De organisatie van de opsporing van cybercrime door de Nederlandse politie

De organisatie van de opsporing van cybercrime door de Nederlandse politie

N. Struiksma
C.N.J. de Vey Mestdagh
H.B. Winter

POLITIE & Wetenschap
pro facto
juridisch en bestuurskundig onderzoek / advies / onderwijs

In opdracht van:
Programma Politie & Wetenschap

Foto omslag:
Mark van der Zouw

Ontwerp:
Vantilt Producties & Martien Frijns

ISBN: 978 90 3524 611 9
NUR: 800, 624

Realisatie:
Reed Business, Amsterdam

Inhoud

1

Plaatsbepaling

1.1 Inleiding

Het gebruik van het internet en daarmee de invloed van het internet op de samenleving nemen sterk toe. Er wordt zelfs wel gesproken van een digitale revolutie die, zoals bij alle revoluties het geval is, een grote invloed heeft op de maatschappij als geheel. Ook criminaliteit via het internet komt steeds meer voor. Het internet kent momenteel niet alleen meer dan een kwart miljard websites, maar is ook een knooppunt voor communicatie en informatieverwerking door inmiddels meer dan twee miljard gebruikers, via chatboxen, fora, massale datatransfer, server access, application serving, enzovoort. De schade die met criminaliteit via internet of met behulp van digitale systemen geleden wordt, bedraagt volgens beveiligingsbedrijf Norton alleen in Nederland jaarlijks al zo'n €250 miljoen. Wereldwijd gaat het om $388 miljard. Dat bedrag is een combinatie van verloren geld ($114 miljard) en verloren tijd ($274 miljard), voor het voorkomen en repareren van digitale schade. Het zijn volgens het bedrijf vooral virussen, phishing en hacks van sociale netwerken die schade opleveren.[1] Een effectieve opsporing en aanpak van cybercrime zijn dan ook van groot belang.

1.2 Onderzoeksvragen

De centrale onderzoeksvraag luidt als volgt.

> Hoe is de opsporing van cybercrime bij de Nederlandse politie georganiseerd, wat kan op basis van literatuurstudie worden gekenschetst als ideale organisatie hiervoor en in hoeverre komt de praktijk hiermee overeen?

3 Zie www.norton.com/cybercrimereport.

Het onderzoek bestaat uit drie onderdelen, voortvloeiend uit de centrale onderzoeksvraag, die hieronder worden uitgewerkt.

I. De opsporing van cybercrime in de praktijk

Het eerste deelonderzoek richt zich op de feitelijke organisatie van de opsporing van cybercrime. Aan de orde komen de formatie die de politie hiervoor ter beschikking heeft, prioriteiten, de beschikbare expertise, taakafbakening, taakprofielen en knelpunten. Ook de context (voorgeschiedenis, kaders) komt in dit deel aan de orde. Dit leidt tot de volgende onderzoeksvragen.

1 Binnen welke context speelt de opsporing van cybercrime zich af?
2 Hoe is de opsporing van cybercrime door de Nederlandse politie georganiseerd?
3 Op welke wijze wordt inhoud gegeven aan de opsporing van cybercrime?

II. Organisatiekundige invalshoek

Deelonderzoek 2 richt zich op inzichten die ontleend kunnen worden aan de organisatiekundige literatuur als het gaat om kennisintensieve organisaties. Deze worden vervolgens geprojecteerd op de opsporing van cybercrime door de politie.

4 Welke inzichten geeft de organisatiekundige literatuur over de organisatie van kennisintensieve organisaties?
5 Wat is op basis van de organisatiekunde aan te duiden als de voorkeursvariant voor de organisatie van de opsporing van cybercrime?
6 In welke mate voldoet de praktijk aan de voorkeursvariant?

III. Conclusies en aanbevelingen

Op grond van de theorie, de praktijk en de confrontatie tussen beide wordt een aantal aanbevelingen voor de organisatie van de opsporing van cybercrime geformuleerd.

7 Welke aanbevelingen kunnen op grond van de theorie en de praktijk geformuleerd worden voor de organisatie van de opsporing van cybercrime?

