie stappen:

1 intake
2 uitvoering
3 oplevering

11.3.1 Intake: het goede gesprek

Onder het devies 'een goed begin is het halve werk' vormt de intake de start van elke analyseopdracht. Een intake kent meerdere contactmomenten. Het begint altijd met een eerste gesprek over een probleem. Zo'n gesprek kan overal ontstaan, van de directietafels tot de koffieautomaat.

Hiermee komt ook een belangrijk werkingsprincipe naar voren: de afdeling Analyse & Onderzoek werkt gedeconcentreerd zo dicht mogelijk op de operatiën. Hierdoor kunnen belangrijke signalen over opkomende veiligheidsproblemen snel opgepikt worden. Voor de afdeling Analyse & Onderzoek betekent dit dat ze zo veel mogelijk in de informatieknooppunten van de informatieorganisatie werkzaam zijn. Deze knooppunten zijn in alle politiële werkvelden georganiseerd: binnen districten, de recherche, de diensten Operationele Samenwerking en Operationele Centra. Tevens wordt er nauw samenwerkt met andere informatieafdelingen. Zo is er intensieve en langdurige samenwerking met de verschillende afdelingen die informatiecoördinatie uitvoeren (zowel op districtelijk, dienst-, als eenheidsniveau) voor het onderhouden en analyseren van informatieposities op specifieke thema's, zoals financieel-economische criminaliteit, contraterrorisme, extremisme en radicalisering (CTER), ondermijning en mensenhandel (zie hoofdstuk 10 Informatiecoordinatie). Ook zijn analisten van de afdeling Analyse & Onderzoek voor een bepaalde periode gedeconcentreerd tewerkgesteld binnen de afdelingen inwinning (zie hoofdstuk 14 Inwinning).

Belangrijke signalen en verzoeken worden door een coördinator van de afdeling Analyse & Onderzoek besproken met de coördinator van het desbetreffende knooppunt. Hier kan een eerste beeld worden ingewonnen over de aard en de omvang van het probleem. Tijdens de intake met de aanvrager worden het analyseverzoek besproken, het doel van de analyse, de doelgroep waaraan geadviseerd moet worden, de doorlooptijd, de beschikbare informatie en worden praktische werkafspraken gemaakt. Een goede intake is onmisbaar om deze zaken duidelijk te krijgen en onaangename verrassingen tijdens de uitvoering te voorkomen.

Terug naar de basis

Ergens in Nederland.

Door de districtsleiding werd het verzoek gedaan om een verdiepende veiligheidsanalyse te maken van een deel van een industrieterrein in een gemeente in relatie tot de aldaar bekende rechtspersonen en natuurlijke personen. Het vermoeden bestond dat er sprake zou zijn van samenwerking op het gebied van het plegen van diverse misdrijven. Ook zouden motorclubs een rol in het geheel spelen.

Er werd tijdens de intake druk uitgeoefend, omdat er tussen het openbaar bestuur en de leiding van het district overleg was geweest en er met de uitkomst van de analyse hoe dan ook tot een aanpak zou worden overgegaan.

Het was lastig tijdens de intake duidelijkheid te krijgen over hoe de vraag was ontstaan en op basis waarvan. Als het probleem niet duidelijk is, valt de basis voor een goede advisering weg – een onbevredigende constatering onder de genoemde druk. Hierop is getracht inzicht te krijgen in de aanwezige informatie rond het probleem. Naar aanleiding hiervan zou de mogelijke analyseopdracht geformuleerd worden.

Bij het doornemen van de informatie bleek dat er diverse processen-verbaal van het Team Criminele Inlichtingen (TCI) waren, met daarin veel actuele informatie over natuurlijke en rechtspersonen. Deze informatie rechtvaardigde een strafrechtelijke aanpak op korte termijn.

>>

>> Vervolgens is het advies gegeven tot het opstellen van een preweeg en vooralsnog geen verdiepende analyse in te zetten. Deze preweeg is korte tijd later afgerond en bij het daaropvolgende opsporingsonderzoek is de afdeling Analyse & Onderzoek aangesloten. Op het gebied van zaaksanalyse is er ingezet, hetgeen uiteindelijk een onderzoek met een positief resultaat heeft opgeleverd.

11.3.2 Uitvoering

Op basis van de intake kan de analist een analysemethode en een aanpak vaststellen. Er zijn vele methoden en technieken ter beschikking en het gaat te ver om deze allemaal te benoemen en beschrijven. Toch is er binnen de werkcontext van zaaksanalyse en veiligheidsanalyse een belangrijk onderscheid. Binnen uitvoering van een zaaksanalyse wordt gesignaleerd en geadviseerd op basis van waarheidsvinding. Iets is een feit en als het niet bewezen is, is het een veronderstelling. Veronderstellingen hebben geen bewijswaarde tijdens een rechtszaak. Het is een zonde om te adviseren op basis van veronderstellingen (tenzij het advies is om de veronderstelling te onderzoeken).

Bij de uitvoering van een veiligheidsanalyse werkt dit anders. Bij veiligheidsvraagstukken kunnen analysemethoden toegepast worden die onzekerheden minimaliseren, maar ze kunnen nog wel worden toegestaan. Veiligheidsanalyse werkt daarmee niet per se vanuit waarheidsvinding, maar vanuit onzekerheidsreductie. Zo kan de bevinding: 'Als je op tijdstip Z op hotspot X niet-geüniformeerd gaat surveilleren, is de kans op een heterdaadsituatie 80 procent. Als je op datzelfde tijdstip op hotspot Y gaat surveilleren, is de kans op een heterdaadsituatie 15 procent', resulteren in het advies: 'Ga op tijdstip Z op hotspot X surveilleren.' Het toepassen van (statistische) onzekerheidsreductie als analysemethode zonder ondersteunende waarheidsvinding is in opsporingsonderzoeken zeer risicovol.

Lucia de B.

'Niemand had Lucia ooit een handeling zien verrichten die geleid kon hebben tot de dood van een patiënt. Aanvankelijk was de verdenking gebaseerd op statistische berekeningen: er was een kans van 1 op 7 miljard, later van 1 op 342 miljoen dat een onschuldige Lucia bij toeval aanwezig was bij alle sterfgevallen. De kans was zo klein dat zij wel schuldig moest zijn. De berekeningen bleken later niet te kloppen. Eén statisticus kwam op een kans van 1 op 9.'[2]

11.3.3 Oplevering

De oplevering vormt het sluitstuk van al het analysewerk. Het is hét moment waarop alle opgedane kennis, expertise en bevindingen worden omgezet in een advies. Bij de verschillende analysevormen is wel sprake van een aantal belangrijke verschillen.

2 Citaat uit NRC.nl, archief.

Bij een veiligheidsanalyse is de advisering vaak het sluitstuk van een langdurig analyseproces. De formele oplevering is een eenmalig moment waarop alle bevindingen worden verwerkt in alle adviezen die er naar de inschatting van de analist toe doen. In een formele setting velt een stuurgroep op dat moment haar oordeel over de adviezen.

Voor een zaaksanalist werkt dit anders. Deze werkt binnen het team in continue nabijheid van de teamleider. Een zaaksanalist heeft meer de mogelijkheid om het moment te kiezen om adviezen over te brengen. Vooral voor een veiligheidsanalist is het daarom zaak om te bouwen aan de relatie met de opdrachtgever en periodiek informeel contact te hebben. Dit contact helpt enorm om besluitvorming bij het formele oplevermoment in goede banen te leiden.

In 2015 is in opdracht van Politie en Wetenschap een onderzoek uitgevoerd naar de impact van veiligheidsanalyse op misdaadbestrijding.[3] Uit dit rapport zijn belangrijke lessen te trekken hoe de uitvoering, oplevering en opvolging van een analyse succesvol kunnen verlopen.

Een belangrijke constatering is het belang van de interactie tussen analist en afnemer tijdens de uitvoering van de analyse, als een voorwaarde voor de mate van impact van de analyse. Zowel tijdens de intake als de uitvoering, maar met name ook bij de oplevering. Het opleveren bestaat niet uit het opsturen van de analyse, maar uit deze toelichten en erover in gesprek gaan; expertsessies organiseren om daarmee een momentum te creëren dat een voedingsbodem is voor het opvolgen van de adviezen. Integraal onderdeel van het analysevak is dan ook het bouwen en onderhouden van een relatie met de opdrachtgever en samenwerken met deze opdrachtgever in de uitvoering, oplevering en opvolging van de analyse.

11.4 Analyse in de nabije toekomst

Informatiegestuurd werken en sturen zijn de afgelopen jaren sterk verankerd in de Nederlandse politie. Waar informatiegestuurd werken voorheen nog een manier van politiewerken was en afgewogen werd tegen *community policing* of *problem-oriented policing,* is informatiegestuurd werken nu een gegeven geworden; *a way of doing business* die onafhankelijk haar bestaansrecht heeft naast politiële interventiestrategieën. De vorming van de elf informatieorganisaties is het sterkste bewijs van deze verankering.

Figuur 11.3 Toekomst

3 Hengst, M. den, et al., *Van intel tot operatie: de impact van veiligheidsanalisten bij de aanpak van misdaad.* Reeks Politiekunde nr. 73. Reed Business Information, Amsterdam 2015.

Het intelligenceproces heeft daarmee een impuls gekregen die ook effect heeft op het analyseproces. Een belangrijke ontwikkeling hierbij is die van de big data (zie ook hoofdstuk 20 Big data). Mede door de komst van de Business Intelligence Competency Centers (BICC's) nemen big data een vlucht binnen de organisatie (zie ook hoofdstuk 22 De business-intelligencestrategie in de politiepraktijk). De snelheid waarmee, en diverse manieren waarop, informatie ter beschikking komt, alsmede de hoeveelheid, neemt ziende ogen toe. De komst van het Raffinaderijconcept (zie hoofdstuk 20 Big data) is hier een tekenend voorbeeld van. Dit verlangt van de analist een andere manier van werken. Waar het vroeger nog mogelijk was om de onderzoeksinformatie volledig bij te houden (te lezen), wordt dit in toenemende mate onmogelijk.

Analyse zal moeten zoeken naar alternatieve werkwijzen, waarmee de analist kan omgaan met deze hoeveelheid en diversiteit aan informatiebronnen en tegelijkertijd invulling kan blijven geven aan zijn kerntaak, namelijk:

1 Het in stand houden van de kwaliteit van adviseren en dus vanuit gevalideerde informatieposities blijven signaleren: wat is de bron van de informatie, hoe is deze broninformatie verwerkt en is deze daarmee voldoende betrouwbaar om richtinggevende uitspraken te doen?
2 Het onderscheiden van hoofd- en bijzaken: is de kern van het probleem nog wel redelijkerwijs te abstraheren uit de wirwar van informatie?
3 Aan de voorkant van het probleem komen: hoe kun je voorkomen dat de permanent lopende informatiestromen een dusdanige claim leggen op het duiden van informatie dat dit druk legt op de kerntaak van signaleren en adviseren?

Het oplossen van dit analysedilemma vraagt de komende jaren om een intensieve samenwerking met de afdelingen die zich bezighouden met kwaliteit van informatie. Hierbij zijn kennisdeling en het opdoen van concrete praktische ervaringen op het gebied van big data en *datamining* de sleutel om de uitvoering van het mooie analysevak door te ontwikkelen, passend in deze nieuwe realiteit.

12 Persoonsgerichte aanpak en risicotaxatie

Erik Theunissen en Dian Aarts

12.1 Inleiding

Nederland is een van de veiligste landen ter wereld. Dat brengt met zich mee dat een verstoring van die veiligheid een grote schokgolf kan veroorzaken. Media en politiek reageren hier vaak op door extra maatregelen en capaciteit van inlichtingen- en veiligheidsdiensten te vragen om elk risico voor te zijn. Het lijkt erop dat we streven naar een *zero risk*-maatschappij. Diverse maatschappelijke ontwikkelingen vragen de politie om vaker en professioneler gebruik te maken van risicotaxatie op het gebied van veiligheid, integrale aanpak en zorg. Denk aan de uitkomsten van de commissie-Hoekstra (2016) naar aanleiding van de moord op Els Borst, maatschappelijke onrust bij rellen als in de Schilderswijk en het 'stalkingincident' – de moord op verpleegster Linda van der Giessen door haar ex-partner in Waalwijk (alle gebeurtenissen in 2015).

De maatschappij en de politiek verwachten van de politie in toenemende mate dat zij ingrijpt voordat het te laat is. Dat geldt ook voor *lone wolves* als Tristan van der Vlist (Alphen aan den Rijn, 2011), Karst Tates (Apeldoorn, 2009) en Anders Breivik (Oslo en Utøya, in Noorwegen, 2011). Ook de terroristische dreiging van onder andere Islamitische Staat en de teruggekeerde Nederlandse Syriëstrijders vragen van de politie om monitoring van personen en inschatting van risico's op het daadwerkelijk uitvoeren van dreigingen. In veel gevallen is het zaak om samen met partners een breed gedeeld persoonsbeeld op te stellen, omdat de zorg bijvoorbeeld heel andere informatie kan hebben dan de politie, zie ook hoofdstuk 13 Informatiegestuurd werken en samenwerkingsrelaties.

Een van de oorzaken voor het afnemen van criminaliteit en overlast de laatste tien jaar, is het succes van allerlei veelpleger- en Top X-aanpakken (zoals de Top 600 in Amsterdam). In feite allemaal vormen van persoonsgerichte aanpak (PGA). De gedachte achter deze aanpak is dat een klein deel van de veroorzakers verantwoordelijk is voor een groot deel van de criminaliteit en overlast. Deze groep is in zijn gedrag niet met alleen strafrechtelijke maatregelen te beïnvloeden, omdat er vaak sprake is van complexe problematiek (verslaving, psychische stoornis enzovoort). Daarom is de aanpak integraal met diverse partners die ook informatie, kennis en interventiemiddelen hebben.

Doel van het landelijk project PGA van de politie is het ontwikkelen van een eenduidige methode voor de persoonsgerichte aanpak van geprioriteerde veiligheidsproblemen. Dit moet bijdragen aan de volgende maatschappelijke effecten:

- daling van recidive en het eerder stoppen van criminele carrières;
- effectieve aanpak van door het gezag geprioriteerde veiligheidsproblemen;

- effectieve en efficiënte ketenaanpak: de politie is daarbij een betrouwbare partner die op een voorspelbare manier handelt, met uniforme informatieproducten.

De landelijk uitgewerkte persoonsgerichte aanpak zorgt dat de politie personen die bepaalde veiligheidsproblemen veroorzaken[1] op een effectieve en eenduidige wijze in de eenheden aanpakt. Dat wil zeggen, dat is de bijdrage die de politie aan de integrale aanpak levert. Per definitie is dat een taartpunt van de samenwerking met partners als gemeenten, Openbaar Ministerie (OM), geestelijke gezondheidszorg (ggz) enzovoort. Regionaal vindt die samenwerking plaats in Veiligheidshuizen, Regionaal Informatie- en Expertisecentrum (RIEC) en lokale PGA in bepaalde gemeenten. Ook kunnen er aparte casusoverleggen voor aanpak terrorisme/radicalisering in grotere gemeenten gehouden worden.

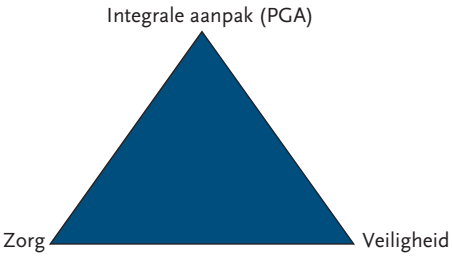
PGA is een manier van (integraal) denken en werken, en heeft geleid tot een beschreven werkproces inclusief hulpmiddelen, de methode PGA. Binnen dit proces zijn alle rollen beschreven voor basisteams, opsporing en voor de informatieorganisatie. Risicotaxatie maakt hier onderdeel van uit, als instrument om te helpen duiden wanneer optreden nodig is, en dat handvatten kan bieden voor de aanpak. De politie maakt gebruik van verschillende risicotaxatie-instrumenten om gevaren door en voor personen in te schatten. Dit varieert van checklists tot deskundigheidsoordelen op basis van wetenschappelijk onderzoek.

Relatie tussen PGA en risicotaxatie (vanuit visie PGA)

Binnen de visie van PGA is er een relatie tussen zorg, veiligheid en de integrale aanpak (PGA in strikte zin). De PGA is een integraal op de persoon toegesneden (mix van) interventie(s), die beoogt te verhinderen dat de persoon in kwestie (opnieuw) een strafbaar feit pleegt. Er zijn ook situaties waarbij er geen sprake is van een integrale aanpak, maar wel van een hoog veiligheidsrisico. Denk aan een stalker of een terrorist. Er kan dan sprake zijn van een acute dreiging die acuut handelen vereist. Hierbij kan een risicotaxatie op de persoon van grote waarde zijn. Naar aanleiding hiervan (de risicoscore) wordt de persoon aangemerkt als geprioriteerd politiepersoon (GPP) en wordt een bejegeningsprofiel of plan van aanpak gemaakt. Indien er sprake blijkt van multiproblemen waarbij een verzwaarde integrale aanpak noodzakelijk is, kan deze persoon tevens aangemeld worden voor PGA in een van de integrale overleggen. Als er geen sprake is van een veiligheidsprobleem, maar van zorg om bijvoorbeeld een kind in relatie tot huiselijk geweld, dan kan er door de politie een zorgsignaal gegeven worden aan de zorgpartners. Ook hierbij kan een risicotaxatie-instrument benut worden (zogenoemde vroegsignalering).

---

1 Ook wel 'doelgroepen' genoemd. Deze term past niet meer goed bij de inzichten in bijvoorbeeld Veiligheidshuizen, waar het gaat om de integrale aanpak van complexe problematiek bij personen, die alleen multidisciplinair aangepakt kan worden. Gevolg is dat Veiligheidshuizen veelal aparte casusoverleggen voor doelgroepen als veelplegers, huiselijk geweld enzovoort hebben afgeschaft.



Figuur 12.1 PGA en risicotaxatie

12.2 Persoonsgerichte aanpak

Figuur 12.2 Persoonsgerichte aanpak

Door binnen de politie overal dezelfde principes van deze basiswerkwijze te hanteren, wordt interne samenwerking effectiever. De politie kan hierdoor ook gestandaardiseerde overdrachtsproducten aanbieden aan partners. Natuurlijk blijft binnen deze uniforme werkwijze ook ruimte voor lokaal maatwerk en voor zowel reactief als proactief optreden. Doelstelling is dat de combinatie van een uniforme methodiek en ruimte voor lokaal maatwerk ertoe leidt dat de werkwijze voldoende uniform wordt gehanteerd in de eenheden.

Binnen de politie is de PGA verder ontwikkeld naar een uniforme, doelgroeponafhankelijke aanpak met professionele hulpmiddelen. Immers: personen die strafbare feiten plegen, houden zich niet aan de gemeentegrenzen. Ook plegen zij vaak meer dan één type

delict. Om deze personen effectief aan te pakken, is het dus essentieel dat iedereen binnen de politie dezelfde taal spreekt. Alleen dan kan een landelijk beeld van geprioriteerde personen ontstaan en is het mogelijk landelijk afspraken met partners te maken. Het project PGA heeft daarom definities vastgesteld voor PGA en voor geprioriteerde personen:

1 'De persoonsgerichte aanpak is een integraal[2] op de persoon toegesneden (mix van) interventie(s) die beoogt te verhinderen dat de persoon in kwestie (opnieuw) een strafbaar feit pleegt.'
2 'Een geprioriteerd politiepersoon is een persoon die enerzijds strafbare feiten, die landelijk of lokaal geprioriteerd zijn, heeft gepleegd of van wie verwacht wordt dat hij deze zal plegen en die anderzijds volgens de politie in aanmerking komt voor een persoonsgerichte aanpak vanuit het bevoegd gezag.'

12.2.1 Het PGA-proces op hoofdlijnen

Uitgangspunt is dat het PGA-proces voor de politie uit drie fasen bestaat: signaleren en adviseren (fase 1), selecteren en prioriteren (fase 2) en aanpak en interventies (fase 3). De uitkomst van fase 3 is weer input voor fase 1. Het PGA-proces start wanneer het bevoegd gezag afspraken heeft gemaakt met de teamchef over de PGA van geprioriteerde veiligheidsproblemen. Deze prioriteiten hebben OM, gemeenten, ministerie van Veiligheid en Justitie en politie landelijk vastgelegd in de Veiligheidsagenda. Lokale prioriteiten zijn als vervolg op de gebiedsscan in bijvoorbeeld het Integraal Veiligheidsplan op gemeentelijk niveau vastgelegd.

Binnen de politie worden in fase 1 de voor PGA benodigde informatieproducten (zoals een politienamenlijst) op uniforme wijze geproduceerd. Na het combineren van systeeminformatie met straatkennis kiest de teamchef welke personen vanuit de politie worden geprioriteerd. De start van fase 2 is dat de PGA-specialist[3] deze personen (met hun politiepersoonsdossier/aanmelding PGA) in een Integraal Veiligheidsoverleg aanmeldt voor triage. Daar vinden selectie en routering van geprioriteerde personen (PGA'ers) plaats. In een passend casusoverleg delen partners relevante informatie en maken een integraal plan van aanpak. Daarna start fase 3: aanpak en interventies door de politie en andere partners.

Een belangrijk uitgangspunt is dat het PGA-proces kan worden gebruikt bij de aanpak van personen die bijdragen aan allerlei geprioriteerde veiligheidsproblemen, zoals:

- plegers van *high impact crimes* zoals overvallen, straatroof en woninginbraken;
- geweld;
- veelplegers;
- jeugdigen met grote kans op een criminele carrière;
- potentieel gewelddadige eenlingen (PGE);
- contraterrorisme, extremisme en radicalisering (CTER);
- verwarde personen.

---

2 De term 'integrale aanpak' is later aangescherpt: het gaat om een aanpak waarbij minimaal drie ketenpartners zijn betrokken. Het gaat dan om partners uit de strafrechtketen plus minimaal één andere keten.

3 In elk basisteam is de rol van PGA-specialist ingericht; deze is specialist op het proces. Meestal is deze rol op operationeel specialist A-niveau belegd. Op districtsniveau is binnen de Dienst Recherche de rol van districtelijk PGA-specialist belegd. Deze is tevens liaison Veiligheidshuis.

Dit is een niet-limitatieve opsomming. Bij sommige thema's is er sprake van een verbijzondering op onderdelen van het PGA-proces, zoals voor de PGE.

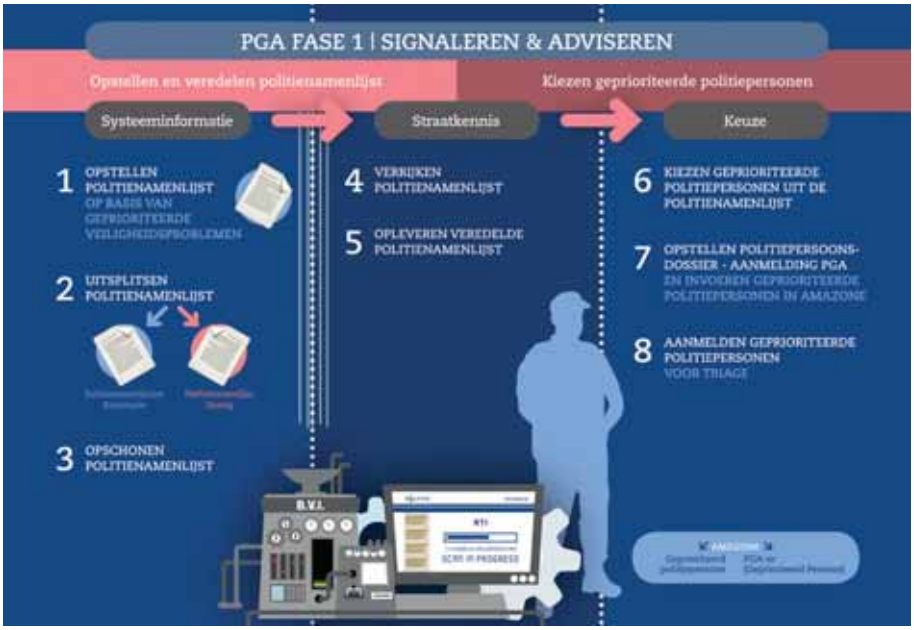
Elk team binnen de politie kan aan de slag met PGA. In de methode is de werkwijze voor een basisteam uitgewerkt. Maar ook de (districts)recherche, een eenheidsteam of de landelijke recherche kan de aanpak toepassen. Het uitgangspunt is: aan de voorkant uniform, aan de achterkant maatwerk. De basiswerkwijze van informatie verzamelen, prioriteren en routeren (fase 1) is in al deze situaties hetzelfde. Vooral bij fase 2 en 3 van PGA wordt themaspecifieke kennis ingezet met als doel: een maatwerkplan en -interventies op de persoon.

De politie prioriteert personen in het kader van PGA, omdat zij:

- (meerdere malen) verdachte zijn geweest op (meerdere) geprioriteerde veiligheidsproblemen;
- een verhoogd risico hebben op het plegen van geweld (zoals aangegeven door inzet van het Risicotaxatie-instrument Geweld).

Bij geprioriteerde politiepersonen is dus altijd sprake van een (dreigend) strafrechtelijk aspect of een hoog veiligheidsrisico. Personen die geen verdachte zijn geweest maar wel veel zorg nodig hebben (bijvoorbeeld psychiatrisch patiënten) worden in het kader van PGA niet geprioriteerd door de politie, maar wellicht door andere partners. De politie vervult hier wel een rol van (vroeg)signalering, waarbij ook vormen van risicotaxatie ingezet kunnen worden.

12.2.2 Concretisering bij Signaleren en adviseren (fase 1)[4]



Figuur 12.3 Signaleren en adviseren in fase 1 PGA

4 Omdat de invloed van intelligence het grootst is in de fase van signaleren, is alleen deze hier nader uitgewerkt. Het betreft overigens een cyclisch proces.

De gedachte is dat medewerkers steeds meer zelf kunnen in hun dagelijks werk en zich daarbij kunnen bedienen van business-intelligencetools die relatief makkelijk te gebruiken zijn voor een generalist. Denk aan integraal bevragen (BasisVoorziening Informatie voor Integrale Bevraging – BVI-IB), BlueSpot Monitor (BSM) en, met name voor PGA, de BVI-Bluelist. Tegelijk wil de informatieorganisatie zich richten op personen in meer complexe zaken. Hier zit haar echte meerwaarde: specialistische kennis en systemen[5], systemen waar een vergaande autorisatie voor is vereist, analyse en inzetadvies. Dit heeft geleid tot het hanteren van het principe *click* (raadpleeg zelf een systeem), *call* (bellen) en *face* (persoonlijk contact). Het uitgangspunt moet wel zijn dat er samenwerking is tussen de operatie en de informatieorganisatie om te werken aan de informatiepositie rondom een geprioriteerd persoon/PGA'er. Hieronder staat de nadere uitleg van de werking van PGA in fase 1.

Stap 1-3: Systeeminformatie (click)

De PGA-specialist doet een voorselectie door op geprioriteerde veiligheidsthema's via BVI-Bluelist een set van personen in een bepaald gebied te selecteren (stap 1). Hierbij maakt hij gebruik van (geautomatiseerde) risicotaxatie-instrumenten, zoals Prokid en Preselect (Jeugd) en het risicotaxatie-instrument (RTI) geweld (volwassenen). Ook kan de PGA-specialist zelf BVI-IB en BSM bevragen. Vervolgens start hij het persoonsdossier (standaard format), waarvan hij de eigenaar is. Het is belangrijk om een eigenaar aan te wijzen, omdat deze verantwoordelijk is voor de actualiteit en kwaliteit van de informatie. Daar worden namelijk beslissingen op genomen binnen de politie en in de keten. Vanuit de operatie wordt het dossier (of delen daarvan) gedeeld met partners onder regie van de PGA-specialist, dus is het logisch dat het eigenaarschap dan ook daar wordt belegd. Vanuit de informatieorganisatie maakt de afdeling Business Intelligence & Kwaliteit (BI&K) indien nodig aanvullende *query's*[6], ondersteunt BI&K bij het gebruik en actualiseert het de *query's*. Tevens adviseert BI&K over diepgaandere kwalitatieve risicotaxatie, waar bijvoorbeeld een gedragspsycholoog voor ingezet wordt.

Stap 4-5: Straatinformatie (call)

De PGA-specialist vraagt informatie bij onder andere wijkagenten en extra informatie wordt in bronsystemen verwerkt, denk aan de informatie uit het zakboekje van de politiemedewerker. Dan wordt de namenlijst geactualiseerd en wordt het persoonsdossier aangevuld. Het informatieknooppunt zet indien nodig een intelligencespecialisme in. Ook kan er advies gegeven worden ten aanzien van registratie of duiding. Dat kan gebeuren als een politiecollega het vermoeden heeft dat er meer informatie moet zijn,

5 Bijvoorbeeld OSINT, open bronnen op internet (zie hoofdstuk 15 Sociale media).

6 Een query is een zoekvraag die geprogrammeerd is in een informatiesysteem om alle data over een onderwerp (in dit geval rondom personen) in een overzicht te presenteren voor de gebruiker. Het onderwerp moet dan wel van tevoren exact geformuleerd zijn door middel van een definitie van het veiligheidsvraagstuk (bijvoorbeeld voor stalking) en het benoemen van de gestructureerde data (bijvoorbeeld maatschappelijke klassen) en ongestructureerde data (woorden als 'ex', 'achtervolging').

dan wel dat er een hit komt in BIV-IB. Deze collega kan dan de Dienst Regionale Informatieorganisatie (DRIO) bellen om mee te kijken, te helpen bij de interpretatie en informatie te betrekken waar de politieambtenaar zelf niet bij kan, omdat er bijvoorbeeld een artikel 9- of 10-autorisatie (zie hoofdstuk 5 De Wpg en hoofdstuk 6 Autorisatiemodel politie) voor nodig is. Een aandachtspunt is actief informatie inwinnen. Stel dat van een geprioriteerd persoon geen kenteken bekend is in de systemen, dan kun je op de briefing een opdracht uitzetten om te achterhalen in welke auto die persoon rijdt.

Stap 6-8: Keuze (face)

Het keuzemoment houdt in dat er overleg is tussen de PGA-specialist en de DRIO, waarbij de veredelde dossiers gepresenteerd worden en geprioriteerde politiepersonen worden besproken en gekozen. Indien nodig worden briefingsitems bepaald om gericht ontbrekende informatie in te winnen. Op basis daarvan wordt het handelingsperspectief bepaald (prioriteren voor PGA ja/nee, of andere route). De vervolgstappen van fase 1: Signaleren en adviseren liggen bij de PGA-specialist.

12.2.3 Informatiedeling met partners

PGA is per definitie een integrale aanpak, dat wil zeggen samenwerken met partners om gedrag van personen met een vaak complexe problematiek positief te beïnvloeden. Het spreekt voor zich dat dit dan ook geldt voor het delen van informatie rondom die personen in alle fasen van PGA. Dit gebeurt dan binnen het kader van de Wet politiegegevens (Wpg), waarvoor vaak een convenant wordt afgesproken om daaraan te kunnen voldoen. Met andere woorden, welke informatie mag je proportioneel, doelgebonden delen?

In fase 1: Signaleren en adviseren wordt vooral de informatiepositie binnen de politie opgebouwd met doorgaans alleen politie-informatie. In een enkele eenheid wordt ook gemeentelijke informatie al betrokken in deze fase, wat uiteraard functioneel kan zijn. De methode PGA sluit dat ook niet uit, maar benoemt het niet; dit om rollen tussen partners duidelijk te houden. Andere partners, zoals diezelfde gemeente, of de zorg, kunnen een eigen proces van signaleren en adviseren hanteren teneinde personen vanuit die hoek te prioriteren voor de integrale aanpak (PGA). Een belangrijke wens vanuit de politie is om meer OM-informatie te ontsluiten binnen de politiesystemen en deze te kunnen gebruiken om de inzet van BVI-Bluelist en risicotaxatie-instrumenten te kunnen versterken. Veelplegersinformatie is inmiddels beschikbaar, detentie-informatie nog niet. Voor risicotaxatie geldt dat informatie over veroordelingen op jonge leeftijd sterke voorspellers zijn.

In fase 2: Selecteren en prioriteren wordt door de politie informatie op tafel gelegd over de betreffende persoon. Dit gebeurt door de uitkomst van fase 1 via het aanmelddossier (een selectie van het totale politiepersoonsdossier) in te brengen in het integrale overleg met partners. Daarin zitten minimaal gemeente (regisseur en bevoegd gezag), OM (bevoegd gezag) en politie, maar bij voorkeur ook andere partijen zoals de zorg. Elke partner brengt in dit overleg de eigen informatie (waarvan risicotaxatie onderdeel kan uitmaken) in, en men kiest dan gezamenlijk welke persoon een PGA krijgt. De politie maakt een bredere

Figuur 12.4 Selecteren en prioriteren in fase 2 PGA

selectie aan in het politiepersoonsdossier – het (volledige) PGA-dossier –, en vult dit. Ook andere partners houden hun informatie bij in (veelal diverse vormen van) dossiers. Voor de informatie die gedeeld kan worden door alle partners ter ondersteuning van casusoverleggen, wordt in en door veel Veiligheidshuizen GECOS (zie paragraaf 12.2.6 Tools beschikbaar voor uitvoering van PGA) gebruikt. De politie muteert hier overigens niet in.

Er zijn wel beperkingen in het delen van informatie vanuit met name de zorg met OM en politie, en andersom. Deze zijn gelegen in bijvoorbeeld het medisch beroepsgeheim. Maar problemen zijn ook cultureel van aard. Zo wil de politie graag alle mogelijke informatie verzamelen, maar niet graag delen uit angst opsporingsonderzoeken te schaden of de privacyregels te overtreden.[7] Inmiddels is wel duidelijk dat er meer mogelijkheden zijn om (ruimer) informatie te delen tussen partners als de Wpg gezien wordt als wettelijk kader voor mogelijkheden in plaats van beperkingen. De ervaren beperkingen liggen meer in de voornoemde factoren.

Geautomatiseerde informatie-uitwisseling in het kader van PGA is nog nauwelijks gerealiseerd vanwege het voorgaande en doordat de informatiesystemen van de verschillende partners niet eenvoudig aan elkaar te koppelen zijn. Er wordt in enkele gemeenten wel gewerkt aan een informatieorganisatie waarin ervaring wordt opgedaan met of en hoe

7 Overigens schuilt er een risico in om bijvoorbeeld zorginformatie in politiesystemen op te nemen; dit is in veel gevallen oneigenlijk, moeilijk actueel te houden en beperkt bruikbaar (alleen voor beeldvorming).

informatie van de politie en partners structureel bij elkaar kan worden gebracht, geanalyseerd en gebruikt voor risicotaxatie en selectie voor PGA. Dit is echter landelijk nog geen gemeengoed.

In fase 3: Aanpak en interventies wordt door de politie het met de partners afgesproken plan van aanpak op een persoon vastgelegd in het hiervoor aangewezen monitoringssysteem Amazone. Hierin kan iedere politiecollega zien welke interventies de politie moet uitvoeren. Die kunnen liggen op het terrein van toezicht en handhaving, maar het kan ook gaan om opsporingsactiviteiten of het puur gericht zijn op informatie-inwinning. Uiteraard worden de resultaten en effecten van de interventies gedeeld met de partners. Nieuwe informatie wordt ingebracht en gewogen teneinde beslissingen te nemen over bijvoorbeeld bijstelling van de aanpak. In Amazone kan ook informatie worden vastgelegd in het kader van de Wet langdurig toezicht zedendelinquenten en (ernstige) geweldplegers.

Figuur 12.5 Aanpak en interventies in fase 3 PGA

12.2.4 Uitgangspunten IGP in relatie tot PGA

Informatiegestuurd politiewerk is een organisatiebreed principe, van waaruit steeds meer wordt gedacht en gewerkt. Briefing/debriefing is hiervan een mooi voorbeeld. Tegelijk wordt binnen de politie ook vaak vanuit veiligheidsproblemen gewerkt. Te denken valt aan huiselijk geweld, radicalisering, problematische jeugd, ook vaak ingegeven door politieke urgentie en prioritering.

Het doel is te werken volgens een geharmoniseerd en gestandaardiseerd werkproces voor de integrale aanpak van (alle) geprioriteerde doelgroepen. Hierbij is PGA het proces

om te komen tot een individuele aanpak. Dit is ongeacht tot welke aangewezen doelgroep dat individu behoort. Het gaat hierbij om een model dat op hoofdlijnen het proces beschrijft, en met voorbeelden inkleurt. De eerste veiligheidsthema's die via de methode PGA werden aangepakt, waren high impact crime (HIC), geweld en veelplegers. Je kunt de methode echter voor veel meer thema's gebruiken en die ontwikkeling is volop aan de gang. Er wordt gebruikgemaakt van een persoonsdossier: een dossier dat geautomatiseerd gegevens verzamelt uit diverse relevante systemen en deze in een standaard format presenteert.

Het PGA-proces verloopt als het ware als goed geleid verkeer over een netwerk van autosnelwegen. In plaats van voor iedere persoon of elk thema (zoals CTER of inbraken) een apart informatieproces (bypasses, lokale of secundaire wegen) te bouwen, kun je gebruikmaken van bestaande opritten. Of indien nodig een nieuwe oprit naar de bestaande snelweg maken. En alleen indien echt nodig, een aanvulling op het generieke informatieproces maken. Hierdoor staat het generieke IGP-proces van PGA steeds sterker, en functioneert het beter. Bovendien begrijpt iedereen elkaar, omdat dezelfde taal gesproken wordt en dezelfde verkeerssymbolen gebruikt worden. Daar hoort dan ook bij dat verkeersdeelnemers zich aan de verkeersregels houden: geen aantekeningen in de berm gooien, allemaal correct informatie vastleggen (het vastgestelde persoonsdossier gebruiken), en niet de bocht afsnijden. De voordelen zijn dan evident: het verkeer loopt beter door, er zijn minder investeringen nodig en het bespaart werk. *Lean and mean*: de DRIO's en de basisteams hebben al (te) veel op hun dagelijkse bord. Het PGA-proces bespaart gewoon tijd.

12.2.5 Uitgangspunten ZSM in relatie tot PGA

Binnen ZSM[8] is in toenemende mate sprake van individuele instroom in PGA. Bij iedere binnengekomen verdachte wordt door Intake & Screening bekeken of het incident/de zaak en de context van de verdachte moeten leiden tot verdieping dan wel snelle afdoening. In dit proces wordt in toenemende mate gebruikgemaakt van het (geautomatiseerd) persoonsdossier en risicotaxatie in overleg met partners. Dit is wel nog in ontwikkeling. Een binnengebrachte verdachte kan in het monitoringsysteem Amazone bekendstaan als geprioriteerd politiepersoon. Deze persoon moet binnen het ZSM-proces dan wel als zodanig herkend worden.

12.2.6 Tools beschikbaar voor uitvoering van PGA

Tools voor de PGA zijn:

- *Handreiking persoonsgerichte aanpak politie*; hierin staat de methode PGA (onder andere werkprocessen) beschreven, aangevuld met verdiepingsdocumenten.
- BVI Bluelist: een applicatie voor onder anderen PGA-specialisten en districtelijke informatieknooppunten (DIK) om personen die verantwoordelijk zijn voor bepaalde veiligheidsproblemen te selecteren en te prioriteren.

8 ZSM staat voor zorgvuldig, snel en op maat met betrekking tot het afdoeningstraject. Binnen ZSM wordt door OM, politie, reclassering, kinderbescherming, slachtofferhulp en hulpverlening nauw samengewerkt.

- Amazone: een informatiesysteem voor het monitoren van personen en (doel)groepen; waarin ook het plan van aanpak op een persoon vermeld is, zoals afgesproken in samenwerkingsverbanden met partners (Veiligheidshuis, Veilig Thuis enzovoort). Dit bevat dan in elk geval de politie-interventies (wat moet bijvoorbeeld een politieambtenaar doen die de betreffende persoon ziet, staande houdt of aanhoudt).
- Persoonsdossier: gegevens die geordend op één plaats worden opgeslagen over een persoon en zijn sociale/criminele omgeving; niet zijnde het zaaksdossier. Hieruit worden selecties gemaakt ten behoeve van verschillende doeleinden: aanmelding PGA'er, dossier PGA'er, ZSM, CTER.
- GECOS: informatiesysteem dat in veel Veiligheidshuizen wordt gebruikt ter ondersteuning van casusoverleggen.
- Interventiematrix: overzicht van beschikbare interventies van politie en partners, gericht op het effectief beïnvloeden van het gedrag van een persoon die in de PGA zit.
- Op politie-intranet en Kompol (Kennis op maat politie) zijn handreikingen en dergelijke te vinden.
- Filmpjes over PGA en over het Risicotaxatie-instrument Geweld zijn te vinden op YouTube:
  - filmpje PGA: http://youtu.be/q61iwM22Gg8;
  - filmpje RTI-Geweld: https://youtu.be/WnDVAD7hSKs.

Figuur 12.6 PGA-overleg

12.3 Risicotaxatie

Zoals beschreven is risicotaxatie een relevant onderdeel binnen het proces PGA. Door middel van risicotaxatie wordt een indicatie gegeven van de kans dat een persoon een delict gaat plegen of mogelijk een criminele carrière ontwikkelt. Ook worden handvatten geboden voor de aanpak, met als doel het voorkomen dat het feit gepleegd wordt.

Risicotaxatie helpt om risico's[9] in te schatten en in het prioriteren van personen die aangepakt moeten worden, waar vervolgens gericht op geïnvesteerd kan worden. Risicotaxatie moet altijd onderdeel uitmaken van organisatiebreed risicomanagement, waarbij doel en context voor risicotaxatie beschreven is en de behandeling van risico's gedefinieerd zijn. Zo kun je het PGA-proces ook zien als een vorm van risicomanagement. Een concrete interventie die daarbinnen past, is bijvoorbeeld het maken van afspraken over te monitoren zedendelinquenten die na detentie terugkeren in de maatschappij.

Een risicotaxatie-instrument is een risicobeoordelingsinstrument waarbij het gaat om:

- het identificeren, analyseren en evalueren/beoordelen van risico's;
- zodat op basis daarvan prioriteiten kunnen worden gesteld;
- en actie ondernomen kan worden.

Er zijn vier soorten risicotaxatie te onderscheiden. Deze komen in verschillende fasen van het PGA-proces aan bod:

1 *Ongestructureerd professioneel oordeel* – is informeel en subjectief en leunt sterk op de kennis en ervaring van de beoordelaar die geheel vrij is wat betreft de informatie die verzameld wordt en hoe deze te wegen. Vaak is dit het risico gebaseerd op het onderbuikgevoel van een politiecollega. Binnen PGA past deze in de kolom straatinformatie.
2 *Checklist* – gebruikt voor het identificeren van risico's, kan door iedereen gebruikt worden om een snelle inschatting te maken op basis van vastgestelde indicatoren. Bijvoorbeeld een checklist voor politiemensen op straat voor verwarde dreigers, om snel in te schatten wat de kans op escalatie is. Kennis in modellen (KIM) is een voorbeeld van een checklist voor radicalisering die wordt gehanteerd binnen een informatieknooppunt.
3 *Actuariële risicotaxatie* – dit is een vorm van geautomatiseerde risicotaxatie op basis van empirisch gevonden risicofactoren die verband houden met het voorspellen van probleemgedrag. Deze vorm van risicotaxatie is gebaseerd op statische factoren, vooral geschikt om risicogroepen te signaleren, en biedt geen basis voor de risicobehandeling. Bijvoorbeeld 'Prokid +', het Risicotaxatie-instrument Geweld[10] en het jeugdtaxatie-instrument Preselect. De genoemde (business intelligence) instrumenten worden gebruikt binnen de methode PGA bij het opstellen van de politienamenlijst om risico's van personen te taxeren.
4 *Gestructureerd professioneel oordeel (GPO)* – momenteel de meest gebruikte vorm van risicotaxatie binnen de forensische psychiatrie. GPO is een combinatie van de hiervoor genoemde vormen: de ervaren professional loopt een checklist met variabelen

9 Risico = waarschijnlijkheid x ernst (impact). Hier speelt ook de *fear factor* een rol. Als een zedendelinquent dreigt actief te worden, dan betekent dit niet alleen iets voor potentiële slachtoffers, maar dient er ook rekening gehouden te worden met de kans op maatschappelijke onrust onder bewoners van een gebied.

10 Van het Risicotaxatie-instrument Geweld wordt onderzocht of dit breder in de strafrechtketen gebruikt kan worden, zoals in ZSM.

langs waarvan op basis van wetenschappelijk onderzoek is aangetoond dat deze van belang zijn voor het inschatten van het risico van recidive, waarna de professional de variabelen weegt om tot zijn inschatting van het risico te komen. De grootste meerwaarde van de GPO-benadering van risicotaxatie ligt dan ook in de directe link met risicobehandeling. Immers: een gestructureerde risicotaxatie biedt inzicht in de statische en de dynamische, in principe veranderbare, risicofactoren voor het probleemgedrag, en daardoor onmiddellijk aanknopingspunten voor risicobehandeling. Deze vorm van risicotaxatie wordt met name gebruikt binnen het Landelijk Team Dreigingsmanagement voor een aantal hoog-geprioriteerde doelgroepen zoals jihadistische eenlingen.

12.3.1 Risico's

Het niet of niet correct toepassen van risicotaxatie kan tot gevolg hebben:

- Onnodige (dodelijke) slachtoffers, zoals de dood van Els Borst, gepleegd door een bekende, psychisch verwarde geweldpleger.
- Aansprakelijk stellen handelingsverlegen medewerkers, dan wel medewerkers die goed gebruik hebben gemaakt van risicotaxatie, maar bij wie er toch een foute classificatie uit is gerold.
- Afbreukrisico's politie (politiek en imago); de politie wordt verantwoordelijk gesteld voor onnodige slachtoffers, zeker als blijkt dat het om een gekende geweldpleger gaat. 'Waarom hebben jullie niet eerder ingegrepen?', kan de politie verweten worden.
- Radicalisering met dreiging van (ongekende) personen. Het niet of niet tijdig onderkennen van het risico op verregaande radicalisering met mogelijke terreurdaden tot gevolg.
- Stigmatisering en etnisch profileren. Het uitgaan van vooroordelen ten aanzien van personen en op basis hiervan risico's inschatten.
- Onvoldoende aansluiting bij ketenpartners waar ontwikkeling en gebruik van risicotaxatie-instrumenten al verder ingericht zijn.
- Wildgroei en overlap risicotaxatie-instrumenten en daarmee samenhangende operationele risico's, ineffectiviteit in ontwikkeling, beheer en onderhoud van deze instrumenten aan zowel de organisatie- als de informatievoorzieningskant.

Het toepassen van risicotaxatie betekent niet dat dit per definitie tot de goede uitkomst leidt. Risicotaxatie is gebaseerd op informatie die beschikbaar is, dan wel die we beschikbaar kunnen krijgen. Een hoge taxatie betekent in principe een hoge kans op geweld, maar er kan een foutmarge in zitten en het blijft mensenwerk. Een lage taxatie betekent idem niet per definitie dat er een lage kans is op geweld. Het kan zomaar zijn dat relevante informatie, die zou leiden tot een hogere taxatie, ontbreekt in het beschikbare dossier. Het is dus goed te beseffen dat, ook bij gebruik van risicotaxatie, iemand ten onrechte als risicovol dan wel onterecht als niet-risicovol kan worden geclassificeerd. Tegelijkertijd weten we ook dat we zonder gebruik van gevalideerde instrumenten veel meer van deze fouten maken.

Figuur 12.7 Risicotaxatie

De politieorganisatie en haar leidinggevenden moeten zich rekenschap geven van deze foutkansen en achter de medewerkers staan aan wie een foute classificatie niet verweten kan worden. Van belang is dat medewerkers beschikken over de juiste gevalideerde tools, dat ze risicotaxatie goed kunnen toepassen. Dan zullen we moeten accepteren dat er, met de beschikbare informatie op een zeker moment, met behulp van risicotaxatie een bepaalde classificatie uit kan rollen met bijpassend handelingsperspectief. Dat dit niet altijd tot het juiste resultaat leidt, moeten we incalculeren.

12.3.2 Vraagtekens

Het inschatten van risico's is van alle tijden. Recent echter heeft dit een grote vlucht genomen, vanwege de maatschappelijke dynamiek waarbinnen we risico's willen indammen en door de technologie om grote hoeveelheden data geautomatiseerd te analyseren. Binnen de politie wordt er volop gebruik van gemaakt, maar er bestaat een aantal dilemma's en vraagtekens:

- Beschikken we wel over de juiste informatie en tools om risico's goed in te schatten? Zijn de gebruikte taxatie-instrumenten voldoende bekend bij politiemensen, zijn ze wel gevalideerd, gebruiken we de juiste tools op de juiste niveaus? Sturen we voldoende op de benodigde informatie, waarover we als politie, dan wel onze partners kunnen beschikken, zodat we een betere taxatie kunnen doen?
- Hoe zit het met de ethische kant van dit vraagstuk? Kunnen we zomaar iemand labelen als risicovol, wat betekent dit voor de maatregelen die we als politie en in samenwerking met ketenpartners treffen, en wat is de impact hiervan op een persoon? Een

voorbeeld is radicalisering: iemand die een hoog-risicovol persoon lijkt, kan bijvoorbeeld niet met het vliegtuig reizen, omdat we deze persoon signaleren als potentiële uitreiziger dan wel terrorist. Ander voorbeeld: een jeugdige persoon over wie zorg bestond; krijgt deze een stigma op basis van verwachtingen?

- Hoe zit het met de samenhang van alle tools die we inzetten en werken we wel eensluidend samen om risico's te minimaliseren? Weet de wijkagent wel dat er op eenheidsniveau dan wel landelijk een taxatietraject loopt op een persoon uit zijn wijk en welke tools of kennis heeft deze wijkagent om zelf een eerste inschatting te kunnen maken?
- Risico's inschatten moet niet een heel traag proces worden, de problematiek waar de politie mee te maken heeft, vraagt om snelheid. Politiemensen in alle gelederen moeten zich bewust zijn, dan wel bewust worden gemaakt, van risico's, zodat zij de juiste beslissingen kunnen nemen. Hoe kunnen zij over de juiste ingrediënten beschikken om tot goede en snelle (real-time) oordeelsvorming en besluitvorming te komen? En wanneer is het tijd voor de specialist?
- Risicotaxatie is een iteratief proces, nieuwe informatie kan zorgen voor een andere uitkomst van de taxatie; de gebruikers dienen zich hier voldoende bewust van te zijn.
- Het komt voor dat risicotaxatie-instrumenten naast elkaar ontwikkeld worden. Voorafgaand aan de ontwikkeling van een nieuw instrument wordt (in- en extern) te weinig stilgestaan bij nut en noodzaak. Een sluitend overzicht van instrumenten ontbreekt.
- Veel informatie ligt bij partners, hoe komen politie en partners samen tot het delen van deze informatie en tot een juiste risicotaxatie? Wat is hierin de rol van de informatieorganisatie?

12.3.3 Toekomst

Er dienen zich steeds meer mogelijkheden aan om het gebruik van risicotaxatie-instrumenten te verbeteren. Er is meer dan voorheen praktisch bruikbare wetenschappelijke kennis beschikbaar om risico's door en voor specifieke doelgroepen in te schatten. Uitvoering van de business-intelligencestrategie zorgt ervoor dat steeds meer informatie integraal beschikbaar is voor risicotaxatie. Actief gebruik van *data science* en zogenoemde 'fuzzy' zoektechnieken voor taxatie gaan een boost geven aan de ontwikkeling van risicotaxatie. Als gevolg daarvan zal wetenschappelijke kennis sneller ingebouwd kunnen worden. En de politiefunctionarissen aan de balie en op straat zullen kunnen beschikken over voldoende kennis om alert te kunnen handelen, met back-up van de informatieorganisatie.

Deel IV
De werking van IGP: informatie verzamelen en delen

13 Informatiegestuurd werken en samenwerkingsrelaties

Marjolein van Tunen-Geldermans, Carl Spruijt en Rutger Rienks

13.1 Inleiding

We leven in een netwerkmaatschappij. Mensen, bedrijven, overheidsorganisaties zijn via netwerken met elkaar verbonden. Hightech wordt gecommuniceerd en *hightouch* wordt open met elkaar informatie en kennis overgedragen. Nederland is in deze netwerkmaatschappij een veilig land waar symptoombestrijding vaker plaats moet maken voor een doel- en effectgerichte aanpak van veiligheidsproblemen. Dit kan alleen door een integrale aanpak en samenwerking met netwerkpartners, zowel tussen opsporings- en overheidsinstanties onderling als tussen overheidsinstanties, het bedrijfsleven en burgers.

Figuur 13.1 De driehoek

Naast de politie is er een enorm palet aan spelers dat een bijdrage levert aan veiligheid in onze samenleving. Nieuwe partnerships dienen zich aan, zoals sociale wijkteams, Veilig Thuis en lokale overleggen persoonsgerichte aanpak (PGA) en bestaande samenwerkingsverbanden als veiligheidshuizen, het Regionaal Informatie- en Expertisecentrum (RIEC) en ZSM[1]. Gemeenten krijgen steeds meer verantwoordelijkheden op het gebied van veiligheid. Zij werken hierbij samen met andere organisaties en met burgers, en nemen steeds vaker de organiserende of regisserende rol over van bijvoorbeeld het Openbaar Ministerie en de politie. Bestuurlijke handhaving, alsmede bestuurlijke aanpak van georganiseerde

1 ZSM staat voor zorgvuldig, snel en op maat met betrekking tot het afdoeningstraject. Binnen ZSM wordt door OM, politie, reclassering, kinderbescherming, slachtofferhulp en hulpverlening nauw samengewerkt.

criminaliteit worden steeds belangrijker. Bestuurlijke handhaving wordt in toenemende mate gebruikt als instrument om openbare-ordeverstoring te voorkomen en aantasting van het woon- en leefklimaat te bestrijden. Steeds meer gemeenten investeren in de inzet van gemeentelijke buitengewoon opsporingsambtenaren (boa's), aangevuld met private beveiligingsbedrijven, handhavings- en interventieteams. Informatie ten behoeve van het beïnvloeden van veiligheidsproblemen is bij gemeenten naar inschatting meer aanwezig dan bij de politie, zeker als we daar informatie over jeugdigen (leerplicht) en bijvoorbeeld kindermishandeling en huiselijk geweld bij optellen.

In een netwerkmaatschappij dragen bovendien allerlei belangenorganisaties, bedrijven en ook burgers zelf steeds vaker actief bij. Burgers organiseren zichzelf in allerlei (kleinschalige) vormen zoals buurtwhatsappgroepen. Private organisaties nemen meer hun maatschappelijke verantwoordelijkheid en luisteren steeds meer en beter naar de burgers.

Ook internationaal wordt samenwerking steeds belangrijker. 'Verre' problemen manifesteren zich op lokaal niveau: 'glocalisering' lijkt een nieuw begrip te worden, zoals het CTER-, migratie- en daaraan ook verbonden polarisatievraagstuk. Een virtuele digitale wereld en ook een virtuele digitale werkelijkheid. De uitspraak van een rechter in de Verenigde Staten veroorzaakt bergen aan informatie over kinderpornografie in Nederland, omdat Amerikaanse providers een meldplicht krijgen.

In samenwerking met de lokale overheid en vele andere partners binnen het brede veiligheidsdomein zijn partners in staat om veiligheids- en leefbaarheidsvraagstukken vanuit ieders specifieke focus en deskundigheid te benaderen en mee te helpen in het vinden van integrale en bestendige oplossingen. Van preventie tot repressie, van beleid tot uitvoering, over de gehele linie werken verschillende instanties, branches en burgers samen aan een veilig Nederland. De samenwerking in het veiligheidsdomein krijgt vaak inhoud langs de lijn van informatie-uitwisseling, een belangrijke dimensie bij informatiegestuurd politiewerk.

Met verschillende van deze spelers heeft de politie *partnerships*, bondgenootschappen op basis van een structurele samenwerking. We beperken ons in dit hoofdstuk tot slechts een paar partnerships, in de wetenschap dat we andere partners tekortdoen. Het concentreert zich met name op de samenwerkingsvormen met de gemeenten, het Openbaar Ministerie (OM) en het RIEC.

13.2 Waarom partnerships?

13.2.1 Bedoeling

Het besef dat veiligheidsproblemen vaak meervoudige problemen zijn met meervoudige oorzaken, en daarmee integrale oplossingen vragen, is steeds breder aanwezig. Wetenschappelijk criminologisch onderzoek en evaluaties van praktijktoepassingen ondersteunen niet alleen dat besef, ze tonen de effectiviteit van integrale aanpak daadwerkelijk aan. Zo is in april 2016 de tussenevaluatie van de ZSM-methode uitgebracht. De conclusie 'dat niemand terug wil naar de situatie voorafgaand aan de ZSM-werkwijze', zegt veel.

Veiligheidspartners passen die integrale aanpak dus steeds vaker en ook beter toe. Plegers van criminaliteit krijgen vaak al op jonge leeftijd integrale aandacht om recidive te beperken. Uit ervaring van wijkteams blijkt dat de lokale aanpak van jeugd in relatie tot veiligheid effectief is. Dat het sociaal domein daarbij een belangrijke bijdrage levert, is alom onderkend. De Raad voor Strafrechtstoepassing en Jeugdbescherming (RSJ) bevestigt dat besef met de *Visie op strafrechtelijke sanctietoepassing*.[2] Een beschouwing door Fijnaut en Rovers over de aanpak van overvallen en overvallers[3] geeft een vergelijkbare conclusie over het sociaal domein, maar maakt ook duidelijk dat vergelding via strafrecht nodig zal blijven.

Het strafrecht als 'optimum remedium' – het optimaal inzetten van opsporing in samenhang met andere instrumenten – krijgt steeds meer navolging. Die term optimum remedium hanteert de minister van Veiligheid en Justitie in juli 2016 in een brief aan de Tweede Kamer bij de tussenevaluatie *Snel, betekenisvol en zorgvuldig* over de ZSM-werkwijze. Die term wordt soms ook gebruikt bij het hanteren van de ISD-maatregel, de plaatsing in een inrichting voor stelselmatige daders. Eind 2014 noemde de minister van Veiligheid en Justitie strafrecht als optimum remedium in de integrale aanpak bij fraudebestrijding. In de eerste editie van de *Fraudemonitor 2015*, uitgebracht door het OM op 12 september 2016, staat dit uitgangspunt centraal. Zo veel mogelijk civiele en bestuurlijke barrières opwerpen, met strafrecht als vergeldingsmiddel waar dat echt wat toevoegt. Tegelijkertijd zien we dat ook bij executie en sanctie-uitvoering het multidisciplinair kader wordt omarmd.[4]

Op basis van elkaars signalen kunnen partijen effectiever werken. Ook kunnen partijen op basis van verschillende bevoegdheden elkaar in de operatie versterken. Bijvoorbeeld bij integrale verkeerscontroles kan een douanebeambte een kofferbak openen op basis van de Douanewet. Een politiemedewerker mag dit alleen als de burgemeester dat gebied als veiligheidsrisicogebied heeft aangewezen. De vraag die zich hier opdringt, is natuurlijk voor welk doel die kofferbak open moet. Zeker als er nog geen sprake is van een verdenking, is het vanuit het burgerperspectief maar goed ook dat alle instanties niet zomaar alles kunnen en mogen. Voor levensbedreigende situaties en de bestrijding van zware georganiseerde criminaliteit kan in theorie dezelfde discussie gevoerd worden. Hier is de kracht van samenwerking niet bedreigend, maar eerder een zegen. Het behoedt de samenleving voor kwaad doordat het sneller en effectiever bestreden kan worden waarbij iedereen onderdeel is van een groter geheel.

De verwachting is dat de hiervoor genoemde integrale aanpak leidt tot het ontstaan en behoud van vertrouwen bij de burger, doordat interventies criminaliteit voorkomen,

---

2 Raad voor Strafrechtstoepassing en Jeugdbescherming, *Visie op strafrechtelijke sanctietoepassing: versterken van samenhang, betrokkenheid en vertrouwen*. Raad voor Strafrechtstoepassing en Jeugdbescherming, Den Haag 2016.

3 Rovers, B. & C. Fijnaut, *De aanpak van overvallen en overvallers in de jaren 2011-2016: een gegronde beschouwing over de resultaten en vooruitzichten*. Ministerie van Veiligheid en Justitie/BVTO, Den Haag 2016.

4 Ministerie van Veiligheid en Justitie, *Koers en kansen voor de sanctie-uitvoering*. Ministerie van Veiligheid en Justitie, Den Haag 2016.

bestrijden en sanctioneren op een wijze die effect en betekenis heeft voor slachtoffer, verdachte en maatschappij. En dit vertrouwen is noodzakelijk voor de legitimiteit van het optreden. Met misschien wel het ultieme doel dat de burger de veiligheidsvraagstukken in het gezin en in de wijk zo veel mogelijk op eigen kracht aankan.[5]

13.2.2 Richtinggevende kaders

In samenwerkingsvormen is het van belang te weten wat de spelregels zijn die zijn vastgelegd (kaders) en welke werkwijze het meest effectief is. Allereerst bespreken we een aantal kaders, te weten die van het *Inrichtingsplan Nationale Politie* en de prioriteiten in veiligheidsthema's.

Inrichtingsplan Nationale Politie

Het *Inrichtingsplan Nationale Politie* geeft uitgangspunten voor partnerships mee:

- De politie zoekt actief contact, geeft inzicht in veiligheidsvraagstukken, ondersteunt initiatieven van anderen en participeert daarin. De politie signaleert en adviseert partners en burgers vanuit haar bijzondere informatiepositie. Daarbij wordt zo veel als mogelijk aangesloten op de lokale situatie.
- De politie participeert zowel actief in externe netwerken en samenwerkingsverbanden zoals de Veiligheidshuizen, de Regionale Informatie- en Expertisecentra en het Landelijk Informatie- en Expertisecentrum (RIEC/LIEC) en de veiligheidsregio, als in interne netwerken. Aansluiting 'van binnen naar buiten' en 'van buiten naar binnen' is cruciaal.
- De politie zet in op de integrale aanpak van veiligheidsproblemen en deelt de politieinformatie met het gezag en partners, binnen de wettelijke kaders, en ondersteunt waar nodig bij het opstellen van de integrale gemeentelijke veiligheidsplannen en in samenwerking met Veiligheidshuizen en andere allianties.
- Binnen het korps zijn heldere sturingslijnen en is duidelijk wie verantwoordelijk is voor de inzet en het optreden van politiemedewerkers en het resultaat daarvan. Verantwoordelijkheden en bevoegdheden worden daar belegd waar de aanpak van de veiligheidsproblematiek plaatsvindt. Het effect van de aanpak staat daarbij centraal en niet de organisatiestructuur.
- De politie werkt zo veel mogelijk volgens gestandaardiseerde processen en op basis van kwaliteitscriteria, zonder afbreuk te doen aan de professionele ruimte van de medewerker en het noodzakelijke maatwerk voor specifieke taken.
- De politie is een flexibele organisatie. In bijzondere situaties is de politie snel en met extra capaciteit, kennis en middelen ter plaatse. Dit kan de vorm aannemen van (horizontale) samenwerking of (verticale) opschaling. De politie organiseert haar personele en materiële capaciteit op een zodanige wijze dat deze flexibel inzetbaar is.

Werkingsdocumenten, geschreven nadat het *Inrichtingsplan Nationale Politie* openbaar werd, zijn eveneens richtinggevende kaders. Vanuit de portefeuille Ketensamenwerking &

5 Bron: werkingsdocument *Districten & Basisteams*, 2016.

Strategische Allianties – mei 2015 – zal het beleid worden vormgegeven langs de volgende lijnen:

1 strategische verkenningen;
2 stakeholdermanagement en relatiebeheer;
3 inzicht en overzicht;
4 cultuur, leiderschap en gedrag;
5 operationele netwerkgerichte strategieën.

In oktober 2016 is een aangepast werkingsdocument *Districten en Basisteams* geschreven, waarin samenwerking met partners duidelijk aan bod komt.[6] In de Herijkingsnota van de politie[7] staan aanpassingen op de districten en basisteams, in samenhang met meer sturing en maatwerk op lokaal niveau.

Prioriteiten in veiligheidsthema's en dus in partners

Periodiek bepaalt de minister van Veiligheid en Justitie, samen met het bestuur, OM en politie de landelijke en regionale prioriteiten in een veiligheidsagenda.[8] In die agenda staan niet alleen de thema's, maar ook specifieke instrumenten, partnerships en te behalen resultaten. Op regionaal niveau komen die landelijke prioriteiten terug, aangevuld met of soms in plaats van regionale prioriteiten. Op lokaal niveau komen die landelijke en regionale prioriteiten ook terug, maar weer aangevuld met ook lokale prioriteiten op veiligheid en overlast.

De prioriteiten bepalen mede de partners met wie de politie samenwerkt. Uiteraard de natuurlijke partners OM, gemeenten en reclassering. Maar ook bijvoorbeeld ondernemers in het Regionaal Platform Criminaliteitsbeheersing, de burgers via buurtwhatsapp, en de geestelijke gezondheidszorg bij de aanpak van personen met verward gedrag.

13.3 Voorbeelden van partnerships

13.3.1 RIEC-LIEC

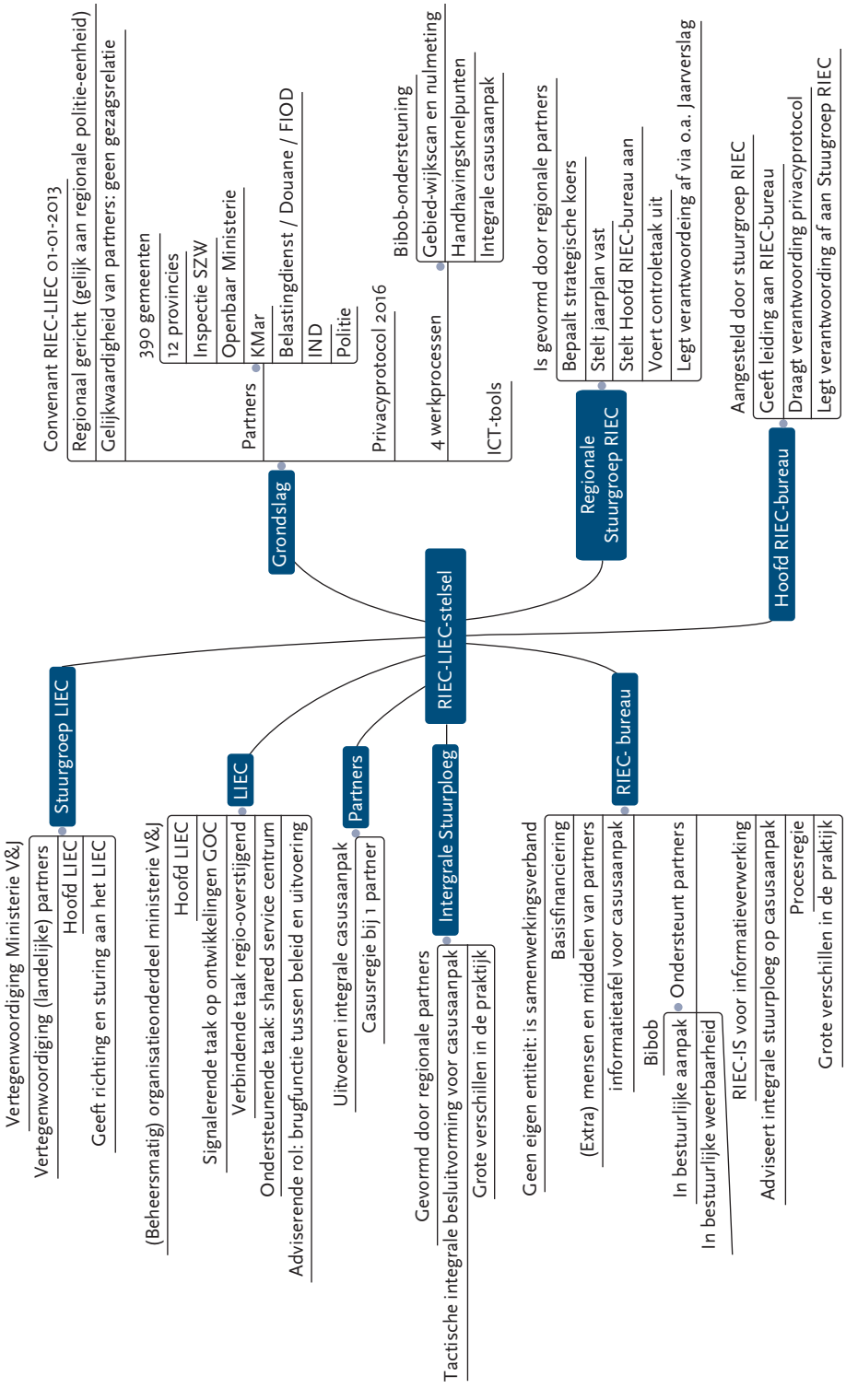
Per 1 januari 2013 is het landelijk convenant RIEC-LIEC van kracht. Eerdere regionale convenanten zijn daarbij vervallen. Dit convenant is een belangrijke grondslag om de Georganiseerde en Ondermijnende Criminaliteit (GOC) te bestrijden. Het convenant wordt ook wel het RIEC-LIEC-stelsel genoemd omdat er diverse deelnemende partners, rollen, beslismomenten en integrale beslissers zijn. In figuur 13.2 is het stelsel uitgelegd. De site www.riec.nl geeft veel achterliggende informatie.

---

6 Werkingsdocument *Districten & Basisteams*, oktober 2016.

7 Ministerie van Veiligheid en Justitie, *Herijkingsnota: herijking realisatie van de nationale politie*. Ministerie van Veiligheid en Justitie, Den Haag 2015.

8 Ministerie van Veiligheid en Justitie, *Veiligheidsagenda 2015-2018*. Ministerie van Veiligheid en Justitie, Den Haag 2014.



Figuur 13.2 RIEC-LIEC-stelsel

De doelstelling van het RIEC-LIEC-convenant is vierledig:

1 bestuurlijke en geïntegreerde aanpak van georganiseerde criminaliteit;
2 identificeren van gelegenheidsstructuren die vatbaar zijn voor beïnvloeding door de georganiseerde criminaliteit, en het voorkomen dat de georganiseerde criminaliteit bewust of onbewust wordt gefaciliteerd door de overheid en daardoor de democratische rechtsstaat wordt ondermijnd;
3 bestrijding handhavingsknelpunten;
4 bevordering integriteitsbeoordelingen (Wet Bibob).[9]

Het convenant benoemt verschijningsvormen van GOC zoals mensenhandel, witwassen en georganiseerde hennepteelt. De regionale stuurgroep RIEC kan meer verschijningsvormen van GOC noemen om bestuurlijk en integraal aan te pakken, zoals verschijningsvormen van handhavingsknelpunten.[10]

RIEC-LIEC en outlaw motor gangs (OMG's)

De 'good practice' OMG's helpt om de RIEC-LIEC-theorie vanuit de praktijk te laten zien. De betrokkenheid bij criminele en ondermijnende activiteiten door OMG's, in combinatie met toegenomen risico's van escalaties en verstoringen van de openbare orde als gevolg van de sterke groei van deze clubs, vormt in 2012 de aanleiding om te starten met een landelijke programmatische integrale aanpak. De aard van de aanpak is strafrechtelijk, bestuurlijk en fiscaal. Uitgangspunt is het doorbreken van het imago van de onaantastbaarheid van OMG's door het verminderen van hun slagkracht. Geprioriteerde probleemgebieden op het gebied van ondermijnende criminaliteit, normoverschrijdend gedrag en de belemmering van overheidsoptreden zijn vertaald naar acht concrete speerpunten:

1 prioriteit strafrechtelijke aanpak van OMG's en hun leden;
2 handhaving van regels voor clubhuizen;
3 tegengaan verwevenheid invloed OMG's in de horeca;
4 tegengaan verwevenheid invloed OMG's in de beveiligingsbranche;
5 tegengaan verwevenheid van OMG's met harde kern voetbalsupporters;
6 niet faciliteren van evenementen van OMG's;
7 aanpakken windhappers;
8 focus op leden OMG's in overheidsdienst.

>>

9 De Wet Bibob is een (preventief) bestuursrechtelijk instrument. Als er een gevaar dreigt dat bijvoorbeeld een vergunning wordt misbruikt, kan het bevoegde bestuursorgaan de aanvraag weigeren of de afgegeven vergunning intrekken. Zo wordt voorkomen dat de overheid criminele activiteiten faciliteert en wordt bovendien de concurrentiepositie van bonafide ondernemingen beschermd.

10 Verschijningsvormen van handhavingsknelpunten zijn bijvoorbeeld industrieterreinen waar veel mis is, of vakantieparken waar criminelen zich schuilhouden en wijken waar criminele families de dienst uitmaken. Soms is sprake van 'vrijplaatsen', een ondermijnende situatie omdat criminelen vrij spel hebben en de samenleving haarfijn aanvoelt dat de overheid 'onmachtig' is.

>> De integrale samenwerking krijgt vorm in de faciliterende rol van de RIEC's en het LIEC. In de structuur van het RIEC-LIEC-stelsel brengen de partners informatie samen in het informatieplein, ze maken gezamenlijk afwegingen over de te voeren strategie, stellen integrale handhavingsacties op en monitoren de integrale voortgang en effecten. Het Landelijk Strategisch Overleg (LSO) OMG's, voorgezeten door een burgemeester, bepaalt de strategie. Elke maand is er overleg van de Landelijke Werkgroep OMG's. Periodiek rapporteert het LSO OMG's over de acht speerpunten aan de partners en de minister van Veiligheid en Justitie. Veel kennis wordt opgedaan, handreikingen worden gemaakt, het bestuur wordt ondersteund. De minister van Veiligheid en Justitie rapporteert periodiek aan de Tweede Kamer, waarbij diverse bijlagen, opgemaakt door onder andere het LIEC, worden meegezonden. Overzicht, inzicht en de context in deze integrale OMG-problematiek zijn ruimschoots en gedetailleerd aanwezig. In 2016 is deze integrale aanpak van OMG's op basis van opgedane ervaringen[11] verder aangescherpt.[12] Burgemeesters pleiten voor een verbod op motorbendes.[13]

13.3.2 De verbindingen van zorg en veiligheid: Veiligheidshuizen

Veiligheidshuizen zijn gericht op strafrecht, bestuursrecht, zorg en toezicht en kennen een brede aanpak, zowel persoonsgericht en groepsgericht als gebiedsgericht. De focus van de Veiligheidshuizen ligt op de aanpak respectievelijk het voorkomen van zogenoemde multicomplexe casussen. De politie is een vaste partner in het Veiligheidshuis. Ze speelt een belangrijke rol in de verbinding tussen preventie, repressie en zorg. Als partner in het Veiligheidshuis levert de politie op verschillende niveaus een bijdrage:[14]

- *Strategisch niveau*: de portefeuillehouder Veiligheidshuizen (Vhh) neemt deel aan de regionale stuurgroepen en draagt bij aan het strategisch kader hiervan.
- *Tactisch niveau*: de operationeel specialist van de districtsrecherche heeft een coördinerende rol op beleidsmatig en teamoverstijgend niveau.
- *Operationeel niveau*: De operationeel specialist van het basisteam ontvangt vanuit het Veiligheidshuis een lijst van geagendeerde personen. Hij vraagt waar nodig informatie op binnen de Dienst Regionale Informatieorganisatie (DRIO). Vervolgens coördineert deze specialist welke collega bij welk overleg aanschuift. Hij kan zelf aanschuiven of een operationeel expert vragen aan het casusoverleg deel te nemen.

In samenwerking met landelijke partners is gewerkt aan het in beeld krijgen van de informatiedelingsmomenten voor het maken van een integraal plan van aanpak op persoonsniveau. Geïnventariseerd is welke informatie op welk moment in het proces

---

11 RIEC-LIEC, *Integrale landelijke voortgangsrapportage Outlaw Motorcycle Gangs (OMG's)*. RIEC-LIEC, Den Haag 2015.

12 Minister van Veiligheid en Justitie, *Kabinetsstandpunt verbod OMG's en voortgang aanpak OMG's*. Ministerie van Veiligheid en Justitie, Den Haag 2016.

13 *Eén Vandaag* Opiniepanel Onderzoek onder burgemeesters: overlast en aanpak motorbendes. 2016.

14 *Politie in Veiligheidshuizen: hoe werkt dat?* Werkingsdocument december 2014.

noodzakelijk is (aanmelding-triage-casusoverleg-afhandeling). Tevens is gerubriceerd welke organisatie eigenaar is van die informatie en dus leverancier. Dit betekent voor de politie dat bijvoorbeeld informatie over schoolverzuim wordt geleverd door de leerplichtambtenaar en niet uit de politiesystemen. Iets dergelijks geldt voor over de geestelijke gezondheidstoestand: die wordt opgevraagd bij de regionale ggz-instelling. De belangrijkste kracht is dat de producten door de partners in gezamenlijkheid zijn ontwikkeld én dat de kanteling is gemaakt naar 'delen, tenzij'. Ten slotte wordt gewerkt aan een digitale tool voor degenen die in de praktijk met het gezin of de persoon aan het werk zijn, zodat wat er kan en wat er mag in een bepaalde casus voor elke organisatie raadpleegbaar is. Beoogd effect hiervan is dat privacydiscussies aan tafel eenvoudig beëindigd kunnen worden.

Figuur 13.3 Integraal partneroverleg

13.3.3 Conflict- en crisisbeheersing

Gecoördineerde Regionale Incidentbestrijdingsprocedure (GRIP) is de naam van de werkwijze waarmee bepaald wordt hoe de coördinatie tussen hulpverleningsdiensten verloopt. GRIP is een bestuurlijke opschaling en kent verschillende niveaus.

Bij GRIP1 gaat het om een incident waarbij goede afstemming tussen de hulpdiensten noodzakelijk is. De officieren van dienst van brandweer, politie en ambulance/GHOR vormen samen met een persvoorlichter van de politie en een voorzitter het Commando Plaats Incident (CoPI). Indien er door het incident ook gevolgen zijn voor de omgeving en er een effectgebied aan te wijzen is, spreken we van GRIP2. Nu komt naast het CoPI ook het Regionaal Operationeel Team (ROT) bijeen onder leiding van een 'ontkleurde' voorzitter. Bij een gemeentelijke ramp wordt GRIP3 afgekondigd. Het volledige ROT en het Gemeentelijk Beleidsteam (GBT) komen bijeen. De hulpverleningsdiensten (brandweer, politie, GHOR) bemensen hun actiecentra en in de desbetreffende gemeente wordt het Gemeentelijk Rampenmanagementteam (GRMT) bij elkaar geroepen om de gemeentelijke processen uit te voeren, zoals de opvang en verzorging van evacués en het registreren van slachtoffers.

Er is sprake van GRIP4 wanneer meerdere gemeenten in een veiligheidsregio betrokken zijn bij of getroffen worden door een ramp. Er wordt een Regionaal Beleidsteam (RBT) gevormd dat onder voorzitterschap staat van een coördinerend burgemeester. Indien er meerdere veiligheidsregio's getroffen zijn, spreken we van GRIP5. Hierbij worden meerdere ROT's gevormd, waarvan er een ook een coördinerende rol vervult. GRIP Rijk wordt gebruikt wanneer er behoefte is aan sturing door het Rijk in situaties waarin de nationale veiligheid in het geding is óf kan zijn. Inhoudelijk is GRIP Rijk veelal hetzelfde als GRIP5, echter het bevoegd gezag ligt nu bij de ministers en de Ministeriële Commissie Crisisbeheersing (MCCb).

13.3.4 Andere voorbeelden

De regionale en lokale driehoek: uitbreiden naar een vierhoek?

De lokale driehoek bepaalt vooral de lokale aanpak van veiligheidsproblemen. De agenda is opgebouwd uit landelijke veiligheidsprioriteiten, gecombineerd met lokale en regionale veiligheidsvraagstukken. Vanuit het groeiend inzicht dat veel problemen zijn gebaat met een (persoongerichte/gezins)aanpak vanuit civiel, bestuur, zorg en straf, zie je op steeds meer plaatsen dat de driehoek wordt aangevuld met de gemeentelijke portefeuillehouder zorg/welzijn – van driehoek naar vierkant.

Op eenheidsniveau bestaat de mogelijkheid op te schalen naar een van de tien veiligheidsregio's met tien regionale driehoeken. Elke regio heeft een regioburgemeester, ondersteund door een Bureau Regioburgemeesters. De website www.regioburgemeesters.nl is erg informatief. Zo is daar te lezen dat diverse regio's veiligheidsallianties hebben gesloten met externe partners. Het Regionaal Platform Criminaliteitsbeheersing is daar een voorbeeld van. Verantwoording over het beleid is te vinden in de regionale (integrale) jaarverslagen.

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)

De NCTV bepaalt voor een groot deel het nationale beleid op het terrein van CTER, cybersecurity en crisisbeheersing. Het Stelsel Bewaken en Beveiligen vormt daar onderdeel van. Sturing op de uitvoering van dat beleid vindt echter veelal plaats in de driehoeken. De CTER-aanpak gebeurt bij uitstek door partnerships, evenals de aanpak van cybercrime en cybersecurity. De politie draagt bijvoorbeeld nadrukkelijk bij aan het periodiek maken van het Dreigingsbeeld Terrorisme Nederland.

13.4 Voorwaarden voor partnerships

Contextgedreven werken

Met het besef en de mindset van een meer integrale aanpak van veiligheidsproblemen en intensieve informatie-uitwisseling met partners, ontstaat ook een meer contextgedreven aanpak. Wat zijn de problemen, wat zijn de oorzaken van problemen, welke instrumenten zijn er en door wie zijn die het best in te zetten om zo veel mogelijk effect te hebben bij de bestrijding van die problemen?

Veiligheidsanalyses

Het maken van veiligheidsanalyses is geen makkelijke opgave. Analyses zijn veelal nog gericht op de minder zware en vaak zichtbare criminaliteit en overlast. Meldingen en aangiften vormen daarvoor een belangrijke basis. Verschijningsvormen van de georganiseerde en ondermijnende vormen van criminaliteit kenmerken zich vaak door het ontbreken van aangiften. In het verleden werd wel gesproken over slachtofferloze delicten, maar dat klopt zeker niet. Denk aan mensenhandel en uitbuiting waarbij slachtoffers vaak geen aangifte kunnen doen of zich zelfs geen slachtoffer voelen.

Soms zijn verschijningsvormen van georganiseerde criminaliteit voor mensen in de samenleving juist van positief belang. Denk bijvoorbeeld aan de hennepteelt die financieel gunstig is 'voor minder draagkrachtigen', maar ook grote risico's kent als die 'georganiseerd' wordt aangestuurd. Crimineel geld is soms ongemerkt geïnvesteerd in de bovenwereld, waardoor de crimineel juist als positief en maatschappelijk betrokken te boek staat, bijvoorbeeld in een sportclub.

Gebruik van informatie van partners kan een deel van de oplossing zijn om betere veiligheidsbeelden te maken. Steeds meer organisaties, zoals gemeenten, maken ook eigen veiligheidsbeelden. Gemeenten beschikken wellicht over meer veiligheidsinformatie dan de politie. Gezamenlijk vraagt dat extra denkkracht, inzicht, speurwerk en nieuwe slimme tools om integraal en contextgericht veiligheidsbeelden te kunnen maken en duiding te geven voor een effectieve aanpak. Met namen en rugnummers door vertaling naar concrete maatregelen voor een integrale en persoonsgerichte aanpak.

Goede informatievoorziening

De politie is in het brede palet van veiligheidspartners een bijzondere speler. Bijna alle veiligheidsproblemen kruisen het pad van de politie. Misschien wel de belangrijkste randvoorwaarde voor integraal samenwerken door de politie is het op orde hebben van de eigen informatievoorziening. Niet alleen in technische zin, maar vooral met een kwantitatief en kwalitatief goed gevuld politieregister als basis (zie ook hoofdstuk 9 Waar kwaliteit toe leidt over kwaliteit en hoofdstuk 22 De business-intelligencestrategie in de politiepraktijk).

Als het gaat over samenwerking tussen verschillende organisaties en het zinvol acteren op basis van informatie, valt op dat met name in het meldkamerdomein (brandweer, politie en GHOR) de incidentbestrijding goed georganiseerd is. Informatiedeling tussen partijen verloopt via een geïntegreerd meldkamersysteem (GMS) waarmee men snel van elkaar weet wat er speelt en er adequaat kan worden opgetreden.

De samenwerkingsverbanden RIEC, Veiligheidshuis, Veilig Thuis, wijkteams en ZSM zijn geen zelfstandige entiteiten. Dit betekent dat er geen informatie verstrekt wordt aan 'het Veiligheidshuis, wijkteam of RIEC', maar aan de partner die de casus heeft aangevoerd en deze in het samenwerkingsverband wil bespreken.

De uitleg van de van toepassing zijnde wet- en regelgeving door de verschillende partners is niet altijd eenduidig en leidt in de praktijk nogal eens tot discussie (zie ook hoofdstuk 5 De Wpg). Of omdat het echt niet mag en daar geen begrip voor is, of omdat men

niet weet of het mag en het daarom niet doet. Het opstellen van convenanten en privacyprotocollen helpt hierbij.

Generalisten en specialisten werken samen

Informatiegestuurd werken aan de integrale aanpak van ketenoverstijgende vraagstukken vraagt om generieke kennis en kunde, aangevuld met specialismen. We mogen niet van elkaar verwachten dat alle kennis en kunde altijd in één persoon te vatten zijn. Wel is het goed om te beseffen dat de generalist ook een vak uitoefent. Dit vak vereist investeren in een brede blik en een basiskennis over veel zaken. Daar waar het specialistische kennis betreft, mogen we van de generalist verwachten dat deze zowel intern als extern een netwerk heeft om de juiste informatie op te halen, te verwerken en vervolgens te delen.

Samenwerking en een betrouwbare partner zijn vragen om medewerkers die kunnen werken vanuit een gemeenschappelijk doel, een collectieve verantwoordelijkheid en met begrip voor de mogelijkheden van partners. Dit vereist:

- om je heen kijken, weten wat er speelt, 'buiten' en 'binnen';
- voor de rol van de politie: schakelen tussen uitvoerend partner en signalerend partner;
- netwerkend werken als basiscompetentie: meedenkvermogen, doortastendheid en soms een lange adem;
- multidisciplinair zien en handelen: een intrinsieke nieuwsgierigheid naar andere werelden;
- vanuit de eigen (wettelijke) verantwoordelijkheid medewerkers met mandaat laten deelnemen aan casusoverleggen; zij zijn afstemmings-, onderhandelings- en beslissingsbevoegd;
- verantwoording afleggen over de gemaakte afweging; dat is inherent aan de beslissing.

Gelijkwaardigheid van partijen

Belangrijk voor succesvolle samenwerking is dat men elkaar vertrouwt en weet wat men van elkaar kan verwachten. Vaak ontstaan er onnodig scheve gezichten in bijvoorbeeld het handhavingsdomein tussen politiemedewerkers en bijzonder opsporingsambtenaren (boa's) met een toezichtfunctie, of tussen politiemedewerkers en portiers.

UIT

De politie in Utrecht heeft een Uitgaans Interventieteam (UIT), dat op basis van een convenant tussen gemeente, politie, OM en de Utrechtse afdeling van Koninklijke Horeca Nederland, gezamenlijk optreedt tegen uitgaansgeweld. Portiers en politiemedewerkers zijn in het verlengde van elkaar gaan werken met vergroot begrip voor elkaars werk. De gemeente liet een app ontwikkelen waardoor politie en portiers makkelijker met elkaar kunnen communiceren. Het vertrouwen onderling is nu zo groot dat portiers zonder directe opgaaf van redenen personen door het interventieteam kunnen laten natrekken. Deze vorm van samenwerking vergroot het zicht en het handelingsvermogen waardoor het uitgaan in Utrecht veiliger wordt.

Ondanks dat de relaties tussen politie en partijen niet altijd gelijksoortig of gelijkwaardig van aard zijn, is het van belang om in een samenwerkingsverband gelijkwaardigheid te allen tijde na te streven. Elke partij wil zich gehoord weten. Een goed oor en gepaste inbreng zal de harmonie in de samenwerking veelal ten goede komen. Positieve ervaringen met samenwerking in de praktijk met jeugd, welzijn en scholen, maar ook met Horeca Nederland onderstrepen dit. Dit vereist overigens ook van de politie een andere houding: luisteren, meedenken vanuit de ander en betrokken blijven. Ook als de uitkomst anders is dan verwacht.

Zet het effect dat je wilt bereiken centraal en niet een resultaat in aantallen

Samenwerken brengt veel, maar kan ook taai zijn. Je moet oog hebben voor elkaars belangen en een gemeenschappelijke ambitie vinden, zeker met partners buiten de politieorganisatie. Ondermijningsvraagstukken bijvoorbeeld zijn nog te veel het domein van de partners in de strafrechtketen, met de politie en het OM voorop. Dat de politie vaak teruggrijpt op de reguliere strafrechtelijke benadering, belemmert de samenwerking met partners buiten de strafrechtketen. Die komen vaak niet of pas laat aan tafel. Dan ligt de focus op het bereiken van resultaten; gericht op de dader of op de aanpak van fenomenen. Er worden pas echt stappen gezet als het dieperliggende maatschappelijk effect centraal staat. Dan gaat het om wat nodig is om het echte probleem aan te pakken.

Neem het gebruik van huurauto's binnen de georganiseerde misdaad. Uit onderzoeken bleek dat verhuurbedrijven dat onbewust faciliteerden. In plaats van de individuele verhuurders aan te pakken, is er samen met branchevereniging BOVAG landelijk samengewerkt aan bewustwording. Zo werd een barrière opgeworpen voor criminelen. In deze benadering staat het effect centraal: welke partner heeft de beste kaart in handen?

Begin en leer

Dat bij samenwerking niet alles vanzelf gaat, wordt onder andere duidelijk uit het onderzoek *Het wijkteam als werkplaats. Samenwerking met impact in 20 dilemma's*, uit de gemeenten Enschede en Uden. Door het te gaan doen, leert men van elkaar en kan men elkaar versterken. Door beleidsmatige kennis over samenwerking, door ontwikkeling van instrumenten en evaluaties plus praktische kennis op basis van integrale casuïstiek wordt nieuwe kennis opgedaan, vult men elkaar aan en worden instrumenten verder verbeterd. Het gebruik van een interventiematrix bijvoorbeeld – ook als inspiratiematrix – helpt om de potentiële interventies te benoemen en integraal aan de slag te gaan.[15]

Deze nieuwe methoden staan soms op gespannen voet met de geldende wet- en regelgeving. Echter, alleen door de grenzen op te zoeken, kun je grensverleggend bezig zijn en ben je in staat te blijven aansluiten op de veranderende maatschappelijke ontwikkelingen.

15 Bureau Beke, *Interventies op maat binnen de persoonsgerichte aanpak (PGA): een inventarisatie van behoeften in het veld*. Oktober 2016.

Nationaal versus lokaal

Het gezag van de burgemeester over de politie is een gegeven. Door de komst van de nationale politie is het uitoefenen van deze gezagsrol er niet eenvoudiger op geworden. Uiteraard is lokale sturing belangrijk, maar zij moet altijd in een bredere context zijn ingebed en de *couleur locale* kan nogal per gemeente verschillen.

Wat is de verhouding tussen centrale en lokale sturing, en wat gebeurt er binnen het lokale zelf? In hoeverre is elk gemeentebestuur in staat om adequaat sturing te geven aan het lokale veiligheidsbeleid? Is de invloed van een lokale instantie op een nationale organisatie iets onnatuurlijks?

Nationale prioriteiten maken dat decentrale capaciteit onder druk kan komen te staan en decentrale invloed en zeggenschap hierover mogelijk beperkt is. Aan de andere kant maakt juist de huidige schaalgrootte van de politie het mogelijk om bij grote lokale problemen extra capaciteit en middelen in te zetten. Bovendien is het wel vaak lonend om vanuit een nationaal of internationaal perspectief te kijken naar bepaalde fenomenen, omdat in sommige gevallen alleen dan het complete beeld kan worden gevormd, dan wel een set van zinvolle interventies kan worden ontwikkeld.

Gelukkig maakt de nationale informatievoorziening van de politie de afgelopen jaren hierin een goede ontwikkeling door en is het vele malen eenvoudiger geworden om gegevens te combineren en uit te wisselen. Het nationale aspect van de politie maakt ook dat zij zich veel eenvoudiger en machtiger als partij kan manifesteren in de richting van andere nationale instanties om bijvoorbeeld afspraken te maken over het uitwisselen van data en informatie.

13.5 Tot besluit

In dit hoofdstuk hebben we nut en noodzaak van samenwerking met partners aannemelijk gemaakt. De samenleving verandert en wordt in hoog tempo complexer. Voor het kunnen voortbestaan van een veilige samenleving waarin wet- en regelgeving kunnen bestaan en worden nageleefd is het in toenemende mate van belang om partnerships te sluiten. Meervoudig zicht op basis van gedeelde informatieposities, bijvoorbeeld vanuit de zorg en veiligheid, en meervoudig handelingsperspectief, bijvoorbeeld vanuit het bestuursrecht en strafrecht, resulteren in positieve resultaten. Blijvend investeren op versterking van samenwerkingsrelaties is echter noodzakelijk.

14 Inwinning

Ab van der Plas en Colin Brown[1]

In de aanloop naar een opsporingsonderzoek verzamelt de politie informatie. Deze informatievergaring aangeduid met het begrip 'inwinning' valt in het beginsel niet onder de regels van het Wetboek van Strafvordering (Sv), maar met name onder de Politiewet 2012 en de Wet politiegegevens (Wpg) en de daarmee verbonden uitvoeringsregelingen. In dit hoofdstuk wordt ingezoomd op een specialistische tak van informatievergaring, namelijk het inwinnen van informatie met gebruikmaking van informanten.

De reden waarom heimelijke informatie-inwinning binnen de politie ingezet wordt, is dat – ondanks het complexe werkproces en de risico's – dit soms de enige wijze kan zijn om te kunnen beschikken over informatie die anders niet bij de politie bekend zou worden, en die van direct belang is voor de openbare orde en veiligheid en de bestrijding van zware criminaliteit. Het komt namelijk in de praktijk regelmatig voor dat personen die een getuigenverklaring zouden kunnen afleggen, uit angst voor represailles vanuit het criminele milieu of andere kringen (bijvoorbeeld extremisten), niet bereid zijn om aan die burgerplicht te voldoen. Soms zijn zij dan wel bereid om informatie te verstrekken in de rol van informant.

Deze informatie, die weliswaar bij proces-verbaal wordt vastgelegd, kan niet voor het bewijs in een strafzaak of bestuursrechtelijke zaak worden gebruikt, omdat met de afscherming van de identiteit van de informant de mogelijkheid om deze in persoon te horen, of op andere wijze in het onderzoek te betrekken, niet aanwezig is. Wel kan de informatie de nodige zogenoemde sturingsinformatie opleveren, waardoor een opsporingsonderzoek kan worden gestart of een lopend onderzoek verder kan. Denk hierbij aan informatie over de voorbereiding van een gewapende overval, betrokkenen bij een drugstransport of moordzaak. Of, met betrekking tot het werkgebied van het Team Openbare Orde Inlichtingen (TOOI), aan een voorgenomen niet aangekondigde demonstratie van rechts-extremisten of een ophanden zijnde gewelddadige confrontatie tussen groepen voetbalhooligans dan wel informatie op het gebied van radicalisering.

14.1 De afdeling Inwinning

De afdeling Inwinning binnen de politie draagt bij aan de bestrijding van zware (georganiseerde) criminaliteit en het voorkomen van bedreigingen en verstoringen van de openbare orde. Elke eenheid binnen de politie beschikt over een afdeling Inwinning. De

1 Dit hoofdstuk is tot stand gekomen in nauwe samenwerking met het Landelijk Overleg Hoofden Inwinning (LOHI).

afdeling is ondergebracht binnen de Dienst Regionale Informatieorganisatie en kent een onderverdeling in twee teams, namelijk het Team Criminele Inlichtingen (TCI) en het TOOI.[2]

Kerntaak

De kerntaak van beide teams is het heimelijk inwinnen van informatie bij personen, genoemd informanten, die vanwege de informatiepositie die zij hebben, ernstige fysieke, sociale en/of maatschappelijke schade kunnen oplopen als bekend zou worden dat zij informatie met de politie gedeeld hebben. Het bestaan van een dergelijke dreiging is de reden waarom heimelijkheid betracht wordt. Dit plaatst de inwinning binnen het opsporingsproces en de openbare orde in een uitzonderlijke positie en maakt dat het inwinnen van informatie op een dergelijke wijze alleen is voorbehouden aan speciaal daarvoor opgeleide executieve politieambtenaren, in de functie van senior-informantenrunner, of kortgezegd runner. In de praktijk betekent dit, dat door de politie, in dit geval de medewerkers van de afdeling Inwinning, aan informanten een vergaande afscherming van hun identiteit gegarandeerd wordt. Dit houdt onder andere in dat buiten de afdeling Inwinning en het direct betrokken bevoegde gezag (zie hierna), niemand de identiteit van de informant kent of zou kunnen achterhalen. Dat geldt dus ook voor anderen binnen de politieorganisatie. Hiermee rust een bijzondere verantwoordelijkheid op alle medewerkers van de afdeling Inwinning voor de veiligheid van de informant.

Gezag

Beide teams kennen een verschillende gezagslijn. Het TCI wint informatie in met betrekking tot de zware en georganiseerde misdaad onder het gezag van een (TCI)officier van justitie. Het TOOI wint informatie in daar waar sprake is van een ernstige bedreiging van de openbare orde. Het TOOI fungeert als ondersteunend team binnen de brede openbare-ordetaak van de politie onder het gezag van de burgemeester.

Kaders

Zowel het TCI als het TOOI verricht zijn werkzaamheden op basis van artikel 3 van de Politiewet 2012. Voorts zijn er ten aanzien van de werkwijze van de afdeling Inwinning nog andere wetgeving en nadere regelingen van kracht. Het wettelijk kader en de uitvoering daarvan hebben betrekking op het verwerken, verstrekken en analyseren van de ingewonnen informatie, alsmede het beheer van de informanten, onder meer vastgelegd in de Wet politiegegevens (Wpg) (zie ook hoofdstuk 5 De Wpg).

Nadere regelingen over het verwerken en uitwisselen van de ingewonnen informatie door met name het TCI, de certificering van de informantenrunners binnen het TCI en de wettelijke termijn waarbinnen zij hun werkzaamheden kunnen uitvoeren, de beveiliging van de werkvertrekken alsmede het daaraan gekoppelde toegangsregime, zijn terug te

2 Ook een aantal landelijke diensten beschikt over een eigen TCI. Zo hebben de Koninklijke Marechaussee (KMar), de Rijksrecherche en de bijzondere opsporingsdiensten (FIOD, ILT-IOD, ISZW-DO en NVWA-OD) een eigen TCI.

vinden in het Besluit verplichte politiegegevens (Bpg). Voorts wordt er sturing gegeven aan de werkzaamheden binnen het TCI middels de werkafspraken van het Landelijk Platform CI-officieren.

Voor het werk van het TOOI is sprake van een leemte in wet- en regelgeving. In tegenstelling tot het TCI is er geen vastgestelde regeling voor de inzet van en controle op bevoegdheden van het TOOI. Deze situatie bestond feitelijk al voorafgaand aan de vorming van de nationale politie, toen de openbare-orde-inwinning een taak was van de toenmalige Regionale Inlichtingendiensten (RID). Deze diensten werden gekenmerkt door de zogenoemde 'dubbele-pettenproblematiek': door dezelfde RID-functionarissen werd zowel onder aansturing van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en onder het regime van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) gewerkt aan bedreigingen van de democratische rechtsorde en onder het bevoegde gezag van burgemeesters aan bedreigingen van de openbare orde. Ook toen was sprake van het ontbreken van wet- en regelgeving voor de openbare-orde-taak. Deze situatie is niet veranderd nu het TOOI als zelfstandig onderdeel van de heimelijke inwinning is ingericht binnen de politie.

In de praktijk zijn er bij het TOOI steeds meer landelijke werkafspraken over het werven en runnen van informanten, waarbij veelal naar analogie van de regelgeving en werkafspraken van het TCI gewerkt wordt. Onder aansturing van de landelijke portefeuillehouder Intelligence zijn voorstellen in ontwikkeling om de rol van het bevoegd gezag nadrukkelijker te positioneren, met name om op basis van uniforme werkafspraken het toezicht op de uitvoering van het werk van het TOOI te verstevigen.

Het Team Nationale Inlichtingen

Bij de afdeling Inwinning van de Landelijke Eenheid is ook het Team Nationale Inlichtingen (TNI) ondergebracht. Het TNI registreert:

a criminele inlichtingen, voor zover deze gegevens van nationale of internationale betekenis zijn;
b personalia of bedrijfsgegevens van overeenkomstig artikel 10, tweede lid, onderdelen a en b, van de Wet politiegegevens geregistreerde personen in de door de ministers aangewezen geautomatiseerde verwijzingsindex;
c codes die zijn toegewezen in het kader van de registratie.

Het TNI analyseert de gegevens, bedoeld als hierboven onder a, en verstrekt mede aan de hand daarvan de gegevens, bedoeld onder a en b, aan hen die daarop bij of krachtens de Wet politiegegevens aanspraak kunnen maken.

Relatie met het buitenland

Het TNI maakt afschermprocessen-verbaal op om broninformatie van een TCI in Nederland dat naar het buitenland moet, af te schermen. Ook broninformatie uit het buitenland, waarbij soms het land van herkomst van deze informatie dient te worden afgeschermd, wordt via het TNI verstrekt. Deze verstrekking wordt, met tussenkomst van het TCI van de ontvangende politie-eenheid, middels een (afscherm)proces-verbaal, verstrekt aan een tactisch team.

Daarnaast behandelt het TNI de beloningsvoorstellen, die opgemaakt worden door de TCI's in Nederland. Deze worden beoordeeld en in overleg met het Landelijk Parket van het Openbaar Ministerie (OM) wordt de hoogte van de beloning vastgesteld.

14.2 Werkprocessen

Er zijn verschillende werkprocessen binnen de afdeling Inwinning, zoals onder andere het werven, beheren en onderhouden van (een netwerk van) informanten, het houden en verwerken van informantgesprekken, het analyseren van artikel 10- en 12-Wpg-informatie, het registreren van nieuwe subjecten artikel 10 Wpg en het verstrekken en ter beschikking stellen van informatie binnen en buiten het TCI- en TOOI-domein. Verstrekking van de informatie afkomstig van het TCI geschiedt uitsluitend per proces-verbaal (pv) en afkomstig van het TOOI uitsluitend met een verstrekkingsrapport of per proces-verbaal, in afstemming met het Openbaar Ministerie.

Informatiegestuurd inwinnen en thematisch runnen zijn het uitgangspunt. De prioritering van de inwinning van inlichtingen is volledig gericht op de doelstellingen van de politie en volgt de lijnen van de vastgestelde nationale en regionale intelligenceagenda's en aangegeven prioriteiten op ondermijningsgebied dan wel op actuele openbare-orde-problematiek. Ook wordt ingewonnen met betrekking tot de landelijk vastgestelde thema's (zie hiervoor ook hoofdstuk 10 Informatiecoördinatie).

De ingewonnen inlichtingen worden veredeld en geanalyseerd. Eventueel aangevuld met reeds ingewonnen informatie, zowel heimelijke als tactische informatie, wordt het geheel gesmeed tot een beeld op het gebied van de zware en ondermijnende criminaliteit en de daarbij betrokken samenwerkingsverbanden, dan wel, in het geval van het TOOI, gebruikt voor het creëren van een veiligheidsbeeld op het gebied van de openbare orde.

14.2.1 Informatieverstrekking door de afdeling Inwinning

Zoals reeds eerder werd gesteld, geschiedt de informatieverstrekking vanuit de afdeling Inwinning alleen door middel van een proces-verbaal (TCI) c.q. rapport en proces-verbaal (TOOI). De informatiestromen lopen via de informatieknooppunten van de informatieorganisatie. Nieuwe informatie afkomstig van het TCI of het TOOI wordt ingebracht bij het regionaal informatieknooppunt (RIK) of rechtstreeks bij de informatieclusters binnen het districtelijk informatieknooppunt (DIK). De verstrekte informatie kan ook gebruikt worden voor het opmaken van een preweegdocument om in die vorm gewogen te worden in de lokale of regionale weegploeg voor de opsporing.

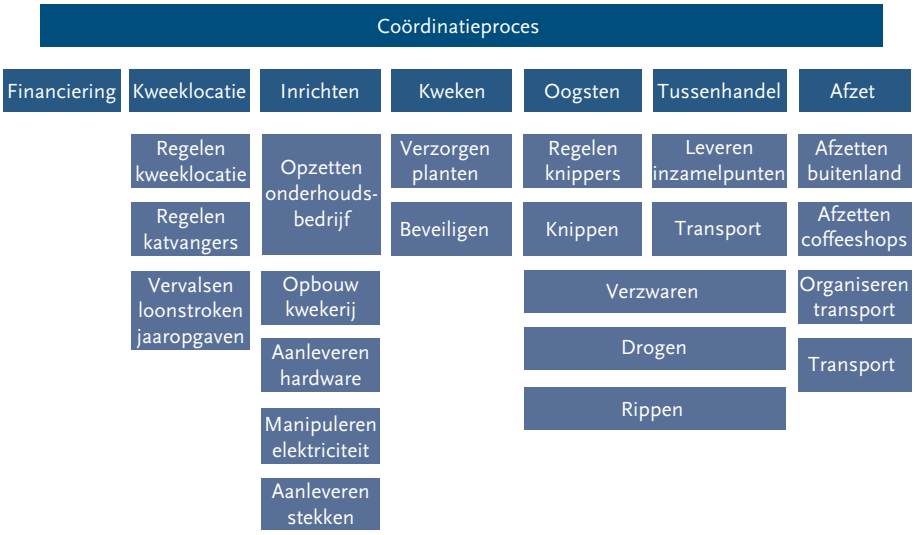
Processen-verbaal afkomstig van het TCI ter ondersteuning van lopende onderzoeken worden ingestoken bij de onderzoeksleiding van deze onderzoeken. Voor Teams Grootschalige Opsporing (TGO's) geldt dat processen-verbaal via de TGO-informatiecoördinator worden ingestoken.

14.2.2 Analyse binnen de Inwinning

Door de analisten werkzaam binnen het TCI wordt gewerkt met de analysemethode Hyperion, die inmiddels landelijk in gebruik is. De basis voor de analyse vormt het duiden van elk stukje ingewonnen informatie uit het criminele-informatierapport (CIR). Dit houdt in dat wordt bekeken:

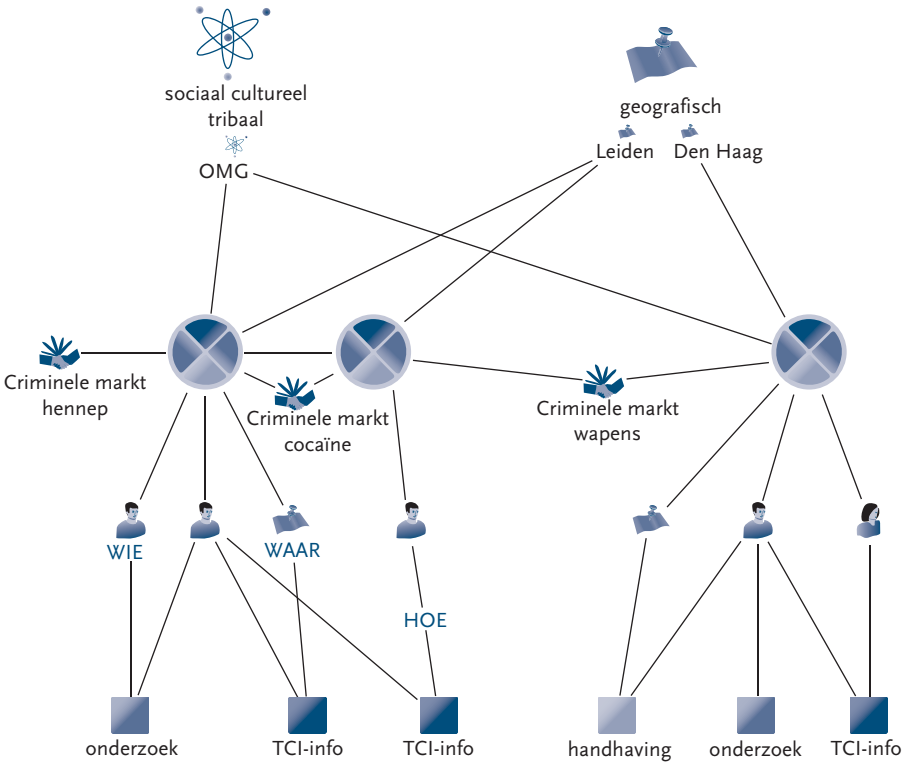
- Welke subjecten maken deel uit van het criminele netwerk?
- Met wat voor soort criminaliteit houden de subjecten zich bezig? En waar doen zij dit?
- Wat is de rol van het subject binnen het criminele proces?

Om de laatste vraag te beantwoorden is op voorhand een breed scala aan criminele markten beschreven. Vervolgens zijn voor elke criminele markt per logistieke fase rollen benoemd (zie figuur 14.1 voor voorbeeld met betrekking tot de criminele markt hennep). Ondanks dat dit tijdrovend werk is, heeft het als groot voordeel dat analyses die hierop gebaseerd worden minder arbitrair zijn dan voorheen; er liggen immers aanwijsbare bronnen en een gevalideerde methode aan ten grondslag. De informatie staat centraal.



Figuur 14.1 Criminele markt hennep: logistieke fasen met daaronder de rollen

Vervolgstap in de methode is dat de analist op basis van de geduide informatie onderbouwd criminele clusters aanmaakt. Clusters zijn kleine groepjes van criminelen (meestal twee tot vijf personen) die structureel samenwerken. Op basis van de geduide informatie kan worden beschreven waar elk cluster zich mee bezighoudt, met welke andere clusters wordt samengewerkt en waar zij dit doen. Maar ook: wat zijn potentiële nieuwe informanten met betrekking tot deze clusters? En waar missen we mogelijk nog informatie? Nog een abstractieniveau hoger maken meerdere clusters onderdeel uit van een zogenoemde scene. De scene kan zowel sociaal (bijvoorbeeld een voetbalclub), tribaal (bijvoorbeeld outlaw motor gangs – OMG), als geografisch (bijvoorbeeld Den Haag) van aard zijn (zie figuur 14.2).



Figuur 14.2 Criminele clusters en scenes

Met behulp van Hyperion kunnen bovendien sleutelpersonen of sleutellocaties worden herkend binnen het netwerk. Zoals hiervoor aangegeven, zijn voor elke criminele markt rollen beschreven. Sommige van deze rollen zijn belangrijker voor het in stand houden van het criminele netwerk dan andere. Hierbij kan gedacht worden aan personen met specifieke kwaliteiten die niet makkelijk vervangbaar zijn voor een criminele organisatie. Het is in bepaalde gevallen het effectiefst gebleken om juist deze personen uit het netwerk te halen in plaats van de zogenoemde 'kopstukken' van het criminele netwerk. Uit onderzoek zal moeten blijken welke rollen in een bepaald crimineel proces tot sleutelrol kunnen worden benoemd. Doordat per CIR de rol van een subject wordt geduid, kan met behulp van een *query* in een database (in dit geval iBase) eenvoudig worden vastgesteld welke personen een dergelijke sleutelrol vervullen. Op basis van de analysemethode kunnen derhalve onderbouwde aanbevelingen worden gedaan met betrekking tot interessante subjecten als onderwerp voor een opsporingsonderzoek.

Momenteel is in onderzoek of (een aangepaste vorm van) de Hyperionmethode ook ingezet kan worden voor het analyseren van openbare-orde-inlichtingen.

14.3 Thema's

14.3.1 Team Criminele Inlichtingen (TCI)

Het team verzorgt de inwinning, analyse en verstrekking van heimelijke informatie op het gebied van zware en ondermijnende criminaliteit. Kerntaken van het team zijn:

- runnen van informanten.
- verzamelen en verifiëren van criminele inlichtingen.
- verwerken van criminele inlichtingen.
- signaleren van criminaliteitsontwikkelingen, alsmede het analyseren van criminele inlichtingen ten behoeve van criminaliteitsbeelden en beschrijvingen van criminele samenwerkingsverbanden. Daarbij komt het vervullen van een versterkende rol bij het maken van keuzes in de prioritering van opsporingsonderzoeken door stuurploegen.
- actualiseren van veiligheidsbeelden op het gebied van zware en ondermijnende criminaliteit.
- verstrekken van criminele inlichtingen ten behoeve van lopende opsporingsonderzoeken.