1.3 Onderzoeksmethoden

In het kader van deelonderzoek 1 (de empirische fase) zijn de volgende personen geïnterviewd:

- Thinka Bethlem (teamchef Bureau Digitale Expertise, politie Amsterdam-Amstelland)
- Stef Cusiël (teamchef Bureau Digitale Expertise, politie Groningen)
- Nico van Dalen (plv. teamleider Digitaal & Internet, KLPD)
- Ruud Elderhorst (teamchef Bureau Digitale Expertise, politie Haaglanden)
- Hans Houben (teamchef Bureau Digitale Expertise, politie Zuid-Nederland)
- Henk Klap (programmamanager Cybercrime)
- Frans Kolkman (teamchef Bureau Digitale Expertise Oost-Nederland)
- Daniëlle Laheij (cybercrime-officier van justitie)
- Ton Niesten (teamchef Digitaal, politie Kennemerland)
- Edwin Posthumus (senior analist Open Bronnen, politie Groningen)
- Erica Rietveld (hoofd afdeling Digitale Technologie en Biometrie, NFI)
- Harry Smits (hoofd Digitale Expertise, politie Utrecht)
- Gerrit van der Streek (programmamanager Programma versterking aanpak georganiseerde misdaad, politie Utrecht)
- Wouter Stol (lector Cybersafety, NHL, en bijzonder hoogleraar Politiestudies, OU)
- Gea Wind (plv. teamleider High Tech Crime Team, KLPD)
- Lodewijk van Zwieten (landelijk cybercrime-officier van justitie)

Ten behoeve van deelonderzoek 1 zijn de in de literatuur opgenomen documenten en literatuur bestudeerd.

1.4 Afbakening

1.4.1 Cybercrime in ruime zin

Cybercrime kan worden gedefinieerd als een onderdeel van het scala aan criminele activiteiten waarbij gebruik wordt gemaakt van informatie- en communicatietechnologie (ICT). In een WODC-rapport wordt voor de gehele verzame-

ling van ICT-gerelateerde criminaliteit de term 'hightech crime' gebruikt.[2] Het begrip verwijst naar een veelheid aan (zware en georganiseerde) criminele activiteiten waarbij gebruik wordt gemaakt van ICT. Cybercrime en computercriminaliteit zijn daarvan deelverzamelingen. Cybercrime en hightech crime worden echter ook wel als synoniemen gebruikt. De Raad van Hoofdcommissarissen (RHC) vatte cybercrime in 2005 op als 'alle criminaliteit uitgevoerd met digitale componenten of waarbij het gebruik van digitale componenten een wezenlijke bijdrage heeft geleverd aan de uitvoering van het delict'.

In de literatuur wordt vaak onderscheid gemaakt tussen cybercrime in ruime zin en cybercrime in enge zin. Bij *cybercrime in ruime zin* gaat het om commune delicten als roof, moord, afpersing, kinderporno, fraude, enzovoort, met een ICT-component. Daarbij kan het gaan om het gebruik van ICT-toepassingen in losstaande gevallen (bij een moord zijn bij de voorbereiding sporen achtergelaten op internet, om een voorbeeld te noemen), maar het internet is ook een middel om voor klassieke vormen van criminaliteit een nieuwe en grotere doelgroep aan te boren. Voorbeelden daarvan zijn identiteitsfraude, kinderporno, grootschalige oplichting (phishing, pharming, hijacking), het illegaal en digitaal verspreiden van auteursrechtelijk beschermd muziek- en filmmateriaal, enzovoort. Bij cybercrime in ruime zin is ICT een middel voor de criminele activiteiten. *Cybercrime in enge zin* betreft relatief nieuwe vormen van criminaliteit die zonder ICT niet zouden kunnen bestaan. ICT is niet alleen een middel maar vormt ook het doel. Voorbeelden hiervan zijn de verspreiding van spam, computerhacking en het platleggen van websites, bijvoorbeeld door er extreem grote hoeveelheden gegevens naartoe te sturen.

Dit onderzoek richt zich op cybercrime in ruime zin. Dat betekent dat het zich richt op een substantieel deel van de opsporing door de politie. In veel van de zaken waarbij de recherche opsporingsactiviteiten verricht, is sprake van een ICT-aspect. Bij vrijwel elke zaak worden de computer en de telefoon van een verdachte onderzocht op aanwijzingen. ICT is zo alom vertegenwoordigd dat de vraag kan worden gesteld of een aparte benaming logisch is. ICT is een middel, niet meer dan dat.

2 R.C. van der Hulst & R.J.M. Neve (2008). *High-tech crime, soorten criminaliteit en hun daders. Een literatuurinventarisatie.* Den Haag: Boom Juridische uitgevers. WODC-reeks Onderzoek en Beleid, nr. 264.