Informatie wordt op de navolgende thema's ingewonnen.

Ondermijning[3]

Onder het begrip ondermijning kunnen tal van thema's worden geschaard. Welke thema's aandacht krijgen, is weer afhankelijk van de prioriteiten benoemd in de nationale intelligenceagenda, de intelligenceagenda per eenheid en de kadernota's per eenheid waar de eventuele nader uitgewerkte speerpunten worden aangeduid (zie ook hoofdstuk 10 Informatiecoördinatie). Onder ondermijning vallen de navolgende thema's:

- grootschalige en georganiseerde hennephandel;
- grootschalige invoer van en handel in harddrugs in relatie tot financieel witwassen van crimineel verkregen gelden;
- wapenhandel;
- OMG's;
- mensenhandel;
- andere vormen van zware en georganiseerde criminaliteit.

High impact crime

Onder *high impact crime* vallen:

- woninginbraken in georganiseerd verband;
- overvallen;

---

3 Een definitie van ondermijning is: 'Het verzwakken of misbruiken van de structuur van onze maatschappij, leidend tot een aantasting van haar fundamenten en/of de legitimiteit van het stelsel dat haar beschermt.' (Hoogewoning, F.C., A.J. van Dijk & W.C. Man, 'Ondermijning en veiligheid'. In: *het Tijdschrift voor de Politie* 72, nr. 5, p. 10.

- straatroven;
- geweld;
- mobiel banditisme;
- criminele jeugdgroepen.

Figuur 14.3 Drugslab

14.3.2 Team Openbare Orde Inlichtingen (TOOI)

Het team verzorgt de inwinning, analyse en verstrekking van heimelijke informatie op het gebied van openbare orde. Kerntaken van het team zijn:

- runnen van informanten;
- verzamelen en verifiëren van openbare-orde-inlichtingen;
- veredelen en analyseren van heimelijk ingewonnen informatie;
- leveren van incidentele verstrekkingen;
- leveren van informatierapporten, risico-inschattingen en dreigingsinschattingen op het gebied van openbare orde;
- actualiseren van veiligheidsbeelden op het gebied van openbare orde.

Door het TOOI wordt op de volgende thema's informatie ingewonnen.

Politiek activisme en -extremisme

Hieronder vallen:

- *Activisme*
  De algemene benaming voor het fenomeen waarbij personen of groeperingen op buitenparlementaire wijze, maar binnen de grenzen van de wet, streven naar verbetering van de rechten en levensomstandigheden van individuen, groepen en dieren.
- *Extremisme*
  Het fenomeen waarbij personen en groepen, bij het streven naar verbetering van de rechten en levensomstandigheden van individuen, groepen of dieren, bewust over de grenzen van de wet gaan en (gewelddadige) illegale acties plegen. Hieronder worden

onder andere begrepen: links-activisme/extremisme, kraken, dierenrechten- en milieuactivisme, rechts-activisme/extremisme.

Maatschappelijke onrust

Onrust binnen groepen in de maatschappij die leidt of kan leiden tot (heimelijke of heimelijk georganiseerde) activiteiten, die op hun beurt leiden of kunnen leiden tot openbare-ordeverstoringen. Hieronder kunnen demonstraties (openbare manifestaties) worden begrepen, maar ook OMG's, voor zover hun bewegingen en activiteiten van invloed zijn op de openbare orde.

(Sport)evenementen

(Mogelijke) ernstige verstoringen van de openbare orde rond (sport)evenementen. Hieronder wordt onder andere voetbal begrepen, maar bijvoorbeeld ook dance-evenementen.

Polarisatie en radicalisering

Het al dan niet opzettelijk vormen of verscherpen van maatschappelijke tegenstellingen, bijvoorbeeld op etnische of religieuze basis. Sommige groepen in onze samenleving proberen door het bewust creëren van tegenstellingen burgers tegen elkaar op te zetten. Hieronder kunnen onder andere worden begrepen:

- Interetnische spanningen, bijvoorbeeld tussen Turken en Koerden, of andere (bevolkings)groepen, afhankelijk van actuele (inter)nationale ontwikkelingen.
- Radicalisering voor zover zich dit binnen het openbare-orde-domein afspeelt en niet binnen het proces opsporing, of niet binnen de taken van de AIVD valt. Waarbij met betrekking tot radicalisering geldt dat de regie op de aanpak van dit onderwerp bij de burgemeester is belegd.

14.4 Afschermprocedure

In een strafrechtelijk onderzoek (bronondersoek) kan het voorkomen dat het voor de afscherming ervan noodzakelijk is een separaat deelonderzoek (doelonderzoek) te starten. Dit deelonderzoek wordt dan gestart met informatie afkomstig uit het bronondersoek. Hierbij kan enerzijds worden gedacht aan informatie over verboden goederen, zoals harddrugs of vuurwapens die in verband met het verbod op doorlaten van artikel 126 ff Sv, als voldoende zekerheid bestaat over hun bergplaats, in beslag moeten worden genomen. Het doelonderzoek voldoet dan aan de eis van het doorlaatverbod, en realiseert tevens dat het bronondersoek afgeschermd blijft bij de tegenpartij.

Anderzijds kan binnen het bronondersoek informatie voorhanden zijn waarop niet meteen behoeft te worden geacteerd, maar waarmee een ander onderzoeksteam om andere redenen direct aan de slag wil. Bijvoorbeeld een uit telefoontaps verkregen – tot dan toe onbekend – telefoonnummer dat van belang is, dan wel een afgeluisterd telefoongesprek dat betrekking heeft op een ernstig delict dat niet in de onderzoeksdoelstelling van het betreffende bronondersoek past.

In verband met vorenstaande is de zogenoemde afschermprocedure ontwikkeld. Door middel van deze procedure is het mogelijk om enerzijds afscherming te bieden aan het

lopende brononderzoek, terwijl anderzijds zo nodig voldoende startinformatie wordt verschaft om een doelonderzoek te kunnen opstarten.

Aan deze procedure is een aantal vereisten verbonden:
- Te allen tijde is toestemming vereist van de zaaksofficier van justitie van het brononderzoek voor gebruik van informatie uit dat onderzoek bestemd voor het doelonderzoek.
- Het TCI is met betrekking tot deze procedure de enige afschermautoriteit.

Werkwijze afschermproces-verbaal (TCI) en kluisproces-verbaal (brononderzoek)

De afschermprocedure is belegd bij het TCI. De kern van de afschermprocedure is het opmaken van het zogenoemde afschermproces-verbaal door de chef van het TCI van de ontvangende eenheid (doelonderzoek). Hij doet dat op basis van een zogenoemde kluisproces-verbaal, dat is opgemaakt door de teamleiding van het verstrekkende (bron)onderzoek.

In dit kluisproces-verbaal is alle relevante informatie uit het brononderzoek vastgelegd:
- naam van het onderzoek;
- zaaksofficier van het onderzoek;
- politie-eenheid die het onderzoek verricht;
- de wijze waarop de informatie ter beschikking is gekomen (toegepaste opsporingsmethodieken en/of bevoegdheden) en bijgevoegde machtigingen van bijvoorbeeld telefoontaps dan wel processen-verbaal van het observatieteam;
- de tekst die in het afschermproces-verbaal dient te worden vermeld en die vooraf met de zaaksofficier van justitie is overlegd.

Met betrekking tot de aan te leveren afschermtekst dient deze, voor zover het de bedoeling is om een nieuw onderzoek te starten, voldoende informatie te bevatten om een verdenking ex artikel 27 Sv te rechtvaardigen. Uiteraard mag de afschermtekst niet te herleiden zijn naar het brononderzoek; dit is nu juist de essentie van de afschermprocedure.

Risico

Het risico van de thans gebruikte afschermmethodiek schuilt in het feit dat de opsporingsambtenaren van het doelonderzoek op de hoogte raken van het lopende brononderzoek. Daar is juridisch en feitelijk niets op tegen, als men zich vanuit het brononderzoek maar bewust is van deze omstandigheid en dit dus de afscherming kan raken. Politie en OM dienen zich bij het gebruik van de afschermprocedure dan ook te realiseren dat die uitsluitend naar buiten toe (dat wil zeggen ten opzichte van de zittingsrechter en de verdediging) volledige afscherming geeft.

14.5 Bijstand van burgers aan de opsporing

De informant levert als burger bijstand aan de opsporing. Om de positie van de informant daarbij te bepalen, zijn de volgende vier rechtsfiguren te onderscheiden:
- de reguliere informant ex artikel 3 van de Politiewet 2012;
- de stelselmatige informatie-inwinnende burger ex artikel 126v Sv;

- de pseudodienstverlener/pseudokoper ex artikel 126ij Sv;
- de burgerinfiltrant ex artikel 126w Sv.

In de dagelijkse inwinningspraktijk wordt vrijwel uitsluitend gebruikgemaakt van de reguliere informant ex artikel 3 van de Politiewet 2012. De grenzen van dit artikel mogen niet worden overschreden, want dan kan er sprake zijn van stelselmatige informatie-inwinning als bedoeld in artikel 126v Sv. In dat geval zou met de informant, op bevel van de officier van justitie, door een opsporingsambtenaar een overeenkomst als bedoeld in het genoemde artikel gesloten moeten worden.

Ook op andere manieren mag een informant de grenzen zoals in de wet vastgelegd niet overschrijden. Hij heeft namelijk, als hij in opdracht van het TCI zou overgaan tot het verwerven van goederen van een verdachte, of het verlenen van diensten aan een verdachte, een overeenkomst strekkende tot pseudokoop of pseudodienstverlening nodig als bedoeld in artikel 126ij Sv. Gaat de informant in opdracht van het TCI deelnemen of medewerking verlenen aan een groep van personen waarbinnen naar redelijkerwijs kan worden vermoed misdrijven worden gepleegd, dan dient hij op basis van een overeenkomst strekkende tot burgerinfiltratie ex artikel 126w Sv als burgerinfiltrant ingezet te worden.

Buiten de vermelde rol van reguliere informant ex artikel 3 van de Politiewet 2012 vallen de andere rollen onder de politiegestuurde burgeropsporing in het kader van de Wet bijzondere opsporingsbevoegdheden (Titel VA, Bijstand aan opsporing door burgers, Sv), zijnde burgers die bijstand verlenen aan de opsporing. De burger voert hierbij actief opsporingshandelingen uit en wordt beschouwd als verlengstuk van politie en justitie. De handelwijze van de burger valt dan ook onder de verantwoordelijkheid van deze instanties. De richtlijnen voor de wijze waarop de politie en het OM met door de politie gestuurde burgeropsporing moet omgaan, staan beschreven in het conceptprotocol 'Bijstand aan de opsporing door burgers' van 2 november 2016.

14.6 Rol van het Team Criminele Inlichtingen in zaken met een hoog afbreukrisico

Het TCI heeft als gesteld een bijzondere positie in het informatie- en rechercheproces, te weten de afscherming. Het TCI kan binnen de wettelijke kaders de anonimiteit van haar informanten waarborgen. Dit regime geeft meteen ook de ruimte om in bijzondere trajecten met een hoog afbreukrisico getuigen te spreken met waarborging van de anonimiteit. In de praktijk zijn dat personen die uit angst voor represailles een anonieme getuigenverklaring willen afleggen. Ook een verkregen tactische verklaring kan soms, in het veiligheidsbelang van de getuige en in samenhang met de zorgplicht van de overheid, niet aan het dossier worden toegevoegd maar moet als kluisverklaring[4] worden behandeld.

4 Kluisverklaringen zijn verklaringen afgelegd onder toezegging van de officier van justitie dat ze in een kluis worden bewaard en pas operationeel gebruikt kunnen worden indien er overeenstemming is bereikt over de voorwaarden waaronder dat gebeurt.

De bijzondere getuigen zijn de getuigen die aangeven een verklaring te kunnen afleggen, maar die dat alleen onder bepaalde voorwaarden willen doen. Met bijzondere getuigen worden bedoeld:

- getuigen met wie mogelijk een overeenkomst als bedoeld in artikel 226g e.v. Sv wordt gesloten (dealgetuigen);
- getuigen die in aanmerking willen komen voor gunstbetoon als bedoeld in artikel 226g lid 4 Sv, zoals een milder detentieregime, schorsing van de voorlopige hechtenis, versnelde teruggave van in beslag genomen goederen enzovoort;
- potentieel anonieme, bedreigde getuigen als bedoeld in artikel 226a Sv;
- overige getuigen die een tegenprestatie in welke vorm dan ook vragen voor het afleggen van een verklaring of waarvoor vrees bestaat voor represailles in verband met het afleggen van een verklaring.

De dealgetuige en de rol van het TCI

Een verklaring afgelegd door een getuige met wie nog onderhandeld wordt over een zogenoemde deal (een toezegging aan een getuige die tevens verdachte is, strekkende tot strafvermindering) valt zonder meer onder de geheimhoudingsverplichting en de zorginspanningen van het TCI. Zolang het onderhandelingsproces loopt en zolang de rechter-commissaris de voorgenomen afspraken nog niet rechtmatig heeft beoordeeld, mogen de verklaringen niet aan het dossier worden toegevoegd. Vormen van tegenprestatie bij het afleggen van een verklaring zijn bijvoorbeeld:

- gunstbetoon;
- getuigenbeschermingsmaatregelen;
- financiële compensatie.

In de praktijk zal het zo zijn dat het OM of de tactische teamleiding contact opneemt met het TCI om de procedure op te starten. Binnen het TCI is de expertise bijzondere getuigen belegd en vanuit die expertise vinden operationele aansturing en uitvoering plaats. In eerste instantie zal een achtergrondonderzoek gehouden worden alsmede een intake met de potentiële getuige. Deze intake gebeurt door medewerkers van het TCI, zo nodig in bijzijn van een psycholoog. Dit altijd in overleg met en met toestemming van het hoofd van het TCI en in overleg met en met toestemming van de officier van justitie. De casuïstiek kan door het TCI worden aangedragen als kans of door de tactiek of de getuige zelf. In dit hele proces wordt getoetst op de motivatie en consistentie en de betrouwbaarheid van de verklaring. Verder zal nadrukkelijk het proces worden uitgelegd en de voorwaarden waaronder een eventuele deal zal gaan plaatsvinden. In het gehele proces is er een duidelijke rol weggelegd voor het TCI in zijn rol van bijzondere getuigenrechercheur. Hierbij kan tevens een beroep worden gedaan op tactische collega's die met toestemming en in overleg met de officier van justitie en onder absolute geheimhouding participeren onder de regie van het hoofd van het TCI. Hierbij is wel landelijk afgesproken dat als tactische collega's betrokken worden in dit proces, zij niet meer terugkeren in het onderzoek waarin de verklaring wordt afgelegd. Dit om de objectiviteit niet te beïnvloeden. In het volgende model wordt deze procedure schematisch weergegeven.

Figuur 14.4 Proces rond dealgetuige

Crime consult

Steeds meer worden specialistische diensten in de voorfase van een strafrechtelijk onderzoek betrokken bij de start ervan. In een consult worden de mogelijkheden onderzocht die de specialistische diensten kunnen bieden. Juist in de voorfase kunnen er keuzes gemaakt worden die van invloed kunnen zijn op het vervolg van het onderzoek. Hierbij is te denken aan een betere informatiepositie, of de keuze om een persoon in te zetten als getuige of informant. Doorgaans heeft inzet als getuige de voorkeur, waarbij alle (persoons)informatie deelbaar is. Maar er zijn nu eenmaal omstandigheden waarin afscherming van een persoon de enige manier is om cruciale informatie te verkrijgen.

In de voorfase van een opsporingsonderzoek, maar ook in het verdere verloop, is het TCI het loket daar waar het gaat om zaken met een groot afschermbelang. Denk hierbij aan trajecten tezamen met Werken onder Dekmantel, Afgeschermde Operaties en Getuigenbescherming. De meerwaarde van het TCI ligt vooral in de informatiepositie die het TCI heeft, die complementair kan zijn aan de posities en de informatiebehoefte van de voornoemde diensten.

15 Sociale media[1]

Frank Smilda en Arnout de Vries

15.1 Inleiding

De opkomst en integratie van sociale media in de samenleving en economie brengen veel veranderingen met zich mee. In kort tijdsbestek hebben ze ook de wereld van de openbare orde en veiligheid en die van de opsporing van criminaliteit en misdaad veranderd. We zouden zelfs willen spreken van een revolutie. Een revolutie waarvan de betekenis misschien nog onvoldoende op waarde kan worden geschat, maar die grote gevolgen heeft en nog gaat hebben voor de organisatie en werkwijze van de politie en al haar partners.

De mondige burger is allang niet meer een passieve volger van de politie en opsporingsdiensten, maar neemt zelf het heft in handen dankzij de mogelijkheden van sociale media. Bijvoorbeeld door vermeende criminaliteit of misdaad te delen met een groot publiek of actief mee te helpen met online zoeken naar daders. Zo verandert door burgerparticipatie de machtsbalans tussen politie en burger.

De mensen die sociale media gebruiken en maken tot wat ze zijn, kunnen ook de oplossing bieden. Omdat steeds meer delicten een digitale component kennen, dragen sociale media er steeds meer aan bij dat rechercheurs een zaak rondkrijgen. De *digital natives* – de generatie van dit millennium – veranderen de komende decennia het criminaliteitsbeeld, in goede en kwade zin. Ze zijn opgegroeid met sociale media en digitale middelen. De virtuele wereld is voor hen als een tweede natuur. Wie had kunnen voorspellen dat zij vuistdikke dossiers van zichzelf op internet zouden zetten?

Maar nog meer dan een open informatiebron zijn sociale media een samenwerkingsplatform waar burgers in de huidige genetwerkte maatschappij zelf actief aan bijdragen. Het zet de volledige politieorganisatie meer dan ooit midden in de samenleving en biedt zo meer kansen om samen te werken met burgers. Zo beïnvloeden sociale media het gehele opsporingsproces van plaats delict tot en met de rechtsgang. Zoals DNA onlosmakelijk met eenieder is verbonden, zijn sociale media de digitale lifestyle van onze maatschappij. Sociale media zouden dus ook in het DNA van iedere politiemedewerker moeten zitten.

'Social media is a tool on our belt'
– Bill Bratton, voormalig politiechef van de politie van Los Angeles, New York en Boston

---

1 Deze bijdrage is gebaseerd op Vries, A. de & F. Smilda. *Sociale media: het nieuwe DNA. Een revolutie in opsporing*. Reed Business Education, Amsterdam 2013.

Als het aan Harm Brouwer – tot 2011 voorzitter van het College van procureurs-generaal – ligt, komt er in Nederland alsnog een breed maatschappelijk debat over de actieve rol van burgers bij de opsporing van misdrijven en verdachten. 'We leven in een tijdperk van revolutionaire ontwikkelingen op het gebied van communicatie en informatisering en de digitalisering van de samenleving. Moderner is wat ik de "youtubisering" zou willen noemen. Burgers onderzoeken andere burgers en zetten hun bevindingen klakkeloos op internet. Bijvoorbeeld filmpjes van hoe de buurman zwart aan het klussen zou zijn, of weblogs van hobbyclubs over waarom toch niet de voor het feit veroordeelde X, maar Y de werkelijke dader is. Feitelijk gaat het niet alleen meer om burgeropsporing, maar meteen ook om burgervervolging.'[2]

Deze veranderingen en mogelijkheden roepen natuurlijk ook vraagtekens en morele dilemma's op. Hoe gaan burgers om met hun nieuwe rol? Wat vinden we als samenleving acceptabel? Hoe ver mag de politie gaan met het vergaren van informatie over burgers? Welke technologie mag daarbij wel en niet gebruikt worden? Wat zijn de gevolgen voor de privacy van burgers en verdachten? Houdt door burgers online verkregen bewijslast juridisch stand? Zoals vaak met revoluties, gaan veranderingen vaak sneller dan beleidsmakers en gezagsdragers kunnen bijbenen. De zogenoemde Facebookrellen in Haren waren in dat opzicht een goede wake-upcall.

De politie kan zich moeilijk permitteren achter de feiten aan te lopen. Als de samenleving – en daarmee de onveiligheid en criminaliteit van die samenleving – zich heeft verplaatst van de straat naar cyberspace, dan moet de politie dáár ook aanwezig zijn. En gelukkig is dat steeds vaker het geval.

15.2 Sociale media als informatiebron

Bij informatiegestuurd politiewerk gaat het om de analyse van informatie en kennis op grond waarvan beslissingen over de uitvoering van de politietaak worden genomen. De politie zit steeds vaker op het web op zoek naar feiten, verbanden en nieuwe aanwijzingen om zaken op te lossen. Dat is publieke informatie uit zogenoemde open bronnen. Die kan de politie dan weer koppelen aan gegevens uit andere (niet-open) bronnen. Dit betekent nogal wat: de klassieke tactische rechercheur krijgt er nieuwe collega's bij, zoals informatiespecialisten en deskundigen op het gebied van informatie- en communicatietechnologie (en straks ook nog analisten voor sociale media). De hoeveelheid informatie is enorm en vraagt om een nieuwe aanpak, met als risico een potentiële tweedeling tussen de opsporing (klassieke rechercheur) en de informatievergaring (*intelligence*). Volgens hoogleraar strafrecht en criminologie Cyrille Fijnaut[3] zal verwerking van big data tot bureaucratie en tweedeling in het korps leiden en zal het recherchewerk verschuiven van intuïtie naar een digitaal korset. Fijnaut kreeg destijds bijval van Tweede Kamerlid Fred Teeven (VVD): 'Ik

2 Gonsalveslezing door mr. H.N. Brouwer, voorzitter van het College van procureursgeneraal, gehouden op 15 februari 2008 ter gelegenheid van de uitreiking van de tweede mr. Gonsalvesprijs. Zie http://www.gonsalvesprijs.nl/?id=136, Den Haag.

3 'Recherche verruilt intuïtie voor digitaal korset.' In: *NRC Handelsblad*, 9 juni 2010.

heb niks tegen informatiegestuurde opsporing, maar het lijkt erop dat het soms doorslaat. Er is geen ruimte meer voor intuïtie. Elke beslissing om rechercheurs vrij te maken voor een onderzoek moet worden ondersteund door een weegdocument waarin wordt bekeken of een onderzoek op basis van de aanwezige informatie kans van slagen heeft.' Jan-Kees Schakel constateert in zijn proefschrift *Kennisgestuurd politiewerk* dat, wanneer de aandacht te veel op (digitale) gegevens ligt, dit ten koste gaat van de (sociale) rijkdom aan 'zachte' kennis van rechercheurs.

Met dit als kanttekening, duiden we in deze paragraaf de impact van sociale media op de zogenoemde acht W's, die hun oorsprong vinden in de (oorspronkelijk zeven W's van de) opsporing: wie, wat, waar, waarmee, welke wijze, wanneer, waarom en de redenen van wetenschap (zie figuur 15.1). Waar in de laatste jaren DNA dé *game changer* is geweest in het forensisch onderzoek, zullen sociale media ditzelfde teweegbrengen in de *intelligence* en de tactische opsporing, en dat gebeurt sneller dan de meeste mensen denken.

Figuur 15.1 De acht gouden W's van intelligence

15.2.1 Wie?

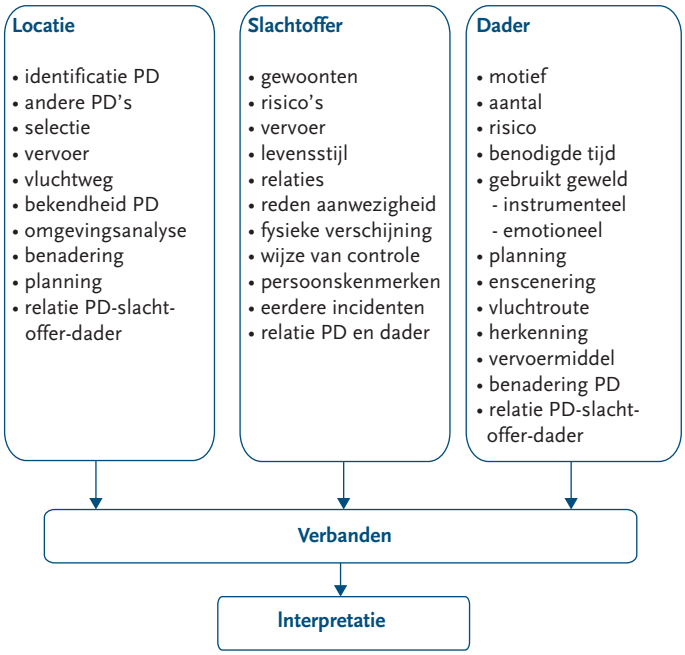
Om wie gaat het? En heeft hij alleen gehandeld? De vraag 'over wie' gaat eigenlijk over iedereen die met een zaak te maken heeft: slachtoffers, verdachten, getuigen, betrokkenen. Negen van de tien Nederlanders maken gebruik van sociale media. Er is dus een grote kans dat iemand die iets heeft gezien of gehoord dat op het web zet. En wat bijvoorbeeld als dat de dader zelf is? Voor een beetje handige jongen is het niet zo moeilijk een andere digitale identiteit aan te nemen en iemand anders verdacht te maken. En dan hoeft hij alleen nog maar te wachten totdat bijvoorbeeld GeenStijl het oppikt. Een grote groep mensen praat er dan al over, terwijl de politie nog rood-witte linten aan het spannen is en de opsporing nog moet beginnen.

Dit soort informatie geeft het opsporingsproces een heel nieuwe dynamiek. De kans bestaat bijvoorbeeld dat burgers op basis van foute informatie het recht in eigen hand gaan nemen. Door de berichten op internet worden getuigen, en daarmee de rechtsgang, beïnvloed. Die berichten kunnen ook informatie bevatten die vroeger alleen de dader kon

weten (daderwetenschap), en daarmee verliest de politie/rechercheur de mogelijkheid om een verdachte met die informatie klem te zetten.

'Nu staan wij vaak met 10-0 achter omdat er al binnen enkele minuten foto's op sociale media verschijnen.'
– *Paul Heidanus, politievoorlichter Groningen*

Het is heel handig voor intelligence dat bijna iedereen te vinden is op het web, ook mogelijke getuigen of mensen die (misschien ten onrechte) in een zaak als verdachte worden gezien. Op basis hiervan kunnen profielen van zowel slachtoffer(s) als dader(s) opgesteld worden. De figuur hierna toont het klassieke model met elementen die door de sociale media ingrijpend zullen veranderen.



Figuur 15.2 Slachtoffer- en daderprofielen

Het slachtoffer- en daderprofiel

Heb je iemands leven in kaart, dan zegt dit misschien ook iets over zijn dood. Door te kijken naar de persoonlijke omstandigheden van het slachtoffer wordt wellicht ook de reden van iemands dood duidelijker. Misschien wijst iets in die persoonlijke omstandigheden zelfs in de richting van de dader. Meestal is de dader een bekende van het slachtoffer. En misschien is die dader wel te vinden tussen de tientallen vrienden van het

slachtoffer op Facebook of tussen zijn volgers op Twitter. Vaak hebben slachtoffer en dader eerder op de een of andere manier contact met elkaar gehad. Is dit op sociale media gebeurd, dan heeft dit sporen achtergelaten. Maar ook informatie over gewoonten, risico's, levensstijl, bekendheid met de plaats van het delict, persoonskenmerken of informatie over eerdere incidenten kunnen in open bronnen vindbaar zijn. Het slachtofferprofiel probeert dergelijke informatie gestructureerd in kaart te brengen. Net als het slachtofferprofiel geeft ook het daderprofiel richting aan een onderzoek.

15.2.2 Wat?

Wat gebeurt er of is er gebeurd en hoe dan? Door de enorme opkomst van weblogs (bijna een op de vijf Nederlanders heeft er een) is de kans groot dat er allerlei verhalen, foto's en/of video's over criminaliteit al op internet zijn geplaatst. Hoe dat in zijn werk gaat, kunnen we bijvoorbeeld illustreren aan de hand van Koninginnedag 2009 te Apeldoorn.

> Terwijl de NOS en de officiële instanties radeloos de eerste duiding probeerden te geven aan wat zich aanvankelijk liet aanzien als een verschrikkelijk ongeluk, knalde het web zo'n beetje uit elkaar. Zoals altijd was *GeenStijl*[4] er weer razendsnel bij. Heel kort na het ongeluk verschenen de eerste foto's en filmpjes op de site, inclusief het kenteken van de auto van de dader. Kort daarop verscheen er op het web een Google Map met de mogelijke route die de dader met zijn auto had afgelegd, gevolgd door een pagina op Wikipedia over de aanslag, een foto van de zwaargewonde dader in de auto, de kentekengegevens (op Twitpic) en de naam en het adres van de dader. De eerste officiële persconferentie van de burgemeester van Apeldoorn moest toen nog beginnen.

Maar het 'wat?' speelt zich tegenwoordig ook geheel digitaal af. Grooming is digitale chantage door bijvoorbeeld te dreigen compromitterende foto's van een meisje online te zetten, wat kan leiden tot gedwongen prostitutie (loverboy 2.0) en mensenhandel (moderne slavernij). Het 'wat' is dan chantage via de digitale weg, en het 'hoe' is dreigen met heimelijk gemaakte of gestolen foto's. De modus operandi is dus deels digitaal geworden. Een dader bouwt hiermee ongewild wel een eigen dossier vol belastende feiten op.

15.2.3 Waarmee?

Waarmee wordt een delict gepleegd? Het web biedt een ideale mogelijkheid om informatie te delen met het publiek, bijvoorbeeld over voorwerpen die op een plaats delict zijn gevonden.

---

4 'Aanslag op Koningin Beatrix.' In: *GeenStijl*, 30 april 2009. http://www.geenstijl.nl/mt/archieven/2009/04/aanslag_op_koningin_beatrix.html

Zo is de beruchte kinderpornozaak rond Robert M. opgelost doordat Amerikaanse rechercheurs zich afvroegen waar het Nijntjedoekje vandaan kwam dat samen met een jongetje in een video te zien was. De video werd vervolgens op de Nederlandse televisie getoond. Het spoor leidde naar Amsterdam en daarmee was de arrestatie van Robert M. alleen nog een kwestie van tijd. Nog tijdens de persconferentie van de zedenzaak in Amsterdam gingen de privégegevens van Robert M. – wiens naam op dat moment nog niet genoemd was door de overheid – al over alle sociale media.

De MO van daders krijgt ook steeds vaker een digitale component. De loverboy 2.0 kan bijvoorbeeld de webcam van zijn slachtoffer op afstand aanzetten of iemands Facebook-account kraken, compromitterende foto's binnenhalen en daarmee zijn slachtoffer onder druk zetten. Gewoon vanachter het toetsenbord. Dat was zeker het geval bij Robert M. Die bewoog zich door de onderwereld van het internet, de zogenoemde *darknets*, die ook niet door Google worden gescand. Een darknet is een 'verborgen' anoniem netwerk waarop door individuen clandestiene bestanden kunnen worden gedeeld. De entreeprijs bij een kinderpornonetwerk is hoog, want alleen mensen die eigen materiaal inbrengen, kunnen lid worden. Dat maakt het voor de politie extra moeilijk: om toegang te krijgen tot een dergelijk netwerk zou de politie dus strafbaar moeten handelen.

15.2.4 Wanneer?

Timing is alles. Bij de Belastingdienst en de Sociale Verzekeringsbank weten ze dat ook. Mensen zetten de gekste dingen op het web en dat kan grote gevolgen hebben. Het is bijvoorbeeld niet zo handig om foto's van de linedancewedstrijd waar je de eerste prijs hebt behaald op Facebook te zetten als je in de Ziektewet zit vanwege rugproblemen.

In de timelines op Twitter en op Facebook kunnen belangrijke aanwijzingen te vinden zijn over daders en slachtoffers. Overal staat immers een precies tijdstip bij. Als deze mensen dan ook nog bijvoorbeeld Foursquare[5] gebruiken, dan weet de politie waar ze zich op dat moment bevonden. Natuurlijk kunnen de eigenaars van een smartphone dan nog altijd zeggen dat ze hun mobieltje net op die dag zijn kwijtgeraakt. Voor het controleren van een alibi is dus nog wel wat meer nodig.

15.2.5 Waar?

Waar gebeurde het, op welke locatie? Met Google Maps en Streetview kan iedere burger zelf een eerste scan van de omgeving doen.

In 2008 werd een 14-jarige jongen door twee mannen beroofd. Een halfjaar later ontdekte het slachtoffer dat er beelden op Streetview stonden die vlak voor de beroving waren gemaakt. Hij nam direct contact op met de politie, maar de foto was niet >>

5 Foursquare is een app waarmee gebruikers kunnen laten zien waar ze zijn.

>> bruikbaar omdat de gezichten onherkenbaar waren gemaakt. De politie verzocht Google de originele foto toe te sturen en daarop herkende een rechercheur een van de verdachten. Omdat de andere dader veel op hem leek, nam de politie aan dat het hier een tweeling betrof. Geconfronteerd met het bewijs gaven de broers toe dat zij op de foto stonden, maar ze ontkenden dat ze de jongen hadden beroofd. Een van de broers bekende wel dat hij geld van het slachtoffer had verduisterd.

Maar de impact van sociale media op het 'waar' gaat nog veel verder. Met Localscope voor de iPhone weet je bijvoorbeeld altijd waar je bent en wat er in de omgeving te doen is. Dankzij Localscope kan een rechercheur die naast een lijk staat, dus ook zien wie er in een straal van vijf kilometer een foto heeft gemaakt en die op Instagram heeft gezet, en wie een berichtje heeft gestuurd met Twitter. Of stel dat het slachtoffer een sporttas bij zich droeg. Dan is het voor de rechercheur kinderspel om te kijken waar de dichtstbijzijnde sportschool is en kan hij daar zijn onderzoek beginnen.

Steeds vaker is ook het web zelf een plaats delict. Naar aanleiding van een digitaal dreigbericht – op een geschreven bedreiging met de dood kan in de fysieke wereld nog altijd een gevangenisstraf tot vier jaar worden opgelegd – op 4chan.org[6] (1 miljoen berichten per dag) werden in april 2013 in Leiden alle middelbare scholen gesloten en door de politie bewaakt. Uiteindelijk bleek de dader zich in Costa Rica te bevinden, waardoor de fysieke dreiging weliswaar gering bleek te zijn. De maatschappelijke impact was echter heel groot. Zo kan een bericht dat iemand in een paar seconden op het web zet, leiden tot een schadepost van miljoenen euro's.

15.2.6 Welke wijze?

Op welke manier het delict is gepleegd, wordt de modus operandi genoemd. De impact van sociale media kan groot zijn als mensen zich door een filmpje op YouTube laten inspireren of hun daad aankondigen via het web.

Copycats zijn er altijd geweest en zullen er altijd zijn. Dat geldt niet alleen voor de man achter de zogenoemde Batman-shooting die zich na zijn daad voorstelde als de Joker, maar dichter bij huis ook voor de mensen die zich toeleggen op het maken van levensgevaarlijke vuurwerkbommen. Maar hier kan het web de politie ook verder helpen. Veel bommenmakers vinden het namelijk leuk om de resultaten van hun werk online met anderen te delen. Die kunnen dan gelijk een brief verwachten van de in 2011 opgerichte Task Force Opsporing Vuurwerk Bommenmakers, een digitale gele kaart dus. Ook Project X in Haren – het volkomen uit de hand gelopen 'feest' in het ingedommelde dorpje in Groningen – kende zijn copycats. Er zijn sindsdien via sociale media wel dertig oproepen geweest om een nieuw Project X te starten ergens in Nederland, maar daar is verder door de overheid weinig ruchtbaarheid aan gegeven. Door een massale inzet van politie ter plaatse was voor eventuele feestgangers de lol er sowieso snel af. Ja, ook hier kunnen sociale media maximale impact hebben.

6 4Chan (2013). *Stats*. http://www.4chan.org/advertis

Er zijn ook criminelen die gebruikmaken van sociale media bij het plannen, organiseren en uitvoeren van een misdaad. Achter dat gezellige vriendinnetje van twaalf jaar op Facebook dat met je afspreekt op een verlaten plek in het park kan zich heel gemakkelijk een pedofiel verschuilen. Of een kinderverkrachter. Berucht zijn ten slotte bijvoorbeeld ook de talloze DDoS-aanvallen door de 'hacktivisten' van Anonymous op doelen die door leden van deze losjes georganiseerde groep als vijandig worden aangemerkt.[7] Overigens vraagt Anonymous de leden via Twitter om nieuwe ideeën.

15.2.7 Waarom?

Met het beantwoorden van de waaromvraag kijkt de politie naar het doel dat werd beoogd; het oogmerk of het motief. Sociale media bieden de politie alle mogelijkheden om het publiek mee te laten denken, zeker in het geval van een zwaar misdrijf.

Zuiderdiepcase

In het geval van de moord op de 65-jarige man in 2011 in Groningen ging de politie nog een stap verder. De man, die onder meer boodschappen deed en allerlei klusjes opknapte voor Groningse prostituees, en regelmatig opschepte dat hij nogal wat geld achter de hand had, was dood in zijn huis aangetroffen met vastgebonden voeten. Kort na het misdrijf had het Team Grootschalige Opsporing (TGO) Zuiderdiep al heel veel gegevens over de man en de zaak zelf op het web gezet, en het publiek uitdrukkelijk uitgenodigd mee te denken over mogelijke scenario's. Er kwamen er niet minder dan 120 binnen. Uiteindelijk bleek het te gaan om een brute roofmoord door een Colombiaan, die tegen de lamp liep toen er een match werd gevonden met het DNA dat hij op de plaats van het delict had achtergelaten. Wat aan deze zaak opvallend was, was echter de grote bereidheid van burgers om actief met de politie mee te denken.

Zeker in het geval van zware misdrijven moet dus altijd de mogelijkheid worden overwogen om een zaak binnen 24 uur online te zetten. Maar kritiek op de zaak was er ook, van wetenschappers. Het Openbaar Ministerie (OM) en de politie werd verweten dat hiermee een serieus vak min of meer tot een gezelschapsspel (Cluedo) werd gedegradeerd. Daarmee ging men wel voorbij aan het feit dat er ook in de opsporing sprake is van democratisering. Het publiek eist en verdient hierin een rol te spelen. Bovendien: het werkt.

15.2.8 De redenen van wetenschap?

Deze achtste gouden W dwingt de individuele politieman of -vrouw kritisch naar zijn of haar werk te kijken. Hoe is het antwoord op de zeven andere W's eigenlijk tot stand gekomen?

---

7 DDoS: een distributed denial-of-serviceaanval is een poging om een computer(netwerk) onbereikbaar te maken door vanaf meerdere computers vele verzoeken te sturen.

Als het om een verdachte persoon gaat, dan zal een rechercheur of uitluisteraar van bandopnamen dus echt met zo veel woorden moeten zeggen: 'Ik heb gehoord dat dit meneer X is. Hij praatte met mevrouw Y. Zij is met hem getrouwd en noemde hem meneer X. Het ging hierbij om dat en dat nummer.' De bedoeling hiervan is ook om subjectiviteit uit te sluiten (zintuiglijke waarneming, zoals 'ik zag' of 'ik hoorde').

Met behulp van internet Research Netwerk (iRN) is het vrij eenvoudig om sociale media en het web te doorzoeken op interessante dwarsverbanden en dit veilig te stellen.

Ook hier moet de politie bij de les blijven. Iemand kan op Facebook wel zeggen dat hij een roofoverval heeft gepleegd, maar wie zegt dat hij op dat moment achter zijn computer zat? Met andere woorden: wie kan er allemaal bij zijn account? Is onomstotelijk vast te stellen dat het bericht daadwerkelijk van een verdachte afkomstig is? Dergelijk digitaal bewijs zal door de rechtbank in de regel zeer kritisch worden bekeken.

In de *Aanwijzing opsporingsberichtgeving* is een duidelijk wettelijk kader vastgesteld, inclusief de nieuwe mogelijkheden die sociale media bieden. Daarnaast gelden de juridische fundamenten bij het opsporingsproces zelf (die trouwens veelal uit de achttiende en negentiende eeuw dateren). Het is niet genoeg op Facebook te lezen dat iemand zegt iets te hebben gedaan. Voor het komen tot, en het opmaken van, een proces-verbaal (het schriftelijke eindresultaat) zijn er kaders. Een goed proces-verbaal zorgt dat opgespoorde verdachten zo eerlijk en doelmatig mogelijk worden berecht. Het proces-verbaal is als onderzoeksverslag het bewijsmiddel tijdens een zitting van de rechtbank. Het rapporteert over gebeurtenissen, feiten en omstandigheden die de opsporingsambtenaar heeft waargenomen en de handelingen die hierbij zijn uitgevoerd. Het proces-verbaal is waarheidsvinding met zowel belastende als ontlastende informatie. De waarheid is hierin kenbaar en gaat over feiten en causale verbanden die daartussen worden aangetoond.

15.3 Sociale media voor samenwerking met burgers

Sociale media hebben het bereik en de snelheid van communicatie enorm vergroot. De impact ervan ook trouwens. Lokale en regionale berichtgeving hebben onbedoeld vaak een landelijke uitwerking. Een incident klein houden is er niet meer bij, zodra iets online staat kijkt de hele wereld mee. Opsporingsberichtgeving kent tal van communicatiekanalen (van de krant tot *Opsporing Verzocht*) en er wordt meestal samengewerkt met mediapartijen die bekendstaan om hun nauwkeurige berichtgeving. Op sociale media is dat anders, daar zijn de informatiestromen vrijwel niet meer te beheersen.

'Vroeger was het inschakelen van het publiek een laatste redmiddel. Nu doen we dat veel sneller. Met YouTube en Twitter en nu met zo'n site. Ik wil af van de geslotenheid bij de politie. De meest cruciale informatie deel je niet, maar de rest geven we weg. Laat mensen maar meedenken. Laat maar zien wat we doen en weten.'
– *Frans Greve, districtsrecherche Groningen*

Was opsporingsberichtgeving vroeger het laatste redmiddel, tegenwoordig begrijpen we dat het in elke fase van het onderzoek te gebruiken is en dat een opsporingsbericht juist ook kort na een misdrijf nuttig kan zijn, omdat de herinnering van eventuele getuigen dan nog vers is. Een opsporingsbericht, bijvoorbeeld in de vorm van een weblog, is dan aan het begin van een opsporingsonderzoek te beschouwen als een uitgebreid buurtonderzoek. Komen er in de loop van het onderzoek nieuwe vragen naar voren, dan kan het OM opnieuw de hulp van het publiek inroepen met een nieuw opsporingsbericht.

Bij de beslissing om al dan niet gebruik te maken van opsporingsberichtgeving maakt het OM altijd een afweging van de verschillende belangen. Aan de ene kant is dat de strafrechtelijke handhaving van de rechtsorde en aan de andere kant de persoonlijke levenssfeer (de privacy) van de betrokkene(n). Het OM houdt hierbij nadrukkelijk rekening met het grote (en steeds grotere) bereik van verschillende mediavormen (zoals internet) en de omstandigheid dat eenmaal gepubliceerde berichtgeving zich niet meer zonder meer laat verwijderen of herroepen.

Opsporingsberichtgeving kan de persoonlijke levenssfeer of andere belangen van betrokkenen raken (verdachte, slachtoffer en eventueel getuigen). Het OM moet bij de beslissing om dit middel in te zetten met ieders belang rekening houden. Net als bij de inzet van andere opsporingsmiddelen gelden de vereisten van proportionaliteit en subsidiariteit.

Proportionaliteit: de zwaarte van het in te zetten middel moet in verhouding staan tot het beoogde doel. Hierbij speelt de ernst van het gepleegde delict een rol.

Subsidiariteit: het middel wordt ingezet als een eventueel minder zwaar middel niet tot voldoende resultaat heeft geleid of zal kunnen leiden. Wordt het doel ook met een voor de verdachte minder belastend middel bereikt, dan moet voor dat middel worden gekozen.

Vertaald naar opsporingsberichtgeving: hoe ernstiger het opsporingsbericht de belangen van de verdachte schendt, hoe belangrijker het is dat het doel in verhouding staat tot het middel én het beoogde doel niet op een andere manier kan worden bereikt die de privacy van de verdachte of andere belangen minder schendt. Een algemeen opsporingsbericht dat informatie geeft over het gepleegde delict en getuigen vraagt zich te melden, zal de privacy of een ander belang van de verdachte niet snel schenden. Dit is natuurlijk anders als er een compositietekening of zelfs camerabeelden worden getoond.

De politiek en instanties zoals het College bescherming persoonsgegevens, waken voor inbreuken op de persoonlijke levenssfeer van burgers, die overigens worden gepleegd door zowel de overheid als door burgers. In de strafzaak is het de zittingsrechter die achteraf de rechtmatigheid van de inzet van het middel toetst. Onderzoek van de Politieacademie wijst uit dat burgers positief zijn over het meedenken in opsporingsonderzoek, hoofdzakelijk vanwege de grote kennisbron en frisse blik die aangeboord wordt. De respons is doorgaans hoog: in de moordzaak van Mostafa Talaie in 2013 kwamen 188 scenario's binnen via de website en 27 telefonische tips.

Een speciale website en een Twitteraccount worden tegenwoordig als online cocreatiemogelijkheden standaard op www.politie.nl aangeboden. Naast het traditionele tipformulier kan men ook nieuwe 'zienswijzen' op een zaak aanbrengen. Op de site zijn diverse bouwstenen om een zaak op een aantrekkelijke en relevante manier aan te bieden, zoals de levensloop van slachtoffer(s), een tijdlijn met gebeurtenissen, beeldmateriaal (foto's, video, 3D-beeld plaats delict) of relevante locatievoorzieningen (kaarten).

De Zuiderdiepcase (vervolg)

'De eerste uren na een overval zijn belangrijk. We plaatsen daarom bijvoorbeeld locatie en signalementen direct op internet.'
– *Frans Greve, recherchechef eenheid Noord-Nederland*

Er werd gekozen om de toegangsdrempel zo laag mogelijk te houden en het indienen van scenario's in een *free format* te laten gebeuren. De scenario's zouden dan simpelweg in de mailbox van de recherche terechtkomen, waarna het rechercheteam kon beslissen of deze ze online zou delen.

Doelgroep

Niet alleen lokale media besteedden aandacht aan de zaak, maar ook de landelijke media, waaronder *Opsporing Verzocht*. Op deze manier kon iedereen meedoen. De motivatie om bij zware geweldsmisdrijven een zaak op te lossen, is overigens onder burgers meestal hoog, zeker als de zaak actueel is.

Figuur 15.3 Foto van de omgeving van het misdrijf, overgenomen van Google Streetview

Communicatie

Er was bewust gekozen om alle communicatiemiddelen (mix) aan elkaar vast te knopen. Dus na de uitzending van *Opsporing Verzocht* op televisie kon men terecht op de website. De schrijvende pers en de lokale pers werden daarnaast in één keer >>

>> bediend. Twitterende wijkagenten hebben aandacht gevraagd voor de zaak en er zijn flyers rondgedeeld onder met name mensen die dicht bij het incident woonden (zelfs in het Engels).

Organisatie

Het openstellen van een zaak voor burgers is niet eenvoudig. Daderkennis moet achterwege blijven en er moet een goede afweging gemaakt zijn van de afbreukrisico's. Na contact met de familie is uiteindelijk door de zaaksofficier besloten de zaak snel online te zetten bij gebrek aan voldoende opsporingsaanwijzingen. Extra hulp van de communicatieafdeling was hierbij onmisbaar.

Doelstellingen

De kerntaak van de opsporing ligt nog altijd bij het verzamelen van feiten, zodat over iemand kan worden geoordeeld in relatie tot de verdenking van een strafbaar feit. Maar de politie van Groningen – mede gestimuleerd door het Centrum Versterking Opsporing – ging een stap verder. Zij wilde:

- Burgers bij de zaak betrekken om de informatiepositie te verbeteren (er waren geen concrete aanwijzingen in een complex gebied met wisselende contacten).
- Burgers als bondgenoot door het online delen van mogelijke scenario's (puzzelstukjes). Voor de politie zelf gold hier: je moet transparanter en met meer verantwoordelijkheid proberen te communiceren over de zaak. De overkoepelende doelstellingen waren betere politieprestaties – de zaak sneller en beter oplossen – en legitimiteit (door wederzijds vertrouwen). Het hielp daarbij dat het om een recente moord ging die bij iedereen vers in het geheugen zat. Bij een bijna verjaarde *cold case* is dat anders.

Er was speciale aandacht voor de cultuur, competenties en vaardigheden in het TGO dat op deze zaak werd gezet. Vanuit de communicatieafdeling werd affiniteit met sociale media ingebracht, door eerdere ervaringen met YouTube en Twitter, en werden de sociale media-middelen voor opsporingsberichtgeving en online cocreatie ingericht en bediend.

'Daar zaten scenario's bij waar wij nog niet aan hadden gedacht en zeer bruikbare tips. Je ziet dat ook mensen reageren die de man of zijn omgeving goed kennen.'
– *Frans Greve, districtsrecherche Groningen*

Met de zaaksofficier als eindverantwoordelijke intensiveerde het team de communicatie met burgers wanneer dat nodig was. Binnengekomen informatie werd besproken binnen de teamleiding TGO. Meer en frequentere online interactie met burgers vereiste een omschakeling, maar leverde wel 120 scenario's op. De tactische >>

>> recherche gebruikte deze scenario's naast de aanvullende informatiebronnen – waaronder open bronnen op internet – om tot een oplossing te komen. Hoewel die oplossing uiteindelijk met een DNA-match uit het lab van het Nederlands Forensisch Instituut tot stand kwam, heeft de *wisdom of the crowd* wel gewerkt: het gros van de burgerscenario's wees in de juiste richting.

Deel V
De werking van IGP: sturing

16 In gesprek met Henk Bril over beslissen

Figuur 16.1 Henk Bril

Henk Bril is sectorhoofd van de Dienst Landelijke Informatieorganisatie (DLIO). Hij heeft net een tweedaagse bijeenkomst van het landelijke Platform Informatieorganisatie (PIO) met de sectorhoofden van de regionale en landelijke informatieorganisaties (DRIO en DLIO) bijgewoond en nieuwe inspiratie opgedaan. Tijdens de tweedaagse werd stilgestaan bij de recente ontwikkelingen rond de informatieorganisatie van de politie en de uitdagingen in de nabije toekomst. Voor Henk is informatiegestuurd politiewerk (IGP) voor de ontwikkeling van het korps een rode draad, waarbij hij stelt dat een aantal IGP-concepten eigenlijk nog niet goed is ingevoerd. Volgens hem is er een risico dat we een nieuw concept starten en daarmee verbloemen dat het vorige nog niet van de grond is gekomen.

'In Nederland was het vooral het voormalige korps Rotterdam-Rijnmond dat in samenwerking met de politie uit Kent (Verenigd Koninkrijk) midden jaren negentig pionierswerk deed met informatiegestuurde opsporing (IGO). Er is toen bij de regionale recherche een andere manier van werken gestart. Men ging investeren in het analyseren van veiligheidsproblemen. Criminele groeperingen werden geïdentificeerd en zaken werden gekozen op basis van goede informatieposities in het criminele milieu, waarbij steeds informatie aan de basis lag van beslissingen over capaciteit en middelen voor de onderzoeken. Daarna werd IGO uitgebreid naar al het politiewerk, met als centrale gedachte dat je op basis van halve informatie geen hele oordelen kunt vellen. Toch blijft die verleiding bestaan. Dat raakt aan de wezenlijke vraag: is het nu informatiesturing of sturen met informatie?'

Meerwaarde

'Informatiegestuurd werken werd aanvankelijk vooral omarmd om bij te dragen aan meer kwaliteit in het nemen van beslissingen. Er werden protocollen en standaardproducten ingevoerd. Een mooi voorbeeld is het zogenoemde preweegdocument dat werd opgesteld voor een stuurploeg die moest beslissen of een mogelijke zaak of subject zou worden omgezet in een projectvoorstel voor onderzoek. In de kern een goede gedachte, maar compleet doorgeschoten als je je realiseert dat zo'n preweegdocument een enorme omvang kreeg met een behoorlijke administratieve last, en dat door de volgordelijkheid de besluitvorming steeds stroperiger werd.

Inmiddels is het besef doorgedrongen dat we veel sneller moeten inspelen op wat buiten gebeurt. Dat er in de informatiemaatschappij van nu nieuwe eisen aan ons worden gesteld, dat ons adaptief vermogen omhoog moet en dat van ons meer alertheid, assertiviteit en proactiviteit worden verwacht. Maar ook het besef dat de hele politie in de kern een informatieverwerkend bedrijf is en informatie dus van iedereen is. Wat is dan nog de meerwaarde van de informatieorganisatie?

De informatiediensten in de elf eenheden van de politie geloven in het actief, innovatief en coöperatief bijdragen aan veiligheid met het leveren van juiste en tijdige *intelligence* voor het politiewerk, als één informatieorganisatie voor de nationale politie. Intelligence is in de definitie geanalyseerde informatie voor de besluitvorming. Dat doet de informatieorganisatie door het opwerken van signalen (van data tot intelligence), door beeldvorming en duiding en door het participeren in de operatie. Ondersteunen van besluitvorming in de operatie staat centraal.

De informatieorganisatie heeft meerwaarde door het aanjagen van informatie-inwinning, het intelligent bevragen van datasystemen, het opbouwen van informatieposities, het creëren van overzicht en inzicht, het actief duiden, taxeren en adviseren, het activeren van briefen en debriefen en het doen van informatiecoördinatie. De informatieorganisatie is zowel informatiedienst voor straatinformatie, zaaksinformatie, sturingsinformatie, als inlichtingendienst voor gesloten bronnen. De informatieorganisatie is met name ook verbindingsdienst, onder andere tussen het lokale, nationale en internationale niveau, tussen overheidsdiensten en tussen informatie en kennis.'

Figuur 16.2 Politie op straat

De toekomst

'De informatieorganisatie heeft een aantal bijzondere uitdagingen voor de boeg. De informatie- en intelligencefuncties die ik noemde, zullen wijzigingen ondergaan om sturing en besluitvorming te blijven ondersteunen. Het is dan ook zaak om goed te kijken naar wat er staat te gebeuren en wat we moeten doen. We zijn bijvoorbeeld bij de landelijke informatieorganisatie al bezig om beeldvorming te verbeteren met behulp van één dagelijks nationaal en lokaal intelligencebeeld. Ook richten we een *Situation Room* in waarin beslissers de wereld om zich heen in beeld krijgen en antwoord kunnen geven op de vragen: wat is er aan de hand, wat hebben we gedaan en wat spreken we af?

Andere aanpassingen betreffen de rol van partners, zowel publiek als privaat, bij het opbouwen van informatieposities. Denk maar aan gemeenten met een eigen informatiedienst, die binnenkort al een behoorlijk beeld kunnen schetsen van wat er lokaal aan de hand is, ook op het terrein van criminaliteit. En om nog een ander punt te noemen, ook de rol van data-analyse kan niet onbesproken blijven. Wij zijn al bezig met *big data solutions* als het gaat om *tooling*, maar denk ook aan de veranderende rol van onze vakmensen, van informatieverwerker tot bevrager. Naast het toepassen van nieuwe technologische mogelijkheden zal er blijvend aandacht moeten blijven voor inwinning van de menselijke bron. In grote onderzoeken zien we dat *human intelligence* belangrijke meerwaarde heeft en houdt.

Als we verder naar voren kijken, dan zien we een ontwikkeling waarin de verbindende functie van de informatieorganisatie steeds belangrijker wordt. De vraag naar voorspellende waarde van informatie (zoals bij *predictive policing*), de verwetenschappelijking van het informatievak, en de privacy- en ethiekdiscussie nemen toe. We zullen ons moeten wapenen tegen de toename van desinformatie en vaker aan de slag moeten met falsificeren van desinformatie. Om al die ontwikkelingen het hoofd te bieden en informatiesturing te helpen, wil ik een stevig pleidooi houden voor experimenteerruimte en het vrijstellen van vakmensen om het noodzakelijke "ongewone" te kunnen doen zodat we met informatie de besluitvorming goed blijven ondersteunen.'

17 Briefen en debriefen: de wortels van IGP?

Michiel In 't Veld, Robert Paul Doorenbosch en Fons Sarneel

Figuur 17.1 Briefing

'De briefing is een goed moment om kaders te scheppen. Het is namelijk onzin dat we helemaal geen sturing willen, iedereen zoekt kaders waarin ie kan werken, ook politieagenten.'
– *Politiemedewerker, mei 2013*

'Hier is het zo dat de briefing gewoonweg voor je voeten wordt geworpen (...) Degene die nu de briefing geeft, is eigenlijk ook een soort toehoorder want hij heeft de briefing niet samengesteld. Wat ik doe als chef is soms de briefing *overrulen*, dus door af te wijken van de briefing en prioriteiten ergens anders te leggen. Dit heeft het nadeel dat ik aan de groep laat zien dat ik de briefing niet serieus neem.'
– *Operationeel leidinggevende, mei 2013*

'Ik vind dat een briefing uitsluitend over het operationele werk moet gaan. Dia's over landelijke protocollen horen niet thuis in een briefing (...) De collega's zitten niet te wachten op informatie over systemen of informatie die ze ook al via de mail hebben gekregen. Op die manier krijg je een overkill aan informatie en schiet je het doel voorbij.'
– *Operationeel leidinggevende, april 2013*[1]

1 Citaten uit: Hengst, M. den & M. In 't Veld, *Briefen voor en door basisteams*. Boom Lemma uitgevers, Den Haag 2014.

Zomaar drie citaten van politiecollega's van enkele jaren geleden over knelpunten rond de politiebriefing. Enerzijds over het wel willen ontvangen van sturing en anderzijds, vanuit de gever, over de wens tot richting willen geven aan het politiewerk zonder daarbij te verzanden in procedurele of protocollaire informatie. Hoe kunnen deze knelpunten aangepakt worden? Dat was de vraag waarmee de projectgroep e-Briefing aan de slag is gegaan. Mede op basis van de planvorming van de nationale politie en wetenschappelijke inzichten zijn een briefingsproces en -tool ontwikkeld en geïmplementeerd, als hulpmiddel voor de basisteams van de politie.

Zijn de knelpunten nu opgelost, en in hoeverre dragen zij bij aan het gedachtegoed van informatiegestuurd politiewerk (IGP)? Dit hoofdstuk gaat hierop in door eerst de roots van de (de)briefing te schetsen, stil te staan bij de planvorming rond het thema briefen en debriefen, te beschrijven hoe het briefingsproces en de briefingstool zijn ontwikkeld en tot slot te evalueren; leiden 'proces en tool' tot gewenste veranderingen in de politiepraktijk? Het hoofdstuk sluit af met een toekomstschets, welke weg slaan we in als het gaat om de politiebriefing?

17.1 Briefen en debriefen: waar komt het vandaan?

De briefing, uiteraard ontleend aan het Engels, kent haar oorsprong in het Amerikaanse leger. In 1897 ontwikkelde kapitein Eben Swift de *Five Paragraph Field Order,* waarmee aan de hand van de vijf begrippen *situation, mission, execution, administration* en *command & signal* informatie op gestructureerde wijze aan militaire eenheden kon worden overgedragen.[2] Het doel van deze wijze van overdragen was drieledig; ten eerste het waarborgen van gecoördineerd optreden onder gezag van de commandant, ten tweede beperking van verstrekking van de hoeveelheid informatie aan ondergeschikten en ten derde het op een gestandaardiseerde en gestructureerde wijze presenteren van informatie zodat zij eenvoudig verwerkt kon worden.

Dit model heeft zich vanaf de jaren zestig en zeventig van de vorige eeuw genesteld binnen de Nederlandse politie. Deze wijze van briefen is bekend geraakt als het zogenoemde 5-paragrafenmodel, waarbij achtereenvolgens de begrippen toestand, opdracht, uitvoering, verzorging en bevelvoering/verbindingen aan de orde komen in een briefing. Gaandeweg heeft dit model zich ontwikkeld als basis voor de briefing in voorbereiding op (grootschalige) evenementen en in voorbereiding op specifieke acties van bijvoorbeeld arrestatie- en verkeerspolitieteams.[3]

---

2 Aan de basis van zijn model lagen de praktijkervaringen van de Duitse generaal-veldmaarschalk Helmuth Graf von Moltke (1800-1891), zie: Smith, M., 'The Five Paragraph Field Order: Can a better format be found to transmit combat information to small tactical units?' In: *School of Advanced Military Studies U.S. Army Command and General Staff College Fort Leavenworth*. First Term AY 88-89, Kansas 1988.

3 Zie voor een uitgebreide beschrijving van het '5-paragrafenmodel': In 't Veld, M. & M. den Hengst, 'Briefen bij evenementen: een verkenning in de praktijk.' In: Adang, O. et al. (red.), *Politie en evenementen: feiten, ervaringen en goede werkwijzen*. Boom Lemma uitgevers, Den Haag 2014, pp. 78-92.

Onlosmakelijk verbonden met briefen is het debriefen. Debriefen kent verschillende doelen, bijvoorbeeld terugblikken op uitgevoerde acties of reflecteren op het eigen of groepsoptreden. Ook het debriefen ontleent haar bestaan aan de toepassing in het Amerikaanse leger. Hier werd de zogenoemde *After Action Review* (AAR) in de jaren zeventig van de vorige eeuw ontwikkeld. Primair als methode om militaire trainingsoefeningen te evalueren. De AAR is interactief van vorm, waarbij teamleden stilstaan bij vier kernvragen:

1 Wat was de geplande opdracht?
2 Wat gebeurde daadwerkelijk?
3 Waarom verliepen de gebeurtenissen op deze wijze?
4 Wat kan de volgende keer beter worden uitgevoerd?[4]

Naast de militaire sector kent de AAR inmiddels een bredere toepassing, bijvoorbeeld in de gezondheidszorg, waar wordt gedebrieft om informatie uit te wisselen tussen verpleegkundigen die hun diensten afwisselen.[5] In ziekenhuizen resulteren briefings en debriefings, doorgaans in de vorm van checklists, in minder fouten, betere onderlinge communicatie en gedeelde verantwoordelijkheid.[6]

Naast bespreking van het groepsoptreden of specifieke uitgevoerde acties kent debriefen ook een psychologische component, namelijk bijdragen aan de verwerking van traumatische ervaringen. Begin jaren tachtig van de vorige eeuw is het bij defensie, brandweer en politie gebruikelijk geworden om na afloop van heftige emotionele gebeurtenissen direct te debriefen, ook wel *hot-debriefing* genaamd.[7] In tegenstelling tot studies naar de vormgeving en het effect van de politiebriefing zijn er weinig studies naar het debriefen binnen de politie.[8] Een van de redenen hiervoor is dat, anders dan bij de

4 Morrison, J. & L. Meliza, *Foundations of the After Action Review Process. ARI Special Report 42*. U.S. Army Research Institute for the Behavioral and Social Sciences, Alexandria (VA) 1999.

5 Grosjean, M., 'From multi-participant talk to genuine polylogue: shift-change briefing sessions at the hospital.' In: *Journal of Pragmatics* 36 (2004), pp. 25-52.

6 Zie bijvoorbeeld: Lingard, L. et al., 'Evaluation of a preoperative checklist and team briefing among surgeons, nurses, and anesthesiologists to reduce failures in communication'. In: *The Archives of Surgery* 143 (2008), 17 (Dec);
Paull, D.E. et al., 'Briefing guide study: preoperative briefing and postoperative debriefing checklists in the Veterans Health Administration medical team training program.' In: *The American Journal of Surgery* 200 (2010), nr. 5, pp. 620-623.

7 Lieverloo, M. van, *Preventieve interventies, onderzoek naar werking en effectiviteit van hotdebriefing bij hulpverleners, na acute situaties*. Masterthesis MCPM 2012.

8 Uitzonderingen vormen studies naar aanleiding van incidenten, bijvoorbeeld de studie van Carlier et al. naar debriefen binnen de politie naar aanleiding van de Bijlmerramp (1992), zie Carlier, I. et al., *Het effect van debriefen: een onderzoek bij de Amsterdamse politie naar aanleiding van de Bijlmerramp*. Intern rapport, Academisch Medisch Centrum bij de Universiteit van Amsterdam, Divisie Psychiatrie, Psychotraumagroep, Amsterdam 1994.
Recenter is de studie naar het debriefen naar aanleiding van een familiedrama in Schalkwijk (2012), zie: Smit, A. & I. Volgelzang, *Debriefen na een ingrijpend incident: Schalkwijk als leerpraktijk*. Politieacademie/Programma Versterking Professionele Weerbaarheid, Apeldoorn 2014.

politiebriefing, het houden van een debriefing binnen de politiepraktijk nog altijd geen gemeengoed is.[9]

17.2 Jaren negentig: opkomst van briefen en debriefen binnen de Nederlandse politieorganisatie

Begin jaren negentig van de vorige eeuw is binnen de politie een ontwikkeling gaande om naast het specialistisch politieoptreden ook teams binnen de Basis Politiezorg (BPZ) te gaan voorzien van een briefing alvorens politieambtenaren de straat opgaan, en te debriefen wanneer zij hun dienst beëindigen. Deze ontwikkeling past in de destijds bredere onderkenning dat door meer informatiegestuurd werken het politieoptreden doeltreffender wordt. Vanaf de start van het informatiegestuurd werken is er geen standaard of leidraad voor het geven van briefings binnen de BPZ.

Eerste ontwikkelingen informatiegestuurd werken: Basiseenheid 'Oude Westen' (1995)

Illustratief voor het informatiegestuurd optreden in de jaren negentig zijn de ervaringen binnen de basiseenheid 'Oude Westen' van het district Centrum van de politieregio Rotterdam-Rijnmond. In 1995 werd gestart met het project 'Sturen op informatie: van beleid naar uitvoering... en terug'. Reden hiervoor: 'We ontdekten dat de dagelijkse informatieverstrekking en de uitgifte van werkopdrachten niet of nauwelijks werden afgestemd of voorbereid.' Het 'operationeel proces' werd ingericht volgens de cyclus van *Plan-Do-Check-Act*. Taakaccenthouders, brigadiers met expertise op het gebied van bijvoorbeeld horeca, huiselijk geweld of drugs, maakten instructieformulieren die besproken werden in het dagelijkse overleg tussen de werkverdeler, informatiemedewerker en chef van de basiseenheid. Dit overleg resulteerde in geprioriteerde instructieformulieren voor de briefing. De briefing werd gehouden door de informatiemedewerker. Na afloop daarvan verdeelde de werkverdeler, destijds een brigadier, de instructieformulieren aan politieambtenaren in de BPZ. De dienst werd afgesloten met een debriefing waar naar resultaten gevraagd werd door de werkverdeler en uitkomsten de basis vormden voor het volgende overleg.[10]

---

9 Scholtens, A., J. Groenendaal & I. Helsloot, *De operationele politiebriefing onderzocht: een onderzoek naar de effectiviteit van de operationele politiebriefing*. Reeks Politiekunde nr. 51. Reed Business Information, Amsterdam 2013.
Terpstra, J. et al., *Basisteams in de Nationale Politie: organisatie, taakuitvoering en gebiedsgebonden werk*. Reeks Politiewetenschap nr. 88. Reed Business Information, Amsterdam 2016.
In 't Veld, M. & M. den Hengst, *'Wat ga jij doen vandaag': evaluatieonderzoek naar de ingebruikname van een briefingtool in acht basisteams van de politie*. Politieacademie, Apeldoorn 2016.

10 Interne video: Basiseenheid 'Oude Westen', *Sturen op informatie: van beleid naar uitvoering... en terug*. Samengesteld door: Egas, J. & R. Klootwijk. Politie intern video. Dienst communicatie: Politieregio Rotterdam-Rijnmond, Rotterdam 1995.

Het jaar 2000 brengt verandering door introductie van het concept informatiegestuurde opsporing (IGO), de voorloper van het hedendaagse IGP. Het programmabureau Aanpak Bedrijfsvoering Recherche, Informatiehuishouding en Opleiding (ABRIO) ontwikkelt een sturingsmodel gebaseerd op het INK Kwaliteitsmodel.[11] Een van de onderliggende principes vormt de Plan-Do-Check-Act-cyclus.[12] Briefen en debriefen kennen binnen het sturingsmodel IGO een cyclisch karakter, waarbij in de briefing 'essentiële informatie en duidelijke instructies voorafgaand aan de uitvoering van het werk' gedeeld worden. De debriefing wordt omschreven als: 'het leren en verantwoorden van uitgevoerd werk door het terugkoppelen van het resultaat van uitgevoerde acties c.q. werkopdrachten en van verworven informatie, alsmede het terugkoppelen van ervaren verbeterpunten in de dienstuitoefening en van ervaringen bij ernstige of emotioneel aangrijpende incidenten'. Ook staat beschreven welke informatie een briefing bevat zoals: informatie over personen, voertuigen, locaties, wijkaandachtspunten, aandachtsvestigingen van modus operandi (MO) en overige bijzonderheden.[13]

Tot slot volgt in 2009 de *Doctrine intelligencegestuurd politiewerk* van de Politieacademie. Het cyclische karakter van het (de)briefingsproces wordt hier schematisch verder uitgewerkt en doelstellingen van de briefing worden eenduidig geformuleerd, te weten:

a het verstrekken van informatie;
b het uitzetten van werkopdrachten.

Wat betreft het debriefen merken de auteurs op dat de functie hiervan drieledig is, namelijk 'het checken of de werkopdracht is uitgevoerd', 'het aftappen van informatie' en tot slot het 'coachen en leren'.[14]

17.3 De nationale politie: 'handen en voeten' aan (de)briefen...

Een impuls voor de inrichting van het briefen en debriefen binnen de basisteams vormt de planvorming van de nationale politie. In 2011 worden het briefen en debriefen in het ontwerpplan omschreven als een van de tien strategische thema's op het gebied van de Operatiën (zie tabel 17.1).

---

11 ABRIO was een samenwerkingsverband tussen het OM en de politie. Het INK-model is in 1992 ontwikkeld door de stichting Instituut Nederlandse Kwaliteit (INK), opgericht door het ministerie van Economische Zaken, teneinde het Nederlandse bedrijfsleven te ondersteunen bij de vormgeving van een kwaliteitsbewakingsmodel.

12 Een organisatorisch hulpmiddel voor kwaliteitsverbetering ontwikkeld door de Amerikaanse statisticus Deming, zie nl.wikipedia.org/wiki/Kwaliteitscirkel_van_Deming.

13 ABRIO, *Briefen en debriefen, voorbereiden en uitvoeren: het procesmodel, de procesbeschrijving en de productbeschrijvingen*. Programmabureau ABRIO, Woerden 2003.

14 Kop, N. & P. Klerks, *Doctrine intelligencegestuurd politiewerk*. Politieacademie, Apeldoorn 2009.

Tabel 17.1 De tien strategische thema's uit het Ontwerpplan Nationale Politie

Strategische thema's Operatiën (2011)	
1 Robuuste basisteams	6 Op- en afschalen
2 Eén concept dienstverlening	7 Uitbouwen van de heterdaadkracht
3 Slagkracht in de opsporing vergroten	**8 Briefing en debriefing**
4 Allianties aangaan met partners	9 Versterken van de interventiekracht op de fysieke en virtuele infrastructuur
5 Collectieve aanpak van high impact crime en ondermijning	10 Internationalisering

Het Ontwerpplan vermeldt over het briefingsproces:

> 'Briefings staan ten dienste van de sturing van de diender, debriefings bieden gelegenheid tot leren en verantwoorden. Om die reden kan de (de) briefing zowel in individueel als collectief verband plaatsvinden. Voor beide geldt dat het een instrument is van de leidinggevende: het is de leidinggevende die brieft en debrieft.'[15]

Nadere uitwerking volgt in het Inrichtingsplan waarin beschreven staat dat de briefing 'het moment [is] dat medewerkers vanuit verschillende processen bij elkaar komen en informatie delen. Debriefing is het moment om informatie en acties terug te koppelen, verantwoording af te leggen en te leren'. Ook wordt een scherpe ambitie geformuleerd: 'Het niveau van (de)briefing bepaalt de doeltreffendheid van de operationele uitvoering van het werk op alle niveaus.'[16] Tot slot vermeldt het daaropvolgende Realisatieplan dat 'operationeel leidinggevenden op elk sturingsniveau briefen en debriefen' en dat 'de informatieorganisatie de leidinggevenden ondersteunt bij de voorbereiding op het briefen en debriefen'.[17] De functie van debriefen als methode om (heftige) incidenten te verwerken komt in de planvorming minder prominent naar voren.

Nederlandse studies naar de politiebriefing

Wetenschappelijk onderzoek uit 2013 en 2014 naar briefen binnen de politiepraktijk leert dat het (de)briefingsproces in elke eenheid (of voormalig politiekorps), verschillend vorm heeft gekregen. En dat de briefing niet het moment is waarop disciplines bij elkaar komen en operationeel leiderschap getoond wordt, bijvoorbeeld uitmondend in de verdeling van persoonlijke opdrachten aan politiemedewerkers. >>

15 Nationale politie, *Ontwerpplan*. 2011.
16 Nationale politie, *Inrichtingsplan*. 2012a.
17 Nationale politie, *Realisatieplan*. 2012b.

>> Daarnaast wordt de functie van de briefing verschillend geïnterpreteerd door de gevers van briefings; is het een middel om slechts informatie te verstrekken of om sturing aan het politiewerk te geven? Ook blijken er geen duidelijke richtsnoeren te zijn over de manier waarop de briefing moet worden vormgegeven, bestaat er onduidelijkheid over de vraag welke informatie in de briefing thuishoort, wordt er in de politiepraktijk nauwelijks plenair gedebrieft na afloop van een dienst en houden de voormalige korpsen er verschillende softwareapplicaties op na, bijvoorbeeld Satijn of STIP, voor het vormgeven en presenteren briefingsdia's.[18]

Daarentegen wordt de rol van de operationeel leidinggevende, diegene die brieft, in de plannen versterkt. Hij dient zijn focus binnen de basisteams te richten op de werkvloer en het overzicht te bewaren. Daarnaast is hij op de hoogte van het actuele veiligheidsbeeld en treedt hij coachend op richting de medewerkers van het basisteam.[19] De operationeel leidinggevende, ook wel operationeel coördinator (Opco) genoemd, stuurt het dagelijks werk in de teams aan. Briefen en debriefen zijn hiervoor dé instrumenten. Het operationele centrum[20], de meldkamer, behoudt de aansturing van het basisteam als het gaat om de spoedeisende meldingen met hoge prioriteit in het werkgebied.[21]

Wat 'we' nog meer weten...[22]

Onderzoek naar het effect van de politiebriefing leert dat een aantal factoren een significant verschil veroorzaakt in beklijving van briefingsinformatie, namelijk:

- het verschil tussen een ochtend- en middagbriefing (een middagbriefing beklijft beter);
- het aantal gepresenteerde dia's (hoe meer dia's, hoe minder onthouden);
- de hoeveelheid informatie (hoe meer informatie aangeboden, hoe minder onthouden);
- verschil tussen binnen en buiten werken (de buitenwerkers onthouden meer informatie); >>

18 Hengst, M. den & M. In 't Veld, *Briefen voor en door basisteams*. Boom Lemma uitgevers, Den Haag 2014.
Scholtens, A., J. Groenendaal & I. Helsloot, *De operationele politiebriefing onderzocht: een onderzoek naar de effectiviteit van de operationele politiebriefing*. Reeks Politiekunde nr. 51. Reed Business Information, Amsterdam 2013.

19 Nationale politie, *Ontwerpplan*. 2011.

20 Het OC neemt 112-meldingen aan, zet niet-spoedeisende meldingen door naar het Regionaal Service Centrum (RSC) en coördineert de inzet van eenheden bij alle spoedmeldingen.

21 Districten Adviesgroep, *Landelijk Werkingsdocument districten & basisteams*. 2016.

22 Deze tekst is ontleend aan de evaluatiestudie van In 't Veld, M. & M. den Hengst (2016), p. 16.

>>

- aantekeningen maken (diegenen die aantekeningen maken, onthouden meer informatie);
- de briefing van een dag ervoor bijwonen (gedeeltelijke herhaling van informatie leidt tot meer onthouden).[23]

Deze bevindingen sluiten deels aan bij eerder onderzoekswerk van de Engelse politiepsycholoog Raymond Bull, die tot de conclusie kwam dat bij een presentatie van zeven items (dia's) in een politiebriefing, het maximale effect bereikt wordt ten behoeve van het onthouden van informatie.[24] Daarnaast liet hij zien dat informatie gegeven via een tv-scherm niet beter of slechter werd onthouden dan informatie gegeven via de traditionele plenaire briefing, en dat ervarener politiemedewerkers beter informatie onthouden.[25] Tot slot leert recent onderzoek van Scholtens (2015) dat bijna alle politieambtenaren opdrachten beter onthielden wanneer die niet plenair, maar persoonlijk werden gegeven, en dat een persoonlijke opdracht krijgen als positief werd ervaren, omdat politiemedewerkers dan verantwoordelijkheid dragen voor een specifieke taak, en duidelijk wordt wat zij kunnen betekenen.[26]

Samenvattend leren de plannen dat briefen en debriefen speerpunten zijn voor de politie. Primair vormen zij de contactmomenten tussen verschillende disciplines binnen het basisteam, zoals tussen wijkagenten, recherchemedewerkers en medewerkers van de Dienst Regionale Informatieorganisatie (DRIO), verzorgd door een operationeel leidinggevende, de Opco. Deze leidinggevende heeft een belangrijke taak in het aansturingsproces van het basisteam. Briefing en debriefing vormen voor hem de instrumenten om daar 'handen en voeten' aan te geven. De vraag blijft met welke hulpmiddelen die instrumenten bespeeld kunnen worden.

17.4 Het instrumentarium: '1 proces en 1 tool'

Ter realisatie van de doelstellingen rond het strategisch thema briefen en debriefen is in 2013 de projectgroep e-Briefing gestart. Zij heeft één landelijk briefingsproces beschreven, dat aansluit bij de genoemde uitgangspunten, en daarbij één softwareapplicatie

23 Dit concludeerden Scholtens et al. (2013, zie noot 9) op basis van uitgedeelde vragenlijsten aan ontvangers van zeventien briefings in drie (voormalige) politieregio's: Brabant-Zuid-Oost, Gelderland-Zuid en Drenthe.

24 Bull, A.R. et al., *Psychology for Police Officers*. John Wiley and Sons, New York 1983.

25 Bull, R. & R. Reid, 'Recall after briefing: television versus face-to-face presentation.' In: *Journal of Occupational and Organizational Psychology* 48 (1975), pp. 73-78.

26 Scholtens, A., *De operationele politiebriefing onderzocht (2): een actie(vervolg)onderzoek om tot een effectieve politiebriefing te komen*. Reeks Politiekunde nr. 51a. Reed Business Information, Amsterdam 2015.

ontwikkeld, de e-Briefingtool. Deze tool vormt het antwoord op de vele verschillende softwareapplicaties waarmee gebrieft werd in de voormalige politieregio's.

Voor beide producten geldt dat voor de totstandkoming ervan gebruikgemaakt is van de *storytelling*-methodiek; hiervoor zijn ervaringen op het thema briefen en debriefen van uitvoerende politiemedewerkers opgetekend en vertaald naar praktijkervaringen, de zogenoemde *user stories*.

Ontwerp van informatievoorzieningen: de user stories

Met behulp van de storytelling-methode zijn praktijkervaringen van politiemedewerkers vertaald naar functionele gebruikerswensen. Hiertoe is een groep van elf adviseurs informatievoorziening, uit elke eenheid één, aan de slag gegaan om met politiemedewerkers in de eenheid in gesprek te gaan over hoe zij de briefing beleven, geven of voorbereiden, resulterend in tachtig interviews bij samenstellers, gevers en ontvangers van briefing. Op basis van deze uitkomsten is een expertgroep samengesteld van dertig politiemedewerkers, waarin de praktijkervaringen zijn uitgediept. Deze aanpak resulteerde in zogenoemde user stories. Dit begrip komt uit de wereld van de softwareontwikkeling, als onderdeel van de Scrum-methode.[27] User stories kennen de volgende vorm:
'Als [type gebruiker] **wil ik** [type functionaliteit] **zodat ik** [type resultaat] **kan behalen**.'[28]

Storytelling is een krachtige methode gebleken die helpt bij het kritisch evalueren van wensen, bij het geven van adviezen en bij het ontwikkelen van nieuwe middelen. Door de operationele organisatie werd het als zeer positief ervaren dat men zo nauw betrokken werd bij de totstandkoming van een nieuw werkproces en bijbehorende informatievoorziening.[29]

17.4.1 Het briefingsproces

Figuur 17.2 geeft schematisch een samenhangend geheel van activiteiten weer van mensen en middelen in het (de)briefingsproces. Het schema geeft teams richtlijnen voor de inrichting ervan. Bij het briefen gaat het om 'het geven van essentiële informatie en duidelijke instructies voorafgaande aan de uitvoering van het werk'. Een briefing dient maximaal vijftien tot twintig minuten te duren en maximaal tien dia's, ook wel briefingsitems genoemd, te bevatten. Uitgangspunt is dat bij elk basisteam tenminste eenmaal per 24 uur gebrieft wordt, door de Opco.

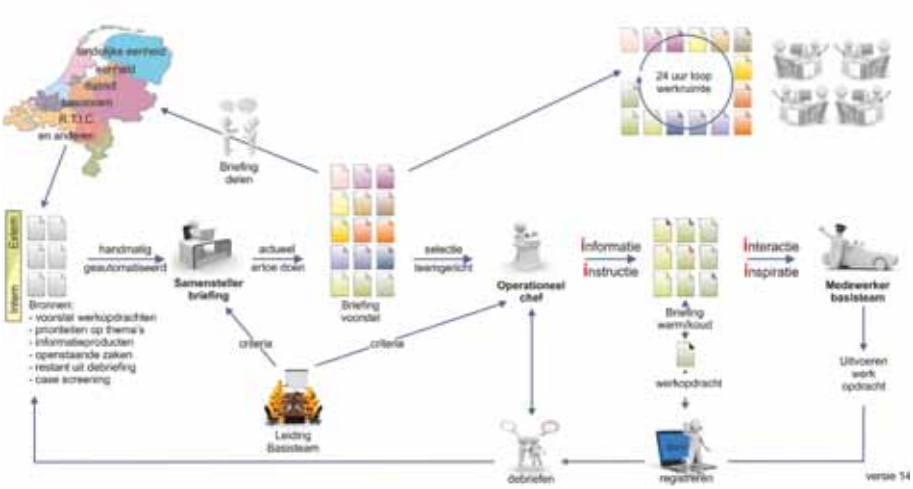
De doelstelling van het debriefen is: 'het leren en verantwoorden van uitgevoerd werk, het vergaren van informatie, en emotionele verwerking'. Ook voor het debriefen zijn

27 'Scrum is een flexibele manier om (software)producten te maken. Er wordt gewerkt in multidisciplinaire teams die in korte sprints, met een vaste lengte van één tot vier weken, werkende (software)producten opleveren. Scrum is een term die afkomstig is uit de rugbysport.' Zie: http://nl.wikipedia.org/wiki/Scrum_(softwareontwikkelmethode).

28 Projectteam e-Briefing, *Verzamelrapport*. 2013.

29 Projectteam e-Briefing, *Verzamelrapport*. 2013.

enkele voorwaarden benoemd zoals 'niemand weg zonder overleg', 'debriefing voedt de briefing van de ander' en het vastleggen van informatie: 'van blauw boekje naar BVH'.[30]



Figuur 17.2 Proces operationeel briefen en debriefen

In de kern voltrekt het briefingsproces, zoals weergegeven in voorgaand schema, zich als volgt:

- De samensteller (een medewerker van de DRIO) maakt briefingsitems en plaatst deze in het briefingsvoorstel. Dat voorstel bevat alle briefingsitems die actueel zijn en relevant zijn voor het desbetreffende team. Doordat het steeds wordt bijgewerkt, is het briefingsvoorstel een dynamische en actuele set van briefingsitems. Het briefingsvoorstel vormt tevens de inhoud van de 24-uursloop.
- De gever (de Opco) van de briefing maakt een selectie van briefingsitems uit het briefingsvoorstel. Hij[31] kiest de items die van belang zijn voor de ontvangers in de komende dienst en presenteert deze in de zogenoemde warme briefing.
- Naast de warme briefings zijn er ook de zogenoemde koude briefingsvormen. Deze briefings kunnen ontvangers (politiemedewerkers) zelfstandig raadplegen, als zij de warme briefing gemist hebben of de briefing achteraf willen terugzien. Dit kunnen zij vanachter hun pc of via hun mobiele telefoon. Zowel de warme briefing als de 24-uursloop is op deze manier voor de politiemedewerkers raadpleegbaar.

Naast beschrijving van de verschillende rollen die medewerkers in het proces hebben, laat het processchema zien dat een goede briefing draait om de vier i's. Diegene die brieft, informeert, instrueert, inspireert en biedt ruimte voor interactie. Informatie gaat dan over:

30 Voor verdere beschrijving van het briefen en debriefen en 'kritische succesfactoren' zie: Landelijke werkgroep Briefen/Debriefen, *A3 Werkingsdocument (DE)briefing*. Landelijke werkgroep Briefen/Debriefen, 2013.

31 Lees uiteraard ook 'zij' waar dat verder in dit hoofdstuk van toepassing is.

'wat, uitvoeringsinfo, veiligheidsinfo en actie-info', en instructie over: 'hoe, werkverdeling en werkopdracht'. De briefinggever inspireert ontvangers om de opdrachten uit te voeren ('waarom, context, motivatie en uitdaging') en nodigt uit om aanvullende of nieuwe informatie met elkaar te delen ('samen, aanvullen en delen').[32]

Briefingswijzer: Alertheid, Sturing, Teambuilding en Leren

In 2014 ontwikkelde het lectoraat Intelligence van de Politieacademie de briefingswijzer. Deze kartonnen kaart bevat tips voor het voorbereiden en presenteren van een warme briefing. Toepassing leidt tot een viertal effecten van de briefing, namelijk:

1 alertheid: herkennen van situaties op straat en daar juist naar kunnen handelen;
2 sturing: door middel van opdrachten richting geven aan het werken op straat;
3 teambuilding: versterken van band tussen directe collega's met andere onderdelen;
4 leren: verbeteren van prestaties door te leren van elkaar.

De briefingswijzer geeft effectieve tips, bijvoorbeeld briefen in een afgesloten briefingsruimte (alertheid), personaliseer wie wat gaat doen (sturing), zet tafels en stoelen in een U-opstelling (teambuilding), en vraag hoe collega's opdrachten zouden uitvoeren (leren).[33]

Tot slot schrijft het briefingsproces voor dat er binnen de basisteams geschikte ruimten zijn om ongestoord een warme briefing te kunnen geven. Idealiter beschikken de basisteams ook over tv-schermen in de werkruimte van het bureau, waarop de 24-uursloop getoond kan worden. Een hulpmiddel om de briefing over meerdere locaties te geven, is de telebriefing. Hiermee kan een video- en spraakverbinding tussen twee, of meer politiebureaus tot stand worden gebracht, zodat een briefing voor meerdere personen gegeven kan worden die fysiek van elkaar gescheiden zijn.[34]

17.4.2 De e-Briefingtool

Naast het briefingsproces is de e-Briefingtool ontwikkeld, een aantal vernieuwende functionaliteiten lichten we hierna toe.

Het briefingsitem (de dia)

De samensteller maakt, met behulp van de e-Briefingtool, briefingsitems (dia's) die hij beschikbaar stelt in het briefingsvoorstel. In figuur 17.3 is een briefingsitem te zien, gemaakt met behulp van de e-Briefingtool. Het briefingsitem bestaat uit maximaal vier informatieblokken, die bijvoorbeeld betrekking hebben op een persoon, voertuig of locatie. De verschillende blokken kan de samensteller naar eigen inzicht plaatsen op de dia. De

32 Projectteam e-Briefing Nationale Politie, *Verzamelrapport*. 2013.
33 Hengst, M. den & M. In 't Veld, *Briefen voor en door basisteams*. Boom Lemma uitgevers, Den Haag 2014.
34 Landelijke werkgroep Briefen/Debriefen, 2013.

onderste balk van de dia dient altijd een opdrachtomschrijving te bevatten, de kern van de instructie. De dia's en onderliggende informatie kunnen real-time gedeeld worden met alle politieteams die werken met de e-Briefingtool. Hierdoor is het delen van informatie een stuk eenvoudiger dan in de oude situatie, toen verschillende teams werkten met verschillende softwareapplicaties wat het delen van dia's bemoeilijkte.

Figuur 17.3 Briefingitem (dia)

De gever selecteert

De gever maakt een selectie van briefingsitems uit het briefingsvoorstel, gericht op de komende dienst (zie figuur 17.4). Hij presenteert vervolgens deze briefingsitems, ondersteund door gesproken notities, als 'warme briefing'. Deze notities van de spreker zijn tevens zichtbaar als contextinformatie wanneer politiemedewerkers de 'koude briefing' vanaf hun eigen werkplek of mobiele telefoon raadplegen.

Figuur 17.4 Het selectieproces: van briefingsvoorstel naar briefingsitems voor de briefing

Vastleggen van interacties tijdens de briefing

Tijdens een warme briefing wordt vaak aanvullende informatie teruggekoppeld door ontvangers van de briefing. Bijvoorbeeld over een bepaald adres waar een verdachte regelmatig verblijft, of een nieuw voertuig waarmee een verdachte zich sinds kort verplaatst. De gever van de briefing heeft de mogelijkheid om deze opmerkingen tijdens de briefing te noteren bij het briefingsitem. De samensteller ontvangt daarvan een melding in de e-Briefingtool. Wanneer de samensteller de warme briefing niet heeft kunnen bijwonen, kan hij zien bij welke dia's medewerkers opmerkingen hebben gemaakt. De samensteller kan vervolgens de informatie nader uitzoeken en desgewenst het briefingsitem aanpassen.

17.5 Een eerste proeve van het 'nieuwe (de)briefen' in de politiepraktijk

Het briefingsproces en de e-Briefingtool zijn respectievelijk in 2015 en 2016 als onderdeel van een pilot in acht basisteams van de politie geïmplementeerd. Organisatorisch veranderen binnen de (in)formele werkpraktijken van basisteams is geen eenvoudige opgave.[35] Van de Opco werd bijvoorbeeld verwacht dat hij zelf de selectie van briefingsitems maakte in voorbereiding op de briefing. Een aantal bevindingen van de pilotteams over de tool en het proces lichten we hierna toe.[36]

17.5.1 Selectie van briefingsitems

Figuur 17.5 Selectieproces

35 Landman, W., R. Kouwenhoven & M. Brussen (2015). *Spelen met weerbarstigheid*. Reeks Politiewetenschap nr. 85. Reed Business Information, Amsterdam 2015.

36 De bevindingen en citaten in deze paragraaf ontlenen we grotendeels aan de evaluatiestudie naar de briefingtool en het briefingproces in acht basisteams van de politie (eind 2015 en begin 2016) van In 't Veld, M. & M. den Hengst, *'Wat ga jij doen vandaag': evaluatieonderzoek naar de ingebruikname van een briefingtool in acht basisteams van de politie*. Politieacademie, Apeldoorn 2016.

'De eerste selectie maak ik altijd op basis van: ochtend, middag of avond. Dat is de eerste schifting. Want het heeft geen zin om iets wat vanochtend belangrijk was, 's middags te briefen. De meeste briefers beperken de briefing van zes tot acht dia's, dat liever dan acht tot tien dia's. Dat vind ik goed. Het is anders het ene oor in en het andere uit, en foto's kun je niet opschrijven. En tegenwoordig met die telefoons, je kunt alles zó goed natrekken.'
– *Operationeel leidinggevende (mei 2016)*

'Ja, dat kiezen van dia's doe je echt op gevoel, ik kies die waarvan ik denk dat die van belang is. Ik probeer echt maximaal tien dia's te selecteren.'
– *Operationeel leidinggevende (mei 2016)*

Het ervaren gebruiksgemak van de briefingtool is hoog, zowel bij de samenstellers als operationeel leidinggevenden. De operationeel leidinggevenden maken eenvoudig zelf een selectie van briefingsitems, bijvoorbeeld voor een ochtend-, middag- of nachtdienst.[37] Anders dan voorheen ligt de nadruk voor selectie niet meer bij de samensteller, doorgaans een informatiemedewerker van de DRIO, die de briefing 'klaarzette'. De operationeel leidinggevende is nu zelf verantwoordelijk voor de keuze van briefingsitems en dus voor de voorbereiding van de briefing en voor de focus, of speerpunten, van de komende dienst van politiemedewerkers.

17.5.2 Briefing: aantal briefingsitems en effect

'Ik merk wel een verschil: met de nieuwe heb je minder tekst. Bij de oude had je meer tekst, die ging je vaak lezen en dat was het eigenlijk. Nu moet je echt luisteren en je krijgt ook een veel overzichtelijker beeld, vind ik.'
– *Politiemedewerker (mei 2016)*

Doordat briefings door operationeel leidinggevenden specifiek voor de komende dienst zijn samengesteld, bevatten zij minder dia's. De hoeveelheid informatie die gedeeld wordt neemt dus af.[38] Doordat minder briefingsitems gepresenteerd worden en de briefings iets korter duren, wordt er meer tijd genomen voor het presenteren van informatie. Hiermee is aannemelijk dat politiemedewerkers meer zullen gaan onthouden, aangezien Scholtens

37 De diensttijden van politiemedewerkers zijn grofweg als volgt: ochtenddienst van omstreeks 07.00 tot 15.00 uur, middagdienst van omstreeks 15.00 tot 23.00 uur en de nachtdienst van omstreeks 23.00 uur tot 07.00 uur.

38 Gemiddeld genomen over de pilotteams bevatten de briefings vijf briefingsitems minder (van dertien naar acht) ten opzichte van de eerder geobserveerde briefings, waarbij de teams nog niet de beschikking hadden over de e-Briefingtool, en de operationeel leidinggevenden daardoor (overwegend) niet zelf een selectie konden maken van briefingsitems. Zie: In 't Veld, M. & M. den Hengst, *'Wat ga jij doen vandaag': evaluatieonderzoek naar de ingebruikname van een briefingtool in acht basisteams van de politie*. Politieacademie, Apeldoorn 2016.

et al. (2013, zie noot 9) aantoonden dat hoe minder dia's en informatie-elementen gegeven worden in een briefing (zowel getoond als gesproken door de gever), hoe hoger politiemedewerkers scoren op het onthouden van informatie.

17.5.3 Briefingsproces: 'landelijk' versus 'stedelijk'

Naast enkele bevindingen die voortvloeien uit gebruikmaking van de tool, valt op dat het briefingsproces verschillend vorm krijgt. Binnen basisteams die te karakteriseren zijn als stedelijk, percipiëren politiemedewerkers de briefing vaker als moment van (algemene) instructie dan de politiemedewerkers in de teams die gelegen zijn in meer landelijk gebied.

Landelijke en stedelijke teams

Landelijke teams kennen meerdere politiebureaus als opkomstlocatie, een groot oppervlak van het werkgebied (meer dan 200 vierkante kilometer), en in vergelijking met stedelijke teams een kleiner aantal medewerkers per vierkante kilometer (doorgaans minder dan één politiemedewerker per vierkante kilometer). Stedelijke teams kennen één opkomstlocatie, een kleiner werkgebied, en in vergelijking meer politiemedewerkers per vierkante kilometer (bijvoorbeeld 20-25 politiemedewerkers per vierkante kilometer). De landelijke en stedelijke teams kennen globaal overeenkomstige diensttijden van de ochtend-, middag- en nachtdienst.

Observaties van briefings in de acht pilotteams bevestigen deze perceptie van politiemedewerkers; in stedelijke teams geeft de operationeel leidinggevende vaker (algemene) instructies tijdens de briefing dan in de landelijke teams. Er bestaan verschillen tussen grootstedelijke en plattelandsteams die doorwerken in het functioneren van de basisteams. Dit gegeven is niet nieuw zoals recentelijke onderzoek van Terpstra et al. (2016) naar de inrichting van de basisteams leert.[39] Wat betekenen deze verschillen voor het proces van briefen en debriefen?

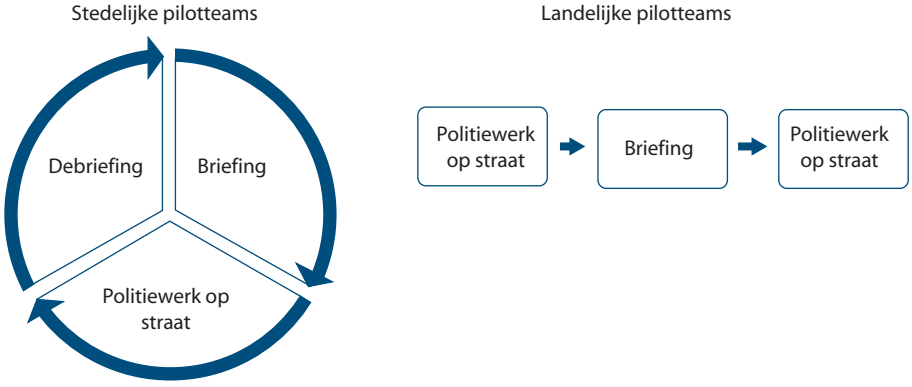
Binnen landelijke pilotteams wordt, met name in de ochtenddienst, in de loop van de dienst gebrieft omdat bij aanvang van de dienst politiemedewerkers verspreid over verschillende locaties van het basisteam opkomen. Hierdoor worden de politiemedewerkers bij aanvang van de dienst niet direct plenair gebrieft, maar doorgaans enkele uren later.

Door in de loop van de dienst te briefen, komt het voor dat politiemedewerkers voor wie de briefing richtinggevend zou moeten zijn, al buiten op straat acteren op meldingen. Deze 'lopende-dienstbriefings' kenmerken zich door een mix van 'ontvangende' disciplines, bijvoorbeeld rechercheurs, wijkagenten of DRIO-medewerkers. De briefing krijgt hierdoor eerder een informatief dan instructief karakter.

39 Terpstra, J. et al., *Basisteams in de Nationale Politie: organisatie, taakuitvoering en gebiedsgebonden werk*. Reeks Politiewetenschap nr. 88. Reed Business Information, Amsterdam 2016.

Binnen stedelijke teams is het eenvoudiger om eenieder bij aanvang van de dienst direct plenair te briefen, er is immers maar één opkomstlocatie. De briefing krijgt hier eerder een instruerend karakter, want er wordt gebrieft bij aanvang van de dienst. De vraag 'wat gaan we doen deze dienst?' komt vanzelfsprekend centraler te staan. Medewerkers van andere disciplines, met name bij de start van de ochtend- en nachtdienst, sluiten bij deze briefing doorgaans niet aan, omdat zij nog niet in dienst zijn.

In figuur 17.6 hebben we deze globale verschillen in dienstverloop tussen teams vereenvoudigd schematisch weergegeven.



Figuur 17.6 Schematische weergave dienstverloop stedelijk versus landelijk

Binnen de landelijke pilotteams wordt de debriefing in vergelijking met de stedelijke teams vaker niet dan wel gehouden. Wanneer zij hier wel plaatsvindt, kent zij doorgaans een anekdotisch karakter omdat in de briefing daarvóór geen instructies zijn uitgedeeld. In de stedelijke teams wordt vaker op structurele basis gedebrieft, in deze teams zijn bij de briefing bij aanvang van de dienst wél (algemene) opdrachten uitgezet, waardoor de operationeel leidinggevende hierop eenvoudig kan teruggrijpen tijdens het debriefen.

Samenvattend, proces en tool zorgen voor kortere briefings met minder overdracht van informatie, waardoor de effectiviteit – in termen van onthouden van informatie – wordt vergroot. Gebruiksgemak bij het maken van briefingsitems draagt bij aan de verdere professionalisering van de politiebriefing. Daarnaast stimuleert de tool gevers van een briefing om zelf te beoordelen en te selecteren, waardoor zij meer invulling kunnen geven aan operationeel leiderschap.

17.6 Toekomst van briefen en debriefen

Dit hoofdstuk is ingegaan op het concept briefen en debriefen, de planvorming van de nationale politie, de producten van de projectgroep e-Briefing en de uitwerkingen van deze producten op 'de werkvloer'. In de volgende alinea's wordt de balans opgemaakt. Waar staan we als het gaat om de politiebriefing, en wat zijn de verwachtingen voor de toekomst?

Briefen en debriefen zullen naar onze verwachting de komende jaren een centraal thema blijven, omdat politiewerk en politiebriefing onlosmakelijk met elkaar verbonden zijn. Enerzijds omdat voor politiemedewerkers de briefing een belangrijk moment vormt om informatie 'af te tappen' en collega's te ontmoeten. Anderzijds door de functie van de operationeel leidinggevenden binnen de teams, zij spelen een belangrijke rol in de aansturing van de teams, en briefen en debriefen zijn middelen om die taak te kunnen vervullen.

De e-Briefingtool wordt als zeer gebruiksvriendelijk ervaren en schept voor de operationeel leidinggevende betere voorwaarden tot het uitzetten van werkopdrachten tijdens een briefing dan voorheen. Daarbij komt dat de briefingsitems altijd voorzien zijn van een (algemene) opdracht, weergegeven in de instructiebalk, zodat duidelijk wordt wat concreet van de politiemedewerkers wordt verwacht. Desondanks is het geven van opdrachten op de persoon tijdens de briefing (nog) geen gemeengoed. Sturing op de persoon vindt momenteel vaak informeler plaats, bijvoorbeeld een-op-een vlak voor of na de briefing.

Voor de politiemedewerker blijft de briefing een middel om snel een overzicht te krijgen van de situatie binnen het basisteam en van mogelijke risico's bij de uitvoering van het werk. Voor hen geldt de briefing nog vaak niet primair als moment van instructie, maar als informatiemoment. Om de briefing ook meer het beoogde sturende karakter mee te geven, zal extra geïnvesteerd moeten worden in operationele sturing en leiderschap door briefinggevers.

Met de komst van IGP is de briefing, in combinatie met de debriefing, een middel geworden om een cyclisch proces van informatiegestuurd werken binnen teams te faciliteren. Het vormgeven daarvan – waarvoor ook de debriefing na afloop van de dienst essentieel is – zal naar verwachting een uitdaging voor alle teams blijven. De diverse kenmerken van basisteams, zoals het verschil tussen stedelijke en landelijke teams, maken dat een *one size fits all*-aanpak in de politiepraktijk niet altijd past. Het briefingproces biedt waardevolle, generieke handvatten, en tegelijkertijd voldoende ruimte om het proces in te richten op een wijze die past bij de lokale setting van een basisteam.

Deel VI
De toekomst is vandaag

18 Community of Intelligence

Mieke Struik

18.1 Het begin

> 'Rond de eeuwwisseling in mijn tijd als kernteamchef in de bestrijding van internationale cocaïnehandel sprak ik regelmatig met collega's over de "intelligence-community" waarvan we deel uitmaakten. Een wereldwijd netwerk van professionals waar operaties, operationele informatie en kennis gedeeld werden. Toen ik later in Nederland hoofd werd van de landelijke informatiedienst van de politie, vroeg ik mij af waarom ik een dergelijke intensieve mondiale grensoverschrijdende samenwerking in ons kleine kikkerlandje niet terugzag. Dit was voor mij reden om later als programmamanager Intelligence aan Cees Sprenger te vragen voor ons te verkennen hoe we een dergelijke community bij de politie zouden kunnen organiseren. Cees kwam met zijn onderzoekers terug met een adviesrapport. Hij zei bij de presentatie: "Wat jij bedoelt, is een *community of practice*. Die kan je als leidinggevende niet zomaar vanuit een ontwerp organiseren. Maar je kan wel randvoorwaarden en condities scheppen om deze community te laten ontstaan, te stimuleren en te realiseren."'
> *– Jan ter Mors, februari 2017*

We kwamen bij elkaar in Utrecht in een kantoor van inspirator Cees Sprenger, die al eens had aangegeven dat hij een *community of intelligence* (CoI) binnen de politie een goed idee zou vinden.[1] Het programma Intelligence heeft dit idee voor een community of practice voor intelligenceprofessionals samen met het lectoraat Intelligence van de Politieacademie verder gebracht als nieuwe manier om intelligenceprofessionals met elkaar te verbinden, een duidelijke systeembreuk in relatie tot traditionele samenwerkingsvormen. De toekomst die het programma Intelligence voor zich zag, was een Community of Intelligence met intelligenceprofessionals die over de grenzen van hun eigen organisatieonderdeel of expertisegebied heen kennis over nieuwe methoden, werkwijzen en goede praktijkvoorbeelden delen, elkaar verder helpen in discussies en documenten met elkaar delen om zo het intelligencevakgebied verder te ontwikkelen. Het programma Intelligence en het lectoraat Intelligence namen het initiatief voor een bijeenkomst. Mariëlle den Hengst en Hans Regterschot hadden een tiental analisten uitgenodigd om de oprichting van een Community of Intelligence te bespreken. Zij hadden gekozen voor een groep jonge analisten, uit verschillende delen van het land, veelal hoogopgeleid en zijinstromer bij de politie.

1 Sprenger, C. et al., *Bouwen aan een Community of Intelligence: succesvolle samenwerking rond IntelligenceGestuurd Politiewerk*. Politieacademie, Apeldoorn 2010.

Enkelen kenden elkaar van de avi-opleiding[2], maar de meesten waren onbekenden van elkaar. De CoI is niet ontstaan uit een *old boys network*.

De bijeenkomst was inspirerend. Alle aanwezigen hadden goede ideeën over het opzetten en uitwerken van een CoI. Dat gaf aan dat veel van ons al eens over dit onderwerp hadden nagedacht vanuit een groeiende behoefte meer en gemakkelijker informatie te delen. Er was met behulp van een externe partij al een opzetje gemaakt van een mogelijke virtuele werkomgeving en iedereen zag de noodzaak voor het delen van informatie met anderen in een community-achtige omgeving.

Er kwamen in het gesprek elementen naar voren die belangrijk zijn voor het functioneren van zo'n community. Ten eerste moet de omgeving veilig zijn; men moet erop kunnen vertrouwen dat de gedeelde informatie en documenten niet meteen op straat komen te liggen. Ten tweede is het belangrijk dat de lijn geen zeggenschap heeft over het delen van de informatie. Uitgangspunt moet zijn dat de community 'van analisten, voor analisten' is om zo het vakgebied verder te ontwikkelen. Ten derde zagen we de meerwaarde van het delen van informatie met partners in de veiligheidszorg. Ketenpartners moeten daarom lid kunnen worden van de community, eventueel na een screening. Ten slotte wilden we graag een community bouwen die zowel een virtueel als een persoonlijk netwerk zou vormen.

18.2 Een virtuele en fysieke community

Het virtuele gedeelte van de community werd ondergebracht bij politiekennisnet (PKN). Daaraan zat een aantal voordelen. PKN is een afgeschermd netwerk voor medewerkers van de politie en de Politieacademie. Mensen van buiten de politie kunnen onder bepaalde voorwaarden ook toegang krijgen. Bovendien werd er aan aantal moderatoren[3] benoemd zonder wier expliciete uitnodiging niemand toegang krijgt tot de virtuele community. Op deze manier waren we in staat om een veilige virtuele omgeving in te richten waar ook ketenpartners lid van konden worden. Nadeel van het onderbrengen bij PKN was dat de vormgeving was gebonden aan die van PKN. De uitstraling van de site kon niet modern of glossy worden gemaakt. Bovendien bleef het voorbehoud dat er geen operationele (persoons)gegevens mogen worden gedeeld. In de praktijk betekent deze restrictie dat er met name tactische en strategische documenten op de virtuele community worden geplaatst. Om te zorgen dat de community een zo veilig mogelijke omgeving blijft voor vakgenoten hebben we een *Code of Conduct* geschreven. Hieraan kleeft altijd het risico dat men door de regels afgeschrikt wordt. Maar we vinden het belangrijk dat de randvoorwaarden voor gebruik van de community voor iedereen helder zijn. Misverstanden kunnen er immers toe leiden dat gedeelde informatie ongewild op straat komt te liggen.

---

2 De avi-opleiding was een tweejarig leerwerktraject ontwikkeld vanuit het programma Intelligence en de Politieacademie, waarin zijinstromers opgeleid werden tot analist veiligheidsinformatie.

3 De moderatoren zijn: Daniel Bulten, Tobias de Wit, Bianca van Beek, Mieke Struik. Neem voor vragen of deelname gerust contact met hen op.

Code of Conduct van de Community of Intelligence

Het doel van de Community of Intelligence (CoI) is om analisten van Politie Nederland een platform te bieden om collegiaal informatie en producten te delen.

Multidisciplinair

Intelligence heeft te maken met het analyseren van multidisciplinaire informatie. Daarom is het belangrijk dat ook de CoI een multidisciplinair karakter heeft. Naast politiemedewerkers kunnen ook werknemers van een aantal andere organisaties lid worden: alle politie-eenheden, de Algemene Inspectiedienst (AID), de Algemene Inlichtingen- en veiligheidsdienst (AIVD), het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT), de Fiscale Inlichtingen- en opsporingsdienst (FIOD), de Immigratie- en Naturalisatiedienst (IND), de Koninklijke Marechaussee, het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), de Directie Politie van het ministerie van Veiligheid en Justitie, het Nederlands Forensisch Instituut (NFI), Openbaar Ministerie (OM), de Politieacademie, de Rijksrecherche, het Recherche Samenwerkingsteam (RST) en de Inspectie van het Nederlandse ministerie van Sociale Zaken en Werkgelegenheid.

Leden

Om lid te kunnen worden van de CoI moet je eerst ingeschreven zijn bij Kompol (Kennis op maat politie). Vul je profiel goed in zodat mensen die op zoek zijn naar expertise je makkelijk kunnen vinden. Een moderator kan je vervolgens lid maken van de CoI.

Informatie delen en verspreiden

Bedenk wat je via de CoI deelt, bijvoorbeeld in het kader van de Wet politiegegevens. We raden af om bijvoorbeeld persoonsgegevens uit onderzoeken en analyses via de CoI te delen. Aan de andere kant vragen we van de ontvangers terughoudendheid in de verspreiding van geplaatste documenten. Ben je van plan een document dat je op de Community of Intelligence gevonden hebt (breed) te verspreiden, sluit dat dan kort met de auteur.

Raak je geïnspireerd door een idee, een onderwerp en/of een methode van een collega op de Community of Intelligence en ga je die zelf toepassen, vergeet dan niet om de bron van je inspiratie te noemen.

Zoeken en vinden

Om het zoeken van documenten te vergemakkelijken, is het belangrijk dat je de documenten die je uploadt een paar goede tags meegeeft. Tags zijn labels waaraan je een document kunt herkennen. Voorbeelden van tags die je kunt gebruiken zijn: publicatiedatum, auteur, onderwerp en thema.

Het beheer van de virtuele community lag voor het technische deel bij PKN en voor het inhoudelijke deel bij het lectoraat Intelligence. De moderatoren kwamen uit de analistengemeenschap. Zo probeerden we de community buiten de lijn vorm te geven. Het was immers een community van analisten voor analisten.

Sinds 2009 wordt jaarlijks een analistendag georganiseerd. De eerste keer lag de organisatie in handen van het programma Intelligence en vanaf 2010 lag deze in handen van het lectoraat Intelligence. Deze vakdag is een jaarlijkse ontmoeting van analisten van vooral politie, maar ook collega's werkzaam bij partners in de veiligheidsketen zijn welkom. De inhoudelijke organisatie van de dag is in handen van analisten; het lectoraat en het congresbureau van de Politieacademie ondersteunen voor de huishoudelijke zaken, zoals voldoende geschikte ruimtes, presentatiematerialen en dergelijke. De thema's van de analistendagen zijn zeer uiteenlopend: in gesprek met portefeuillehouders over thema's op de intelligenceagenda, open bronnen, innovatie, trends en toekomst, de veelzijdigheid van het analysevak zijn de revue al gepasseerd. De analistendagen zijn steeds goed bezochte en inspirerende dagen. Opvallend zijn de interesse die men in elkaars werk heeft, hoezeer we van elkaar willen leren en het enthousiasme in de gesprekken en discussies. Zo is de analistendag een van de persoonlijke ontmoetingsplekken van de Community of Intelligence. Ook voor de analistendagen geldt het motto 'voor analisten, door analisten'.