1.4.2 Focus op de politie

Bij de aanpak van cybercrime zijn veel organisaties betrokken, zowel binnen als buiten de politie en zowel binnen als buiten de overheid. Zo hebben eind 2007 het team High Tech Crime van de Dienst Nationale Recherche (onderdeel van het KLPD) en telecommunicatiewaakhond OPTA een protocol gesloten dat een efficiënter aanpak van cybercrime mogelijk maakt door de uitwisseling van kennis en informatie. Met netwerken van gekaapte computers, zogeheten botnets, persen zware criminelen mensen af en kunnen persoonsgegevens van computers worden gestolen. Het verspreiden van spam en illegale reclamesoftware gebeurt veelal ook via deze netwerken. Hier komen de twee werelden waarop het team High Tech Crime en de telecomwaakhond OPTA toezicht houden elkaar tegen. Reden voor beide organisaties om de handen ineen te slaan in de strijd tegen cybercrime.

Tussen KLPD/THTC en het Computer Emergency Response Team van de Nederlandse overheid (GOVCERT.nl), dat ondersteuning biedt aan organisaties die een publieke taak uitvoeren over incidenten en ontwikkelingen op het gebied van cybercrime, bestaat frequent overleg. Het GOVCERT brengt regelmatig rapportages uit, waaronder een jaarlijks Trendrapport (*Inzicht in cybercrime: trends & cijfers*). De laatste trendrapporten (2008 en 2009) laten een aanzienlijke groei van de omvang van cybercrime zien, signaleren nog geen verbetering van de veiligheid op het internet en benadrukken het belang van actuele, betrouwbare en accurate technische en juridische informatie. Ook andere bij de opsporing betrokken organisaties zoals het Openbaar Ministerie[3] en het Nederlands Forensisch Instituut (NFI)[4] gaan daarom meer aandacht aan cybercrime besteden.

Vermeldenswaardig is ook de publiek-private samenwerking in het programma Nationale Infrastructuur ter bestrijding van Cybercrime (NICC) en in het Nationaal Adviescentrum Vitale Infrastructuur (NAVI). Het NICC brengt partijen bij elkaar in een Nationale Infrastructuur ter bestrijding van Cybercrime. Het NAVI brengt overheid en bedrijfsleven samen bij het beschermen van de vitale infrastructuur in Nederland.

Het grensoverschrijdende karakter van cybercrime maakt internationale samenwerking noodzakelijk. In de Europese Unie wordt onder meer samenge-

3 Zie onder andere www.om.nl/cybermap/expertmeeting/aanpak_cybercrime_om/.

4 Zie onder andere NFI Info januari/februari 2009 3e jaargang nr. 1, www.forensischinstituut.nl/Images/2009%20NFI-Info%20nummer%201_tcm68-243315.pdf.

werkt in de recent opgerichte European Union Cybercrime Task Force van Europol. De Europese Raad van Ministers wil bovendien een centrale organisatie opzetten om cybercrime aan te pakken.[5] Tot slot is vermeldenswaard dat de Europese Unie samenwerkt met enkele Europese landen in de European Working Party on Information Technology Crime van Interpol.

In dit onderzoek ligt de focus op de Nederlandse politie. Bovenstaande en andere initiatieven in samenwerking met het bedrijfsleven en door andere organisaties dan de Nederlandse politie laten we buiten beschouwing.

1.4.3 *Focus op opsporing*

Wij richten ons in dit onderzoek specifiek op de *opsporing* van aan cybercrime gerelateerde zaken. Op deze plaats benoemen we een aantal andere aspecten van de *aanpak* van cybercrime die buiten de scope van het onderzoek vallen. Door deze hier te benoemen, wordt de afbakening van het onderzoek inzichtelijk.

Voor de politie is internet een middel om zich een algemene informatiepositie te verwerven. Internetsurveillance is hiervan een voorbeeld. In het Programma Aanpak Cybercrime (waarover in hoofdstuk 4 meer) wordt dit als volgt omschreven:

> 'Het op structurele en systematische wijze zoeken naar en gericht volgen van specifieke sites, het volgen van specifieke geschriften, personen en groepen ten behoeve van een keuze of maatregelen getroffen moeten worden en zo ja, welke maatregelen het meest wenselijk zijn. Met internetsurveillance wordt het internet proactief in de gaten gehouden, hetgeen kan leiden tot opsporing, inlichtingmatig volgen (monitoren), handhaving van de openbare orde en bestuurlijk advies.'