Figuur 18.1 Analistendag op de Politieacademie

Tijdens de analistendag in juni 2011 stond de virtuele omgeving klaar om gebruikt te worden.[4] Op die dag introduceerden we de virtuele community aan de analisten. Alle 200 deelnemers die zich via de mail voor de dag hadden aangemeld kregen ook meteen toegang tot de virtuele omgeving. Zo werden de virtuele en de persoonlijke community aan elkaar gekoppeld, en vond er een vliegende start plaats van het delen van informatie in de virtuele Community of Intelligence.

18.3 De kracht van de Community of Intelligence

Om het succes van de community te bepalen, hebben Mariëlle den Hengst en Jan ter Mors in 2012 een onderzoek gedaan naar het aantal actieve deelnemers en unieke bezoeken per

4 Voor toegang via internet: https://dw.politieacademie.nl/sites/coi
Voor toegang via de politiewerkomgeving: http://dw.politieacademie.politie.nl/sites/coi

maand. Uit dit onderzoek bleek dat de community als een succes kan worden beschouwd. Het aantal leden was in het eerste jaar gegroeid van 300 naar meer dan 500. Inmiddels (2016) is dat gegroeid naar meer dan 650 leden. In 2012 waren er ongeveer 150 unieke bezoekers per maand.[5] In de eerste helft van 2015 was dit aantal rond de 100 per maand.

In 2016 is het unieke bezoekerspatroon erg grillig en neemt in de tweede helft van het jaar af. Dit heeft waarschijnlijk te maken met de overgang van PKN naar de nieuwe virtuele omgeving van de Politieacademie Kompol. De overplaatsing van de Community of Intelligence naar een ander webadres hebben we onvoldoende gecommuniceerd. Mogelijk konden de leden de community daarom niet meer vinden.

Andere mogelijke oorzaken voor de daling van het aantal bezoekers is het beëindigen van de alerts die periodiek door het lectoraat naar alle leden verstuurd werden. In de alerts stonden de nieuw geplaatste items op de community, en dat herinnerde de leden eraan om weer eens even een kijkje te gaan nemen.

Of een community een succes is, is natuurlijk niet alleen af te lezen aan het aantal bezoekers. Juist de mogelijkheid om kennis te nemen van elkaars werk en expertise is een belangrijke opbrengst; het uitwisselen van kennis over nieuwe tools en (juridische) processen. Af en toe krijg ik een vraag van iemand die op de CoI heeft gezien dat we met hetzelfde onderwerp bezig zijn. Hij of zij wil dan even sparren.

Veelvuldig gebeurt het dat er een vraag wordt gesteld of een oproep wordt gedaan op de Community of Intelligence, maar dat de antwoorden telefonisch of per mail worden gegeven. Dit kan zijn omdat even snel bellen wel zo gemakkelijk is. Het kan ook zijn dat er naar aanleiding van de vraag operationele informatie moet worden gedeeld en dat kan niet binnen de CoI. Zulke activiteiten kun je niet terugvinden in de bezoekersaantallen, maar zijn wel een belangrijke opbrengst van de virtuele omgeving. Rond cybercrime is er bijvoorbeeld een groepje afgesplitst naar een aparte werkomgeving. De start van het onderlinge contact van deze themagroep vond plaats op de CoI. Daar bemerkten de leden het succes van een gezamenlijke virtuele omgeving. Maar voor het onderwerp was het een groot gemis dat er geen operationele data konden worden uitgewisseld. Daarom zijn zij met een kleine groep verder gegaan in een omgeving waar dat wel kon. Ook dit voorbeeld bewijst het succes van de CoI dat niet in de cijfers terug te vinden is. Bovendien laat dit voorbeeld zien dat de community zonder hiërarchische sturing van bovenaf een inhoudelijk vraagstuk op kan pakken. De analisten zagen cybercrime als fenomeen dat over de grenzen van de regiokorpsen heen opgepakt zou moeten worden. Tegelijkertijd bleef een landelijke behoefte via de officiële kanalen uit. Daarop groepeerde een aantal leden van de community zich om op die manier overzicht en inzicht te krijgen in het fenomeen.

Misschien is dit soort onverwachte spin-offs juist de beste indicator voor het succes van de CoI. Een ander voorbeeld van een ontwikkeling die we niet hebben voorzien is dat er zo nu en dan ook analisten geworven worden voor bepaalde afdelingen binnen de politie. Hoewel we expliciet een advertentievrij medium voorstaan, is het leuk om te

5 De cijfers van unieke bezoekers per maand is een onderschatting van het werkelijke aantal bezoekers. Het betreft namelijk uitsluitend de bezoeken vanuit de politieomgeving. Bezoeken van politiemensen die vanaf een externe computer werken, en de communityleden die sowieso niet op het politienetwerk zitten (ketenpartners), worden niet meegeteld.

ontdekken dat de CoI ook op deze manier gebruikt wordt voor het vinden van de juiste expertise.

Ten slotte is een belangrijke kwaliteit van de CoI dat deze een specifieke niche vult in het delen van informatie binnen de politie. Het is namelijk het enige (virtuele) platform waar alle analisten van Nederland onderling informatie kunnen uitwisselen. Veel van de virtuele kantoren en gezamenlijke netwerklocaties zijn thema- of regiogebonden zodat alleen een deel van alle analisten toegang heeft. De CoI is toegankelijk voor alle analisten uit heel Nederland die werkzaam zijn binnen de politie en bij partnerorganisaties en staat open voor alle onderwerpen.

Oprichters van een community hopen altijd dat hun platform uiteindelijk meer zal gaan opleveren dan er wordt ingestopt. Met andere woorden hopen ze dat er vanuit de community zélf diensten en producten gaan ontstaan. De regio-overstijgende analyse naar cybercrime, zoals hierboven genoemd, is een voorbeeld hiervan. En er zijn andere voorbeelden. Als vliegwiel dient daarvoor de jaarlijkse essaywedstrijd. Sinds 2013 wordt door het lectoraat Intelligence jaarlijks een essaywedstrijd georganiseerd met een aan informatie of intelligence gerelateerd thema. De wedstrijd staat open voor alle politiemedewerkers en voor iedereen werkzaam in het veiligheidsdomein, maar veel van de bijdragen komen van collega's uit het intelligencevak. De prijsuitreiking is altijd op de analistendag.

Een van de beoordelingscriteria voor de essays is de praktische toepasbaarheid van de beschreven ideeën. In 2014 schreef Dominique Roest haar essay: '*Undercover analyst*, de serie', waarin ze betoogde dat analisten eens undercover zouden moeten gaan binnen de politie om beter te begrijpen hoe het eraan toegaat op de blauwe werkvloer. Naar aanleiding van dit essay zijn enkele CoI-leden undercover gegaan, en hebben hun ervaringen onderling gedeeld. Ook dit is een voorbeeld van een idee dat is ontstaan vanuit de community, en dat – buiten 'de lijn' – door de community is uitgewerkt.

18.4 De toekomst

Al met al bevat de CoI alle ingrediënten voor een succesvol recept, en... het smaakt naar meer. Wat zouden we nog meer van de CoI willen of wat kunnen we verwachten?

Bij een zich ontwikkelende community hopen we op meer producten en diensten die vanuit de CoI zelf ontstaan en uitgevoerd of ontwikkeld worden, zoals de undercover analyst. Op die manier kunnen de communityleden met behulp van elkaar verder professionaliseren en het vakgebied ontwikkelen. In een echt volwassen community zullen de leden niet alleen inhoudelijk kennis van elkaars werk nemen, maar ook samen de kwaliteit van het vakgebied verbeteren. Het zal echt een stap voorwaarts zijn als de communityleden onderlinge afstemming zoeken over de opzet, uitvoering en presentatie van onze analyses. Dit kan bijvoorbeeld door het introduceren van een *peer review* systeem, waarbij men vóór oplevering van het product eerst feedback vraagt van een collega met vergelijkbare expertise (*peer*). Deze feedback moet niet waarderend zijn – je hoeft niet bang te zijn dat je product afgekraakt wordt. De expertise van een collega kan juist bijdragen aan verduidelijking van je analyse, nieuwe inzichten en uiteindelijk een kwalitatief beter product.

We leven in toenemende mate in een informatiemaatschappij en het netwerkend werken in communities zal sterker worden. Voor de analisten van de politie kan de CoI daarin een faciliterende rol blijven spelen. Voorwaarde daarvoor is wel dat actief beheer van het platform ten minste gecontinueerd, maar liever nog verder versterkt wordt. Dat geldt zowel voor de virtuele als voor de fysieke ontmoetingen. Met sterker wordende communities kan ook gedacht worden aan verdere uitbreiding.

De CoI is begonnen als platform van analisten, maar met de brede ontwikkeling van informatiegestuurd politiewerk (IGP) is het tijd om de scope te verbreden naar alle intelligenceprofessionals. Het intelligencevak is inmiddels breder dan analyse. Ontwikkelingen die elders in dit boek zijn beschreven, zoals de briefing op de teams, het real-time intelligence center, predictive en prescriptive policing, hebben raakvlakken met analyse maar zijn tevens overkoepelend over het gehele intelligencevakgebied. Door een verruiming van analistenplatform naar een ontmoetingsplek voor alle intelligenceprofessionals zal de community een nog grotere bijdrage kunnen gaan leveren aan de ontwikkeling van het intelligencevak en IGP.

Met het oog op verbreding van de scope is ook een stap naar het internationale podium niet ondenkbaar. Politiekorpsen van Europese landen werken op operationeel niveau al samen, het zou een mooie ontwikkeling zijn als ook de intelligencemedewerkers elkaar weten te vinden. Een dergelijke stap zal het aangezicht van de CoI wel veranderen. Immers, we zullen moeten nadenken over Engelstalige analyses of vertalingen van ons werk. Ook is de inrichting van de veiligheidszorg en criminaliteitsbestrijding in diverse landen anders georganiseerd. Wie hoort er dan wel bij en wie niet?

In vijf jaar is de Community of Intelligence gegroeid van niets naar een functionele, succesvolle community waarin de deelnemers zowel virtueel als in levenden lijve met elkaar samenwerken. Doorontwikkeling van de community zal inspanning vragen van de leden en ontwikkelruimte binnen de politie. Met het perspectief dat verdere ontwikkeling van de community een stimulans geeft aan professionalisering en kwaliteitsverbetering van het intelligencevak en met een blik vooruit op internationale samenwerking denk ik dat de CoI een levendige toekomst tegemoet gaat. Voor professionals, door professionals.

19 Real-time intelligence (RTI)

Waldo de Boer en Christiaan van den Berg

19.1 De wereld verandert waar je bijstaat: van informatiesturing naar real-time intelligence

In ons privéleven zijn we gewend geraakt aan informatie, op elk moment van de dag, en over alles in de wereld. Een nieuwtje van de andere kant van de wereld bereikt ons in luttele seconden. Ook vinden we het heel normaal dat ons navigatiesysteem in de auto rekening houdt met files, en dat een optimale route wordt aangeraden.

Het is logisch dat veiligheidsprofessionals dit soort mogelijkheden ook in hun werk willen benutten. En hun werkomgeving (partners, burgers) verwacht dat ook. Een politiemedewerker op straat moet weten wat er speelt in een wijk, of in het land. Je kunt het je niet meer veroorloven om aan te komen rijden na een melding van een ongeval en je niet bewust te zijn van de Twitterstorm waarin mensen elkaar oproepen om óók te komen. Dan sta je met 1-0 achter op straat. Het is niet alleen een kwestie van effectiviteit, maar uiteindelijk ook een kwestie van legitimiteit van de politie.

Als je het uiteenrafelt, hebben we drie belangrijke verwachtingen ten aanzien van de informatievoorziening in het huidige tijdperk.

1 Een grote actualiteit en compleetheid van de beschikbare informatie. In het navigatievoorbeeld: actuele wegopbrekingen en files moeten worden meegenomen in het routeadvies.
2 Ook verwachten we dat deze informatie zonder merkbare vertraging tot ons komt. Als we een verkeerde afslag nemen, willen we direct een alternatieve route krijgen.
3 Bovendien verwachten we een handelingsperspectief, of anders gezegd: een ondersteuning voor de besluitvorming. We hoeven geen lijsten met mogelijke routes, maar we willen de beste of hoogstens de twee beste opties. Voor dit advies wordt gebruikgemaakt van kennis over wegen, toegestane snelheden, verkeerslichten enzovoort.

RTI staat wat ons betreft dus voor actuele informatie, direct beschikbaar en geschikt om op basis ervan besluiten te nemen. Dat begint bij een actueel situationeel beeld. Idealiter staat in dit beeld alles wat relevant is voor de uitvoering van veiligheidstaken. De relevantie is een complex element om te realiseren. Idealiter bevat RTI nooit informatie die de ontvanger al kent. En ook geen informatie die op dat moment voor die specifieke situatie niet van toepassing is. Dat vereist een op maat gesneden informatievoorziening.

RTI is een concept of een visie: het is nooit klaar. Er blijven voorlopig nog kansen genoeg om meer real-time, minder vertraagde, completere (betere combinaties van open en gesloten bronnen), relevantere en zeker méér (bruikbare) *intelligence* te realiseren. Het Real-Time Intelligence Center (RTIC) zien we als een eerste stap in die richting.

Uit de praktijk van het RTIC: ANPR-hit

Melding van een zwaar mishandelde man die het wijkbureau binnen kwam lopen. Van de daders was op dat moment niets bekend. Later werd het RTIC gebeld door het betreffende wijkbureau met de mededeling dat het voertuig van het slachtoffer na de mishandeling is weggenomen. Hierop heeft het RTIC het kenteken in de automatic number plate recognition (ANPR) gezet. Nog geen vijf minuten later kwam er een ANPR-hit binnen. Het voertuig werd vervolgens door twee politievoertuigen aan de kant gezet. De inzittende is aangehouden; het bleek dat hij internationaal gesignaleerd stond voor Italië.

19.2 Het RTI-concept nader uitgewerkt voor de politiepraktijk

In deze paragraaf gaan we langs een aantal typische onderdelen (contexten) van de politiepraktijk, en geven we een schets van recente ontwikkelingen richting real-time intelligence.

Spoedmeldingen

De ondersteuning van spoedmeldingen die door het operationeel centrum (DROC) worden uitgegeven, was de eerste expliciete toepassing van real-time intelligence. Dit vraagt een 24-uurs-ondersteuning op de meldkamer, waarbij in zeer korte tijd relevante informatie over de betreffende melding wordt toegevoegd. De RTIC's van de Nederlandse politie hebben zich bij hun oprichting hier in eerste aanleg op gericht. De RTIC's richten zich primair op het beschikbaar stellen van informatie die betrekking heeft op de inschatting van gevaar en heterdaadkracht (zie ook de volgende paragraaf over de RTIC's). Informatie over eerdere geweldsincidenten op een adres van de melding of eventueel vuurwapenbezit zijn bepalend voor een optreden van politiemensen. In de eerste minuten wordt ook informatie over mogelijke verdachten veredeld. Hierdoor wordt het mogelijk eerder tot een aanhouding te komen.

Wijkzorg

De real-time ondersteuning voor wijkzorgmeldingen is een volgende relevante context voor RTI. Deze context vraagt andere informatie en heeft een langere tijdshorizon. Meer dan bij spoedmeldingen is bij dit soort meldingen een probleemgerichte aanpak gewenst. Context en kennis zijn nog belangrijker en er is een duidelijke relatie met beleidskeuzes. Een voorbeeld hiervan zijn meldingen van overlast door (jeugd)groepen. Het hebben van een actueel beeld over welke personen deel uitmaken van de groep en welke afspraken gemaakt zijn, is van groot belang voor een succesvolle aanpak. In de toekomst zouden deze veiligheidsbeelden ook gemakkelijker op straat beschikbaar moeten komen.

Probleemgerichte aanpak

Een actueel en direct beschikbaar beeld van de veiligheidsproblemen is ook nodig bij de probleemgerichte aanpak. Bij de aanpak van bijvoorbeeld woninginbraken zal een

mogelijke aanpak gerichte surveillance zijn. Er is dan behoefte aan actuele informatie over hotspots en op welke tijdstippen de grootste kans voor effectief optreden is. Het Criminaliteitsanticipatiesysteem (CAS) uit Amsterdam geeft een voorspelling van mogelijke inbraken in een wijk. Het systeem levert daartoe kaartjes van de stad met kleine gebieden met een verhoogde kans op inbraak. De voorspelling is gebaseerd op onder andere historische gegevens (zie ook hoofdstuk 21 Predictive policing).

Incidenten

Bij incidenten met een grote publieke impact of impact op de politieorganisatie is er uiteraard ook behoefte aan een direct beschikbaar beeld, zodat er snel een duiding van de veiligheidsproblematiek gegeven kan worden. Bij een aantal thema's is er op basis van de intelligenceagenda[1] al zo'n beeld voorhanden. Bij onverwachte incidenten rond voetbalwedstrijden is niet alleen een goede informatiepositie van belang, maar ook de mogelijkheid deze direct te ontsluiten voor diegenen die met het incident te maken krijgen. Door bijvoorbeeld de leiders te identificeren en uit de groep te halen, kan een potentieel groot incident klein gehouden worden. Een integraal actueel veiligheidsbeeld is op dit moment in beperkte mate beschikbaar. De nationale briefing probeert hieraan invulling te geven.

Opsporing

Collega's belast met opsporingstaken kennen een andere informatiebehoefte. Het speelveldmodel in de opsporing impliceert dat er actueel kan worden ingespeeld op kansen die zich voordoen. De beschikbare informatie bepaalt voor een groot deel welke kansen op welk moment benut kunnen worden. Hiervoor is een actueel beeld van bijvoorbeeld sleutelplaatsen en sleutelpersonen noodzakelijk. In het geval van een melding van een hennepkwekerij is het bijvoorbeeld van belang om te weten of de betrokkenen deel uit maken van een bekend netwerk en welke rol ze in zo'n netwerk spelen. Het antwoord hierop kan aanleiding zijn voor rechercheurs van het lopende onderzoek met het lokale wijkteam mee te gaan bij een instap.

Intake

Via een telefonische intake, een contact op straat of aan de balie worden incidenten gemeld. Om te voorkomen dat deze meldingen alleen incidentgericht worden behandeld, is het wenselijk zo veel mogelijk relevante informatie al in dit eerste stadium toe te voegen. Hierdoor wordt een meer probleemgerichte aanpak mogelijk. Door bijvoorbeeld al bij de aangifte van stalkingzaken relevante informatie toe te voegen – zowel de feiten als de context en de kennis – kan een betere inschatting worden gemaakt. Dan is de kans op een succesvolle aanpak groter. Voor deze context liggen innovatieve ontwikkelingen in het verschiet: huidige risicotaxatiemodellen zouden kunnen worden ingezet als bron voor bruikbare real-time ondersteuning van de intake.

---

1 De intelligenceagenda is het beleidsplan voor de informatieorganisatie. Die bepaalt op welke vooraf vastgestelde onderwerpen een informatiepositie verworven moet worden. Meer over de intelligenceagenda is te lezen in hoofdstuk 10 Informatiecoördinatie.

Uit de praktijk van het RTIC: Valse naam

Via 0900-8844 kwam een melding binnen dat een persoon zichzelf zou gaan neersteken. De enige informatie die het RTIC had, was een voornaam en een mogelijke woon- en/of verblijfplaats. Het RTIC maakte een zoekslag in de politiesystemen. Op de genoemde voornaam in combinatie met woon- en/of verblijfplaats kwamen diverse hits naar voren, onder andere een persoon die een valse naam gebruikt en psychische klachten heeft. In de politiesystemen stonden ook de juiste personalia vermeld. Op deze manier werd alles in korte tijd snel duidelijk en konden de politiemensen goed geïnformeerd de melding behandelen.

19.3 Het Real-Time Intelligence Center

Bij de inwerkingtreding van de nationale politie is het RTIC als een van de gezichtsbepalende onderdelen benoemd. De ontwikkeling van het RTIC komt voort, als hiervoor al aangegeven, uit de behoefte aan actuele informatie ten behoeve van besluitvorming op straat. In een groot aantal voormalige regio's en bij de landelijke eenheid is er in de jaren vóór de invoering van de nationale politie op verschillende manieren geëxperimenteerd met real-time intelligence. De komst van de nationale politie gaf de mogelijkheid al deze ontwikkelingen te bundelen.

Figuur 19.1 RTIC Den Haag

In de oorspronkelijke plannen voor het RTIC is een groot aantal ambities benoemd, op hoofdlijnen zijn dit:

- Het real-time ondersteunen van de politiemensen op straat bij incidentafhandeling. Als gevolg van een melding van een burger of inzet op eigen initiatief (bijvoorbeeld een verdachte situatie).

- Bij opschaling relevante informatie verstrekken aan eenheden (bijvoorbeeld Team Grootschalige Opsporing – TGO, Staf Grootschalig en Bijzonder Optreden – SGBO en Observatieteam – OT).
- Het reageren op sensingtechnieken (zoals ANPR en *track & trace*). Enerzijds door het leveren van informatie nadat een hit leidt tot operationeel optreden. Anderzijds door het na een incident opnemen van informatie in sensingmethoden.
- Het 24/7 monitoren van de buitenwereld door het signaleren van informatie ten behoeve van de aanpak van veiligheidsproblemen. Het gaat hier om relevante extra informatie uit open bronnen, die real-time wordt gekoppeld aan politiekennis en politie-informatie.
- Het inhoudelijk voorbereiden van verschillende briefings door het 24/7 voeden van deze briefings, waardoor de kwaliteit van de dagrapporten toeneemt.

Het RTIC is operationeel sinds begin 2013. Daarmee is er een landelijk dekkend netwerk beschikbaar gekomen met dezelfde taak. Bij de start was er sprake van een minimale bezetting om de basistaken in alle eenheden uit te kunnen uitvoeren. De basistaken zijn verwoord in het Inrichtingsplan[2]: het RTIC biedt ondersteuning aan politiemensen en leidinggevenden op straat en voegt (on)gevraagd real-time informatie toe aan collega's, gekoppeld aan de afhandeling van de spoedeisende incidenten die te maken hebben met de veiligheid van burgers en collega's (0-5 minuten, als elke seconde telt).

Bij het in werking brengen van het RTIC speelde de uitgangspositie in een eenheid een grote rol, zeker als het gaat om de acceptatie van de rol van het RTIC. Eenheden die werkten met een andere vorm van het toevoegen van real-time informatie aan meldingen, konden daar in de uitvoering vaak moeilijk afscheid van nemen. Dit is te begrijpen, de collega's op straat hebben jarenlang gebruikgemaakt van een werkwijze waarbij ze zich goed en veilig voelden. Ook hebben enkele meldkamers het RTIC als concurrent gezien, omdat zij de informatie voorheen zelf toevoegden aan meldingen.

'Ik krijg mijn informatie altijd van mijn wachtcommandant of wijkagent. Die luisteren altijd mee. Als er wat bijzonders met een melding is, geven zij dat door over het teamkanaal. Iedereen weet dan wat er aan de hand is en kan er nog wat aan toevoegen. Dit gaat altijd sneller dan via de meldkamer.'
– Intern onderzoek naar beleving van functie van het bureaukanaal politie Den Haag, 2013

In de praktijk heeft het in een aantal eenheden dus even geduurd voordat het RTIC geaccepteerd werd. De toegevoegde waarde van de RTIC's bij de ondersteuning van (spoed) meldingen staat inmiddels steeds minder ter discussie.

2 Nationale politie, *Inrichtingsplan*. 2012.

Uit de praktijk van het RTIC: meisje gevonden op straat

Rond 19.30 uur werd een meisje aangetroffen op straat. Bij het RTIC was alleen bekend dat zij 4 jaar oud was. Het RTIC heeft een zoekslag gemaakt in de gemeentelijke basisadministratiepersoonsgegevens (GBA) op de postcode van de straat waar het meisje was aangetroffen. Hier kwamen twee meisjes uit naar voren. De collega's zijn met deze wetenschap langs de adressen gereden. Daar bleek het meisje inderdaad thuis te horen.

De werkwijze die gevolgd wordt om real-time informatie bij de politiemensen op straat te krijgen, loopt in de meeste gevallen via de meldkamer (het DROC). Medewerkers van het RTIC voegen de relevante informatie toe aan de melding door in het Geïntegreerd Meldkamer Systeem (GMS) mutaties te maken. In één melding kan dit meerdere keren gebeuren als er, door verder te zoeken in de systemen, meer informatie beschikbaar komt. De centralist van de meldkamer beslist welke informatie daadwerkelijk via de mobilofoon of portofoon wordt doorgegeven aan de politiemensen op straat. De centralist van de meldkamer heeft bij een spoedmelding de regie en het totale overzicht, en kan als beste inschatten welke informatie nodig is. In een aantal eenheden zijn er ook nog andere kanalen die gebruikt worden om de informatie van het RTIC bij de politiemedewerker op straat te krijgen, zoals direct telefonisch contact of via de Mobiele Dataterminal rechtstreeks naar de auto.[3]

Gaandeweg zijn ook steeds meer van de ambities, zoals verwoord in de hiervoor genoemde businesscase, gerealiseerd en zijn er bovendien nog nieuwe taken aan toegevoegd. Zo is het RTIC verantwoordelijk gemaakt voor het Actueel Operationeel Beeld (AOB) en het spoed-AOB. Dit zijn informatieproducten die het strategisch management informeren over relevante zaken uit alle eenheden. In de afgelopen jaren is het RTIC ook gestart met het reageren op ANPR-meldingen en het betrekken van open bronnen, met name de sociale media, bij het veredelen van meldingen. Met de mogelijkheid in begin 2016 om extra personeel aan stellen, is er een versnelling gekomen in de ontwikkeling van het RTIC. Het betrekken van meer informatie uit open bronnen en de ondersteuning bij calamiteiten worden daarmee verder ontwikkeld.

3 Dit is vooral relevant bij niet-spoedmeldingen. Bij spoedmeldingen kijken de noodhulpeenheden zelden op het MDT-scherm en varen ze voornamelijk op wat de centralist doorgeeft (Scholtens, A., M. den Hengst & R. Waterreus, *Het real-time informeren van noodhulpeenheden: een onderzoek naar de RTI-functie om frontlijnpolitiefunctionarissen snel te voorzien van relevante informatie*. Reeks Politiekunde nr. 77. Reed Business Information, Amsterdam 2016).

Uit de praktijk van het RTIC: zoeken op fonetische naam

Er kwam een verzoek binnen of het RTIC wilde zoeken naar een persoon. Er was alleen een fonetische naam bekend, die werd genoemd door het slachtoffer van een beroving. Het slachtoffer wist te vertellen dat de verdachte elke dag met de trein van A naar B op een tussenstation uitstapte om naar school te gaan. Uit BlueView bleek dat er een familie met een dergelijke fonetische naam in de nabijheid van het eindstation woonde. De gevonden informatie is door het RTIC doorgegeven aan de collega die niet veel later met de recherche een instap in de woning van de verdachte kon doen.

19.4 Ontwikkelingen in het RTI-concept

Real-time intelligence als concept legt de nadruk op actuele, relevante informatie, die direct beschikbaar is om op basis daarvan besluiten te nemen, ook doordat het handelingsperspectief wordt aangereikt. Het actuele beeld beschrijft enerzijds het nu. Anderzijds moet het beeld ook ondersteuning bieden voor het begrip: waarom gebeurt dat? En voorspellend: wat gebeurt er vervolgens? Onderzoeksorganisatie Gartner schetst een interessant perspectief op de ondersteuning door 'slimme systemen'. Computerondersteuning zal steeds meer analyse gaan overnemen ten behoeve van de besluitvorming. Met als extreme uiterste: autonoom door 'het systeem' genomen besluiten. Daarmee komen de toekomstbeelden uit films als *Minority Report* en *Robocop* in beeld.

Hoever we willen en kunnen gaan met de ontwikkeling richting meer ondersteuning en meer autonomie is natuurlijk onderwerp van onderzoek en maatschappelijk debat. De *human factor* is daarbij een belangrijk perspectief: hoe reageren mensen op steeds verdergaande computerondersteuning? Wat vraagt deze van mensen? Blijven we zelf nog wel nadenken?

Het RTI-concept blijft in ontwikkeling: nieuwe technologische mogelijkheden, nieuwe toepassingen en nieuwe vragen dienen zich steeds weer aan. Daarom heeft de politie samen met TNO en The Hague Security Delta een experimenteerprogramma opgezet rond real-time intelligence; dit programma heeft de naam 'Het RTI-lab'. In het RTI-lab vindt kruisbestuiving plaats tussen wetenschap, bedrijfsleven, overheid en maatschappij (burgers) om met elkaar te leren en te innoveren hoe de volgende stappen richting RTI eruitzien (zie de RTI-lab-film op https://vimeo.com/161504721/c7b7af403a). Het doel van het RTI-lab is de toegevoegde waarde van nieuwe producten, diensten of concepten op het gebied van RTI aan te tonen en nieuwe toepasbare kennis rond real-time intelligence te ontwikkelen. Inmiddels hebben er verschillende experimenten plaatsgevonden.

20 Big data

Ingrid de Vries

20.1 Big data... wat is het?

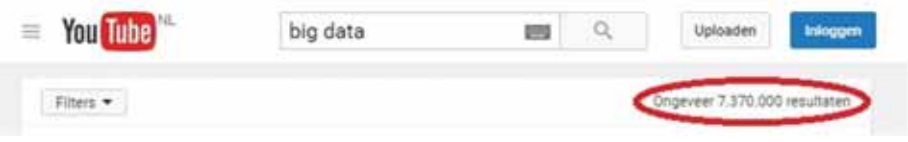
De zoektocht naar een eenduidige, laat staan bondige, definitie van big data kan al snel frustrerend zijn. We beginnen bij Google:

Figuur 20.1 Zoekresultaten voor 'big data definition' op Google

Ook Wikipedia biedt weinig soelaas, getuige het aantal verwijzingen dat is opgenomen.

Figuur 20.2 Verwijzingen naar definities voor big data op Wikipedia

YouTube dan?



Figuur 20.3 Zoekresultaat op YouTube naar bigdata-video's

Nee, wie in dit hoofdstuk op zoek is naar een eenduidig antwoord op de vraag 'Wat zijn big data?', moet ik teleurstellen. Dat is er niet, vindt trouwens ook de Wetenschappelijke Raad voor het Regeringsbeleid (WRR):

> 'Big data is een wijdverspreide en veelgebruikte term. Toch bestaat er geen consensus over de betekenis en is er geen breed gedeelde definitie van big data (...) Op de vraag wat big data precies is, geven verschillende auteurs verschillende antwoorden. De meeste auteurs focussen op de hoeveelheid data, anderen noemen de verscheidenheid en complexiteit van de data. Weer anderen leggen de nadruk op een revolutie in methoden om met de data om te gaan (...) of op de nieuwe maatschappelijke, economische en beleidsmatige mogelijkheden die ontstaan door het gebruik van big data.'[1]

Zelf vind ik het eerlijk gezegd ook eigenlijk helemaal niet interessant of iets nu wel of niet als big data moet worden aangemerkt. Wat vandaag voor 'big' wordt aangezien (bijvoorbeeld omdat de beschikbare informatie- en communicatietechnologie (ICT) nog niet goed met de hoeveelheid of variëteit van data overweg kan) is over een halfjaar waarschijnlijk al weer gewoon 'gewoon'. En wat voor de ene bedrijfstak 'big' is, wordt in een andere bedrijfstak als de normaalste zaak van de wereld beschouwd.

Helder is wel dat de hoeveelheid beschikbare data in de maatschappij steeds verder groeit (alles met een batterij of stekker eraan kan in potentie data opleveren). Maar wat hebben we daaraan? Uit de hiervoor gegeven eenvoudige zoekvoorbeelden is wel duidelijk dat het hebben van meer data niet automatisch leidt tot een betere informatie-, laat staan kennispositie.

De essentie – waar het wat mij betreft elke keer wél over zou moeten gaan – staat helemaal los van de hoeveelheid data: hoe zorgen we ervoor dat de gebruiker die informatie vindt of krijgt die voor hem of haar waardevol is? Welke slimme informatievoorziening (IV) kan daarbij helpen?

20.2 Big data binnen de politie

20.2.1 In het begin

Voordat de term 'big data' zijn intrede deed, bestond binnen de politie op verschillende terreinen natuurlijk al langer het besef dat het datavolume en de variëteit toenemen, dat de wereld digitaliseert en dat nieuwe IV-technieken en -middelen nodig (en mogelijk) zijn om criminaliteit effectief aan te kunnen pakken, en meer informatiegestuurd te kunnen werken. In verschillende korpsen zijn analysemethoden en -producten ontwikkeld die, vertaald naar die tijd, hoogstwaarschijnlijk aan een van de vele definities van 'big data' hadden voldaan. Het betrof vooral regionale initiatieven en oplossingen. Maar ook voor de landelijke voorzieningen destijds, als het Herkenningssysteem (HKS), de centrale verwijzingsindex (CVI) (1978), het landelijk informatiesysteem (LIST) (1994) en BlueView (2007), gold

1 Dit citaat komt uit het rapport van de Wetenschappelijke Raad voor het Regeringsbeleid, *Big data in een vrije en veilige samenleving*. Amsterdam University Press, Amsterdam 2016. Ik kan iedereen die meer wil weten over big data in het algemeen, en over de bigdata-ontwikkelingen in het Veiligheidsdomein in het bijzonder, aanraden dit rapport te lezen.

hetgeen we nu verbinden aan zogenoemde bigdata-oplossingen: het ging om data die niet of lastig met traditionele verwerkingstechnieken te beheersen waren en waar uitdagingen lagen op het gebied van verzamelen, opslaan, ontsluiten, bevragen, doorzoeken enzovoort.[2]

In 2009 is met het programma BasisVoorziening Informatie (BVI) een start gemaakt om binnen de politie meer samenhang en samenwerking op het gebied informatievoorziening te realiseren, zodat het mogelijk zou worden '(...) relevante, gestructureerde en ongestructureerde politie-informatie, informatie van ketenpartners en extern beschikbare informatie samen te brengen en in samenhang bevraagbaar, signaleerbaar, analyseerbaar en rapporteerbaar te maken waardoor de informatiepositie verbetert (ter kwalitatieve en kwantitatieve verbetering van het politiewerk)'.[3]

Inmiddels is de BVI 1.0 een feit en maken de Business Intelligence Competency Centers (BICC's) en gebruikersvoorzieningen als integrale bevraging (BVI-IB) en BVI-BlueSpot Monitor (BSM) daar onder de motorkap dankbaar gebruik van.[4]

Toch worden dit soort voorzieningen zelden in relatie tot big data genoemd. De op de BVI 1.0 ontwikkelde risicotaxatie-instrumenten (Criminaliteitsanticipatiesysteem (CAS), Risicotaxatie-instrument voor geweld, ProKid, Preselect Recidive), waar met behulp van indicatoren en algoritmen de kans dat een probleem zich in de toekomst voordoet, wordt berekend, zullen nog het meest aanvoelen als een bigdata-ontwikkeling.[5] Het verkrijgen van inzicht uit data door het gebruik van slimme algoritmen, is immers waar de kracht van big data kan zitten.

20.2.2 En toen...

Met het exponentieel verder digitaliseren van de samenleving, zijn ook de technieken voor dataverwerking, -opslag en -analyse mee veranderd.

Ook binnen de politie wordt gebruikgemaakt van nieuwe technieken. Op allerlei plekken, zie dit citaat:

> 'Sommige van voornoemde ontwikkelingen waren (en zijn nog steeds) autonoom in het maken van keuzes in techniek, organisatie en bemensing. Een korpsbrede visie en strategie is noodzakelijk om als politie effectief om te kunnen gaan met een continu groeiende stroom aan informatie. Daarnaast is het van belang gebruikers niet te belasten met een gefragmenteerd applicatielandschap, waarbij de beheersbaarheid en betaalbaarheid van de IV niet gegarandeerd is.'[6]

2 Terzijde: het afgelopen jaar zijn HKS en LIST buiten gebruik gesteld en is de vernieuwing van BlueView gestart.

3 Zie Buuren H. van, G. Kuijlaars & I. de Vries, *Basis Voorziening Informatie: overkoepelende notitie*. Voorziening tot Samenwerking Politie Nederland, 2009.

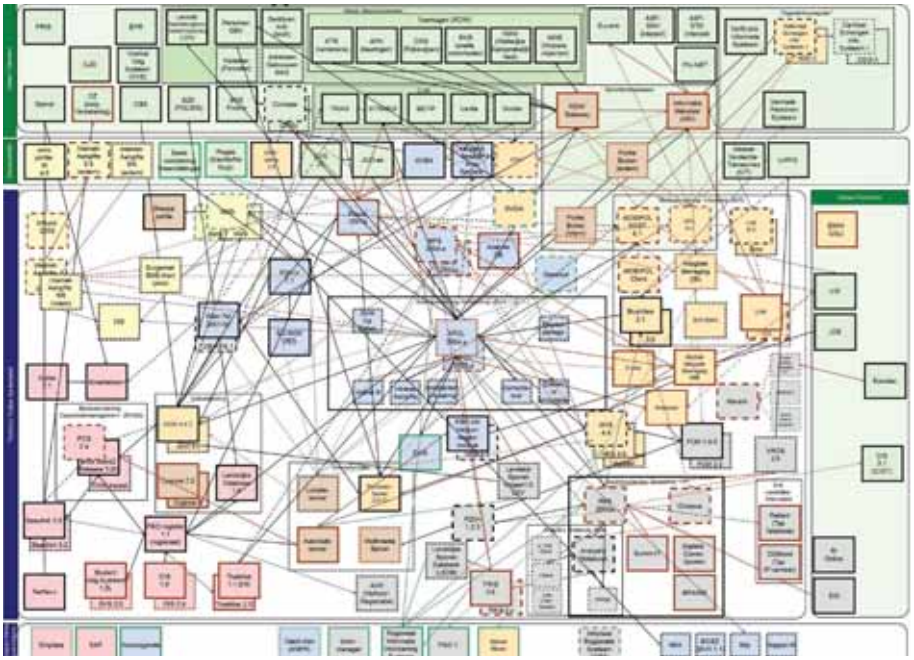
4 Kort gezegd is dat het datawarehouse waarin diverse handhavingsbronnen bij elkaar zijn gebracht.

5 Voor het inschatten van het risico op respectievelijk woninginbraken, gebruik geweld, het verkeerde pad opgaan en recidive, zodat er vroegtijdig/preventieve maatregelen kunnen worden genomen.

6 Middendorp, G., *Visie op Big data: handelingsperspectief*. Directie IV, Politie, 2015.

Wat een goed, korpsbreed gesprek daarover echter lastig maakt, is dat het binnen de politie bij big data al snel gaat over allerlei techniek: architecturen, platforms, infrastructuren, databases, *datalakes*, integraties, *pipelines*, *clouds*, *frameworks*, plug-ins... Wellicht dat enkele technici en *data scientists*[7] weten waar het over gaat, maar voor de operatie is het een ver-van-mijn-bedshow en lastig te beoordelen wat er van die techniek wáárom nodig is. Zeker zolang er geen functionaliteit beschikbaar is waarmee de gebruikers kunnen ervaren waar big data over gaat en hoe het hen verder kan helpen.

Ter relativering, een aantal jaar geleden (2009) moesten we het doen met figuur 20.4:



Figuur 20.4 Applicatielandschap politie 2009

Maar hoe complex die afbeelding er ook uitzag, toch was het toen eenvoudiger om er met elkaar gesprekken over te voeren. Het ging namelijk over 'tastbare' applicaties waarvan iedereen (lees: de operatie/gebruikers) in elk geval nog een beetje wist waar het over ging. Het waren immers voorzieningen waar men in de praktijk mee werkte. Bigdata-tools als Hadoop, MapReduce, R, Python, ElasticSearch, Kibana, Spark en dergelijke spreken nu eenmaal minder tot de verbeelding dan BVI-IB, BlueView, Excel en iBase.

7 Met de komst van big data is ook de functie van data scientist ontstaan. En ook in dit geval is er geen eensluidend antwoord op de vraag wat een data scientist precies is en/of wat het verschil is met bijvoorbeeld een data-analist. Meestal wordt een data scientist gezien als iemand met statistische kennis, kennis van programmeren en domeinkennis, die in staat is om – met behulp van *datamining*, algoritmen enzovoort – uit de grote hoeveelheden (on)-gestructureerde data juist die informatie te halen die voor de operatie relevant is.

Een voorbeeld: Hansken

Met de voortschrijdende digitalisering van de samenleving en criminaliteit groeit ook de hoeveelheid in beslag genomen gegevensdragers in strafzaken (zoals telefoons, computers, laptops, servers) en de hoeveelheid data die daarop staat. Om die data effectief en snel te kunnen onderzoeken, heeft het Nederlands Forensisch Instituut (NFI) de forensische zoekmachine Hansken ontwikkeld. In beslag genomen gegevensdragers worden gekopieerd en ingelezen in Hansken. Door gebruik te maken van bigdata-technieken is Hansken vervolgens in staat enorme hoeveelheden data en sporen te herkennen/identificeren en doorzoekbaar te maken (zoals documenten, foto's, mailverkeer, bezochte internetpagina's, contactlijsten).

20.3 Business intelligence

Zoals in figuur 20.4 is te zien, is kenmerkend voor het ICT-landschap van de politie dat het (van oudsher) om veel systemen gaat waarin informatie wordt vastgelegd.[8] Tel daarbij op alle informatie van partners in het veiligheidsdomein (en burgers) die van belang is voor de politie, en het is helder dat het verkrijgen van een goede informatiepositie een zeer omslachtige en tijdrovende klus is als er geen business-intelligencevoorzieningen zijn om daarbij te helpen.

> 'Er komen steeds meer gegevens beschikbaar. Intern en extern. Gestructureerd en ongestructureerd. Tekst, foto, video, gegevens uit *sensing*, sociale media, etc. Gelijk met het aanbod groeit de vraag naar informatie. Professionele politiemedewerkers verwachten snel en mobiel over de juiste informatie te beschikken.(...) Business Intelligence is het geheel van processen, producten, hulpmiddelen en organisatorische inrichting ten behoeve van het geautomatiseerd verzamelen, integreren en veredelen van gegevens en het analyseerbaar maken, presenteren en distribueren van informatie.'[9]

De definitie klinkt ingewikkeld, maar vrij vertaald gaat het er bij business intelligence (BI) om te zorgen dat 'de juiste informatie, op het juiste moment, bij de juiste persoon, op de juiste manier' beschikbaar is (zie ook hoofdstuk 2 Informatiegestuurd werken en business intelligence).

8 BVH voor handhavingsinformatie, Summ-IT voor opsporingsinformatie, Executie & Signalering (E&S) voor executieopdrachten, Amazone voor doelgroepen, DCS voor telefoongegevens, OPS en NSIS voor signaleringen, ORCA voor tapgesprekken, Verona voor wapenvergunningen enzovoort.

9 Programma Intelligence Politie Nederland, *Business intelligence strategie*. 2012.

En naarmate de hoeveelheid beschikbare data groeit, wordt het steeds belangrijker daar de juiste BI-voorzieningen voor te hebben.[10] Al die data mogen dan kansen bieden voor de politie, maar tegelijkertijd vormt die stortvloed ook een bedreiging. *Information overload* (het niet meer wijs kunnen worden uit de beschikbare gegevens) ligt op de loer, waardoor belangrijke informatie niet of te laat gezien wordt en verkeerde, onvolledige, onbetrouwbare of verlopen informatie ten onrechte wordt gebruikt bij het nemen van een besluit en/of handelen.

20.4 Raffinaderij-pilot

20.4.1 Algemeen

In 2011 werd in de Holitna-zaak, het onderzoek naar het netwerk van Robert M., de hoofdverdachte in de omvangrijke kinderpornozaak uit Amsterdam, duidelijk dat er behoefte was aan een werkwijze en ondersteunende BI-voorzieningen om rechercheurs en analisten beter in staat te stellen grote hoeveelheden data op een intelligente manier te ontsluiten, betekenis te geven en te analyseren. Die waren eigenlijk niet voorhanden. In elk onderzoek moest veel moeite worden gedaan om data te verzamelen, was het vrijwel onmogelijk om verschillende bronnen in combinatie met elkaar te analyseren, werd elke keer het wiel weer opnieuw uitgevonden, werden losse tools aangeschaft of ontwikkeld enzovoort.

Dat was de aanleiding om op vier grote rechercheonderzoeken van de Landelijke Eenheid en de Eenheid Amsterdam een proeftuin te starten met als doel: kijk wat de informatiebehoefte van de verschillende partijen in dergelijke onderzoeken is (rechercheur, analist, Openbaar Ministerie (OM), teamleider enzovoort) en ontwikkel daar een passende BI-voorziening voor.

De proeftuin werd Raffinaderij genoemd[11] en is na de positieve evaluatie uitgebreid tot een bredere operationele pilot die tot eind 2017 loopt. Op twee landelijke thema's (liquidatie en contraterrorisme) wordt er op dit moment binnen de recherche en informatieorganisatie ervaring mee opgedaan.

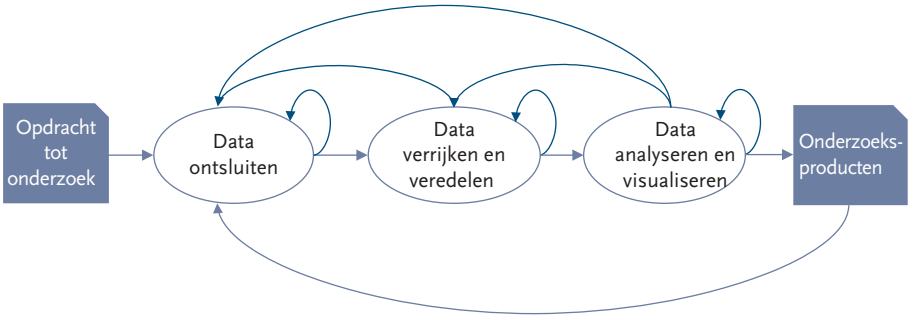
Raffinaderij is kort gezegd een voorziening die het mogelijk maakt om snel grote hoeveelheden politiegegevens in samenhang met elkaar te analyseren en visualiseren. Zo kunnen data afkomstig van in beslag genomen telefoons en computers (uit Hansken) in samenhang met alle andere relevante onderzoeksdata (uit onder andere BasisVoorziening Handhaving (BVH), Summ-IT, via de BasisVoorziening Informatie (BVI), van telefoontaps, bakens, internetdata, gegevens van automatic number plate recognition (ANPR)

---

10 Business-intelligencevoorzieningen? Bigdata-voorzieningen? Wat is het verschil? Ook daar zijn weer vele zienswijzen en meningen mogelijk. Veelal is het antwoord afhankelijk van het perspectief waarmee men naar de vraag kijkt en in welke sector men opereert. Kijkend vanuit de BI-strategie van de politie én vanuit het perspectief van de gebruiker, dekt BI de lading.

11 In een olieraffinaderij wordt ruwe olie opgewerkt tot verschillende bruikbare eindproducten; binnen deze Raffinaderij worden ruwe data opgewerkt tot voor de politie bruikbare informatie en kennis.

worden ontsloten en geanalyseerd. Door inzicht te hebben in het geheel (in plaats van alleen te kijken naar óf informatie uit open bronnen, óf digitaal beslag óf de registratie in politiesystemen enzovoort), kunnen verbanden worden ontdekt tussen schijnbaar ongerelateerde gebeurtenissen of kunnen veronderstelde verbanden juist in een vroeg stadium worden ontkracht.



Figuur 20.5 Op elk moment in het onderzoek kunnen vragen en onderzoekshypothesen (opnieuw) worden uitgelopen gebruikmakend van alle onderzoeksdata

Een voorbeeld: 26Koper

'Bij het plegen van criminele moordaanslagen en overvallen in georganiseerd verband worden veelal snelvuurwapens en bijzonder krachtige automobielen gebruikt. De plegers van dergelijke zware delicten maken gebruik van andere criminelen, die zijn gespecialiseerd in het verkrijgen en verhandelen van dergelijk instrumentarium. De politie slaagt er in toenemende mate in om dergelijke criminele dienstverleners te traceren en op te rollen. Hierdoor wordt het moeilijker om liquidaties te plegen. Om aan de voorkant van het liquidatieprobleem te komen, werd geïnvesteerd op leveranciers van gestolen auto's. Door geavanceerde analyse met behulp van de Raffinaderij lukte het relaties te leggen tussen meerdere zaken. Een gestolen Audi S5 bleek te zijn doorgeleverd aan een groep zwaar criminelen. Hierop werden meerdere verdachten en voertuigen onder intensief toezicht geplaatst (...) Het team en de zaaksofficieren wilden zo veel mogelijk bewijs verzamelen van het voorbereiden van liquidaties, maar tot elke prijs moest worden voorkomen dat een liquidatie daadwerkelijk zou worden uitgevoerd. Het resultaat was een reeks aanhoudingen en de vondst van een groot wapenarsenaal, kogelwerende vesten en speciale schoonmaaksets voor het verwijderen van forensische sporen. Eveneens aangetroffen beeldmateriaal en een "boekhouding" leveren waardevol bewijs op van voorbereidingshandelingen.'[12] >>

12 Huisman, S. et al., *Handelen naar waarheid: sterkte- en zwakteanalyse van de opsporing*. Amsterdam 2016.

>> In de zaak zijn veel bijzondere opsporingsmiddelen ingezet (telefoontaps, afluisterapparatuur, sensoren en dergelijke) die veel te analyseren data opleverden. De uitdaging in de zaak was te bewijzen dat de hoofdverdachten bezig waren met de voorbereiding van meerdere moorden. Dat de verdachten de beschikking hadden over wapens en andere spullen die nodig zijn om een liquidatie te plegen, is daarvoor niet genoeg. Justitie moet ook bewijzen dat ze de intentie en de opzet hadden om die wapens daadwerkelijk te gebruiken.
De rechtbank heeft op 28 november jl. de vier hoofdverdachten veroordeeld tot acht jaar celstraf. Dat is aanzienlijk minder dan de zeventien jaar die het OM tegen de hoofdverdachten had geëist. De rechtbank is van oordeel 'dat niet met voldoende bepaaldheid is gebleken welk crimineel doel de verdachte en zijn medeverdachten voor ogen hebben gehad. Weliswaar heeft verdachte deelgenomen aan een criminele organisatie die het plegen van liquidaties (moord gevolgd door brandstichting) tot oogmerk had, echter uit het onderzoek 26Koper is onvoldoende bewijs verkregen om te spreken van een concreet voorbereid misdrijf'.[13]
Met andere woorden: weliswaar is bewezen dat de verdachten lid zijn van een criminele organisatie die het plegen van liquidaties als oogmerk heeft en hadden de verdachten een concreet slachtoffer op het oog, maar daarmee is nog niet bewezen dat ze hem ook daadwerkelijk wilden vermoorden.
Het OM is inmiddels in beroep gegaan tegen de uitspraak. Ook wordt gepleit voor een wetswijziging om de voorbereiding van liquidaties strafbaar te maken[14]. 'Om te voorkomen dat we liquidaties alleen achteraf onderzoeken, heeft de recherche nieuwe tactieken ontwikkeld om dit soort misdaden te voorkomen', zegt Plooij. 'Dat is succesvol maar de maximale straf die kan worden opgelegd voor lidmaatschap van een criminele organisatie, spoort niet met de ernst van dit soort feiten.'[15]

20.4.2 Big data?

Raffinaderij maakt voor de opsporing effectieve informatieverwerking mogelijk op een schaal die voorheen niet te realiseren viel. Een gebruiker die voor het eerst kennismaakt met Raffinaderij zal gemakkelijk overdonderd worden door de hoeveelheid data en verschillende bronnen die beschikbaar zijn om mee te werken.

Raffinaderij wordt daarom vaak in één adem genoemd met big data. Het gaat in Raffinaderij echter om behapbare hoeveelheden data, bronnen die een onderzoeksteam normaliter ook ter beschikking heeft, gegevens die rechtmatig in een onderzoek zijn gebracht, verwerking die plaatsvindt met een duidelijke doelbinding, waarbij geen gebruik wordt

13 Zie http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2016:7769. Ook in de media is veel gepubliceerd over de zaak. Zie bijvoorbeeld: https://www.nrc.nl/nieuws/2016/11/28/flink-lagere-straf-na-wapenvondst-in-nieuwegein-a1533952.

14 Tweede Kamer, plenaire vergadering 13 december 2016.

15 'OM wil strengere wet om liquidatiegolf te stoppen.' In: *NRC*, 11 december 2016. Plooij is officier van justitie.

gemaakt van technieken als ongerichte datamining of geautomatiseerde besluitvorming enzovoort.

> 'De Raffinaderij is – in de wijze waarop deze binnen de proeftuin wordt ingezet – geen methode om aan risicoanalyse en profiling te doen. Hoewel op intelligente wijze gegevens geanalyseerd kunnen worden, is er geen sprake van ongerichte datamining.'[16]

Wel of geen big data? Belangrijker is het stil te staan bij de vraag a) hoe IV-voorzieningen een concrete bijdrage kunnen leveren aan het werk van de politie b) zonder dat daarbij de privacywaarborgen verloren gaan.

Raffinaderij wordt in de operatie in het algemeen gezien als een beloftevolle innovatieve IV-ontwikkeling waar succesvolle ervaringen mee worden opgedaan, dus met vraag a zit het vooralsnog wel goed.

Maar hoe zit het met vraag b? Het verzamelen en verwerken van grote hoeveelheden data kunnen in specifieke situaties immers op gespannen voet staan met de bescherming van de persoonlijke levenssfeer, oftewel het recht op privacy (zie ook hoofdstuk 7 IGP en ethiek, ofwel: wat mag en wat mag niet? en hoofdstuk 8 In gesprek met Peter Holla over ethiek).

20.4.3 Privacy?

Al tijdens de proeftuinfase van Raffinaderij is er daarom voor gekozen om een Privacy Impact Assessment (PIA)[17] uit te voeren, zodat vanaf de ontwikkelfase rekening kon worden gehouden met de principes van *privacy by design*. Het uitvoeren van een PIA is verplicht met de komst van nieuwe Europese wetgeving.[18]

> 'Privacy by design houdt in dat al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) aandacht wordt besteed aan privacyverhogende maatregelen en rekening wordt gehouden met dataminimalisatie: dat wil zeggen dat alleen gegevens worden verwerkt die noodzakelijk zijn voor het doel van de verwerking.'[19]

Kunnen we dus achteroverleunen met Raffinaderij? Nee, dat zeker niet!

Doordat Raffinaderij het makkelijk maakt om gegevens te verwerken, zullen medewerkers eerder dan vroeger geneigd zijn om zo veel mogelijk gegevens in een onderzoek te betrekken, in de hoop met behulp van Raffinaderij een relevant verband te vinden (wat

16 *Privacy Impact Assessment Raffinaderij*. In: *Considerati*, december 2013.

17 *Privacy Impact Assessment Raffinaderij*. In: *Considerati*, december 2013.

18 De nieuwe naam van de PIA is de gegevensbeschermingseffectbeoordeling (GEB). Een GEB wordt binnenkort ook verplicht voor het Wpg-domein.

19 Zie definitie Autoriteit Persoonsgegevens.

op gespannen voet staat met dataminimalisatie[20]). Bovendien zal de verleiding bij medewerkers groot zijn om gegevens te gebruiken voor een ander doel dan waarvoor ze mochten worden verwerkt, simpelweg omdat de gegevens beschikbaar zijn en omdat het (technisch) kan.

Het feit dat Raffinaderij zich verder ontwikkelt, breder wordt uitgerold binnen recherche en informatieorganisatie; het feit dat de opsporing zich verplaatst van reactief handelen naar voorkomen en tegenhouden; het feit dat er naast Titel V- en Titel IVa-onderzoeken (de klassieke opsporingsonderzoeken)[21] ongetwijfeld ook gebruikgemaakt zal gaan worden van verkennende onderzoeken (Titel VE) en onderzoeken ter opsporing van terroristische misdrijven (Titel VB); dit alles maakt dat de privacy een onderwerp is om continu scherp op te zijn en maatregelen op te nemen.

> 'Naast het "klassieke" opsporingsonderzoek kan de politie ook "verkennend onderzoek" doen (art. 126gg e.v. WvSv). Doel van zo'n onderzoek is de voorbereiding van de opsporing van georganiseerde misdrijven, waaronder terrorisme. Hier vervaagt in zekere zin de grens tussen opsporing op basis van een redelijk vermoeden dat een misdaad beraamd wordt of gepleegd is, en meer algemene doelen om misdaad te voorkomen.'[22]

20.4.4 Na de pilot

De Raffinaderij-pilot gaat in wezen niet alleen over de BI-voorziening zelf. Het gaat er ook om gevoel te krijgen bij de impact die het werken met dergelijke voorzieningen gaat hebben op de organisatie. Belangrijke vragen die spelen zijn bijvoorbeeld: wat betekent het op deze manier met data kunnen omgaan voor het werk en de werkprocessen bij de recherche en informatieorganisatie? Voor de samenwerking tussen de eenheden? En voor de samenwerking binnen de gehele veiligheids- en strafrechtketen? Hoe kan het bijdragen aan de verbetering van de kwaliteit van opsporing? Wat vraagt het aan kennis, expertise en vaardigheden van medewerkers? Hoe zit het met de juridische kaders, informatiebeveiligings- en privacyaspecten? Hoe is de aansluiting bij de verdere ontwikkeling van BI-voorzieningen binnen de politie?

Elke dag merken we dat het gebruik en verder uitrollen van Raffinaderij tot nieuwe inzichten en ideeën leidt. In de onderzoeken waar met Raffinaderij wordt gewerkt; in het Raffinaderij-team waar samen met de gebruikers continu wordt gewerkt aan nieuwe functionaliteiten; maar ook als het gaat om genoemde vragen.

Omdat Raffinaderij een pilot is, is het tot nog toe mogelijk, binnen een aantal gestelde grove kaders, flexibel en snel stappen te bepalen en te zetten, samen met de operatie en zonder eerst allerlei blauwdrukken en gedetailleerde (verander)plannen op te stellen en ter besluitvorming voor te leggen aan overlegorganen. We kunnen geen gebaande wegen

20 Het begrip dataminimalisatie wordt uitgebreid besproken in hoofdstuk 5 De Wpg.

21 Zie Wetboek van Strafvordering, Titel V: opsporingsonderzoek naar het beramen of plegen van ernstige misdrijven in georganiseerd verband, en Titel IVa: opsporingsonderzoek ter handhaving van de rechtsorde in een bepaald geval.

22 Kooijmans, T. & P.A.M. Mevis, *ICT in the context of criminal procedure*. TLS/EUR/AIDP, 2013.

bewandelen, dus voor iedereen is het zoeken en uitproberen. Maar het doel is helder: gezamenlijk een directe bijdrage leveren aan de veiligheid in Nederland, aan het voorkomen en bestrijden van criminaliteit en aan de bescherming van de burgers.

In 2017 wordt Raffinaderij geëvalueerd en besloten of het een ontwikkeling is om mee door te gaan en, zo ja, op welke manier.

20.5 Tot slot

Helder is dat bigdata-ontwikkelingen snel gaan. Technisch zijn er geen beperkingen meer om de meest ingenieuze dingen met data te doen. Alles is te automatiseren. Het waarnemen, het verzamelen, het interpreteren en analyseren... Zelfs besluitvorming is te automatiseren.

Het wordt steeds meer de vraag wat we daarmee als samenleving en als politie zouden moeten willen. Zeker als bedrijven en de overheid meer met algoritmen, gedragsmodelleringstechnieken, *machine learning* en kunstmatige intelligentie gaan werken. Het praten over bigdata-platforms en -architecturen is al abstract (zie paragraaf 20.2.2 En toen...), maar dergelijke algoritmen zijn, als ze al transparant zijn, compleet onnavolgbaar voor de meeste mensen. Hoe weet je dat het systeem is gevoed met juiste data om van te leren? Hoe weet je welke wegingsfactoren er aan verbonden moeten worden?

Zelfs voor experts wordt het steeds ondoorzichtiger hoe resultaten tot stand komen, terwijl het effect van die resultaten op het leven van mensen alleen maar toeneemt.[23,24]

> 'De specifieke samenstelling van de data en de precieze werking van de algoritmen zijn bepalend voor de uitkomsten van de analyse. Een dataverzameling die niet up-to-date is of incompleet zal tot andere resultaten leiden dan een volledige en bijgewerkte verzameling. Daarnaast heeft de keuze om bepaalde categorieën data wel te verwerken en andere niet gevolgen voor de uitkomsten. Ook kunnen de gebruikte algoritmen bepaalde aspecten uit de data benadrukken en andere aspecten onderdrukken. In het gebruik van de resulterende profielen uit een data-analyse is het van belang om na te gaan hoe "fair" de resultaten van de analyses zijn, en in welke mate er sprake is of kan zijn van bepaalde vooraf gemaakte keuzes die van invloed kunnen zijn op de uitkomst van de analyse.'[25,26]

23 Broeders, D., *Het geheim in de informatiesamenleving*. Oratie uitgesproken bij de aanvaarding van het ambt van bijzonder hoogleraar Technologie en Samenleving aan de Faculteit der Sociale Wetenschappen van de Erasmus Universiteit Rotterdam op vrijdag 30 oktober 2015 EUR. Textcetera, Den Haag 2015.

24 Aupers, S., '"The Force is Great": Enchantment and Magic in Silicon Valley'. In: *Masaryk University Journal of Law and Technology* 3 (2009), nr. 1, pp. 153-173.

25 *Zie Licht op de digitale schaduw, Verantwoord innoveren met big data*, Rapport van de expertgroep Big data en privacy aan de minister van Economische Zaken.

26 Een voorbeeld waar het misging: 'How Data Failed Us in Calling an Election'. In: *New York Times*, 10 november 2016.

'De overheid staat bovendien nog maar aan het begin van wat mogelijk is met big data-analyse. De grootschalige verzameling, het hergebruik van data en geautomatiseerde gegevensanalyses met profielen – de kern van big data-toepassingen – brengen echter ook risico's met zich mee, die te maken hebben met privacy, discriminatie en *chilling* effecten op de vrije meningsuiting. De WRR meent dat de kansen die big data biedt voor opsporing en surveillance gepaard moeten gaan met sterke waarborgen voor de vrijheidsrechten van burgers. Het reguleren van het verzamelen van data – het zwaartepunt in de huidige juridische kaders – moet daartoe aangevuld worden met de regulering van en het toezicht op de fases van analyse en het gebruik van big data.'[27]

Een voorbeeld

Sinds 2009 maakt Google gebruik van gepersonaliseerde zoekresultaten. Leidde voor die tijd een zoekvraag altijd tot dezelfde resultaten, vanaf 2009 krijgt iedere gebruiker andere zoekresultaten terug, afgestemd op bijvoorbeeld eerdere zoekvragen of locatie van de gebruiker. Google gebruikt meer dan tweehonderd algoritmen om te bepalen wat er boven aan in de zoekresultaten van een gebruiker terechtkomt: 'We bepalen de relevantie van elke webpagina aan de hand van meer dan tweehonderd signalen en met behulp van verschillende technieken, waaronder ons gepatenteerde PageRank™-algoritme. Dat analyseert welke sites de meeste 'stemmen' (links) hebben ontvangen van andere pagina's op internet en dus waardevolle informatiebronnen zijn', aldus Google.[28]

Dat kan natuurlijk best handig zijn, maar het brengt ook nieuwe vraagstukken met zich mee. Hoe kan voorkomen worden dat op die manier een *filter bubble* (met andere woorden een soort tunnelvisie) ontstaat bij mensen? Als zoekresultaten, nieuws en reclame worden afgestemd op wat je al eerder zag, dan bereiken andere invalshoeken, meningen en ideeën je steeds lastiger.[29]
En hoe kan voorkomen worden dat 'nieuwtjes' die niet kloppen maar wel viral gaan op internet, hoger in de lijst zoekresultaten komen te staan dan informatie die wel juist is?[30] Hoe kan gezorgd worden dat het algoritme dat je zoekvraag automatisch aanvult, met goede suggesties komt?[31]

27 Zie WRR-rapport, *Big data in een vrije en veilige samenleving*. Amsterdam University Press, Amsterdam 2016.

28 www.google.com/intl/nl/about/company/philosophy.

29 Zie onder andere Pariser, E. & E. Helsper, *The filter bubble, what the internet is hiding from you*. 2011.

30 Zie onder andere 'Google en Facebook nemen maatregelen tegen nepnieuws na kritiek'. In: *de Volkskrant*, 15 november 2016.

31 Voor andere voorbeelden zie bijvoorbeeld 'Google, democracy and the truth about internet search'. In: *The Guardian*, 4 december 2016. Overigens ook leuk om zelf mee te testen.

Figuur 20.6 Een mooi voorbeeld

Allemaal vraagstukken waar Google de afgelopen maanden mee in het nieuws kwam en lering uit trekt. Maar dat geldt natuurlijk niet alleen voor Google. Het zijn vragen die gelden voor elke omgeving waar met veel data en intelligente IV-technieken wordt gewerkt.

In de inleiding bleek al dat het hebben van meer data niet automatisch leidt tot een betere informatie – laat staan kennispositie. Het voorbeeld hiervoor maakt duidelijk dat ook het inzetten van slimme technieken niet automatisch leidt tot een betere, betrouwbare informatie- en kennispositie. Het blijft opletten.

Gelukkig groeit de laatste jaren de bewustwording en komt er meer en meer aandacht voor het onderwerp en voor maatregelen en IV-technieken die ingezet kunnen worden om ongewenste effecten te minimaliseren.

Een kleine bloemlezing van onderwerpen die de afgelopen maanden in het nieuws waren: de verspreiding van nepnieuws[32] (en welke maatregelen partijen als Google en Facebook daar vervolgens tegen nemen); het delen van gebruikersgegevens tussen WhatsApp en Facebook (en het voorlopig stopzetten daarvan naar aanleiding van ontstane privacydiscussies in Europa); de toegang van Evernote tot gebruikersnotities om te zien of de algoritmen en machine learning die het bedrijf toepast goed werken (en het binnen een paar dagen na bekendmaking van het plan er alsnog van afzien door de ophef die erover ontstond); de aandacht voor de wetswijzigingen op het gebied van de bewaarplicht van telecommunicatiegegevens, de 'hackbevoegdheid' van de politie (Wet computercriminaliteit III), de bewaartermijn van kentekengegevens door de politie, de aftapmogelijkheden voor de inlichtingen- en veiligheidsdiensten...

Binnen de politie vergen de digitaliserende samenleving (en criminaliteit) en het werken met bigdata-voorzieningen een verandering binnen de operatie en de bedrijfsvoering. De omgeving, wensen en technieken wijzigen snel en van de organisatie wordt verwacht dat zij kan meebewegen.

32 Het woord *post-truth* is door Oxford Dictionary zelfs uitgeroepen tot het internationale woord van het jaar 2016.

> 'Organisaties hebben geen jaren meer om zich voor te bereiden op de toekomst. Die tijd ligt definitief achter ons. Lokale, lineaire en rustige ontwikkelingen behoren tot het verleden. Vervangen door globale en exponentieel snelle ontwikkelingen. (...) Willen wij onszelf omvormen tot een adaptieve organisatie? Dat is niet de vraag. De politie moet zich omvormen tot een adaptieve organisatie.'[33]
> 'Leiders zijn graag "in control". Dat geeft het prettige gevoel de boel te beheersen en de macht in handen te hebben om de loop der gebeurtenissen in de gewenste richting te sturen.(...) Het is een vergissing om te denken dat leiders het moeten hebben van blauwdrukken die weergeven "waar het naar toe moet", en strakke implementatie met een plan A en een plan B voor als het niet lukt. Oversteken in transitie gaat namelijk over de sprong van verandermanagement naar een gids voor de toekomst; van dirigeren naar inspireren; van koers bepalen naar koers zoeken; van simplificeren naar visioneren. (...) Het hoge woord moet er maar uit. Beheersbaarheid is geen goede optie voor transitie naar een nieuw tijdperk'[34]

Raffinaderij is een van de voorbeelden waaruit blijkt dat er op dit moment al veel mogelijk is. Met data, met techniek, in de organisatie, met het verkrijgen van een goede informatie- en kennispositie uit big data[35], op een verantwoorde wijze...

We hebben de ruimte (gekregen) om op een andere manier te werken en hebben geluk met leidinggevenden die ons die ruimte geven, en met collega's uit allerlei hoeken van de organisatie die graag mee willen helpen. Wars van urencodes en veelal in hun eigen tijd.[36] Dat bepaalt voor een groot deel het huidige succes van Raffinaderij.

Grappig eigenlijk: terwijl aan de organisatiekant de beheersbaarheid moet worden losgelaten[37], zou aan de technologie- en gegevensverwerkingskant (en het begrijpen wat daar gebeurt met algoritmen en dergelijke) juist meer beheersbaarheid en transparantie moeten komen. Misschien dat het 'delen, tenzij'-principe van de Wpg, ook een goed credo is om te introduceren in de bigdata-wereld?

33 Akerboom, E., Toespraak op Innovatiecongres *Tomorrow is today*. 03-11-2016.

34 Zie Zwart, C., 'Perspectieven voor een toekomstbestendige politie.' In: *het Tijdschrift voor de Politie* 78 (2016), nr. 5, p. 16.

35 Of beter gezegd: lots of small data.

36 De beveiliger in het pand waar we zitten, noemt ons niet voor niets gekscherend 'de hobbyclub'.

37 Zwart, C., 'Perspectieven voor een toekomstbestendige politie.' In: *het Tijdschrift voor de Politie* 78 (2016), nr. 5, p. 16.

21 Predictive policing

Dick Willems, Marjolijn Bruggeling, Arnout de Vries en Reinder Doeleman

Predictive policing is, zeer algemeen gesteld, het gebruik van statistische voorspellingen zodat de politie kan anticiperen op criminele incidenten. Statistiek baseert zich altijd op gegevens, oftewel data. Dat geldt dus ook voor predictive policing. Als de politie kansberekening uitvoert op basis van politiegegevens, is dat dus een voorbeeld van predictive policing, het inschakelen van een helderziende is dat niet. De film *Minority Report*, het voorbeeld dat vaak gebruikt wordt voor predictive policing, gaat dus niet over predictive policing.

Hoewel deze definitie zeer ruim is en hierdoor in veel verschillende situaties van toepassing kan zijn, zal in dit hoofdstuk de term alleen worden gebruikt voor de variant van predictive policing waar op het moment van dit schrijven de meeste ervaring mee is opgedaan. Dat is het voorspellen van plaatsen waar, en tijden waarop, de kans op criminele incidenten het grootst is, en het inzetten van daaraan gekoppelde politiemiddelen. Predictive policing is een vorm van informatiegestuurd politiewerk (IGP). Een belangrijk onderdeel van IGP is immers het verkrijgen van inzicht in risicolocaties (hotspots) en risicotijden (*hottimes*). Predictive policing geeft dat inzicht richting de toekomst door trends door te trekken die door de data ondersteund worden.

21.1 Systemen

Om te bepalen of een trend doorgetrokken kan worden, moeten veel zaken worden meegenomen, en niet in het minst het gebied waar het over gaat en het type criminaliteit. Wat geldt voor inbraken in Amsterdam-West hoeft immers niet te gelden voor fietsendiefstallen in Groningen Ommelanden. Om iets dergelijks te kunnen bepalen, moet veel informatie worden verwerkt, zoveel dat het voor een menselijke analist eigenlijk niet te doen is. Daarom zullen dergelijke overwegingen onderdeel zijn van een geautomatiseerd proces. Dit soort automatische processen werkt grofweg op de volgende manier: vind criminaliteitspatronen in een historische dataset, en beoordeel vervolgens wat deze patronen betekenen voor de nabije toekomst. Het vinden van een patroon in criminaliteit wordt ook wel het bouwen van een model genoemd. Een dergelijk model bevat als het ware de ingrediënten die historisch samengaan met criminaliteit, en als een risicovolle mix van dergelijke ingrediënten op een bepaalde locatie aanwezig blijkt te zijn, zal dit zich vertalen in een hogere kans op criminaliteit in de toekomst.

Er worden al sinds 1931 statistische technieken toegepast om misdaad te voorspellen, in eerste instantie door socioloog Clifford R. Shaw en criminoloog Henry D. McKay. Toch werd pas in 2008 een belangrijke stap gezet door toenmalig korpschef Bill

Bratton van het Los Angeles Police Department. Hij durfde het aan om wiskundige technieken toe te laten in de politiepraktijk. Samen met Jeff Brantingham van de Universiteit van California, Los Angeles werkte de politie het idee uit om de algoritmen die aardbevingen konden voorspellen toe te passen op oude misdaadstatistieken. Dit systeem kreeg de naam PredPol. Het bleek een gouden greep. Waar voorheen informatiegestuurd politiewerk nog bleef steken bij het maken van hotspotkaartjes, kon men nu ineens veel meer dan alleen lijntjes doortrekken. Van de ene op de andere dag kon men een veelvoud aan factoren (zoals variaties in criminaliteitstypen, plaatsen en tijden) meewegen. De voorspellingen leken ook daadwerkelijk beter te zijn. PredPol claimt in een recente publicatie anderhalf tot twee keer beter risicogebieden in te schatten dan de politieanalisten.[1] De oplossing van PredPol wordt momenteel wereldwijd het meest gebruikt. Onder andere Los Angeles, Santa Cruz, Modesto, Richmond, Chicago, Atlanta, Alabama, Seattle en Little Rock in de Verenigde Staten, en Kent in het Verenigd Koninkrijk hebben of hadden PredPol in gebruik, soms alleen als pilot, soms ook operationeel. Het bleek echter niet overal succesvol te zijn. In Richmond is men zelfs gestopt met PredPol, ondanks een lopend contract. De reden: gebrek aan bewijs dat het werkte.

Nederland

Predictive policing wordt niet alleen toegepast in de Verenigde Staten, ook binnen de Nederlandse politie wordt het steeds gebruikelijker om voorspellende informatie te betrekken in de planning van politiewerk. De Nederlandse politie gebruikt hiervoor het Criminaliteitsanticipatiesysteem (CAS). Dit systeem is in Eenheid Amsterdam ontwikkeld, en het gebruik ervan breidt zich sinds 2015 uit over heel Nederland. Het systeem deelt het gebied dat een basisteam, district of eenheid bedient op in vakjes van 125 bij 125 meter. Gebieden waarvan de kans op een incident vooraf al laag kan worden ingeschat, zoals weilanden en open water, worden verwijderd. Van de overblijvende vakjes wordt een grote hoeveelheid gegevens verzameld: criminaliteitshistorie, afstand tot bekende verdachten, en demografische en sociaaleconomische gegevens van het Centraal Bureau voor de Statistiek (CBS). Van elk vakje wordt een historie van twee jaar opgebouwd; wekelijks wordt op een peilmoment bepaald welke gegevens er op dat moment bekend zijn (de ingrediënten). Vervolgens bepaalt men wat er in de week na deze peiling aan incidenten heeft plaatsgevonden (de uitkomst). Daarna wordt wiskunde toegepast om te bepalen welke ingrediënten samenhangen met de uitkomst. Belangrijker nog: hiermee kan worden beoordeeld waar zulke risicovolle ingrediënten aanwezig zijn. CAS identificeert de top 3-procent van de locaties binnen het gebied met de meest zorgwekkende combinatie van ingrediënten. Verder brengt CAS ook de ontwikkeling van het risico binnen deze top 3-procent aan het licht. Het is immers niet zo dat het risico op bijvoorbeeld een woninginbraak op elk moment van de week even groot is.

1 Mohler, G.O. et al., 'Randomized controlled field trials of predictive policing.' In: *Journal of the American Statistical Association* 110 (2015), nr. 512.

Figuur 21.1 Een CAS-kaart

Behalve CAS en PredPol zijn er meer systemen die het criminaliteitsrisico in kaart brengen. Over het algemeen gaat het om pakketten die, net als PredPol en CAS, de hoog-risicolocaties met behulp van gekleurde vierkantjes op een kaart afbeelden. Bekende voorbeelden hiervan zijn HunchLab (toegepast door Philadelphia PD), PreCobs (getest in Zürich en het Duitse Beieren) en Daily Crime Forecast (in samenspraak met Edmonton Transit System). Andere manieren om voorspellende informatie te leveren, worden geboden door bijvoorbeeld IBM, Accenture en BAIR Analytics in de vorm van uitgebreide analysepakketten.

Voor al deze systemen geldt dat minimaal incidentdata voorhanden moeten zijn, voorzien van tijd, datum en plaats. Dit is niet vreemd, aangezien de belangrijkste component van de voorspelling het herhalingskarakter van het incident zelf is. Extra variabelen, zoals CAS toelaat, kunnen het voorspellend vermogen van het systeem verder verhogen.

Als een dergelijk systeem beschikbaar is, rijzen twee vragen. 1) Klopt de voorspelling? 2) Wat kunnen we doen om deze niet uit te laten komen? En die tweede vraag is minstens zo belangrijk als de eerste.

21.2 Voorspellend vermogen

Het antwoord op de eerste vraag is uiteraard van belang: is het nu echt zo dat de op de kaart aangemerkte locaties een verhoogd risico hebben op criminaliteit? Dat wil zeggen: als er geen speciale acties worden ondernomen in de getoonde gebieden, vinden er dan daadwerkelijk relatief meer criminele incidenten plaats dan in de niet-gekleurde gebieden? Uiteraard is dit afhankelijk van de criminaliteitsdynamiek in het gebied waar het over gaat, maar de meeste voorbeelden uit de praktijk geven hierop een positief antwoord.

Hierbij hoort wel een aantal kanttekeningen. De eerste is dat niet elke accurate voorspelling ook praktisch gezien interessant is. Als voorbeeld van een geval van een voorspelling met hoge nauwkeurigheid maar een mogelijkerwijs lagere praktische significatie nemen we zakkenrollerij in een grote stad. Stel nu dat blijkt dat zakkenrollerij uitermate goed te voorspellen is. Het blijkt dat ongeveer 70 procent van de incidenten plaatsvindt in de voorspelde locaties, en wel tussen 12.00 en 16.00 uur.

De eerste kanttekening die geplaatst moet worden is: hoe wordt een en ander geregistreerd? In het algemeen zal het slachtoffer niet precies weten waar dit heeft plaatsgevonden, en zal de locatie worden geregistreerd als ofwel een locatie waarop het slachtoffer nog niet was beroofd, ofwel de locatie waarop deze erachter kwam dat hij gerold was. Daarnaast zullen dit over het algemeen ook geen precieze adressen zijn (bijvoorbeeld: ergens op de Oude Gracht in Utrecht). Stel nu dat in het algemeen de locatie wordt gemuteerd waarop het slachtoffer achter de diefstal komt, dan zullen de gekleurde vakjes op de kaart niet de locaties met de hoogste kans op zakkenrollerij aangeven, maar de locaties met de hoogste kans dat een slachtoffer van zakkenrollerij erachter komt dat hij gedupeerd is. Dit is overigens een kanttekening die niet alleen bij voorspellende systemen geplaatst moet worden, maar bij elke variant van *heat mapping*. Het is de vraag of dit soort informatie dan als basis van politiewerk gebruikt kan worden.

Een tweede kanttekening heeft verband met een incidentele trendbreuk: het kan voorkomen dat een incident in zijn algemeenheid goed te voorspellen is, maar dat er zich een gebeurtenis voordoet die de bestaande dynamiek verstoort. Stel bijvoorbeeld dat het systeem de beschikking heeft over politiedata, maar dat uit andere bronnen blijkt dat er een trendbreuk aan zit te komen. Het zou bijvoorbeeld zo kunnen zijn dat een internationale organisatie achter de zakkenrollerij zat en dat deze is opgerold in het buitenland, of dat de voorspelde locaties voornamelijk metrostations zijn, maar dat in verband met werkzaamheden de metro's een tijd niet zullen rijden. Aangezien deze informatie buiten de politiedata valt, zullen deze voorbeelden niet leiden tot een verandering in het beeld dat het systeem weergeeft.

Genoemde kanttekeningen laten zien dat een voorspellend systeem geen kristallen bol is en zeker niet als zodanig moet worden geïnterpreteerd. Als er op enige wijze specifieke en relevante informatie aanwezig is binnen de organisatie (zelfs al is het in de hoofden van de medewerkers) moet deze, naast de informatie die predictive-policingsystemen kunnen bieden, uiteindelijk betrokken worden in de beslissing om tot politieacties over te gaan. Het is dus zaak om een goede informatiepositie op te bouwen waar een voorspellend systeem onderdeel van is.

21.3 Effectmeting: van predictive naar prescriptive policing

De vraag die het meest wordt gesteld in het kader van predictive policing is naar het effect. Het antwoord is echter niet zo eenvoudig. Waar de voorspellende kracht tamelijk eenvoudig is vast te stellen door simpelweg te meten wat er gebeurt in de hoog-risicovakjes, hangt de effectiviteit van predictive policing voornamelijk af van het gebruik van deze informatie door de politie zelf. Wat de aanbieders van dergelijke systemen dan ook mogen beweren, er is nog nooit ter wereld ook maar één crimineel incident voorkómen, louter door het aanschaffen van een softwarepakket.

Een betere vraag zou zijn: hoe kan er zo veel mogelijk rendement uit de geboden informatie worden gehaald? Bij deze vraag hoort een effectmeting. Een effectmeting is iets anders dan het meten van incidenten of arrestaties. Dit soort cijfers zijn wel een onderdeel van een effectmeting, maar cruciaal is ook dat de interventie zelf wordt vastgelegd. Wat ideaal zou zijn, is als de politie uitspraken zou kunnen doen als: een

surveillance van vijf minuten vermindert de kans op een crimineel incident in een straal van tweehonderd meter met 50 procent, gedurende dertig minuten. Deze cijfers zijn geheel uit de lucht gegrepen, maar zouden zeer bruikbaar zijn in het planningsproces.

De politie wordt momenteel aangestuurd naar inzet (manuren) in plaats van effectiviteit. Juist deze drang naar 'meer blauw op straat' kan een slimmere inzet in de weg zitten. Er is niet direct een basis om effectiever te gaan werken. Ook is er binnen de politie de neiging tot 'better safe than sorry'. Opschalen gaat makkelijker dan afschalen, ook als zou blijken dat dit niet of nauwelijks effectiever is.

De effectiviteit van beveiligingsmaatregelen is helaas vaak lastig te bepalen.[2] Het is meestal onmogelijk om de afwezigheid van een dreiging toe te kennen aan een specifieke beveiligingsmaatregel: is er geen overval uitgevoerd omdat er geen potentiële overvaller was, of omdat de overvaller is afgeschrikt door een recente mediacampagne om burgers te stimuleren beelden te verzamelen op hun mobieltjes? Dit is een fundamenteel probleem van effectiviteitsstudies in criminologie.

Waterbedeffect en detection dilemma

Een vaak gehoorde opmerking over informatiegestuurde surveillance is dat dit geen criminaliteit voorkomt, maar dat er alleen een waterbedeffect teweeggebracht wordt. Een waterbedeffect wordt vaak gedefinieerd als: het voortzetten van crimineel gedrag als reactie op een maatregel die de criminaliteit moet voorkomen, waarbij een al gemotiveerde dader een delict pleegt buiten de reikwijdte van deze maatregel. Kort gezegd, de criminaliteit verdwijnt niet, ze verplaatst zich.

Er zijn verschillende vormen van dit soort verplaatsingen:

- Er kunnen andere doelwitten worden uitgekozen.
- De criminaliteit kan zich verplaatsen naar andere tijdstippen.
- Er kan een ruimtelijke verplaatsing van de criminaliteit optreden, bijvoorbeeld naar aanliggende gebieden.
- Er kan sprake zijn van een functionele verplaatsing waarbij daders overstappen van het ene delicttype op het andere.
- De werkwijze (modus operandi – MO) bij delictpleging kan veranderen.

Bij een grote 'schoonmaakactie' op station King's Cross in Londen bleek bijvoorbeeld dat de drugshandel zich enkel had verplaatst naar een ander station. Ook het openbaar drinken van alcohol werd bij die actie bestreden, maar daar wisten notoire gebruikers wel iets op: ze goten hun alcohol gewoon over in flessen van een bekend sportdrankje. Hoe groot het waterbedeffect is, hangt vaak af van hoe moeilijk de verandering is. Hoewel een verplaatsing naar een ander gebied simpel lijkt, zorgt de onbekendheid ermee al wel voor onzekerheid bij criminelen.

Een ander probleem is het *detection dilemma*: het is lastig om te meten hoeveel criminele delicten er zijn voorkomen, omdat we niet weten hoeveel het er in werkelijkheid hadden kunnen zijn. Als er al data over incidenten zijn, dan zijn deze voor veel typen

2 Rest, J. van, M. Roelofs & A. van Nunen, *Afwijkend Gedrag: maatschappelijk verantwoord waarnemen van gedrag in context van veiligheid*. TNO-rapport: TNO 2014 R10425. TNO, Delft 2014.

dreigingen (bijvoorbeeld terrorisme) vaak zo gebrekkig dat we er geen significante conclusies aan kunnen verbinden. Zo blijkt het bijvoorbeeld heel moeilijk te zijn om antwoord te geven op de vraag: 'Hoeveel terroristische aanslagen zijn voorkomen door politieoptreden?' De minimale controle op externe omgevingsfactoren in evaluatiestudies maakt het meten van effectiviteit er niet gemakkelijker op.[3]

Hoe moet het dan wel?

In theorie is het nodig om ten opzichte van een uitgangssituatie (nulmeting) vast te stellen of er verschillen optreden tussen vergelijkbare omgevingen waarin wel een interventie is gepleegd op basis van voorspellingen, en omgevingen waar dat niet is gebeurd.

In de praktijk zou dat betekenen dat we om te beginnen heldere indicatoren zouden moeten vastleggen. Vervolgens zouden interventies zorgvuldig gepland moeten worden, om ten slotte de activiteiten te monitoren om te zien of de verschillende indicatoren zich in de juiste richting ontwikkelen (de zogenoemde *Plan-Do-Check-Act-cyclus*). De vraag is of zo'n aanpak zich leent voor de dagelijkse praktijk van handhaving, waar meestal geen strak omlijnde definitie is van de interventie, en waar het strikt kanaliseren en plannen van activiteiten indruist tegen het karakter van incidentrespons, en tegen de intuïtie en professionaliteit van de politiemedewerker op straat.

Een eerste stap hiertoe zou in elk geval zijn het vastleggen van (eventueel geanonimiseerde) gps-informatie van operationele politiemedewerkers. Met deze data kunnen al zeer interessante analyses gedaan worden. Is er bijvoorbeeld een verband te zien tussen politieaanwezigheid en criminaliteit? Zijn er bepaalde typen criminaliteit die meer of minder gevoelig zijn voor politieaanwezigheid? Dit soort informatie zou niet alleen interessant zijn voor effectmeting van politieacties, maar mogelijkerwijs ook voor het verbeteren van de voorspelkracht van predictive-policingsystemen.

Een volgende stap zou dan kunnen zijn het kwalificeren van de activiteit van de politiemedewerker. Op deze manier zouden de effecten van verschillende soorten politieacties op verschillende soorten criminaliteit kunnen worden onderzocht. De ene soort criminaliteit is wellicht gevoeliger voor preventieve surveillance, terwijl een andere soort misschien beter bestreden kan worden met een persoonsgerichte benadering op een klein aantal veelplegers. En laten we niet het nut van samenwerking met externe partners uit het oog verliezen. Wellicht kan een signaal naar een wooncorporatie over het hang-en-sluitwerk in een inbraakrisicogebied op een veel hoger rendement rekenen dan de politie teweeg kan brengen.

Naar prescriptive policing

Als dit soort informatie beschikbaar is, ligt het binnen handbereik om na predictive policing, *prescriptive* policing in te voeren. Met predictive policing kan worden aangegeven waar en wanneer de kans het grootst is op criminaliteit. Het doel wordt dan om dit te gaan voorkomen. Prescriptive policing geeft een advies over wat gedaan kan worden om het maximale effect te bereiken. Dit vindt plaats op basis van de nieuwe gegevens over de effecten van politie-interventies.

---

3 Hemert, D.A. van & H. van den Berg, 'Effectiviteit van menselijk toezicht'. In: *Security Management* (2013), nr. 12.

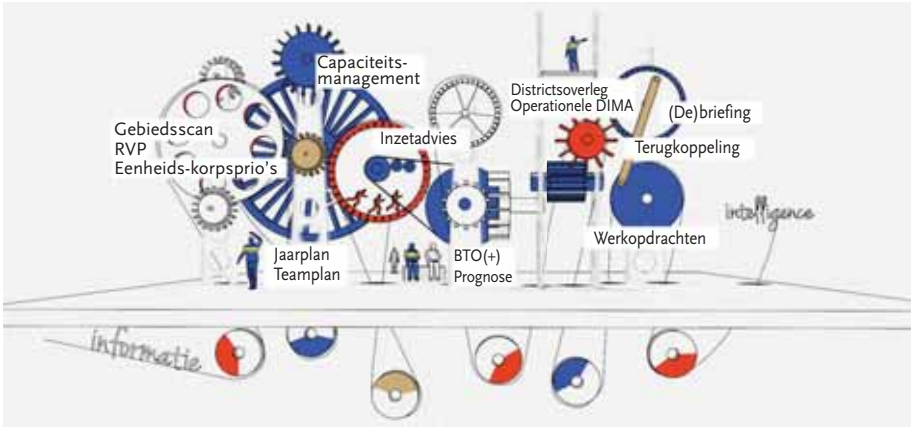
Uiteraard moet bij dit soort overwegingen ook de privacy van de poltiemedewerker worden betrokken. Niemand houdt er van voortdurend op zijn vingers te worden gekeken, en het is uiteraard niet de bedoeling dat een politiemedewerker hinder ondervindt van iets wat juist bedoeld is om de politietaak efficiënter en effectiever te maken. Desalniettemin moet ervoor worden gewaakt dat de politie in dit informatietijdperk niet in een situatie terechtkomt waardoor iedereen weet waar de politie is, behalve de politie zelf. Dit is, ook met het oog op de veiligheid, buitengewoon onwenselijk.

Het doel van predictive policing is om uiteindelijk zinvol politiewerk te kunnen doen. Zoals uit het voorgaande kan worden begrepen, gaat het om meer dan alleen de beschikking hebben over technologie. In de praktijk blijkt dan ook dat het daadwerkelijk dóen van predictive policing veel om het lijf heeft. Niet vreemd, omdat er wordt ingegrepen in een onderdeel van de bedrijfscultuur.

21.4 De praktijk: informatiegestuurde inzet bij de politie, een integrale aanpak

Binnen de Nederlandse politie is ruime praktijkervaring opgedaan met predictive policing. Na ervaring op te hebben gedaan met pilots in Eenheid Amsterdam en een pilot in de basisteams Enschede, Groningen-Noord, Hoefkade en Hoorn,[4] hebben de eenheden Amsterdam, Midden-Nederland en Noord-Nederland ervoor gekozen om met voorspellende informatie te gaan werken.

De langetermijndoelstelling van deze politie-eenheden is om de inzet van politiecapaciteit vanuit lokale veiligheidsvraagstukken intelligencegericht te sturen, en dat op een zo efficiënt en effectief mogelijke wijze te doen. Met andere woorden: de vraag stuurt het aanbod. Dat kan door alle relevante processen met elkaar te verbinden (zie figuur 21.2).



Figuur 21.2 Verbinding van processen

4 Mali, B., C. Bronkhorst-Giesen & M. den Hengst, *Predictive policing: lessen voor de toekomst*. Politieacademie, Apeldoorn 2016.

21.4.1 Vraaggerichte sturing op basis van datagedreven verwachtingen

Om vanuit de vraag te kunnen werken, gebruiken de eenheden de hiervoor besproken tool CAS. Die tool wordt gebruikt binnen een nieuwe werkwijze van de eenheid, waarbij predictive policing onderdeel is van een integrale aanpak. Enkel de implementatie van een intelligencetool zoals CAS is daarbij echter niet toereikend. Er is een totaalpakket aan integrale aanpassingen nodig. CAS genereert weliswaar belangrijke basisinformatie (waar en wanneer bestaat het hoogste risico op bepaalde criminaliteit?), maar die informatie is niet bruikbaar zonder verrijking met lokale kennis en actualiteiten. Toch weegt de berekening die CAS automatisch opmaakt zwaar mee. Het is een onafhankelijk, richtinggevend instrument op basis van data, en niet op basis van onderbuikgevoel.

De politieorganisatie heeft veel lokale kennis en kunde die op een betere manier gebruikt kunnen worden bij het maken van sturingskeuzes over politie-inzet. Die lokale input wordt dan ook samengevoegd met de datagedreven verwachtingen uit CAS. Het doel is dus niet om ervaring en lokale kennis te vervangen. Juist de combinatie van datagedreven sturing en lokale kennis leidt tot het maken van betere, doordachtere en bewustere sturingskeuzes. Dit betekent dat het kan gebeuren dat een door CAS opgemaakte risicoberekening bewust opzij geschoven wordt, omdat de betrokken lokale politiemedewerkers ervan overtuigd zijn dat er op dat moment op een andere plek inzet vereist is dan op de plek die de verwachting uit CAS aangeeft. Een dergelijke keuze wordt zelfs gestimuleerd, omdat er op zo'n moment grondig, weloverwogen én in samenwerking tussen verschillende politiedisciplines naar het betreffende probleem is gekeken en daardoor plussen en minnen bewust tegen elkaar afgewogen kunnen worden.

CAS is daarmee een van de bronnen voor sturing. De basisteams leveren focusspeerpunten aan op basis van de lokale veiligheidsvraagstukken. De wekelijkse CAS-voorspellingen hebben betrekking op deze speerpunten. Maar behalve de CAS-kaarten wordt er in sommige eenheden ook een driemaandelijks inzetadvies gemaakt om de roostervorming te verbeteren. Indien nodig kan er maandelijks bijgestuurd worden.

Wekelijkse prognoses worden opgebouwd op basis van CAS-kaarten die gebaseerd zijn op focuspunten van het betreffende basisteam, zoals woninginbraak of jeugdoverlast. De CAS-kaarten geven een wekelijks inzicht in deze overlast- en criminaliteitsfocuspunten, ten aanzien van waar en wanneer er een verhoogde kans is op dergelijke incidenten.

Lokale intelligencespecialisten gebruiken deze kaarten als startpunt voor intelligenceproducten ten behoeve van sturingskeuzes binnen het basisteam. De CAS-kaarten worden door de intelligencespecialisten verrijkt met lokale kennis (van bijvoorbeeld wijkagenten en op basis van meldingen binnen het aangewezen gebied) en actualiteiten. Op basis van deze gecombineerde blik op de criminaliteitsverwachting geven intelligencespecialisten vervolgens een advies aan de basisteamleiding ten aanzien van sturingskeuzes. Dit advies wordt meegenomen bij onder andere het samenstellen van werkopdrachten en politieacties.

Op die manier wordt er gestuurd op basis van de visie, en zijn de keuzes die uit de visie voortvloeien verder terug te zien in bijvoorbeeld het basisteamoverleg, de dagelijkse briefing en de roostervorming. Het basisteam is en blijft dus het hart van het politiewerk, waarbij de focus ligt op een integrale aanpak.

21.4.2 Veranderingen in de praktijk

Deze manier van werken brengt grote veranderingen teweeg in de dagelijks processen; incidentmanagement alleen is niet meer toereikend. Door de vele veranderingen die gaande zijn (niet alleen het intelligencegericht sturen, maar ook de verdere vorming van de nationale politie), kost die implementatie veel tijd.

Het loslaten van de oude werkwijze kan ingewikkeld zijn, en vraagt zowel organisatorische als cultuuraanpassingen. De ervaring leert namelijk dat politiemedewerkers graag mee willen werken aan de nieuwe werkwijze, maar het in de praktijk ook lastig vinden. Dat komt doordat er zo veel factoren samenhangen in dit proces. Het is niet alleen een kwestie van een nieuw intelligencedocument opmaken, of de briefing net iets anders inrichten. Juist de samenhang in het geheel maakt dit een belangrijke, maar ook lastige stap binnen de organisatie. Er wordt veel in geïnvesteerd, maar het blijft een uitdaging om alle aspecten met elkaar te laten samenvallen.

Er moeten veel praktische zaken worden geregeld om deze manier van werken te introduceren. Om de basisteams en ondersteunende diensten te ondersteunen bij het uitvoeren van het nieuwe sturingsconcept, is er bijvoorbeeld een toolkit ontwikkeld. Die toolkit bevat alle benodigde informatie om te starten met het werken met prognoses. Daarbij kan gedacht worden aan: een plan van aanpak, een introductievideo, een globale routekaart en verschillende praatplaten met bijbehorende spelregels. Daarnaast zijn er in verschillende eenheden presentaties gehouden, en trainingsdagen en feedbacksessies georganiseerd – over het nieuwe werkproces – voor alle betrokken managementteamoverleggen en medewerkers (van wijkagent tot intelligencespecialist tot inzetcoördinator en capaciteitsmanagementadviseur).

Inmiddels zijn verschillende eenheden op een dergelijke manier van start gegaan. In deze eenheden worden werkgroepen en bijeenkomsten gehouden om steeds verder vorm te geven aan het nieuwe werkproces, en om de ervaringen en de vervolgstappen te bespreken. Er worden bijvoorbeeld expertteams opgericht, die kennis en kunde over het maken van prognoses delen en toepassen bij de ontwikkeling van nieuwe sturingsproducten.

21.4.3 Wat is er bereikt en wat is er nog nodig?

Een aantal eenheden heeft ondertussen het gedachtegoed van predictive policing omarmd. Het werkproces is nog niet overal volledig ingericht, sommige teams zijn daar verder mee dan andere. Wel zijn alle teams bezig om hun eigen overlegstructuren en ondersteunende intelligenceproducten ten aanzien van sturingsmomenten te analyseren en af te stemmen op het nieuwe werkproces.

Wel is dus het overkoepelende doel al bereikt dat er een stevige aanzet is gemaakt tot een andere *mindset*: het nadenken over inzetten op verwachtingen in plaats van op incidenten is gemeengoed geworden. Veel mensen zijn van het belang daarvan inmiddels overtuigd. Toch is het loslaten van werkvormen die inzetten op incidenten soms nog een issue, ook bij de intelligenceafdelingen. Zo is er veel tijd geïnvesteerd in het controleren van systeemuitkomsten, maar blijven de lokale verrijking en kennis om een compleet beeld te schetsen soms wat achterwege, terwijl díe juist de doorslag geven bij het geven van een

goed beeld over verwachte criminaliteit binnen een bepaald gebied.[5] Het combineren van die twee aspecten blijkt soms lastig, omdat er nu iets anders van de intelligencespecialisten wordt gevraagd dan in de voorgaande jaren. Het daadwerkelijk durven sturen op verwachtingen en het loslaten van incidentgericht sturen lijkt in theorie logisch, maar kan in de praktijk een spannende keuze zijn. Liever nog beide doen dan een stevige keuze te maken. Daardoor is er nog een en ander te winnen aan efficiëntie.

Er zijn nog veel vervolgstappen en ontwikkelingen nodig om het nieuwe werkproces (sturen op basis van verwachtingen) volledig in te richten. Dat is dan ook de focus van de eenheden voor nu en de komende jaren.

Een van die ontwikkelingen is een integraler regionaal veiligheidsplan, waarbij de politie meer lokale criminaliteitsverwachtingen als input levert. Een andere stap is het onderzoeken van de mogelijkheid om verdiepende effectevaluaties te houden. Op dit moment kan dat namelijk, zoals al eerder gesteld, nog maar heel beperkt worden gedaan, omdat nog niet altijd goed inzichtelijk is waar politiemedewerkers precies zijn geweest, hoe ze binnen een bepaald gebied hebben gehandeld en in welke hoedanigheid. Pas wanneer dat beter gebeurt, kan ook beter onderzocht worden welke soort politie-inzet het meest effect heeft gehad binnen een bepaald gebied.

Daarnaast zal meer en meer integraal worden samengewerkt met externe partners, zowel op het gebied van implementatie als voor de doorontwikkeling van producten. Daarbij geldt dat samen beter en slimmer inzetten op criminaliteitsverwachtingen het doel is; het is niet alleen een taak van de politie.

Er dient aandacht te blijven voor het feit dat een cultuurverandering tijd kost. Hoewel de politie die tijd neemt, blijft bewuste investering daarin noodzakelijk. Er moet betrokkenheid worden gecreëerd, vervolgens moeten werkwijzen worden verbeterd, en daarnaast dienen politiemedewerkers gemobiliseerd en gestimuleerd te worden om de uitdaging aan te gaan. Het ging en gaat om een grootschalige integratie van processen en producten. Door met toewijding te investeren in dit proces worden en zijn aspecten die al goed verliepen versterkt, evenals de gewenste cultuurveranderingen.

Tot op heden zijn de ervaringen binnen verschillende eenheden positief. Toch kan het zo zijn, gezien de grote mate van samenhang tussen alle aspecten, dat de organisatie een aantal jaar verder is voordat alle radertjes in figuur 21.2 met elkaar samenvallen.

21.5 Tot slot

Predictive policing is een natuurlijke volgende stap in IGP. Predictive policing zoals het wordt toegepast door de Nederlandse politie omvat, behalve een voorspellend systeem, ook een werkproces dat is opgesteld om de voorspellingen te duiden. Dit is arbeidsintensiever dan hoe het door veel voorstanders van predictive policing wordt voorgesteld, maar resulteert in betere informatieverstrekking en creëert daarom meer acceptatie bij de operationele collega's. Daarnaast is het zo dat door deze werkwijze het makkelijker wordt om de volgende fase te bereiken: prescriptive policing. Behalve dat de politie dan weet waar en

5 Mali, B., C. Bronkhorst-Giesen & M. den Hengst, *Predictive policing: lessen voor de toekomst*. Politieacademie, Apeldoorn 2016.

wanneer de kans op criminaliteit het hoogst is, wordt het dan ook mogelijk om aan te geven wat voor soort actie naar alle waarschijnlijkheid het beste resultaat gaat geven.

Toch is het goed om nogmaals te onderstrepen dat systemen maar een onderdeel zijn van een groter geheel, en geen doel op zich. Het is belangrijk dat de geleverde voorspellingen en suggesties worden geduid voordat er actie op wordt gebaseerd, en het is niet de bedoeling dat dit soort expertsystemen in de praktijk de politiemedewerkers gaan overstemmen. Het is goed om te leren van het verleden, maar het belang van creativiteit moet niet uit het oog worden verloren. De rol van technologie in de politiepraktijk is om het werk makkelijker te maken, niet moeilijker.

22 De business-intelligencestrategie in de politiepraktijk

Anne Jan Oosterheert

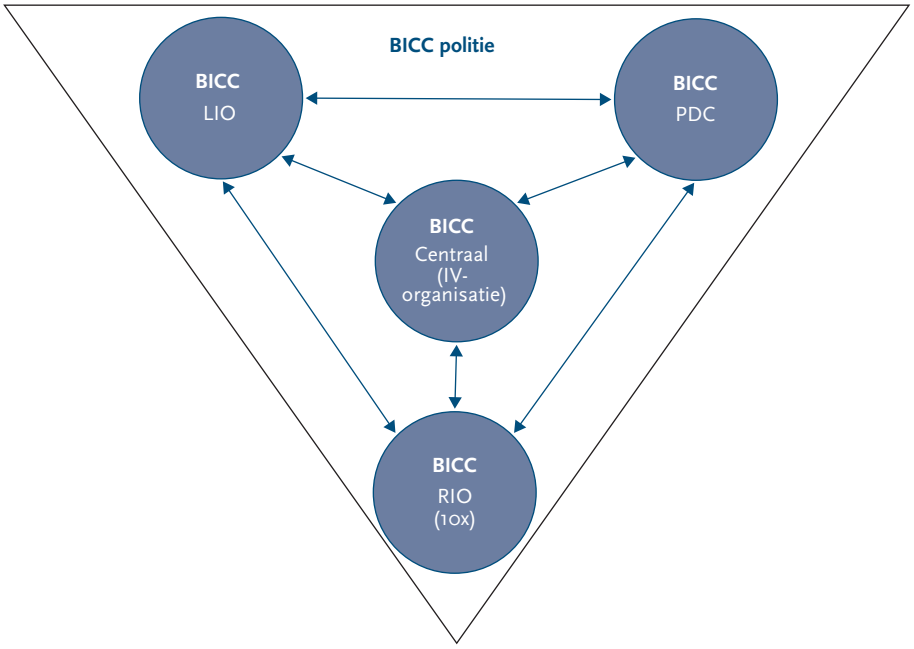
22.1 De rol van het BICC in het borgen van de business-intelligencestrategie van de politie

Zowel binnen als buiten de politie zijn data in overvloed voorhanden. De politie verzamelt, integreert en veredelt deze gegevens tot informatie voor alle politieprocessen. Vervolgens maken we de informatie analyseerbaar en presenteren en distribueren de informatie zodat collega's en andere afnemers deze kunnen gebruiken (zie hoofdstuk 2 Informatiegestuurd werken en business intelligence over de business-intelligencestrategie – BI).

Om de BI-strategie te borgen en te voorzien in de groeiende informatiebehoefte is in het *Ontwerpplan Nationale Politie* voorzien in een Business Intelligence Competency Center (BICC). Het BICC zorgt dat er diensten en informatieproducten zijn om informatievragen te kunnen beantwoorden. Het BICC ontwikkelt slimme, innovatieve toepassingen en het standaardiseert en automatiseert veelvoorkomende informatieverzoeken. Daartoe brengt het BICC verschillende competenties bij elkaar:

- *business*: politiemensen met relevante kennis van processen en prioriteiten. Zij weten wat er in het veld speelt en hebben daar de juiste contacten.
- *analyse*: analisten met verstand van en plezier in data, die het maximale uit de informatie halen.
- *technologie*: specialisten informatie- en communicatietechnologie (ICT) met kennis van BI-tools, methodieken en ontwikkelingen. Zij onderhouden de relatie met andere ICT'ers.

Het BICC van de nationale politie is een samenwerkingsverband van de decentrale BICC's van de Dienst Landelijke Informatieorganisatie (DLIO) en de Diensten Regionale Informatieorganisatie (DRIO's), het politiedienstencentrum (PDC) en de informatievoorzieningsorganisatie.



Figuur 22.1 BICC politie

In totaal bestaat het BICC van politie dus uit:

- tien decentrale teams bij de Dienst Regionale Informatieorganisatie binnen de regionale eenheden (gericht op informatie voor de eigen eenheid en nationale portefeuille zoals terreur of milieu);
- een decentraal team bij de Landelijke Eenheid (gericht op landelijke informatie en coördinatie, standaardisatie en integratie);
- een decentraal team bij het PDC (gericht op informatie voor bedrijfsvoering);
- centrale teams in de IV-organisatie (gericht op ontwikkeling en beheer van het BI-platform en de structurele ontsluiting van landelijke bronnen).

Samen zorgen zij dat in de toenemende vraag naar (verrijkte) informatie wordt voorzien.

22.2 De diensten en informatieproducten van het BICC

In de afgelopen jaren heeft het BICC van de politie mooie resultaten geboekt. Er zijn diensten en informatieproducten ontwikkeld voor:

- directe ondersteuning van de politiemedewerker op straat;
- ondersteuning van analyse en onderzoek;
- ondersteuning van de sturing van de operatie;
- informatie-uitwisseling met burgers, partners en internationaal.

22.2.1 Directe ondersteuning van de politiemedewerker op straat

Tot 2012 was informatie vooral regionaal beschikbaar. In de afgelopen jaren heeft het BICC een belangrijke rol gespeeld in het landelijk beschikbaar maken van data door mensen en technieken bij elkaar te brengen. De politiemedewerkers op straat kunnen nu landelijke data raadplegen. Concrete voorbeelden van applicaties met landelijke data zijn integrale bevraging (BasisVoorziening Informatie voor Integrale Bevraging – BVI-IB) en BlueSpot Monitor (BSM).

Figuur 22.2 Directe ondersteuning op straat

Integrale Bevraging

Integrale Bevraging (BVI-IB) was een bestaand product uit Amsterdam voor het doorzoeken van registers, dat is vernieuwd en landelijk ingevoerd. Sinds 2012 maakt de gehele politieorganisatie gebruik van BVI-IB. Het gebruik is de afgelopen drie jaar verdrievoudigd naar rond de vijftig miljoen bevragingen per jaar. BVI-IB haalt met een eenvoudig in te voeren zoekvraag (bijvoorbeeld een kenteken, locatie of persoon) real-time gegevens op uit twintig registers. BVI-IB voegt het resultaat van de bevraging van die (regionale en landelijke) registers samen en presenteert het als één geheel. Gebruikers kunnen BVI-IB op kantoor (de desktop) gebruiken of op straat (via Mobiel Effectiever Op Straat – MEOS), en BVI-IB is niet alleen beschikbaar voor gebruikers binnen de politie, maar ook bij externe partners.

BlueSpot Monitor

BSM is een gebiedsmonitor voor onder andere (wijk)agenten en analisten. BSM toont geografische incidentoverzichten op basis van actuele, landelijke data. Twintig minuten nadat informatie in de BasisVoorzieningen Handhaving (BVH) is ingevoerd staat deze al in de overzichten in BSM. BSM is ontwikkeld door het centrale BICC. Een succesfactor is de performance; door intensieve samenwerking tussen het BICC en de Dienst ICT/IM is het gelukt om de snelheid zo te verbeteren dat de BSM op 95 procent van de vragen binnen twee seconden een antwoord geeft.

22.2.2 Ondersteuning van analyse en onderzoek

De politie verzamelt in het kader van de handhavings- en opsporingstaken een enorme hoeveelheid data in diverse vormen: gestructureerd, tekst (processen-verbaal, tapverslagen) en ongestructureerd, zoals beeldmateriaal. De politie gebruikt deze gegevens primair voor de zaak waarvoor ze verzameld zijn. Maar mogelijk zit er ook nog onontdekte[1] informatie tussen waarmee andere, niet-gerelateerde zaken zijn op te lossen en misdaad wellicht is te voorkomen. Ook externe bronnen kunnen relevante, onontdekte informatie bevatten. Het BICC en de afdeling Analyse & Onderzoek van de informatieorganisatie werken steeds intensiever samen om goede informatie beschikbaar te krijgen voor:

- Analyse van bestaande zaken voor bijvoorbeeld:
  - inzicht in criminele netwerken;
  - identificatie van indicatoren (bijvoorbeeld aanwijzingen voor mensenhandel, opstellen voorspelmodel huiselijk geweld);
  - opsporing van nieuwe zaken (bijvoorbeeld aanwijzingen voor radicalisering en/of terroristische activiteiten);
  - identificatie van trends (bijvoorbeeld toename van een bepaald type autodiefstallen).
- Analyse van de vragen die aan de informatieverstrekkende systemen gesteld worden; deze kunnen duiden op een nieuwe trend.

Deze samenwerking heeft als meerwaarde dat de afdeling Analyse & Onderzoek zich echt kan richten op het analyseren van de informatie en niet meer extreem veel tijd kwijt is met het verzamelen en combineren van data.

Voorbeeld digitale opsporing: samenwerking Opsporing, BICC en Analyse & Onderzoek

In een groot onderzoek zijn meerdere grote databestanden in beslag genomen. Om inzicht te krijgen in de werkwijze van de verdachten, is het noodzakelijk deze zeer grote databestanden te duiden en in relatie met elkaar te brengen.

Nadat het verzoek voor ondersteuning van het opsporingsteam is binnengekomen bij de regionale informatieorganisatie, gaat een analist aan de slag met de concrete vraag. Al snel blijkt dat de databestanden te groot zijn om met de normale politiesystemen te analyseren. Daarom schakelt de analist de hulp in van het BICC.

Ook voor het lokale BICC zijn de bestanden te groot om zonder extra rekenkracht te kunnen koppelen. Daarom besluit het BICC het centrale BICC in te schakelen, dat beschikt over nog meer mogelijkheden. Het centrale BICC zorgt uiteindelijk door de inzet van nieuwe technologie voor het koppelen en visualiseren van de data. Daarna kan de analist verder, en is hij in staat inzicht te geven in de criminele activiteiten van de verdachten.