Opsporing is dus maar één van de (ondergeschikte) doelen van internetsurveillance. We laten internetsurveillance daarom in het onderzoek verder buiten beschouwing.

Om beter zicht te krijgen op de problematiek en criminaliteit effectief te kunnen bestrijden hebben de ministers van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties en de Nationaal Coördinator Terrorismebestrijding

5 Zie www.computable.nl/artikel/ict_topics/security/3339226/1276896/europa-wil-anticybercrimeorganisatie.html.

(NCTB) opdracht gegeven tot oprichting van het Meldpunt Cybercrime (MCC). Dat heeft geleid tot een website (www.meldpuntcybercrime.nl) die wordt beheerd door het Korps Landelijke Politiediensten (KLPD). Op dit moment is het nog slechts mogelijk meldingen over kinderporno en terrorisme (zoals radicale en terroristische uitingen, oproepen tot haat en geweld, fondsenwerving voor terroristische doeleinden) via deze website door te geven. Het KLPD zorgt dan voor het doorsturen van de meldingen naar het juiste loket. Daarnaast werkt het meldpunt nauw samen met andere partners binnen het internetdomein, zoals providers. Ook dergelijke aspecten laten we in het onderzoek buiten beschouwing door ons specifiek te richten op de *opsporing* van cybercrime door de politie.

1.5 Leeswijzer

In hoofdstuk 2 van dit rapport wordt de context van het onderwerp van onderzoek beschreven. Daarbij gaat het om het wettelijk kader en de voorgeschiedenis (de opsporing van cybercrime sinds eind jaren tachtig). Onderzoeksvraag 1 wordt in dit hoofdstuk beantwoord. Hoofdstuk 3 is een empirisch hoofdstuk, waarin de feitelijke (organisatie van de) opsporing van cybercrime wordt beschreven. Hierin wordt ingegaan op de onderzoeksvragen 2 en 3. Hoofdstuk 4 is organisatiekundig van aard. De onderzoeksvragen 4 en 5 worden in dit hoofdstuk beantwoord. Hoofdstuk 5 ten slotte bevat de conclusies en aanbevelingen, waarmee wordt ingegaan op de onderzoeksvragen 6 en 7.

2 Context

2.1 Inleiding

In dit hoofdstuk wordt de context van de huidige opsporing van cybercrime in Nederland beschreven. Deze beschrijving is zowel inhoudelijk (wetten en bevoegdheden) als chronologisch van aard.

2.2 *Wettelijk kader*

2.2.1 *Inleiding*

De wetgever houdt zich intensief bezig met de toenemende dreigingen van cybercrime en de problemen die zij opleveren voor de opsporingsdiensten. Het in 2010 gepubliceerde conceptwetsvoorstel *Versterking bestrijding computercriminaliteit* is hiervan een goed voorbeeld. De kritiek op dit voorstel van organisaties als Bits of Freedom benadrukt het probleem van onzekerheid rond de juridische bevoegdheden van de opsporingsdiensten en de juridische status van cybercriminaliteit.[6] Ook een brief van de minister van Veiligheid en Justitie over de wenselijkheid en mogelijkheid van een algeheel strafrechtelijk verbod op de verspreiding van extreem gewelddadig beeldmateriaal[7] en de brief van de minister van Veiligheid en Justitie over het WODC-onderzoek *High-tech crime en voorlichting* zijn in dit kader relevant.[8]

In de volgende subparagrafen gaan we in op verschillende relevante wetten, bevoegdheden en jurisprudentie op het gebied van de opsporing van cybercrime.

6 Zie onder andere http://oerlemansblog.weblog.leidenuniv.nl/2010/07/30/wetsvoorstel-versterking-computercrimina.

7 Brief (nr. 279) van de minister van Veiligheid en Justitie aan de Voorzitter van de Tweede Kamer der Staten-Generaal, Den Haag, 28 juni 2010: https://zoek.officielebekendmakingen.nl/kst-28684-279.html.