1 Onontdekt houdt in dat bij het verzamelen nog niet bekend was wat de waarde was van een verband.

22.2.3 Ondersteuning voor de sturing van de operatie

Voorbeeld Preselect Recidive: samenwerking onderzoekers, BICC en ZSM

Na uitgebreid onderzoek is het Preselect Recidive Model ontwikkeld om zo vroeg mogelijk herhalingsrisico van criminaliteit in te schatten bij jongeren (12 t/m 17 jaar). Preselect biedt inzicht in risico- en beschermende factoren en geeft handvatten voor behandeling. Preselect is niet meer weg te denken in het ZSM-proces, waar Openbaar Ministerie (OM), politie, reclasseringsorganisaties, Raad voor de Kinderbescherming en Slachtofferhulp Nederland intensief samenwerken. Het mooie aan dit voorbeeld is dat onderzoek, BI en toepassing in de praktijk samenkomen. Daarnaast is het gelukt op ketenniveau afspraken te maken over het delen van informatie.
De actualiteit van het model is drie uur en de bron is de BasisVoorziening Informatie (BVI).

Met BVI BlueSpot Report hebben de eenheden toegang tot rapportages over operationele thema's en managementinformatie voor de aansturing van de operatie. In 2015 hebben het AVP[2] en de decentrale BICC's in de eenheden in nauwe samenwerking bijna honderd landelijk gestandaardiseerde rapportages met landelijke informatie opgeleverd. Deze rapportages zijn te benaderen via het BlueSpot Report-portaal.

Het BICC PDC heeft bovendien bedrijfsvoeringsinformatie (zoals ziekteverzuim, formatie en bezetting) inzichtelijk gemaakt. De komende jaren wordt ingezet op het combineren van de bedrijfsvoeringsinformatie met operationele informatie, zodat we verder kunnen investeren in het doordacht inzetten van schaarse middelen bij de politie.

Voorbeeld: Verdachtenmonitor

Product	De Verdachtenmonitor geeft een totaaloverzicht van aangehouden arrestanten voor het ZSM-proces. Het geeft een overzicht van gegevens over deze arrestanten voor de betrokken ketenpartners buiten de politie en het OM. De ketenpartners hebben op basis van de verdachtenmonitor de mogelijkheid om proactief te handelen op basis van beschikbare gegevens.
Afnemers	ZSM-kamer, Jeugdcoördinator, Raad voor de Kinderbescherming, OM, Bureau Halt
Data	BVH, BOSZ

>>

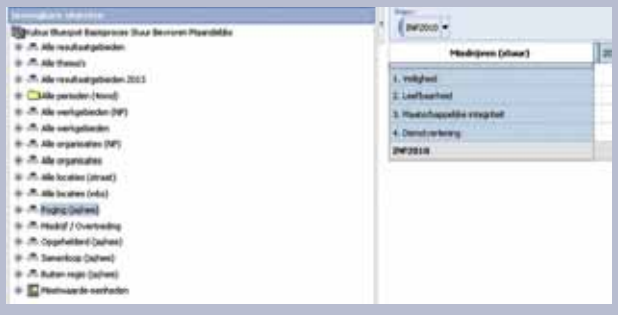
2 Het Aanvalsprogramma Informatievoorziening Politie (AVP) is vanaf 2011 ingezet om een belangrijke verbeterslag in de informatievoorziening van de politie door te voeren.

>> Actualiteit Real-time

Figuur 22.3 Verdachtenmonitor

Voorbeeld: Stuurkubus & Nationale Dashboard

Product	Op de Stuurkubus kunnen de eenheden zelf met behulp van de BVI zogenoemde views (een soort rapport) maken en deze aanbieden aan gebruikers. Hierin zijn ten behoeve van stuurinformatie gegevens verwerkt uit de bronsystemen BVH en Betere Opsporing door Sturing op Zaken (BOSZ), ingedeeld naar het zogenoemde Informatiemodel Politie. Dit zijn onder andere het aantal aangiften, incidenten, misdrijven, Halt-afdoeningen, verdachten- en slachtofferzaken. De Stuurkubus en het Nationale Dashboard maken het mogelijk cijfers van gebieden onderling te vergelijke en trends te zien.
Afnemers	Management, analisten, Centraal Bureau voor de Statistiek (CBS)
Data	BVH, BOSZ
Actualiteit	Dagelijks



Figuur 22.4 Stuurkubus

Voorbeeld: BOSZ-overzichten

Product	BOSZ verzorgt coördinatie voor de opsporing en de vervolging van misdrijven. Met BOSZ kunnen opsporing en vervolging van politie en OM van begin tot eind worden gevolgd. Het aanbod van 'zaken' is groter dan de politie en het OM kunnen oppakken. Met behulp van BOSZ kunnen keuzes worden gemaakt. De kubussen onderzoeksdossier van politie, verdachte politie en verdachte OM worden dagelijks bijgewerkt vanuit BOSZ. Hierdoor hebben de eenheden bij de politie en het parket bij het OM altijd een actueel landelijk en gemeenschappelijk overzicht van de status van onderzoeken en de daarbinnen genomen beslissingen. De rapportages zijn real-time beschikbaar voor onder andere de coördinatiepunten van de politie.
Afnemers	Operationeel Coördinatiepunt Politie, teamchefs, OM, Control
Data	BVH, BOSZ
Actualiteit	Real-time (rapportages), Cognos-kubussen (dagelijks)

22.2.4 Informatie-uitwisseling met burgers, partners en internationaal

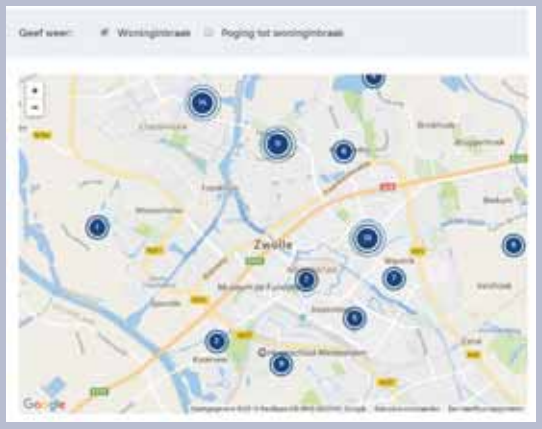
De politie roept voor preventie, handhaving en opsporing steeds vaker de hulp in van het publiek (burgers en private organisaties). Onderdeel hiervan is dat de politie ook transparanter is en informatie verstrekt over bijvoorbeeld misdaadcijfers. Het BICC heeft daarom informatieproducten ontwikkeld om data actief te delen. Een mooi voorbeeld is Misdaad in kaart op politie.nl, waar burgers zelf kunnen zien hoeveel inbraken in de wijk plaatsvinden om daar actie op te kunnen ondernemen. Ook stelt de politie steeds vaker open data op internet beschikbaar. Voorbeelden zijn:

- reactietijd prio1 landelijk en per eenheid;
- criminaliteit per gemeente;
- HRM-cijfers politie landelijk en per eenheid.

De politie is zich ervan bewust dat zij haar preventie- en opsporingstaak effectiever kan uitvoeren als ze samenwerkt met andere overheidspartijen, die elk hun eigen opsporings- en handhavingsinstrumenten hebben om een bijdrage te leveren (zie ook hoofdstuk 13 Informatiegestuurd werken en samenwerkingsrelaties). Dit betreft overheden op diverse niveaus, en zowel nationaal als internationaal. Samenwerking betekent ook steeds vaker afspraken maken over onderlinge data-uitwisseling. De politie ontvangt gegevens van externe partijen, maar stelt zelf ook gegevens beschikbaar. Deze uitwisseling kan op regelmatige, structurele basis plaatsvinden op een manier die tussen beide partijen afgestemd is. Voorbeelden zijn de aanlevering van data aan de Infobox Crimineel en Onverklaarbaar Vermogen (ICOV), de levering van aanrijdingsgegevens aan Stichting Processen Verbaal (SPV) en Rijkswaterstaat en uiteraard het CBS. Tot slot vindt er ook in internationaal verband data-uitwisseling plaats met onder andere Europol en Interpol.

Voorbeeld: Misdaad in kaart

Product	Op de website www.politie.nl is 'Misdaad in kaart' te raadplegen, hier worden woninginbraken op een kaart aan de burger getoond. Doel van Misdaad in kaart: – burgers betrekken bij de veiligheid in de eigen wijk; – burgers bewust maken van het belang van preventie. De BVI voorziet op dagelijkse basis Misdaad in kaart met actuele gegevens over deze woninginbraken uit alle eenheden.
Afnemers	Politie.nl, burgers
Data	BVH
Actualiteit	Dagelijks



Figuur 22.5 Misdaad in kaart

22.3 Hoe verder met business intelligence bij de politie?

Door de BI-strategie is de afgelopen jaren veel geïnvesteerd in het organiseren van mensen, het samenbrengen van politiedata en het delen van deze data met verschillende afnemers, zowel intern als extern. In de beginfase (2012) heeft de nadruk gelegen op technische ontsluiting van data en het aanbieden van rapportages aan eindgebruikers. De interactie met de eindgebruikers was daarbij beperkt.

In de afgelopen jaren zijn gebruikers een steeds prominentere rol gaan spelen bij de ontwikkeling van BI en heeft BI een strategische plek gekregen binnen de organisatie. Zo is geïnvesteerd in een landelijke dekkend BICC en in nieuwe technische infrastructuren. Is het BICC dan af? Nee, zeker niet, het is juist zaak om de BI-strategie krachtig door te zetten en verder te investeren in mensen en technologie. Voor de komende jaren zien we, naast de personele ontwikkeling, drie belangrijke inhoudelijke thema's:

- uitbreiden van het BICC-netwerk met nieuwe kennis en kunde over opsporing en ketensamenwerking;

- optimaliseren van het zoeken en vinden van informatie;
- verdere integratie van verschillende soorten data.

22.3.1 Uitbreiden BICC-netwerk

In de afgelopen jaren was er een sterke focus op informatie voor de processen noodhulp en handhaving. De eerste tekenen zijn dat het BICC al een enorme meerwaarde heeft voor opsporing. Dit vraagt om uitbreiding van de bestaande BICC's of om nieuwe BICC's, specifiek voor de opsporing.

Daarnaast ontwikkelt de keten (gemeenten, OM, jeugdzorg, veiligheidsregio's, internationale partners) zich ook verder op het BI-gebied. Samenwerking daarbij vraagt om BICC-medewerkers die de taal spreken van deze partners en de juridische kennis hebben op het gebied van het delen van data. Ook dit vraagt om uitbreiding van de bestaande BICC's of om nieuwe BICC's, specifiek voor de samenwerking met ketenpartners.

22.3.2 Optimaliseren van het zoeken en vinden van informatie

De politie heeft op dit moment verschillende zoekmachines om informatie te vinden, voorbeelden zijn BlueSpot Report, BSM, BlueView en BasisVoorziening Informatie voor Integrale Bevraging (BVI-IB). De komende jaren staan in het teken van het samenbrengen van de verschillende zoekalgoritmes. Hierdoor ontstaat meer eenduidigheid voor de eindgebruiker. Deze zoekalgoritmes zijn dan ook goed te gebruiken bij het invoeren van gegevens, zodat de datakwaliteit omhooggaat.

22.3.3 Verdere integratie van verschillende soorten data

De politie voelt de noodzaak om, uiteraard binnen de kaders van de wet, versneld standaardisatie van data door te voeren, zodat iedereen toegang krijgt tot de informatie die voor de rol noodzakelijk is (zie ook hoofdstuk 6 Autorisatiemodel politie). Deze standaardisatie zorgt ervoor dat de politie veel sneller kan leren. Teams moeten kunnen rekenen op juiste, tijdige en volledige informatie om zo efficiënt mogelijk te kunnen werken. Nu zijn er nog te veel belemmeringen, met name op het gebied van opsporingsdata, internetdata, internationale data en data van partners. Door deze standaardisatie van data blijft de politie ook in het digitale tijdperk lokaal verankerd en (inter)nationaal verbonden.

23 In gesprek met Ruud Staijen over informatievoorziening

Figuur 23.1 Ruud Staijen

Een gesprek met de programmamanager Operationele voorzieningen binnen het Aanvalsprogramma Informatievoorziening Politie (AVP). Over verleden, heden en toekomst. En over hoe alles samenhangt. 'Ik zou de collega's direct willen aanspreken: het gaat echt om de laatste meter!'

'Reis met me mee, tien jaar terug in de tijd. Jelle Kuiper nam mij van Amsterdam mee naar Arnhem. In mijn bagage: het IGP[1]-gedachtegoed en een brok ervaring in de informatiehoek en het politiewerk. Dat zou in het Arnhemse goed van pas komen...

Groot was dan ook mijn teleurstelling toen ik aan den lijve ondervond dat we in Gelderland-Midden het gereedschap ontbeerden om echt informatiegestuurd politiewerk te leveren... Een districtschef die meters achter de muziek aan loopt, zo voelde ik mij. Niet dat de collega's op straat en bij de recherche nou aan de voorkant liepen, die hadden dezelfde problemen. Gelukkig wel een topteam waarin iedereen zijn stinkende best deed met de middelen die hij had.

En toen kwam er een onverwachte kans: eind 2011 ging het Aanvalsprogramma Informatievoorziening Politie van start! Het AVP. Men zocht hulp van politiemensen. Die kans greep ik met beide handen aan. Helpen het gereedschap te verbeteren waarmee wij politiemensen ons werk doen. Ik zag mijn kans schoon. Geen idee waarin ik zou belanden...'

En, wat trof je aan?

'Omdat ik bij vier korpsen gewerkt had, dacht ik wel zo'n beetje te weten hoe het applicatielandschap van de politie in elkaar stak. Decennialang had ik in Groningen, bij het korps landelijke politiediensten en het Korps Amsterdam-Amstelland met menig andere collega aan verschillende informatievoorzieningen mogen bouwen. Daar waren we trots op. En

1 Informatiegestuurd politiewerk.

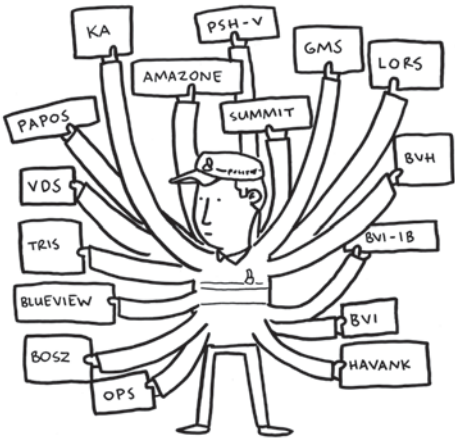
zeker, dat heeft tóén geleid tot meer veiligheid. Al wist ik ook wel dat het landelijke applicatielandschap er niet overzichtelijker van was geworden.

Maar hoe dat landschap er écht bij lag, merkte ik pas goed aan het begin van het AVP. Honderden, nee duizenden systemen... en dan heb ik het alleen over wat er bekend was, hè. Niet over wat er daarna nog aan applicaties en koppelingen uit de kast is komen vallen...'

Lekker werken als politieman of -vrouw...

'Deed je als wijkagent, rechercheur of analist je werk, dan stond er een onverzadigbaar IV[2]-monster tegenover je dat steeds vroeg om opnieuw in te voeren. Politiemedewerkers moesten dagelijks hun werk verantwoorden in tientallen systemen. Voor elk probleem hadden we wel een systeem! En waren de gegevens eindelijk ingevoerd, zag ze er dan nog maar eens uit te krijgen. En liefst zo dat je er ook nog een beetje soep van kon koken. Daar draait het toch om bij informatiegestuurd werken? Regionaal ging het nog wel, landelijk was het een ramp. Vraag een willekeurige analist naar zijn werk van toen, en hij begint over eindeloos zoeken en bij elkaar brengen van data. Het grootste deel van de dag ging er aan op. Natuurlijk lijdt de kwaliteit van de data eronder, als je keer op keer moet invoeren.

De bikkelharde realiteit was wel dat op die manier puzzelstukjes van onopgeloste zaken bleven liggen. Veel informatie van de regionale politiekorpsen was bovendien niet eens landelijk beschikbaar en doorzoekbaar. Dat verhoogde de kans op fouten; het was gebruikersonvriendelijk en uiteindelijk ging het ten koste van het boeven vangen.



Figuur 23.2 GMS, BVH, Summ-IT, AMAZONE, TRIS, PAPOS, OPS

Kortom: gebruiksgemak nul, overlappend en zelden actueel. En een beheerslast! Meer dan 90 procent van het budget ging op aan dat boeltje in de lucht houden. "Beperkte ruimte voor innovatie", heette dat dan. Frustratie en polarisatie tussen het IV-bedrijf en het blauw waren het gevolg.'

2 Informatievoorziening.

Figuur 23.3 Gebruiksgemak

Dit soort fasen hoort bij een organisatie die volwassen wordt, zegt de literatuur.

'Banken, verzekeraars en multinationals maken dit soort groeistuipen door. Dus ook de politie... Ja, dat is mooi gezegd, maar in een organisatie van 65.000 mensen waar informatie- en communicatietechnologie (ICT) letterlijk van levensbelang is, kun je nu net geen groeistuipen gebruiken. De dag dat de IV in Noordoost-Nederland uitviel, staat velen van ons nog helder voor de geest. Vernieuwingen duurden te lang, waren niet meer betaalbaar en de stabiliteit kwam in het gedrang. Alles wordt dan te complex.

Gelukkig waren er ook oppeppende geluiden die een betere toekomst voor de politie als geheel voorspelden als de IV van de politie volwassen zou worden. Juist om die volwassenheid te bewerkstelligen, om te stabiliseren, te verbeteren en te vernieuwen, werd het AVP in het leven geroepen.

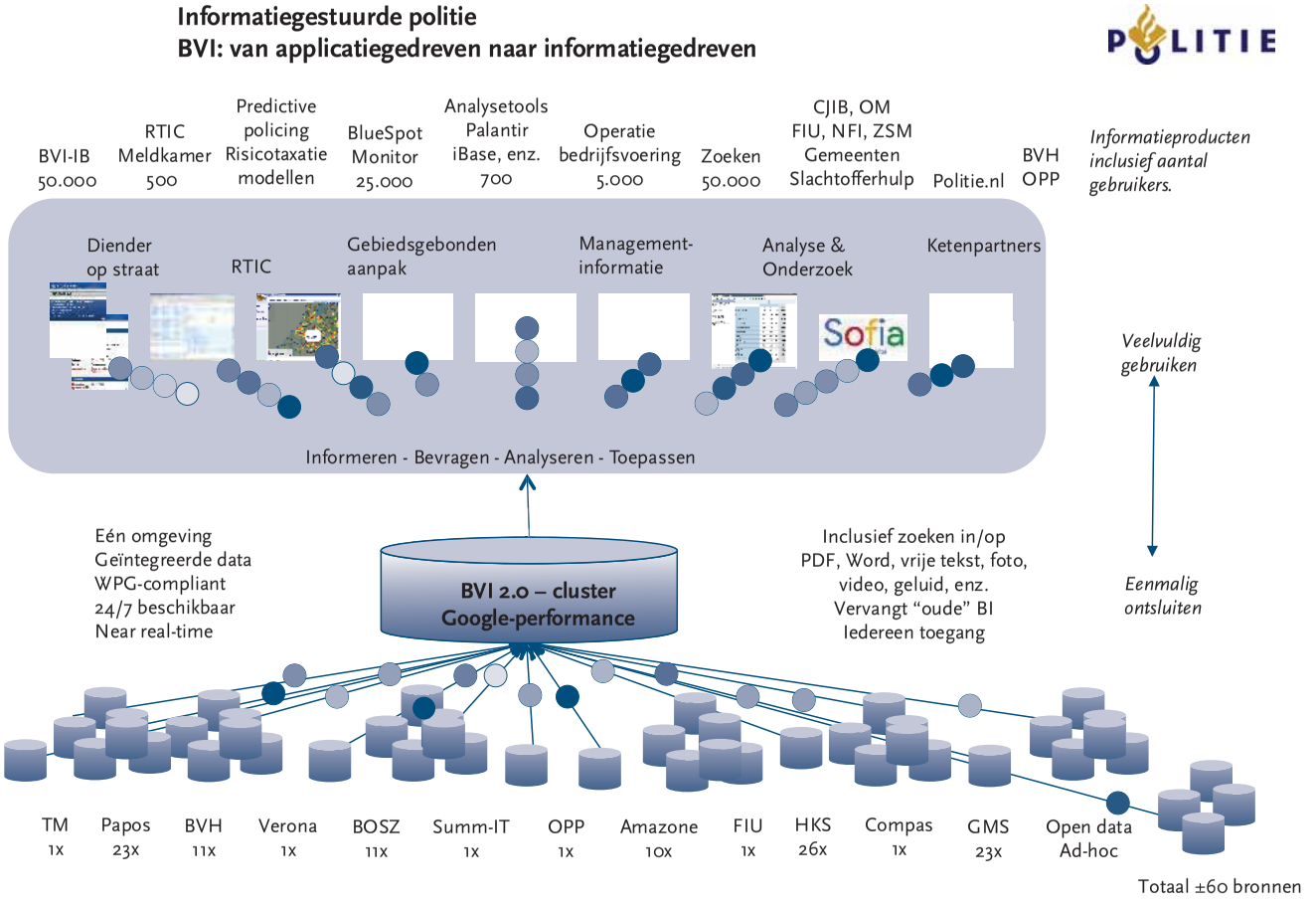
Kamerstukken zijn onze getuigen: we kregen een paar honderd miljoen om dat voor elkaar te krijgen. Het roer moest om. Dat begon met het ontwarren van de infrastructuurspaghetti en het indikken van het applicatielandschap. Stabiliteit draait om het borgen van de continuïteit, wegwerken van achterstallig onderhoud, veiligstellen van beheer en het leveren van 24/7 ICT-dienstverlening. In politietaal: dat ding moet het doen!

Sindsdien zijn er "onder de motorkap" nieuwe technieken toegepast, waardoor kernapplicaties als de BasisVoorziening Handhaving (BVH) en de BasisVoorziening Informatie voor Integrale Bevraging (BVI-IB) nu veel stabieler zijn.'

Licht aan de horizon, dus?

'Zeker, en er is méér gebeurd. Van 25 opsporingsapplicaties zijn we naar één verbeterd Summ-IT gegaan, van 23 regionale sporenapplicaties naar één landelijke voorziening, en we werken inmiddels met een landelijke locatieserver met geo-bestanden. Er is nog maar één echte operationele zoekmachine: BVI-IB. Die wordt maar liefst 50 miljoen keer per jaar bevraagd. En zo zijn er tientallen voorbeelden.

Je kunt alleen vooruit als je eerst opruimt, wordt wel gezegd. En oude applicaties uitzetten is moeilijker dan nieuwe aanzetten, heb ik geleerd. Veel dure systemen zijn de afgelopen jaren uitgezet om ruimte te maken voor nieuwe ontwikkelingen en om het



Figuur 23.4 Informatiegedreven

werkbaar te maken voor de collega's. Even een rijtje noemen? HKS, VPS, CVI, LIST, BLUE INFO, BINK, IB, MIB, P-INFO, GIDS, RIVS, LORS, PAPOS, BVO enzovoort, enzovoort. Ik hoorde eerder vandaag op de radio een liedje van Thé Lau met The Scene: "Waar zijn de helden, wat is een heldendaad." Nou, wat mij betreft onder andere op dat vlak: kanjers die niet altijd zichtbaar zijn, "stille" helden.

Mijn gedachten dwalen bijvoorbeeld af naar Tristan Da Cunha, de man die met zijn team LIST (landelijk informatiesysteem) na twintig jaar wist uit te zetten zonder dat het werk eronder leed, zich eindeloos vastbijtend in de problematiek. Je wilt niet weten hoeveel andere organisaties aan LIST vast bleken te zitten en voor hun werk daarvan afhankelijk waren. Daar moesten allemaal nieuwe oplossingen voor gezocht worden.

Die helden maakten en maken ruimte voor verbetering. Van 1800 systemen bij aanvang van het programma zijn we nu terug naar zo'n 400, een knappe prestatie. Dat vraagt wat van het hele bedrijf. Lang niet iedereen ziet wat er allemaal nodig is om het informatiegestuurd werken een stap verder te brengen, naar echt informatiegestuurd politiewerk. Het was en is hard werken, maar het kon ook niet meer. Negentien registers doorzoeken voor één boete omdat we evenzovele Parket politiesystemen (PAPOS'en) hebben, is niet werkbaar. En onbetaalbaar.'

Tijd om het verleden te laten rusten en ons te richten op wat er nu mogelijk is

'Jazeker! Op drie nieuwe voorzieningen krijgen blauw en grijs in hoog tempo nieuwe operationele toepassingen voorgeschoteld. Eén vraag stellen en via BVI-IB direct antwoord krijgen uit vele applicaties maakt het voor gebruikers een stuk plezieriger. Even op een kaartje zien wat we als politie allemaal weten: BVI-BSM maakt verbanden snel inzichtelijk. We kunnen ook data uit systemen combineren in een monitor of rapport dat risico's signaleert met BlueSpot Report en de risicotaxatie-instrumenten. Zo wordt het vinden van puzzelstukjes veel makkelijker. Ook zoekmachine Sofia draagt hieraan bij. In het programma AVP is hiervoor een prototype ontwikkeld. Onder de naam BlueView 4.0 ontwikkelt het IV-bedrijf van de politie ook deze voorziening met veel elan verder...

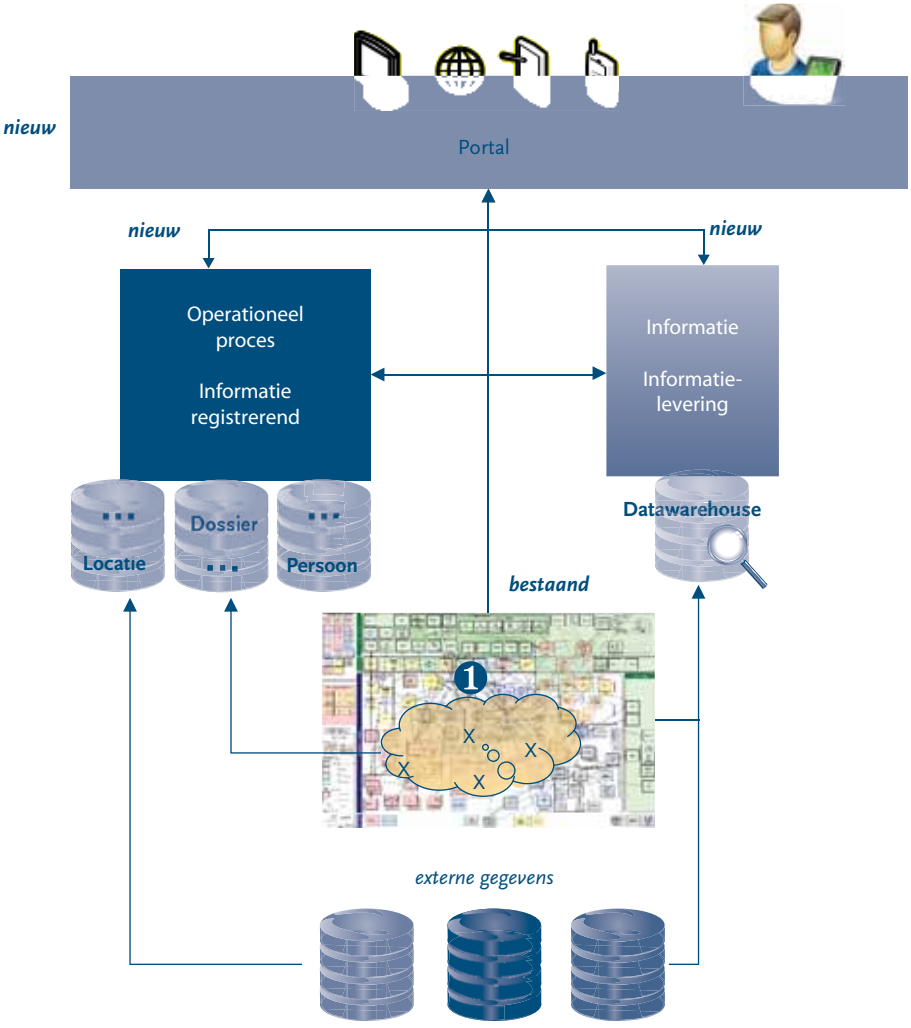
En zo komt IGP stukje bij beetje dichterbij. Als districtschef, als politieman zou ik vijf jaar geleden blij geweest zijn als een klein kind als ik dit allemaal tot mijn beschikking had gekregen. En het smaakt naar meer!'

Je komt op stoom...

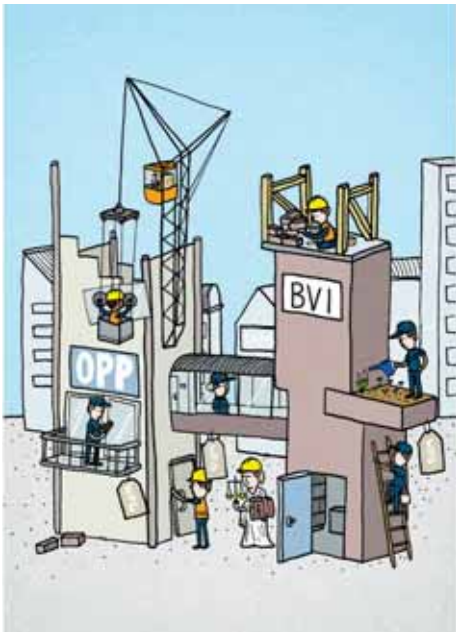
'(Lacht) Ik begin net! Ook aan registreren is gedacht. De opsporingsambtenaar heeft nieuwe voorzieningen die gebruikmaken van data van derden en van de BVI. Nieuwe straatnamen hoeven niet meer in de tabellen van elke applicatie ingevoerd te worden door beheerders. Er is een locatieserver die bij zeventien andere overheidsinstellingen de geodata geautomatiseerd ophaalt. Dat scheelt veel typen en veel fouten. Delen van informatie en kennis maakt ons steeds effectiever. De landelijk gestandaardiseerde en geharmoniseerde e-Briefingsvoorziening is een flinke stap vooruit. En de data komen uit de BVI. Ook dat scheelt typen. Ook de nieuwe functionaliteit Executie & Signalering (E&S) is in heel Nederland operationeel. En de data komen geautomatiseerd van het Centraal Justitieel

Incassobureau (CJIB). De mazen in het net van de opsporing worden kleiner... Informatie delen en onderling communiceren hebben een stap vooruitgezet met wat we bij de politie AGORA noemen. Honderden teams, afdelingen en projecten gebruiken het, terwijl de introductie amper een jaar geleden was.

Briefing, E&S en AGORA versterken elkaar. Bovendien worden ze steeds vaker ook mobiel aangeboden. Als gebruiker heb je bij de politie de afgelopen jaren dus behoorlijk wat veranderingen meemaakt en we zijn er nog niet. Misschien gebeurt het nog dat we klachten krijgen dat we te snel innoveren...'



Figuur 23.5 AGORA, OPP en BVI



Figuur 23.6 BVI, OPP en Wpg

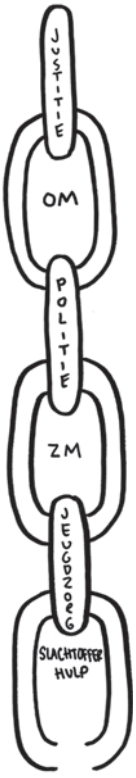
Hoe zorg je dat de collega's bijblijven met al die goede, maar razendsnelle veranderingen?
'Dat is een heel belangrijk punt. Het heeft geen zin om dure ICT te implementeren als de gebruikers niet weten dat het er is en hoe ze er optimaal gebruik van kunnen maken. Pas wanneer politiemensen het door hen zelf mede-ontwikkelde gereedschap gebruiken en het wérkt, zal het politiewerk beter worden en buiten veiliger. Uit een dertiental evaluaties van nieuw IV-gereedschap weten we dat politiemensen van politiemensen leren en niet van e-mail of publicaties. We weten inmiddels ook dat je echt niet al die collega's in de klas krijgt, zoals wij bij Summ-IT nog probeerden. Steeds meer zijn we gaan werken met filmpjes, met korte demosessies, train-de-trainer-aanpak, en goed laten zien wat de principes zijn die in alle systemen terugkomen.

Toch duurt het wel een jaar of twee à drie voordat voorzieningen zoals BlueSpot Monitor, e-Briefing, operationeel politieproces (OPP) en E&S zijn geland. De gebruikersinbreng aan de voorzijde bij de ontwikkeling, en aan de achterzijde bij het in gebruik nemen, heeft ruim baan gekregen en helpt om dit te versnellen. Het AVP is een groots en complex programma gebleken, maar de organisatie waarbinnen het moet vallen, is altijd groter. Het kan dus alleen samen met het veld, met andere programma's, met collega's die heel Nederland door rijden om hun kennis te delen. Ook dit zijn helden hoor, die werken aan veiligheid. De verandering is met andere woorden veel omvangrijker dan enkel de ICT. Het gaat om mensen en de manier waarop ze werken. We hebben in het programma dan ook bewust geprobeerd dat te ondersteunen met warme en beeldende communicatievormen waarin veel collega's hebben geacteerd.'

En als je een blik op de toekomst werpt?

'Opsporingswerk draait om informatie en het nemen van beslissingen. We hebben nu drie nieuwe platformen: OPP om te registeren, BVI om data te delen en om te zetten naar informatieproducten en AGORA als communicatieportal. Het programma mobiel werken zal bovendien ervoor zorgen dat niet meer alles op een politiebureau hoeft te worden gedaan. De informatie die je nodig hebt, in het juiste format, op de juiste plaats, en dan goede beslissingen nemen. Dat is IGP. Dat geldt voor de wijkagent, de noodhulp, de meldkamer, de rechercheur, de teamchef enzovoort. Het nieuwe gereedschap verder uitbouwen en gebruiken waar het voor is. Dan maken we de IV van de politie betaalbaar en een stuk gebruikersvriendelijker. Tegelijkertijd wordt Nederland er een stuk veiliger van.

En wie weet: misschien bieden deze ontwikkelingen ook kansen voor de collega's bij de bijzondere opsporingsdiensten (BOD'en) en andere partners? Je kunt en we willen er onze ogen niet voor sluiten: de politie werkt steeds meer samen met andere maatschappelijke organisaties, in en buiten de veiligheidsketen. Informatie speelt hierbij een cruciale rol, want samenwerken betekent: informatie delen. Van mij mag IGP best een beetje organisatiegrensoverschrijdend zijn, dat zou de integrale aanpak ten goede komen. Een moderne, goed functionerende intelligenceomgeving is dan cruciaal. En natuurlijk betekent dat kiezen en worstelen met de schaarse middelen. Maar ook hier geldt dat "samen" meer oplevert dan de som der delen.'



Figuur 23-7 Keten

Wat heb je nou geleerd de afgelopen jaren en wat zou je graag zou willen overdragen van die kennis en ervaring?

'De samenhang tussen horizontale verbanden in verticale structuren: op hoofdlijnen is het de kunst dát te organiseren. Je kunt niet over ICT praten zonder dat je weet hoe het werk in elkaar zit en wat de mensen beweegt. Het omgekeerde is ook waar: je kunt niet over verbeteren van het werk praten met inzet van ICT zonder dat je daarbij kennis hebt van de problemen van het ICT-bedrijf. En dat gaat vaak niet alleen over de inhoud: we hebben nog wel te maken met stammenstrijden tussen bloedgroepen, applicaties, technieken, eenheden en werkwijzen.

Verandering of verbetering in één big bang kan dan ook helemaal niet, stapsgewijs samen leren is het enige wat werkt. En omdat veel dingen samenhangen, moeten we dondersgoed weten aan welke touwtjes we trekken en wat het gevolg is. Het helpt om het probleem van onze vroegere eilandautomatisering goed te doorgronden en te doorleven. Weten wat een en ander zal betekenen voor het politiewerk, en dán overtuigd strategie kiezen en die consequent vasthouden, is vervolgens erg belangrijk. Lastig bij de politie, want van nature zijn we nu eenmaal incidentgedreven. En natuurlijk is het dubbel lastig als je in een reorganisatie zit die veel langer duurt dan verwacht en als nieuwe leiders het proces opnieuw moeten doorleven.

Warme communicatie en een programmatische aanpak is ook een rode draad. We kunnen naar mijn mening pas echt vooruit als

we weten hoe we willen werken. Die werkprocessen standaardiseren en harmoniseren maakt het mogelijk om goede informatievoorziening voor de collega's te creëren en die betaalbaar te maken. Dat doe je samen. In de ontwerpfase, in de realisatie, maar bovenal in de implementatie.

Tot slot, en dat komt echt uit mijn hart en ik zou de collega's daarop ook direct willen aanspreken: dertien evaluatieonderzoeken van recent geïmplementeerde nieuwe IV wijzen het uit – het gaat echt om de laatste meter! Investeer daarin, anders maken we mooie en dure IV en niemand weet wat je ermee kunt of moet. Segmentatie en formele benaderingen werken niet. Integrale teams dicht bij de gebruiker, mensen die mensen inspireren, dan gaat het allemaal een stuk sneller. Overzie en doorgrond de samenhang. Wees koersvast en ga door, ook bij tegenwind. En redeneer bij alles wat je doet vanuit de burger en de politiemedewerker: wordt Nederland hier veiliger van? Want dat is uiteindelijk voor ons allemaal – of we nu in een programma werken, in de staande organisatie of in de ICT – het doel.'

Figuur 23.8 Signalering en executie

24 Informatiemaatschappij

Christiaan van den Berg, Hans van Vliet en Stephan den Hengst, met medewerking van Erik Fledderus (directeur SURF)

'We leven niet in een tijdperk van verandering, maar in een verandering van tijdperk.'[1]

De politie staat midden in de maatschappij en de wereld om ons heen verandert snel. Ontwikkelingen in onder meer sociale media, internettechnologie en platformen leiden tot nieuwe diensten en resulteren in andere manieren van samenwerken, en versnellen daarmee ook maatschappelijke veranderingen. In het tweede decennium van de eenentwintigste eeuw kunnen we stellen dat we ons volop in de informatiemaatschappij bevinden.

Digital natives (mensen die opgegroeid zijn in het internettijdperk) signaleren bijvoorbeeld verdacht gedrag op straat via Snapchat en Instagram. Bellen met 112 is voor hen niet vanzelfsprekend. En de verdachten van de MH17-crash werden na een paar maanden door een groep internationaal samenwerkende individuen van het onderzoeksplatform Bellingcat aangewezen. Criminaliteit verschuift ook naar de onlinewereld: mensen worden steeds vaker online opgelicht, bijvoorbeeld met een nepadvertentie op een gehackt Marktplaatsaccount. Dat gehackte account is met bitcoins gekocht op een handelsplatform op het *darkweb*.

De politie moet meebewegen met de ontwikkelingen in de maatschappij. Dat is op zich geen nieuwe opgave. Maar veranderingen gaan in de informatiemaatschappij sneller dan ooit. Daarom moet de politie ook het vermogen hebben om versneld te veranderen om effectief te kunnen zijn en haar relevantie en legitimiteit te behouden.

In dit hoofdstuk presenteren we een aantal belangrijke maatschappelijke, organisatorische en technologische trends om de actuele veranderingen te duiden.[2, 3] Vervolgens gaan we in op consequenties en handelingsperspectief voor de politie: hoe hiermee om te gaan?

1 Rotmans, J. et al., *Verandering van tijdperk*. Aeneas, 's-Hertogenbosch 2014.

2 TNO, *RTI-radar*. TNO-rapport; rapportnummer: TNO 2016, R10354 (14 maart 2016). TNO, Delft 2016.

3 Bussel, G.J. van et al. (red.), *De informatiemaatschappij van 2023: perspectieven op de nabije toekomst*. GEA Consultancy/Lectoraat Digital Archiving & Compliance Hogeschool van Amsterdam, Amsterdam 2013.

24.1 Trends: hoe verandert de wereld? Wat zijn de grote bewegingen?[4]

24.1.1 Maatschappelijke trends informatiemaatschappij

Snelle veranderingen in een genetwerkte maatschappij

De informatiemaatschappij kenmerkt zich door snelle veranderingen, zowel op technologisch als sociaal-maatschappelijk en economisch gebied. Informatie is de ruggengraat van onze economie en samenleving geworden en is de basis voor grote veranderingen in de maatschappelijke sectoren, zoals gezondheid, energie, onderwijs, industrie, leefomgeving en veiligheid. De informatiemaatschappij heeft de drempel om te innoveren en nieuwe bedrijvigheid te ontwikkelen verlaagd, maar heeft tevens als effect dat de samenleving en het bedrijfsleven steeds meer afhankelijk worden van informatie- en communicatietechnologie en door die verwevenheid mogelijk ook kwetsbaarder worden. Nieuwe rollen ontstaan en nieuwe vaardigheden zijn nodig vanwege de steeds verder toenemende complexiteit van slimme en genetwerkte systemen.

Data zijn in toenemende mate in grote hoeveelheden aanwezig. Informatie uit data krijgt economische en maatschappelijke waarde en wordt een te verhandelen goed. Zo kan Google waardevolle kennis over verkeersstromen destilleren uit de locatie-informatie van smartphones met Google-navigatie. Deze kennis is geld waard, bijvoorbeeld voor gemeenten en verzekeringsmaatschappijen. In alle sectoren in de maatschappij groeien de genetwerkte informatiestromen verder en worden deze steeds belangrijker. Onze economie transformeert zich tot een genetwerkte informatie-economie[5], waarin (technologische) systemen steeds meer met elkaar samenhangen.[6]

Informatie steeds belangrijker

Informatie en het delen van informatie staan steeds meer centraal in de samenleving. Dit is al helemaal het geval bij de jongere generaties (generaties Y en Z). Toegang tot informatie is voor iedereen gemakkelijker geworden. Wie gebruikt er niet Buienradar voor realtime informatie over het weer, en openbaar-vervoersreisinformatie? De manieren en vormen waarop we informatie uitwisselen zijn in verscheidenheid toegenomen. Nieuwe vormen van sociale media maken dat we veel meer foto's delen dan dat we nog berichten typen of bellen: een razendsnelle verschuiving van spraak via tekst naar beeld.

Ook bedrijven en overheidsorganisaties stellen informatie steeds meer centraal. Aan de ene kant om hun klanten betere producten en betere dienstverlening te leveren, zoals

---

4 Paragraaf 24.1 Trends: hoe verandert de wereld? Wat zijn de grote bewegingen? is gebaseerd op: TNO, *RTI-radar*. TNO-rapport; rapportnummer: TNO 2016, R10354 (14 maart 2016). TNO, Delft 2016, en Bussel, G.J. van et al. (red.), *De informatiemaatschappij van 2023: perspectieven op de nabije toekomst*. GEA Consultancy/Lectoraat Digital Archiving & Compliance Hogeschool van Amsterdam, Amsterdam 2013.

5 TNO, *Speurwerkprogramma 2015-2018: thema ICT*. TNO-rapport, rapportnummer: 0100109731 (26 september 2014). TNO, Delft 2014.

6 Raad voor de leefomgeving en infrastructuur, *Verkenning technologische innovaties in de leefomgeving*. Raad voor de leefomgeving en infrastructuur, Den Haag 2015.

KLM bijvoorbeeld aan *webcare* doet via Twitter. Aan de andere kant om de interne processen efficiënter en effectiever te laten verlopen en de flexibiliteit van de organisatie te vergroten, zoals dat bijvoorbeeld gebeurt bij de grotendeels automatische distributiecentra van internetwarenhuizen en pakketbezorgers. Ook de politie maakt deze beweging, via hitlijsten en automatic number plate recognition (ANPR) worden bijvoorbeeld selectief voertuigen staande gehouden waar een hit op is.

Alles met elkaar verbonden

De informatiemaatschappij is een netwerkmaatschappij geworden (*connected world*). Via sociale media en andere communicatiekanalen en netwerken is alles en iedereen in toenemende mate met elkaar verbonden. Het *Internet of Things* verbindt de hele aardbol en alle dingen erop. Interactieve netwerken vervangen traditionele hiërarchische structuren. Steeds meer kennis van over de hele wereld komt online beschikbaar. Het is daarmee eenvoudiger geworden om grote groepen mensen te betrekken om bijvoorbeeld het waarnemend vermogen te vergroten (crowdsourcing).

Voor het veiligheidsveld zien we dat berichten op sociale media worden gevolgd en geanalyseerd om een beter beeld te krijgen van een incident. Daarnaast zijn er steeds meer applicaties die het politie en burgers mogelijk maken samen te werken rond het thema veiligheid. De netwerkmaatschappij vergroot de mogelijkheden tot burger- dan wel politieparticipatie.

> 'Als gevolg van het gemak waarmee informatie samengebracht, vergaard en gebruikt kan worden, wordt het speelveld van aloude professies opnieuw gestructureerd. Met soms pijnlijke confrontaties tussen de gevestigde kenniscentra en de nieuwe kennis van de massa. (...) De professionals merken dat hun zienswijzen in het digitale tijdperk in het beste geval naast die van evenzoveel andere opvattingen staan die op internet circuleren.'[7]

Groepsvorming én individualisering

Sociale media ondersteunen het vormen van groepen met gemeenschappelijke interesses of belangen (*community building*). Een voorbeeld zijn het gebruik van WhatsApp-, Telegram- en Facebookgroepen van bewoners in een wijk voor buurtpreventie. Rond specifieke onderwerpen of belangen kan men zich gemakkelijk verenigen.

Aan de andere kant wordt juist individualisering verder versterkt door informatisering. Groepen of personen hebben ieder hun eigen informatievoorziening. We kunnen daardoor steeds meer in onze eigen informatiebubbel terechtkomen, met informatie die is gefilterd volgens onze eigen voorkeuren. Verdere individualisering en personalisatie van diensten en informatie gebeuren in toenemende mate op basis van die persoonlijke voorkeuren, opgeslagen in profielen. Daarmee stellen bijvoorbeeld diensten als Google, Facebook en Netflix ons steeds minder bloot aan andersdenkenden of compleet nieuwe perspectieven.

7 Bussel, G.J. van et al. (red.), De *informatiemaatschappij van 2023: perspectieven op de nabije toekomst*. GEA Consultancy/Lectoraat Digital Archiving & Compliance Hogeschool van Amsterdam, Amsterdam 2013.

Globale en directe informatie-uitwisseling

De informatisering versterkt globalisering: informatie kan vrijwel direct overal ter wereld zijn. Niet alleen het geografische bereik is vrijwel onbeperkt; het verspreiden van informatie gaat ook nog eens razendsnel. Direct wanneer er ergens iets is gebeurd, wordt dit geregistreerd door mensen met hun smartphones, action cameras, dashcams of andere apparatuur. Via sociale media, maar ook direct via nieuwssites wordt de informatie gedeeld. Diverse toepassingen bieden naast het uitwisselen van tekst, beeld en filmpjes ook de mogelijkheid tot live streaming van beelden. Steeds vaker zien we incidenten die live gefilmd en gedeeld worden via bijvoorbeeld Periscope, nog voor de hulpdiensten zijn gearriveerd.

Verwevenheid fysieke en virtuele wereld

De fysieke en de virtuele digitale wereld zijn steeds meer met elkaar gekoppeld en vervlochten. Logistieke processen in de fysieke wereld worden gemonitord en aangestuurd vanuit gedigitaliseerde systemen met steeds minder menselijke bemoeienis. Netwerken en energienetwerken worden in toenemende mate slimme netwerken (*smart grids*). Deze hyperconnectiviteit, waarbij van alles met van alles is verbonden, heeft aan de ene kant potentiële kwetsbaarheid tot gevolg: wanneer een computersysteem of communicatienetwerk uitvalt, kunnen bijvoorbeeld de treinen niet meer rijden. Aan de andere kant biedt de vervlechting van de fysieke en de virtuele wereld vele nieuwe mogelijkheden tot optimalisatie en innovatie, zoals slimme steden (zie paragraaf 24.1.3 Technologische trends informatiemaatschappij).

Voor het veiligheidsvraagstuk betekent de verwevenheid het toevoegen van een geheel nieuwe dimensie. De kwetsbaarheden die de connectiviteit met zich meebrengt, kunnen evengoed misbruikt worden: een aanslag op een politicus kan bijvoorbeeld digitaal plaatsvinden via de slimme interface van zijn pacemaker (zoals we in *House of Cards* al konden zien).

Aandacht voor privacyaspecten

Privacyvraagstukken vormen een belangrijk onderwerp in de informatiemaatschappij. De informatisering heeft het mogelijk gemaakt persoonlijke informatie op te slaan en te volgen. Dat is handig voor gepersonaliseerde dienstverlening. Indien oneigenlijk gebruikt, vormen deze mogelijkheden echter al snel een inbreuk op onze privacy. Hierbij speelt eveneens de vermenging van de fysieke en virtuele wereld. Onze bewegingen en activiteiten in de fysieke wereld laten in toenemende mate sporen achter in de virtuele wereld. Waar wettelijke en ethische grenzen zouden moeten liggen, is momenteel onderwerp van maatschappelijk debat. Bijvoorbeeld rond bevoegdheden van inlichtingen- en veiligheidsdiensten, maar ook rond de Belastingdienst met betrekking tot het verzamelen van persoonsgegevens.

24.1.2 Organisatorische trends informatiemaatschappij

Nieuwe manier van interactie en de-institutionalisering

De informatisering leidt niet alleen tot een andere interactie tussen klanten en bedrijven en tussen burgers en overheid, maar ook tot een andere manier van zakendoen.

Informatieplatformen kunnen een disruptief effect hebben op bestaande instituties. Zo hebben nieuwe spelers als Booking.com en Airbnb een disruptief effect op traditionele wijzen van het aanbieden van hotelkamers. In de taxibranche (Uber) of financiering van bedrijven (Kickstarter) verschijnen nieuwe spelers die de gevestigde orde uitdagen.

Op het gebied van veiligheid is een goede informatiepositie niet langer voorbehouden aan de politie. Via sociale media en internetplatformen hebben burgers of bedrijfsleven nu al in sommige gevallen een betere informatiepositie. Platformen voor *DIY-intelligence* (zoals Bellingcat) zijn de eerste voorbeelden van democratisering van intelligence.

Veel van de informatieplatformen brengen vraag en aanbod op effectieve wijze bij elkaar, waarmee intermediairs (zoals reisbureaus of banken) overbodig worden: de-institutionalisering. Gedistribueerde databasetechnologieën (blockchain)[8] maken naast autonoom werkende systemen zelfs gedistribueerde autonome organisaties (zonder intermediairs) mogelijk. Interessant is ook dat deze nieuwe spelers door verregaande automatisering en door het vermijden van fysieke producten – het gaat om informatietransacties – heel snel kunnen opschalen. Hierdoor wordt exponentiële groei voor bedrijven mogelijk, terwijl de productiekosten slechts lineair stijgen. Dit *exponential organisation*-principe geldt voor veel grote internetbedrijven.[9]

Van centrale aansturing naar netwerkorganisatie

De snelle veranderingen in de informatiemaatschappij vragen om zelfsturende en wendbare organisaties en verbindend leiderschap, die continue aanpassing mogelijk maken. In onze huidige netwerkmaatschappij zien we dat in toenemende mate binnen en buiten de organisatie wordt samengewerkt in netwerken van entiteiten met verschillende rollen en belangen. Dit betekent – ook voor de politie – een verschuiving in de manier van werken: van centrale aansturing (*command & control*) naar een netwerkorganisatie. Mensen nemen zelf hun beslissingen op basis van gedeelde informatie en (real-time) intelligence: *power to the edge*.

Continu leren en innoveren

Vanuit de softwareontwikkeling is de *agile/scrum*-aanpak afkomstig.[10] Kenmerkend voor deze aanpak is het voortdurend ontwikkelen van nieuwe functionaliteiten in kleine stappen. Binnen korte tijdperiodes wordt ontwikkeld, getest en toegevoegd. En vervolgens start weer een nieuwe iteratie. Deze benadering wordt ook wel op de ontwikkeling van organisaties toegepast: sneller veranderingen in kleine stappen doorvoeren. Deze aanpak draagt bij aan de ontwikkeling van sneller lerende en meer wendbare organisaties: continu leren en innoveren met daarbij ruimte voor experimenteren.

24.1.3 Technologische trends informatiemaatschappij

Bij de genoemde maatschappelijke en organisatorische trends hebben we al heel wat technologische ontwikkelingen de revue laten passeren. We lichten er hier nog een paar uit: *smart everything, data analytics* en *portables & wearables*.

---

8 Blockchain is de oorspronkelijke datastructuur achter het bitcoinnetwerk. Deze is het best te vergelijken met een grootboek dat open en decentraal beschikbaar is.

9 Ismail, S., Y. van Geest & M. Malone, *Exponential Organizations*. Diversion Books, New York 2014.

10 Gerelateerd zijn: *design thinking* en *lean start-up*.

Smart everything

Door toepassing van sensoren, informatie- en communicatietechnologie en internet kunnen allerlei voorheen weinig intelligente systemen en infrastructuren steeds slimmer worden: *smart cities, smart buildings, smart roads, smart cars* enzovoort. Het begint bij het op afstand uitlezen van sensorinformatie waaruit bijvoorbeeld de staat van een brug kan worden afgeleid, of de drukte bij een afrit op de snelweg. Dat is natuurlijk al slimmer dan zonder die mogelijkheid. Maar het blijft niet bij uitlezen: het interpreteren van data van sensoren en het automatisch daarop slim aansturen door bijvoorbeeld de toeritdosering automatisch aan te passen, resulteert in écht slimme systemen en infrastructuren. *Internet of Things* in optima forma.

Data analytics

Data uit allerlei mogelijke bronnen kunnen worden gecombineerd om tot intelligenceproducten te komen (data analytics). Ook worden er voorspellende modellen (*predictive analytics*) mee gemaakt, die weer als basis voor geautomatiseerde beslissingen (expertsystemen) kunnen dienen. Predictive analytics omvat een verscheidenheid van statistische technieken en kunstmatige intelligentie zoals *deep learning*, om real-time en historische data te analyseren. Daarmee kan een voorspelling worden gedaan over de toekomst. Een voorbeeld is *predictive policing* (zie ook hoofdstuk 21 Predictive policing), waarbij een verwachting wordt gegeven over tijd en plaats van toekomstige criminele activiteiten.

Portables & wearables

Portables & wearables lopen uiteen van smartphones tot *smart glasses, smart watches, smart sensors, bodycams* en *smart clothing*. Dan gaat het over ontwikkelingen op het gebied van de interfaces tussen mensen en apparaat. Daarmee wordt het voor mensen steeds gemakkelijker om te interacteren met machines. Zo maakt *gesture recognition* het voor machines mogelijk om menselijke houdingen en bewegingen te interpreteren. *Augmented reality* combineert de werkelijke en de virtuele wereld in beeld.

In toenemende mate worden sensoren geïntegreerd in apparaten. Slimme sensoren verzamelen en verzenden niet alleen gegevens, maar kunnen leren, zich aanpassen en configureren en gegevens valideren, interpreteren en combineren. Combineren van data afkomstig van verschillende typen sensoren tot informatie kan sneller leiden tot meer nauwkeurige informatie (sensorfusie). Intelligente sensornetwerken kunnen worden gebruikt voor het detecteren van afwijkingen, voor het identificeren van fenomenen, personen of goederen en voor het controleren van zaken.

24.2 Hoe kan de politie inspelen op de trends en ontwikkelingen?

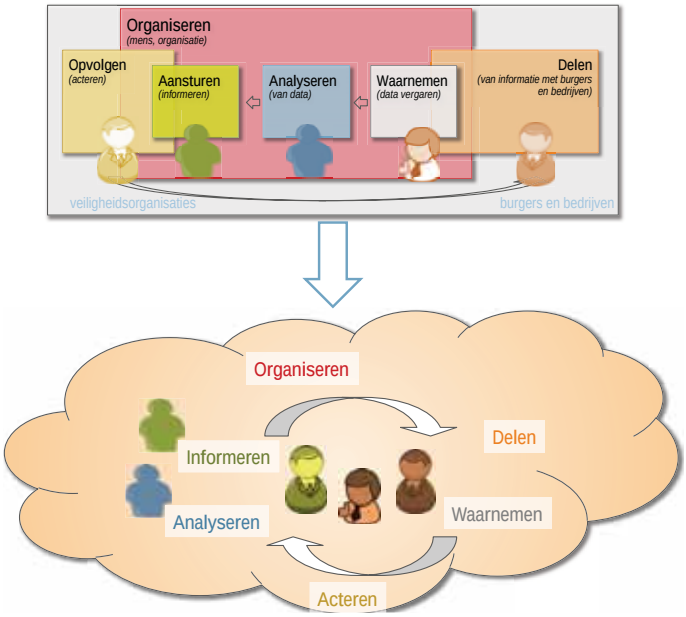
De politie is onderdeel van de maatschappij en zal zich vanzelfsprekend daarin mee moeten ontwikkelen. Er is echter meer. Met deze veranderende maatschappij verandert ook het werkveld van de politie. Meer (economisch) belang in de digitale wereld maakt die wereld voor criminelen steeds interessanter. Om een bank te beroven hoef je niet meer een gebouw binnen te stormen en het personeel te bedreigen met een wapen. En we noemden de interface van de pacemaker al.

Deze verschuiving maakt dat de politie op een andere manier moet gaan werken. Het gaat daarbij niet alleen om uitvoerende zaken zoals preventie, toezicht en opsporing maar vooral om de manier van informatievergaring en zelfs om sturing. Zo is bijvoorbeeld de digitale vorm van criminaliteit veel minder zichtbaar. Traditioneel meet politie criminaliteit door gerapporteerde aangiftes en misdrijven te tellen. Het is maar de vraag of deze traditionele manier van meten van criminaliteit blijft volstaan. Zien we dan nog wel waar zich de criminaliteitsproblemen manifesteren?

Er is nog een belangrijke reden die maakt dat het verstandig is om als politie volop mee te gaan in de informatiemaatschappij: effectiever zullen we nauwelijks meer worden met meer personeel of geld, dat lijkt niet realistisch. Wel in het meer en slimmer omgaan met informatie. Wil je verbetering van effectiviteit realiseren? Dan zit er eigenlijk niets anders op dan dit (ook) te doen op het vlak van informatie.

24.2.1 Transities realiseren

Gebaseerd op de real-time intelligenceradar[11] schetsen we hierna zes transities, gekoppeld aan globale functies in het IGP-proces: organiseren, delen, opvolgen/acteren, aansturen/informeren, analyseren en waarnemen. Figuur 24.1 geeft een geabstraheerd lineair beeld van de functies van het informatiegestuurd politiewerk (IGP; zie bovenste afbeelding). In de praktijk lopen zaken natuurlijk door elkaar heen (zie onderste afbeelding). Onder invloed van de hiervoor beschreven trends zullen verschuivingen optreden.



Figuur 24.1 Globale functies in het IGP-proces
Bron: RTI-radar

11 TNO, *RTI-radar*. TNO-rapport; rapportnummer: TNO 2016, R10354 (14 maart 2016). TNO, Delft 2016.

De politie kan inspelen op de trends en ontwikkelingen door de volgende transities te realiseren.

Organiseren: stimuleren van power to the edge

Onder invloed van veel van de hiervoor beschreven trends zien we bij tal van organisaties dat de organisatievorm verandert van verticaal (met sterke hiërarchische sturing) naar een meer horizontaal organisatiemodel, waarbij mensen zelf hun eigen verantwoordelijkheid kunnen nemen (power to the edge).

Inspelen op deze ontwikkelingen biedt kansen om de verbinding tussen leiderschap en operatie een nieuwe betekenis te geven. Met als resultaat een flexibele en wendbare organisatie, waarin eigen inbreng en creativiteit worden gestimuleerd. Dit draagt bij aan het vermogen de buitenwereld sterker te betrekken en effectiever te zijn: met minder geld meer effect bereiken.

Delen: wederkerig uitwisselen van informatie

De interactie tussen politie en burgers verandert, gedreven door grotere megatrends in de maatschappij. Het is de vraag of we nog wel moeten spreken van burgerparticipatie. Doen burgers mee met de politie, of doet de politie mee met burgers? De denkrichting verandert naar: 'delen, tenzij'.

In plaats van apps waarmee burgers de politie helpen, zou een tweeledige beweging kunnen worden gemaakt. Het gaat dan om de samenleving helpen door participatie, onder meer door het gebruik van nieuwe kanalen van interactie (zoals Het Nieuwe Melden).[12] Delen van informatie wordt in toenemende mate interactief en wederkerig. Dat vraagt om nieuwe serviceverlening zoals webcare en bijbehorende capaciteit.

Opvolgen/acteren: eigen handelingsperspectief faciliteren

Opvolgen op basis van aansturing verschuift naar acteren vanuit het eigen handelingsperspectief. Dit handelingsperspectief moet worden gefaciliteerd. De collega op straat wordt in staat gesteld om op basis van (real-time) informatie betere en meer op de context toegesneden beslissingen te nemen en te handelen. Dit geldt zowel voor de politieman of -vrouw als voor de burger. Ook hier is de interactie tussen politie en burgers van belang. De sturing komt vanuit de samenleving in plaats van vanuit de overheid.

Deze ontwikkelingen bieden de mogelijkheid te organiseren dat op straat direct de juiste (operationele) beslissingen genomen kunnen worden, waarbij de professionele ruimte wordt benut. Want de professionele ruimte en het optimaal faciliteren daarvan staan haaks op strakke (rigide en directieve) aansturing.

Aansturen/informeren: transitie van aansturen naar informeren

Aansturen van mensen verschuift naar informeren van mensen, zoals hiervoor ook beschreven. Daarmee verplaatst het accent zich naar faciliteren, zodat zowel de mensen van veiligheidsorganisaties als burgers zelf beslissingen kunnen nemen. Wat betreft het nemen van beslissingen voor de operationele activiteiten is sprake van twee bewegingen

12 TNO, *Wie belt er nog?: het Nieuwe Melden, een toekomstverkenning*. TNO, Delft januari 2016.

tegelijkertijd: centralisatie en decentralisatie. Dit betreft ontwikkelingen van centrale systemen die besluitvorming voor centrale aansturing ondersteunen, en ontwikkelingen naar decentrale systemen die informatie en analyse mogelijk maken voor besluitvorming ter plekke. Dit heeft zeker gevolgen voor IGP.

Er ligt de mogelijkheid om de ontwikkelingen te richten op het bieden van handelingsperspectief. Dat betekent een verschuiving van aansturen naar meehelpen, door overheid én burgers. Dit door de mogelijkheid te creëren om anderen informatie te leveren, bijvoorbeeld voor contextduiding. Het gaat er daarbij om met z'n allen het verschil te kunnen maken: context voor iedereen.

Analyseren: van data naar informatie voor besluitvorming (intelligence)

Vanuit het analyseren van data kan het aansturen en informeren van politiefunctionarissen en burgers nog meer *knowledge-based* worden, dus gebaseerd op (real-time) inzichten. Macht verschuift van traditionele productiefactoren naar het hebben en kunnen analyseren van data. Hierbij is eveneens sprake van de hiervoor genoemde twee bewegingen: aan de ene kant gaat het om steeds complexere centrale tools waarbij analisten samenwerken met anderen; aan de andere kant steeds eenvoudigere decentrale tools op mobiele apparaten, waardoor relatief eenvoudige analyses voor ieder individu mogelijk worden. Daarmee komt (real-time) informatie sneller in de haarvaten van de organisatie.

Belangrijke onderdelen om in te spelen op deze ontwikkelingen zijn: selectief informatie analyseren, voorspellende mogelijkheden (*predictive*) inpassen en informatie delen.

Waarnemen: bronnen selecteren voor IGP

Data vormen in toenemende mate de basis voor het verbeteren van het situationele bewustzijn, waardoor we beter kunnen anticiperen en effectiever kunnen acteren: de juiste beslissing maken over wie en hoe. Data worden verzameld vanuit eigen waarneming of door te koppelen aan data van derden. Vanwege het verder toenemende belang van data moet worden bepaald wat organisaties in het veiligheidsdomein vanuit hun doelstellingen aan data willen en mogen verzamelen.

Een dreiging is het gevaar van blinde vlekken; het risico om belangrijke informatie te missen. Informatieachterstand kan leiden tot onveiligheid en imagoschade wanneer burgers wél over informatie beschikken. Anderzijds kan een te grote hoeveelheid data leiden tot problemen bij de verwerking en opvolging ervan. Een hieraan gerelateerd risico is de verwachting vanuit de maatschappij. Wanneer informatie wordt gedeeld, wordt ook aangenomen dat er iets mee wordt gedaan. En er wordt verwacht dat zorgvuldig en verantwoord wordt omgegaan met data.

24.2.2 Door experimenteren, leren en innoveren

De politie kan op de ontwikkelingen in de informatiemaatschappij inspelen en genoemde transities in gang zetten door zich deze daadwerkelijk eigen te maken door: experimenteren, leren en innoveren. Experimenteren in samenwerking met de buitenwereld (externe oriëntatie): met burgers, bedrijfsleven en kennisinstellingen. Experimenteren, leren en innoveren vraagt om een agile/scrum-aanpak als hiervoor geschetst; kortcyclisch met interacties tussen strategie en experiment en tussen innovatie en operatie. Experimenten

zijn er niet alleen voor het ontdekken van bruikbare nieuwe werkwijzen en technologieën, maar kunnen tevens bijdragen aan het vestigen van nieuwe manieren van werken en handelen: de transitie van een verticale (hiërarchische) organisatie naar een meer horizontale organisatie waarin het handelingsperspectief van mensen op straat wordt gefaciliteerd (netcentrisch werken). Via continu experimenteren, leren en innoveren met genoemde transities als actielijnen, kan de politie meebewegen met de ontwikkelingen in de informatiemaatschappij.

Over de auteurs

Pieter-Jaap Aalbersberg

Pieter-Jaap Aalbersberg is sinds 1 januari 2013 politiechef van de Eenheid Amsterdam. Daarvoor was hij korpschef van IJsselland en heeft hij uiteenlopende functies binnen de politie bekleed. Na zijn opleiding aan de Nederlandse Politieacademie was hij voornamelijk werkzaam op het gebied van criminele inlichtingen en bestrijding van georganiseerde misdaad, op regionaal, nationaal en internationaal niveau. Hij gaf hierbij leiding aan een aantal belangrijke strafrechtelijke onderzoeken. Hij was daarnaast lid van verschillende commissies van de Europese Unie die zich bezighielden met de aanpak van georganiseerde criminaliteit binnen de grenzen van de Europese Unie. Onder zijn leiding kwam het informatiegestuurd werken bij de Nederlandse politie van de grond en hij was verantwoordelijk voor een nieuwe strategie op het vlak van humanresourcemanagement. Pieter-Jaap leidde de repatriëringsmissie in de Oekraïne die stoffelijke resten en persoonlijke eigendommen van de slachtoffers van de vliegramp met de vlucht MH17 opspoorde. Hij is een politiechef met sterk leidinggevende capaciteiten, gericht op operationele resultaten, maar wel zeer betrokken bij de mensen in de organisatie.

Dian Aarts

Dian Aarts besloot aan het einde van haar studie Bedrijfskunde in Rotterdam dat het werken bij een op winst gerichte organisatie toch niet haar ding was. Werken bij de politie lonkte en toen ze erachter kwam dat de politie in Rotterdam academici zocht, heeft ze meteen gesolliciteerd. Aansluitend aan haar studie is Dian naar de Politieacademie gegaan. In haar *management development traject* heeft ze zich voornamelijk gericht op de opsporing en is ze haar carrière gestart binnen de Dienst Regionale Recherche. Vanuit deze dienst heeft ze de doorstap gemaakt naar de milieupolitie en daar de reorganisatie gedaan. Na acht jaar opsporing werd haar interesse in intelligence gewekt en is ze aan de slag gegaan als hoofd Infodesk in Rotterdam. Na een doorstap naar de functie van plaatsvervanger van de regionale informatieorganisatie, waarbij ze onder meer met een team het werkingsdocument voor de Dienst Regionale Informatieorganisatie Rotterdam heeft opgesteld, besloot ze te solliciteren als sectorhoofd. In deze rol en als lid van het Platform Informatieorganisatie richt Dian zich landelijk onder andere op de thema's persoonsgebonden aanpak en risicotaxatie.

Karin van Baarle

Karin van Baarle studeerde Nederlands Recht aan de Universiteit van Utrecht en is afgestudeerd in het strafrecht. Tijdens het afstuderen raakte zij geboeid door het politiewerk en volgde de officiersopleiding aan de Politieacademie. Na ruim tien jaar werkzaam te zijn geweest in de toenmalige regio Kennemerland in zowel blauw als opsporing en informatie, maakte zij in 2010 de overstap naar de Landelijke Eenheid. Door de Master Informatiemanagement aan de Universiteit van Amsterdam verdiepte zij zich verder in het werkveld van

informatie en intelligence. Op dit moment werkt zij als teamchef C van de afdeling Landelijke Informatie, een onderdeel van de Dienst Landelijke Informatieorganisatie. Vanuit haar huidige functie werkt zij actief mee aan de bevordering van innovatie en kwaliteit binnen de informatieorganisatie en de verdere professionalisering van kennis en competenties van medewerkers binnen dit domein. Daarnaast maakt zij met veel enthousiasme deel uit van het bestuur van het Netwerk voor Innovatie en Kwaliteit.

Christiaan van den Berg

Christiaan van den Berg heeft een passie voor innovatie: organisaties in staat stellen om nieuwe technologieën, werkwijzen en processen uit te vinden en eigen te maken. Christiaan werkt altijd in het snijvlak tussen organisatie en informatie- en communicatietechnologie, en heeft dat de afgelopen jaren in allerlei branches gedaan: van banken tot luchthavens en overheden. Christiaan heeft zijn masterstudie afgerond aan de Technische Universiteit Delft (Innovatiemanagement aan de faculteit Industrieel Ontwerpen).

Waldo de Boer

Waldo de Boer is sectorhoofd van de Dienst Regionale Informatieorganisatie, Eenheid Den Haag. Hij is lid van het Real Time Intelligence Lab, een samenwerkingsverband met onder andere TNO en The Hague Security Delta. Hij is algemeen commandant Staf Grootschalig en Bijzonder Optreden en Operationeel Leider Veiligheidsregio Den Haag. Waldo vervulde daarvoor diverse functies binnen de politie, waaronder Districtschef Duin- en Bollenstreek, plaatsvervangend hoofd korpsrecherche en portefeuillehouder woninginbraken & jeugd en veelplegers.

Henk Bril

Henk Bril is op straat als agent begonnen en studeerde later bedrijfskunde aan de Radboud Universiteit Nijmegen en volgde de officiersopleiding aan de Politieacademie. In zijn 35-jarige loopbaan is hij, naast een uitstapje naar het bedrijfsleven, onder andere chef Inlichtingendienst, districtschef en recherchechef geweest in Oost- en Midden-Nederland. Op dit moment is hij op (inter)nationaal niveau actief in de Landelijke Eenheid als hoofd van de Landelijke Informatieorganisatie. Hij is voorzitter van het Platform Informatieorganisatie.

Tjeerd ten Brink

Tjeerd ten Brink studeerde psychologie met als specialisatie methodenleer aan de Universiteit van Amsterdam. Daarna promoveerde hij aan de Vrije Universiteit op onderzoek naar de ontwikkeling van kinderen tijdens een periode van psychiatrische hulpverlening. Daarnaast en daarna deed hij evaluatieonderzoek naar verschillende soorten van intensieve, ambulante gezinshulpverlening. Als vers aangenomen strategisch onderzoeker bij de politie deed Tjeerd welgeteld één onderzoek: naar de risico's van de invoering van de euro. Daarna ging het eigenlijk alleen nog maar over informatiegestuurd werken, informatie-uitwisseling, *Nationaal Intelligence Model*, business-intelligencestrategie, risicotaxatie en programma intelligence. Naast heel veel informatie is hij dol op Bach, zijn iPad, rondkijken, foto's, New York en mijmeren.

Colin Brown

Colin Brown is sectorhoofd van de Dienst Regionale Informatieorganisatie, Eenheid Midden-Nederland. Al tijdens zijn jaren in het managementteam van de regionale recherche van het toenmalige korps Utrecht werkte hij aan het versterken van de verbinding tussen opsporing en intelligence. Sinds het bijdragen aan de oprichting van de Divisie Informatie binnen het korps Utrecht werkt Colin binnen de informatieorganisatie en was hij kwartiermaker voor de Dienst Regionale Informatieorganisatie Midden-Nederland. Colin heeft ervaring als leidinggevende binnen de voorlopers van de huidige inlichtingendiensten van de politie, en is namens het Platform Informatieorganisatie portefeuillehouder Inwinning en voorzitter van het Landelijk Overleg Hoofden Inwinning.

Marjolijn Bruggeling

Marjolijn Bruggeling-Joyce is een ervaren politiekundige, zowel op het operationele als het beleidsmatige vlak. Ze heeft tien jaar bij de politie in Amsterdam gewerkt en is onlangs naar New York geëmigreerd om haar carrière in de Verenigde Staten voort te zetten. Professioneel gezien ligt haar focus op veranderingsprocessen, kennisdeling en *predictive policing*. Tot voor kort werkte Marjolijn als projectleider voor de politie-eenheid Amsterdam, waar ze zich bezighield met de nieuw te ontwikkelen informatiesturingsprocessen voor de basisteams, die uitgaan van sturen op basis van intelligence. Inmiddels werkt ze in de Verenigde Staten als projectcoördinator voor het Chicago Crime Fighting Initiative bij de Department of Justice, ter ondersteuning van de Chicago PD.

Reinder Doeleman

Reinder Doeleman studeerde Technische Informatica aan de Technische Universiteit Delft en kwam via zijn afstudeeronderzoek terecht bij de politie Amsterdam-Amstelland. Daar trad hij in 1997 in dienst en werkte hij aan het realiseren van het intranet voor het korps. Reinder werd vervolgens chef van de ontwikkelafdeling die onder andere Integrale Bevraging, Aangifte via Intranet en BOSZ realiseerde. In 2005 stapte hij van het technische domein over naar het informatiedomein, waar hij programmamanager Informatiegestuurde Politie werd. In de daaropvolgende jaren heeft Reinder zich beziggehouden met het ontwerpen en realiseren van de regionale informatieorganisatie in de rol van plaatsvervangend dienstchef en sinds 2015 als sectorhoofd Dienst Regionale Informatieorganisatie. Zijn interesses liggen in de combinatie van technologie en intelligence, zoals blijkt uit zijn voorzitterschap van de stuurgroepen basisvoorziening informatie, *predictive policing* en *open source intelligence*.

Robert Paul Doorenbosch

Robert Paul Doorenbosch is integraal projectleider e-Briefing, het project van waaruit het nieuwe werkproces briefing en de nieuwe, landelijke e-Briefingtool zijn ontwikkeld. Robert Paul heeft leiding gegeven aan meerdere projecten in het politiedomein. Zo gaf hij in 2004 leiding aan het project dat de Integrale Bevraging ontwikkelde. In 2005 was hij betrokken bij het programma Informatiegestuurde Politie bij de politie Amsterdam, waar hij de projectleiders binnen het programma begeleidde en coachte bij het projectmatig werken. Van 2007 tot 2010 was hij projectleider van de vorming van de Dienst Regionale Informatie Organisatie in Amsterdam. Inmiddels is hij 18 jaar werkzaam als extern projectcoach/

projectleider van veranderopdrachten bij verschillende klanten, waaronder de politie. Eerst negen jaar bij Pentascope (bureau voor implementaties) en sinds 2008 als zelfstandige. Robert Paul is ervan overtuigd dat een mensgerichte manier van werken uiteindelijk tot de beste resultaten leidt.

Suzanne Franken

Suzanne Franken werkt voor de Gegevensautoriteit, onderdeel van de Directie Informatievoorziening. Ze houdt zich bezig met het Wpg-technisch op orde brengen van belangrijke informatievoorzieningen als BasisVoorziening Handhaving en BasisVoorziening Informatie. Ook zorgt ze voor de verdere ontwikkeling van *privacy & security by design* in het korps en een goede inbedding van de Wpg in het opleidingsaanbod. Ze heeft tussen 2009 en 2013 verschillende Wpg-implementatietrajecten gedaan in de toenmalige korpsen. Daarvoor werkte Suzanne als business- en informatieanalist en tekstschrijver. Ze studeerde psychologie en kunstmatige intelligentie.

Marjan Hanrath

Marjan Hanrath is jurist en criminoloog, afgestudeerd aan de Vrije Universiteit te Amsterdam. Na enkele jaren met veel plezier als unitdirecteur in het gevangeniswezen gewerkt te hebben, maakte zij in 2002 de overstap naar de politie. Zij werkte als adviseur en leidinggevende achtereenvolgens bij het korps Zaanstreek-Waterland, het Nederlands Politie Instituut, de Politieacademie en de Staf Korpsleiding – altijd in een mix van beleid, strategie, communicatie en bestuur. Marjan benut haar kennis op dit gebied nu bij het programma Herijking Opsporing en de Directie Operatiën van het korps, waar haar focus ligt op de versterking van de opsporing.

Mariëlle den Hengst

Mariëlle den Hengst-Bruggeling was van 2009 tot 2017 als lector Intelligence verbonden aan de Politieacademie. Zij combineerde dit met een functie aan de Technische Universiteit Delft (sinds 1994). Van 2005 tot 2008 heeft zij haar werk aan de universiteit gecombineerd met werk als onderzoeker bij TNO. In 2002 deed Mariëlle onderzoek bij de Department of Management Information Systems van de University of Arizona. In 1999 promoveerde zij aan de Technische Universiteit Delft, nadat zij hier in 1994 cum laude was afgestudeerd in informatica. Haar onderzoeksinteresse ligt op het gebied van informatie en besluitvorming, *informed decision making*. Zij onderzoekt een scala aan mechanismen die het gebruik van informatie bij besluitvorming versterken of juist in de weg staan.

Stephan den Hengst

Stephan den Hengst is *chief data officer* van de politie. Hij geeft leiding aan de Gegevensautoriteit. Met dit team werkt hij aan een stabiele en hoogwaardige gegevenshuishouding waarmee de digitale transformatie ingezet kan worden. Stephan heeft informatica gestudeerd aan de Technische Universiteit Delft. Hij heeft een voorliefde voor techniek, vooral wanneer deze succesvol ingezet wordt voor een maatschappelijk vraagstuk. Vanuit die drijfveer heeft hij vanaf medio 2004 business intelligence – oorspronkelijk gebruikt voor sturing en control – ingezet voor het operationele politiewerk. Vanaf 2011 heeft hij dit nationaal verankerd: de basisvoorziening informatie is inmiddels niet meer weg te denken

uit het dagelijkse politiewerk en het werk van vele partners. Sinds 2014 richt Stephan zich op de gegevens die de kern vormen van alle mogelijkheden.

Peter Holla

Peter Holla is plaatsvervangend politiechef Noord-Holland en 36 jaar werkzaam bij de politie. De eerst helft van zijn carrière werkte hij in Amsterdam, waar hij onder andere betrokken was bij de opzet van misdaadanalyse in Nederland. Hier is zijn interesse begonnen voor de informatievraagstukken. Naast zijn opleiding aan de Politieacademie heeft hij criminologie gestudeerd in Leuven. Zijn brede interesse in het politievak kwam mede tot uiting in zijn redacteurschap voor het *Tijdschrift voor de Politie* en de redactieraad voor Politie en Wetenschap. De afgelopen jaren is Peter actief geweest in verschillende stuurgroepen voor het ontwikkelen en in gebruik nemen van informatiesystemen; niet alleen op het gebied van business intelligence en integrale bevraging, maar ook voor de handhaving, het aanleveren van zaken bij het Openbaar Ministerie. Zijn motto: 'Succesvol bezig zijn met informatievoorziening kan alleen als informatiemanagement, informatietechnologie en de business met elkaar samenwerken. Mensen uit de lijn moeten daar hun verantwoordelijkheid in nemen.'

Michiel In 't Veld

Michiel In 't Veld is onderzoeker aan de Politieacademie. Hij doet onderzoek naar de (onvoorziene) effecten van informatietechnologie op politiewerk en politieorganisatie. Na een loopbaan als onderzoeker aan het Instituut voor de Fysieke Veiligheid werkte hij achtereenvolgens voor het lectoraat Intelligence van de Politieacademie en als onderzoeker en docent bij Crisislab, de onderzoeksgroep die de leeropdracht 'Besturen van Veiligheid' ondersteunt aan de Radboud Universiteit Nijmegen. Michiel is in brede zin vooral nieuwsgierig naar de uitwerking van de informatiesamenleving op het functioneren van het openbaar bestuur, bijvoorbeeld in crisissituaties. Van huis uit is hij bestuurskundige, hij volgde de studie Integrale Veiligheidskunde (Saxion Hogeschool) en de bestuurskundemaster Besturen van Veiligheid (Vrije Universiteit).

Nicolien Kop

Nicolien Kop is psycholoog en sinds 2010 lector Criminaliteitsbeheersing & Recherchekunde aan de Politieacademie. Sinds begin jaren negentig doet zij op breed terrein onderzoek bij en naar de politie, waarvan de afgelopen veertien jaar specifiek binnen de opsporing. Hierover publiceert zij regelmatig. Voorheen werkte Nicolien als onderzoeker bij de Universiteit Utrecht en het Nederlands Instituut voor Internationale Betrekkingen Clingendael. In 2012 sprak zij haar lectorale rede uit: *Van opsporing naar criminaliteitsbeheersing*. Momenteel is zij betrokken bij en verantwoordelijk voor de onderzoekslijnen technologie & informatiedeling en ondermijning die de Politieacademie uitvoert in het kader van de strategische onderzoeksagenda voor de politie. Verder is zij als copromotor betrokken bij diverse promotietrajecten.

Guus Meershoek

Guus Meershoek is lector Politiegeschiedenis aan de Politieacademie en universitair docent Bestuurskunde aan de Universiteit Twente. Hij heeft onderzoek verricht naar de politiegeschiedenis, in het bijzonder in verband met de Duitse bezetting, en naar hedendaags

politiewerk, in het bijzonder georganiseerde misdaad en misdaadbestrijding, verkeerspolitiewerk en verdekt optreden. Guus studeerde politicologie aan de Universiteit van Amsterdam en schreef een proefschrift over de Amsterdamse politie tijdens de Duitse bezetting (*Dienaren van het gezag,* Amsterdam, 1999). Voorts publiceerde hij diverse boeken en artikelen, waaronder *De Gemeentepolitie in een veranderende samenleving* (Amsterdam, 2007) en *De Groep IJzerman* (Amsterdam, 2011). Samen met Jos Smeets en Tommy van Es publiceerde hij *In de frontlinie* (Amsterdam, 2014). Hij schrijft maandelijks een politiecolumn op www.nrc.nl/rechtenbestuur.

Jan Mellema

Jan Mellema is teamchef Business Intelligence & Kwaliteit binnen de Eenheid Oost-Nederland. Hij is 35 jaar werkzaam in meerdere eenheden en het Politiedienstencentrum in de vakgebieden handhaving, opsporing intelligence en project- en verandermanagement. Hij was onder andere als programmamanager Implementatie Autorisatiemodel Politie verantwoordelijk voor de eerste fase van het programma en heeft meegeschreven aan de visie op autoriseren *Autoriseren: zo doen we dat hier!* Daarnaast heeft hij ervaring op gebied van testmanagement, identity en access management, data governance en business intelligence. Op dit moment bouwt hij mee aan de informatiegestuurde organisatie Oost-Nederland, de basisvoorziening informatie en andere daaraan gekoppelde systemen.

Gerbrand Mijzen

Gerbrand Mijzen is in 1999 afgestudeerd als medisch informatiekundige en sindsdien werkzaam op het snijvlak van informatievoorziening en overheid. Hij werkte als programmeur, onderzoeker en projectleider bij het Leids Universitair Medisch Centrum en daarna ongeveer vijftien jaar als adviseur informatievoorziening voor diverse ministeries en andere overheidsorganisaties. Gerbrand is in dienst bij het Uitvoeringsinstituut Werknemersverzekeringen als business consultant informatiemanagement en op basis van detachering werkzaam bij de Gegevensautoriteit van de Staf Korpsleiding.

Jan ter Mors

Jan ter Mors begon in 1984 als inspecteur bij de Haagse politie. Hij werkte als leidinggevende bij de wijkpolitie in Den Haag en Delft, de lokale en centrale recherche en de staf. Eind jaren negentig leidde hij het Prisma-kernteam, belast met de aanpak van grootschalige cocaïnehandel. Na de aanslagen in New York gaf Jan leiding aan de dienst Nationale Recherche Informatie. Hij werkte onder andere aan vervanging van Havank, het stelsel Bewaken en Beveiligen en de ontwikkeling van het *Nationaal Intelligence Model* (NIM). In 2008 nam hij afscheid als diensthoofd en werd hij belast met de implementatie van het NIM bij de politie. Met de portefeuillehouder Intelligence werkte hij als landelijk programmamanager aan de business-intelligencestrategie en realisatie van de basisvoorziening informatie, versterking van politieonderwijs, verbetering van informatiegestuurd werken en realisatie van de informatieorganisatie bij de nationale politie. Jan vindt het belangrijk om als dienende en verbindende leider mee te helpen aan het constant verbeteren en vernieuwen van de politie.

Paul van Musscher

Paul van Musscher is werkzaam als politiechef van Eenheid Den Haag, waar hij onder andere verantwoordelijk is geweest voor de veiligheidsmaatregelen rondom de Nuclear Security Summit, The Cyber Security Top en het wereldkampioenschap hockey. Daarnaast is hij binnen de Nederlandse politie portefeuillehouder Vreemdelingenzaken en Migratiecriminaliteit. Eind 2015 was Paul nauw betrokken bij de oprichting van zeven identificatie- en registratiestraten om de zeer grote asielinstroom ordentelijk te laten verlopen. Voorheen was Paul plaatsvervangend korpschef Haaglanden en daarvoor op meerdere plaatsen districtchef in de regio Hollands Midden. Naast zijn jarenlange ervaring binnen de opsporing heeft hij veel ervaring binnen het grootschalig en bijzonder optreden. Zijn interesse gaat in hoge mate uit naar veiligheidssturing en samen met Peter Versteegh heeft hij hierover diverse artikelen gepubliceerd.

Anne Jan Oosterheert

Anne Jan Oosterheert rondde zijn Master of Science met de richting *Business Process Management and IT* in 2009 af. Hij is afgestudeerd in het toepassen van kennismanagement in de politiepraktijk. Zijn afstudeeronderzoek ging in op kennis waarbij goede interactie tussen mensen, informatie en technologie essentieel is. In 2010 werd Anne Jan eindverantwoordelijk voor de aansturing van het analyseteam in politiekorps IJsselland. Het team voert veiligheids- en zaakanalyses uit met als doel besluiten te ondersteunen op operationeel, tactisch en strategisch niveau. In 2012 werd Anne Jan verantwoordelijk voor het opzetten van een nieuw team: het Business Intelligence Competency Center (BICC) bij de politie Oost-Nederland en later geeft hij ook sturing aan het centrale BICC van de politie. In 2014 startte hij als chef Analyse & Onderzoek bij de politie-eenheid Oost-Nederland.

Peter van Os

Peter van Os was tot voor kort directeur Onderzoek, Kennis & Ontwikkeling aan de Politieacademie. Hij heeft ruim dertig jaar ervaring op verschillende posities, aanvankelijk bij de Rijkspolitie en later bij de regiokorpsen Gelderland-Midden en Noord- en Oost-Gelderland. Als districtschef in Arnhem en Apeldoorn heeft hij zich vooral hard gemaakt voor een gebiedsgebonden politie, fijnmazig, in de samenleving verankerd en gericht op probleemoplossing door partnerschap. Veiligheid is in eerste instantie van de mensen zelf en het vraagt nogal wat van de professie om hier echt handen en voeten aan te geven. In de loop der jaren heeft Peter hierover diverse publicaties geschreven.

Ab van der Plas

Ab van der Plas is teamchef Inwinning, Eenheid Den Haag en al 25 jaar actief binnen de opsporing op zowel lokaal, regionaal als internationaal terrein. Op het gebied van intelligence heeft hij ervaring opgedaan als teamleider bij de Criminele Inlichtingeneenheid van de toenmalige Nationale Recherche.

Ronald Reijneveld

Ronald Reijneveld studeerde Bedrijfskunde, specialisatie Strategisch Management aan de Erasmus Universiteit Rotterdam. Tijdens zijn traineeship bij een management-

development-organisatie werd hij gevraagd om leiding te geven aan een project binnen de toenmalige Regiopolitie Flevoland. In 2002 is hij in dienst gekomen van dit korps. Na projectleiderschap ten behoeve van meerdere projecten binnen de bedrijfsvoering nam hij vanaf 2008 het programma Intelligence voor zijn rekening in de rol van programmamanager. Vanaf 2011 gaf Ronald leiding aan de afdelingen Projectvoorbereiding & Analyse van de korpsen Flevoland en Gooi & Vechtstreek. Sinds 2014 is hij chef van Analyse & Onderzoek van de Eenheid Midden-Nederland.

Rutger Rienks

Rutger Rienks is een voorvechter van datagedreven denken in Nederland. Hij promoveerde als informaticus in het machinaal waarnemen van menselijk gedrag in 2007 en werkte daarna bijna acht jaar voor de politie in het intelligencedomein. Hij is een veelgevraagd spreker, doceert aan de Universiteit Nyenrode en schreef wetenschappelijke artikelen over hoe de politie meer met techniek en data kan doen. In 2015 schreef Rutger een veelbesproken boek over *predictive policing*. Inmiddels werkt hij voor de gemeente Amsterdam, waar hij als programmamanager helpt met het ontwikkelen van het datagedreven denken en het inrichten van de Amsterdamse datavoorzieningen.

Fons Sarneel

Fons Sarneel is na diverse andere werkervaringen in 1988 zijn politieloopbaan begonnen als agent bij gemeentepolitie Haarlemmermeer. In de Regio Kennemerland heeft hij tussen 1994 en 2000 een grote impuls gegeven aan de repressieve en preventieve aanpak van woninginbraken. Vanaf 1996 heeft hij het Politiekeurmerk Veilig Wonen geïntroduceerd en via publiek-private samenwerking overgedragen aan gemeenten en bedrijven. Van 2003 tot 2012 gaf Fons leiding, onder andere aan integrale beroepsvaardighedentraining en basisteam Duinrand (Heemstede/Bloemendaal), waar hij door fusie met het Zandvoort Team Kennemer Kust heeft opgebouwd. Vanaf 2012 heeft hij de realisatie van Dienst Regionale Operationele Samenwerking Noord-Holland voorbereid. Momenteel is Fons als projectleider verantwoordelijk voor diverse innovatieve projecten, het laatste jaar voornamelijk als projectleider e-Briefing. Zijn professionele drijfveer ligt in de vermindering van de kans op slachtofferschap.

Frank Smilda

Frank Smilda is sectorhoofd van de Dienst Regionale Informatieorganisatie bij de politieeenheid Noord-Nederland. Tot 2009 werkte hij bij de recherche in Utrecht. Zijn fascinatie voor de rol van sociale media in de opsporing begon in 2005, het jaar waarin Maurice de Hond zich vastbeet in de Deventer moordzaak. Frank begreep al snel dat burgers dankzij sociale media steeds vaker actief zullen zijn in de opsporing. Voor zijn initiatief www.politieonderzoeken.nl ontving hij in 2007 de Politie Innovatieprijs.

Carl Spruijt

Carl Spruijt begon in 1980 zijn politieloopbaan in Aalsmeer. Als wijkagent, mentor en specialist bijzondere wetten maakte hij via het ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieu de overstap naar het Team Zware Milieucriminaliteit van de

Centrale Recherche Informatiedienst. Met zijn hbo-kennis van handhaving milieuwetgeving draaide hij uiteenlopende milieuonderzoeken en was een tijd gedetacheerd bij het Kernteam Zware Milieucriminaliteit. Als landelijk coördinator werkte Carl voor het Nationaal Netwerk Drugsexpertise, waarbij onder andere georganiseerde hennepteelt op de politieke agenda kwam. Na zijn hbo-opleiding Bestuurskunde en Overheidsmanagement heeft hij verschillende leidinggevende functies bij de politie vervuld. Hij ondersteunt de landelijke politieportefeuille RIEC-LIEC en werkt nu bij de Staf van de Landelijke Eenheid, team Politieprofessie. 'Partnerships en veiligheid' zijn een rode draad in zijn politieloopbaan.

Ruud Staijen

Ruud Staijen is politieman, socioloog en bedrijfskundige. De laatste vijf jaar werkte Ruud als programmamanager operationele voorzieningen binnen het Aanvalsprogramma Informatievoorziening Politie. Samen met anderen heeft hij gewerkt aan de ontwikkeling en implementatie van verschillende applicaties zoals e-Briefing. Daarvoor was Ruud districtschef in Arnhem, diensthoofd van de Dienst Bedrijfsinformatie in Amsterdam en diensthoofd van de Afdeling Bijzondere Taken en waarnemend diensthoofd Nationale Recherche Informatie bij het Korps Landelijke Politiediensten. Ruuds politiewortels liggen in Groningen, waar hij zijn loopbaan is begonnen.

Ries Straver

Ries Straver startte zijn loopbaan bij de Politie Haarlem in 1966. Hij is medeauteur van het rapport *Politie in Verandering* (1977) en was korpschef van politie Haarlem (1987), Kennemerland (1991) en Hollands Midden (1997-2004). Van 2000 tot en met 2004 was Ries namens de Raad van Hoofdcommissarissen landelijk programmamanager van het ABRIO-programma waarmee de landelijke verbreiding van het concept informatiegestuurde politie werd ingezet. Na zijn pensionering was hij tien jaar adviseur/onderzoeker bij het lectoraat Gebiedsgebonden Politie van de Politieacademie. In die periode heeft hij onder andere het actieonderzoek naar het frontoffice/backoffice-concept geleid. Momenteel is hij werkzaam als zelfstandig adviseur.

Mieke Struik

Mieke Struik heeft medische biologie gestudeerd aan de Universiteit van Amsterdam met als specialisatie neurobiologie. Daarna is ze gepromoveerd aan de Universiteit Utrecht op onderzoek naar zintuigsystemen. De essentie van een zintuig is dat een prikkel uit de buitenwereld wordt opgevangen, wordt doorgegeven aan je hersenen, waar het in context wordt verwerkt. Hierdoor ben je in staat op de juiste manier op de prikkel te reageren. De kennis en ervaring van deze systemen heeft Mieke meegenomen naar haar huidige functie van strategisch analist bij de afdeling Analyse en Onderzoek van de Eenheid Oost-Nederland. De stap van biologie naar de politie lijkt groot, maar in essentie gaat het allemaal om informatiegestuurd werken. De politie staat continue aan prikkels bloot zoals aangiften, incidenten en verstoringen van de openbare orde. De taak van een analist is om deze te verzamelen, te duiden en in de juiste context te plaatsen. Om zo te adviseren hoe de politie op die prikkels zou kunnen reageren. Het liefst werkt Mieke in haar analyses trouwens niet

aan reactie op prikkels, maar juist aan anticipatie op toekomstige gebeurtenissen: het voorzien van veranderingen in criminaliteit, maatschappij en organisatie zodat we weten wat er op ons af zou kunnen komen. Dat is soms een ingewikkeld vraagstuk en daarom werkt ze niet alleen graag samen met collega's binnen de politie maar ook met academische instellingen zoals de Universiteit Utrecht, de Technische Universiteit Delft en de Politieacademie.

Peter Tazelaar

Peter Tazelaar studeerde Nederlands recht in Leiden en begon als juridisch medewerker bij de Directie Politie van het toenmalige ministerie van Justitie. Hij schreef de uitvoeringsregelingen voor de Wet wapens en munitie en organiseerde de implementatie van die wet en de eerste in Nederland gehouden 'inleveractie' voor wapens. Tevens was hij delegatieleider voor dit onderwerp bij de onderhandelingen over de Schengen Uitvoeringsovereenkomst. Na een overstap naar de Centrale Recherche-informatiedienst in 1990 raakte Peter betrokken bij het onderwerp dataprotectie, zowel nationaal als internationaal (Schengen, Europol, Interpol), maakte veertien jaar deel uit van de Raadswerkgroep Europol in Brussel en nam deel aan EU-projecten in Turkije, Roemenië en Bulgarije om te adviseren inzake privacywetgeving. Thans is hij juridisch adviseur bij de Staf Landelijke Eenheid en adviseert hij onder meer op de nationale en internationale informatie-uitwisseling en samenwerking, waarbij ook het adviseren van de operatie veel aandacht krijgt.

Erik Theunissen

Erik Theunissen studeerde Nederlandse taal- en letterkunde (psycholinguïstiek). Hij werkte in diverse communicatiemanagementfuncties in het bedrijfsleven en non-profitorganisaties. Vervolgens was hij hoofd Communicatie bij achtereenvolgens politie Zuid-Holland-Zuid en Utrecht. Daarna werd hij programmanager voor de Landelijke Aanpak van Geweld en de laatste jaren houdt hij zich als landelijk projectmanager samen met diverse collega's bezig met het verder professionaliseren van de persoonsgerichte aanpak (PGA) binnen de politie. Sinds kort is hij ook programmamanager bij Directie Operatiën. Erik verbindt strategie en praktijk met elkaar en laat daarvoor mooie dingen ontwikkelen. Door de ontwikkeling van het Risicotaxatie-instrument Geweld en PGA kwam er steeds meer interesse in intelligence en de kansen die dit biedt om politiewerk slimmer te maken. Hij verdiepte zich in risicotaxatie.

Marjolein van Tunen-Geldermans

Marjolein van Tunen-Geldermans startte – na haar studie Rechtsgeleerdheid – haar loopbaan op een gemeentelijke afdeling Sociale Zaken. Hierna werkte zij als beleidsadviseur Werk & Inkomen en werd zij leidinggevende binnen Welzijn. In 2003 maakt zij de overstap naar de politie als diensthoofd Bestuurlijke Aangelegenheden. Omdat de gemeentelijke wereld bleef trekken, werd Marjolein in 2006 gemeenteraadslid, een nevenfunctie die zij negen jaar vervulde. Op basis van haar kennis van bestuur, sociaal domein en strafrechtketen werd zij in 2013 gevraagd als adviseur voor de landelijke portefeuille Veiligheidshuizen. Sinds 2016 is zij ook landelijk adviseur op de portefeuilles Jeugd en Sociaal Domein. Hiernaast blijft zij maatschappelijk verbonden als lid van Raden van Toezicht in

het primair onderwijs en voor maatschappelijke opvang. Ten slotte is zij sinds januari 2016 directeur van 'Un-wind: ontrafelen-verbinden-ontwikkelen' en adviseert zij teams en teamleden op veranderopgaven.

Hans van Vliet

Hans van Vliet is senior business consultant bij de afdeling Strategic Business Analysis van TNO. Hij richt zich op innovatiemanagement en het realiseren van de maatschappelijke en business impact van innovaties in het veiligheidsdomein. Daarbij werkt hij op het snijvlak van de behoeften vanuit maatschappelijke rollen of bedrijfsprocessen en de technische mogelijkheden die innovaties daarvoor ter ondersteuning bieden. Hans is actief in advies- en ontwikkelprojecten op het gebied van innoveren met informatie- en communicatietechnologie en toekomstverkenningen in de vorm van trend- en technologieradars. Hans studeerde in 1986 af aan de faculteit Elektrotechniek van de Technische Universiteit Delft. Hij trad in 1988 – na zijn militaire dienst bij de Koninklijke Marine – in dienst bij TNO.

Bert Voerman

Bert Voerman is plaatsvervangend hoofd van de Dienst Landelijke Informatieorganisatie van de Landelijke Eenheid en commissaris van politie. Hij is ruim dertig jaar werkzaam bij het Korps Landelijke Politiediensten en de voorgangers daarvan in het vakgebied intelligence, onder andere als liaison officer, hoofd van afdelingen met taken op het gebied van informatie en expertise, programmamanager Informatie & Intelligence en korpsprojectleider Nationaal intelligencemodel. Daarnaast is hij betrokken bij de inrichting van de informatieorganisatie nationale politie en realisatie van de Dienst Landelijke Informatieorganisatie.

Harold van Voornveld

Harold van Voornveld is bedrijfskundige en sinds 2006 als adviseur actief binnen de politie. Tot 2010 werkte hij binnen de Dienst Regionale Informatieorganisatie van de regiopolitie Amsterdam-Amstelland, onder meer aan de vorming van de informatieorganisatie. Na wat uitstapjes naar de rechtspraak en het Openbaar Ministerie (Programma Herontwerp Strafrechtketen) vervult Harold vanaf eind 2012 de rol van bedrijfsarchitect binnen de Directie Operatiën van de politie, met als aandachtsgebieden de informatie-organisatie, evenementen en administratieve lastenverlichting. Rode draad in zijn werk is het helpen bouwen aan een betrouwbare, effectieve werking van de politieorganisatie, met oog voor lokale verschillen en beperking van administratieve lasten. Harold draagt bij aan impactanalyses, voorbereiding van implementaties, bedrijfsarchitectuuradvies en landelijke harmonisatie van werkprocessen.

Arnout de Vries

Arnout de Vries is senior onderzoeker en adviseur op het gebied van sociale media en maatschappelijke veiligheid bij TNO. Na zijn studie Industrieel Ontwerpen en Innovatiemanagement onderzocht hij bij KPN Research al *virtual community's* voor iemand ervan had gehoord. Vanaf 2000 werkte Arnout aan mobiel internet, de revolutionaire

ontwikkeling van dat moment. In 2003 werd KPN Research ondergebracht bij TNO. Daar ontwikkelde Arnout een brede visie op de rol die informatie- en communicatietechnologie in de maatschappij van morgen zal spelen. Samen met gedrags- en organisatiewetenschappers en briljante techneuten zet Arnout expertkennis om in concrete toepassingen, zoals in de bestrijding van cybercrime in brede zin. Of, zoals hij dat zelf beschrijft: 'Door onlinesamenwerking met burgers en bedrijven breng ik digitale innovaties in het DNA van organisaties.'

Ingrid de Vries

Ingrid de Vries is sinds 2009 werkzaam bij de politie als adviseur op de portefeuille Intelligence/IGP. Ze opereert op het grensvlak van informatie- en communicatietechnologie en operatie en maakt zich sterk voor het verbeteren van de informatievoorziening en -positie van de operatie. Ze zit het liefst dicht bij of in de operatie om ter plekke en in het hier en nu te helpen, maar ook om met de ervaringen die ze daar opdoet, gevraagd en ongevraagd advies uit te brengen op tactisch en strategisch niveau over benodigde verbeteringen en innovaties in de toekomst. Ingrid gaat ervan uit dat er altijd anderen zijn die meer weten en kunnen en/of andere dingen weten en kunnen. Daar is ze dan ook continu (en graag) naar op zoek. Om er zelf van te leren en om bruggen te kunnen slaan. Ze heeft een juridische achtergrond. Voordat ze bij de politie kwam, heeft ze gewerkt bij verschillende organisaties (Universiteit van Amsterdam, Exact Software, ministerie van Sociale Zaken & Werkgelegenheid, Logica/CMG, ministerie van Defensie).

Dick Willems

Dick Willems is in dienst van de politie-eenheid Amsterdam, waar hij sinds 2012 werkt als *data scientist*. In die hoedanigheid houdt hij zich onder meer bezig met *predictive policing, text mining* en netwerkanalyses. Het Criminaliteitsanticipatiesysteem is door hem ontworpen en gebouwd. Voordat Dick in dienst kwam bij de politie was hij werkzaam als data-analytisch consultant in het bedrijfsleven en daarvoor als statistisch adviseur en onderzoeker bij de Universiteit Maastricht en de Radboud Universiteit Nijmegen. Dick is van oorsprong mathematisch psycholoog, en als zodanig afgestudeerd aan de Radboud Universiteit Nijmegen.

Lijst met afkortingen

AAR	After Action Review
ABRIO	Aanpak bedrijfsvoering recherche, informatiehuishouding en opleiding
ABS	Autorisatiebeheersserver
AID	Algemene Inspectiedienst
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
ANPR	automatic number plate recognition
AOB	Actueel Operationeel Beeld
AVG	algemene verordening gegevensbescherming
AVI	analist veiligheidsinformatie
AVP	Aanvalsprogramma Informatievoorziening Politie
BI	business intelligence
BI&K	business intelligence & kwaliteit
BICC	Business Intelligence Competency Center
BOA	buitengewoon opsporingsambtenaar
BOD	bijzondere opsporingsdiensten
BOSZ	Betere Opsporing door Sturing op Zaken
Bpg	Besluit politiegegevens
BPZ	Basis Politiezorg
BSM	BlueSpot Monitor
BSN	burgerservicenummer
BVH	BasisVoorziening Handhaving
BVI	BasisVoorziening Informatie
BVI-IB	BasisVoorziening Informatie voor Integrale Bevraging
BVO	BasisVoorziening Opsporing
BZK	Binnenlandse Zaken en Koninkrijksrelaties
CAS	Criminaliteitsanticipatiesysteem
CBS	Centraal Bureau voor de Statistiek
CIE	Criminele Inlichtingeneenheid

CIOT	Centraal Informatiepunt Onderzoek Telecommunicatie
CIR	criminele-informatierapport
CJIB	Centraal Justitieel Incassobureau
CoI	Community of Intelligence
CoPI	Commando Plaats Incident
CTER	contraterrorisme, extremisme en radicalisering
CVI	centrale verwijzingsindex
DDoS	distributed denial of service
DIB	dagelijks intelligencebeeld
DIK	districtelijk informatieknooppunt
DJI	Dienst Justitiële Inrichtingen
DLA	drieletterafkorting
DLIO	Dienst Landelijke Informatieorganisatie
DRIO	Dienst Regionale Informatieoganisatie
DROC	Dienst Regionaal Operationeel Centrum
DRR	Dienst Regionale Recherche
E&S	executie & signalering
EMPACT	European Multidisciplinary Platform Against Criminal Threats
EMTP	Executive Master of Tactical Policing
FCM	fotoconfrontatiemodule
FIOD-ECD	Fiscale Inlichtingen- en Opsporingsdienst – Economische Controledienst
GBA	gemeentelijke basisadministratie persoonsgegevens
GBT	gemeentelijk beleidsteam
GEB	gegevensbeschermingseffectbeoordeling
GGB	gegegevensgebruik en -beheer
GGP	gebiedsgebonden politie
ggz	geestelijke gezondheidszorg
GHOR	Geneeskundige Hulpverleningsorganisatie in de Regio
GMS	geïntegreerd meldkamersysteem
GOC	georganiseerde en Ondermijnende Criminaliteit
GPO	gestructureerd professioneel oordeel
GPP	geprioriteerd politiepersoon
GRIP	gecoördineerde regionale incidentbestrijdingsprocedure
GRMT	gemeentelijk rampenmanagementteam

HAVANK	Het Automatisch Vinger Afdrukkensysteem Nederlandse Kollektie
HIC	high impact crime
HKS	Herkenningssysteem
HOvD	hoofdofficier van justitie
IB	Integrale Bevraging
IBAN	international bank account number
IBT	integrale beroepsvaardighedentraining
ICOV	infobox crimineel en onverklaarbaar vermogen
ICT	informatie- en communicatietechnologie
IGO	informatiegestuurde opsporing
IGP	informatiegestuurd politiewerk; voorheen: informatiegestuurde politie
IGV	informatiegestuurde veiligheidszorg
ILT-IOD	Inspectie Leefomgeving en Transport/Inlichtingen- en Opsporingsdienst
IM	Informatiemanagement
IND	Immigratie en Naturalisatiedienst
INK	Instituut Nederlandse Kwaliteit
iRN	internet Research Netwerk
ISD	inrichting stelselmatige daders
ISZW	Inspectie Sociale Zaken en Werkgelegenheid
IT	informatietechnologie
IV	informatievoorziening
KIM	kennis in modellen
KLPD	Korps landelijke politiediensten
KMar	Koninklijke Marechaussee
Kompol	Kennis op maat politie
LFNP	Landelijk Functiehuis Nederlandse Politie
LIEC	Landelijk Informatie- en Expertisecentrum
LIST	landelijk informatiesysteem
LOHI	landelijk overleg hoofden inwinning
LORS	Landelijk Overvallen RegistratieSysteem
LSO	landelijk strategisch overleg
MBT	Mobiele Dataterminal
MCCb	Ministeriële Commissie Crisisbeheersing
MDT	Mobiele Dataterminal

ME	mobiele eenheid
MEOS	Mobiel Effectiever Op Straat
MO	modus operandi
MRO	melding rechercheonderzoek
NAS	nieuwe autorisatiestructuur
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NDB	nationaal dreigingsbeeld
NFI	Nederlands Forensisch Instituut
NIM	*Nationaal Intelligence Model*
NSGBO	Nationale Staf Grootschalig Bijzonder Optreden
NSIS	Nationaal Schengen Informatiesysteem
NVWA-IOD	Nederlandse Voedsel- en Warenautoriteit – Inlichtingen- en Opsporingsdienst
OM	Openbaar Ministerie
OMG	outlaw motor gang
Opco	operationeel coördinator
OPP	operationeel politieproces
OPS	opsporingssysteem
OS	operationeel specialist
OT	observatieteam
OvD-I	officier van dienst – informatie
OvD-OC	officier van dienst – operationeel centrum
OvD-R	officier van dienst – recherche
PAPOS	parket politiesysteem
PD	plaats delict
PDC	politiedienstencentrum
PGA	persoonsgerichte aanpak
PGE	potentieel gewelddadige eenlingen
PIA	Privacy Impact Assessment
PIO	Platform Informatieorganisatie
PiV	*Politie in Verandering*
PKN	Politiekennisnet
POP	problem-oriented policing
PSH-V	politiesuite handhaving vreemdeling
pv	proces-verbaal

PVOV	programma versterking opsporing en vervolging
RBT	regionaal beleidsteam
RDW	Rijksdienst voor het Wegverkeer
RID	Regionale Inlichtingendienst
RIEC	Regionaal Informatie- en Expertisecentrum
RIK	regionaal informatieknooppunt
RKC	Raad van Korpschefs
ROT	regionaal operationeel team
RSC	Regionaal Service Centrum
RSJ	Raad voor Strafrechtstoepassing en Jeugdbescherming
RST	recherchesamenwerkingsteam
RTI	real-time intelligence; risicotaxatie-instrument
RTIC	Real-Time Intelligence Center
SGBO	Staf Grootschalig en Bijzonder Optreden
SIOD	Sociale Inlichtingen- en Opsporingsdienst
sitrap	situatierapportage
SKN	strafrechtketennummer
SLA	service level agreement
SOCTA	Serious and Organised Crime Threat Assessment
SPV	Stichting Processen Verbaal
Sr	Wetboek van Strafrecht
Summ-IT	politieregistratiesysteem voor de verwerking van strafdossiers en onderzoeken
Sv	Wetboek van Strafvordering
SWOT	(analyse van) strengths, weaknesses, opportunities and threats
TCI	Team Criminele Inlichtingen
TGO	Team Grootschalige Opsporing
TNI	Team Nationale Inlichtingen
TNO	Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek
TOOI	Team Openbare Orde Inlichtingen
VERONA	centrale registratie rond wapenvergunningen
VG	verzorgingsgebied
Vhh	Veiligheidshuis
VOG	Verklaring Omtrent het Gedrag
VROM	Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer

VROS	Verwijzingsindex Rechercheonderzoeksysteem
VtSPN	Voorziening tot Samenwerking Politie Nederland
Wbp	Wet bescherming persoonsgegevens
Wet Bibob	Wet bevordering integriteitsbeoordelingen door het openbaar bestuur
Wet BOB	Wet bijzondere opsporingsbevoegdheden
WID	Wet op de identificatieplicht
Wiv	Wet op de inlichtingen- en veiligheidsdiensten
Wjsg	Wet justitiële en strafvorderlijke gegevens
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum (ministerie van Veiligheid en Justitie)
Wpg	Wet politiegegevens
WRR	Wetenschappelijke Raad voor het Regeringsbeleid
ZSM	Zorgvuldig, snel en op maat
zwacri	zware criminaliteit in georganiseerd verband

www.politieacademie.nl

Informatiegestuurd politiewerk heeft een enorme ontwikkeling doorgemaakt. Vorming van de nationale politie, technologische ontwikkelingen en de alsmaar groeiende informatiestroom hebben hieraan bijgedragen. Dit boek schetst deze ontwikkeling. Het bevat bijdragen van de mensen die in de praktijk bezig zijn met de uitvoering en ontwikkeling van informatiegestuurd politiewerk. Vakmensen, die met alle politiecollega's en partners samen leren hoe het verder gaat. Met dit boek krijgen collega's op straat, leidinggevenden, partners en beleidsmakers zicht op kansen en knelpunten, standpunten, handvatten, dilemma's en ontwikkelingen rond informatiegestuurd politiewerk. Voer voor een professionele discussie daarover. Discussie die helpt het vak verder te versterken in de snel ontwikkelende informatiemaatschappij.

vakmedianet

9 789463 500067

« waakzaam en dienstbaar »

17-006