8 Zie https://zoek.officielebekendmakingen.nl/kst-28684-275.html.

2.2.2 *Wetten en bevoegdheden*

In 1988 bracht de commissie-Franken haar rapport uit onder de titel *Informatietechniek en strafrecht*. Onderdeel hiervan vormde het voorstel om het zogenaamde 'hacken', nu 'computervredebreuk' geheten, strafbaar te stellen. In 1993 werd de Wet computercriminaliteit (WCC) van kracht, onder meer gebaseerd op het rapport van de commissie-Franken. De huidige WCC is sinds 1 september 2006 van kracht. De belangrijkste wijzigingen in vergelijking met de wet van 1993 waren de volgende.

- Bij computervredebreuk is elke vorm van wederrechtelijk binnendringen strafbaar, ook als daarbij geen beveiliging wordt doorbroken (zoals het geval was).
- De definitie van virussen en malware is aangescherpt: een programma moet bedoeld zijn om schade aan te richten, maar niet per se (zoals in de oude wet) 'door zichzelf te vermenigvuldigen in een geautomatiseerd werk'.
- De maximale straf voor veel delicten is verhoogd.

Per 1 januari 2010 is de WCC uitgebreid met drie nieuwe strafbaarstellingen met betrekking tot kinderporno en kindermisbruik. Het is nu strafbaar om via internet naar kinderporno te kijken en om aan kinderen seksuele handelingen te tonen voor seksuele doeleinden. Daarnaast is *grooming* (het bewust benaderen en verleiden van jongeren op internet met als doel het plegen van seksuele handelingen) strafbaar gesteld.

Op 1 september 2004 is de Wet vordering gegevens telecommunicatie van kracht geworden, met nieuwe bevoegdheden ten aanzien van gegevens over (al dan niet verdachte) gebruikers van telecommunicatie.

Specifieke digitale opsporingsmethoden zijn het in beslag nemen van elektronische gegevens zoals bestanden. Bij huiszoekingen kunnen elektronische gegevens in beslag worden genomen. Art. 125i Wetboek van Strafvordering (Sv) bepaalt dat de rechter-commissaris het bevel kan geven dat hem toegang moet worden gegeven tot elektronische gegevens, of dat hiervan een kopie wordt gemaakt. Dit bevel mag niet worden gegeven aan de verdachte, omdat die niet verplicht is mee te werken aan zijn eigen veroordeling. Een verdachte mag ook niet worden bevolen om wachtwoorden te onthullen. Als anderen, zoals de provider of de systeembeheerder, het wachtwoord toevallig weten, moeten ze het op grond van art. 125k Sv wel afgeven. De politie mag vrijwel alle elektronische communicatie aftappen en opnemen. Op grond van de Telecommunicatiewet kan de politie, maar ook opsporingsdiensten zoals de AIVD,

met een gerechtelijk bevel eisen dat een internetprovider naam en adres van een abonnee aan hen bekendmaakt. Ook kunnen ze eisen dat alle e-mail van deze abonnee wordt gekopieerd naar een speciale mailbox of dat gesprekken via bijvoorbeeld MSN Messenger of Facebook opgenomen worden. Voor mobiele telefonie is opnemen van alle gesprekken en vastleggen wie wanneer met wie belde mogelijk.[9]

2.3 *Voorgeschiedenis*

In 1996 bood de beleidsadviesgroep Computercriminaliteit de visienota *Op weg naar… digitaal rechercheren* aan de Raad van Hoofdcommissarissen aan. Naar aanleiding van de uitkomsten van een themabijeenkomst werd eind 1997 het Nationaal Actieprogramma *Op weg met… digitaal rechercheren* opgesteld. Hierin werden voor de periode 1998-2000 aanbevelingen en verbetervoorstellen gedaan voor de verdere ontwikkeling van digitaal rechercheren binnen de Nederlandse politie. De eerste versie van het Nationaal Actieprogramma Digitaal Rechercheren werd in januari 1998 aan de Raad van Hoofdcommissarissen aangeboden. Feitelijk was iedereen het erover eens, zo werd bij de herziening in 2002 aangegeven, dat men niet meer om digitaal rechercheren heen kon. 'Investeren op dit onderwerp is voor komende jaren absolute noodzaak.' Er werd onder meer voorgesteld om te investeren in een verbreding van kennis op het gebied van ICT binnen de basispolitiezorg en in het verder opbouwen en ontwikkelen van specialismen.

In 2001 werd de tweede versie van het Nationaal Actieprogramma vastgesteld, getiteld *Digitaal blauw. Aan de slag met digitaal rechercheren!* Het actieprogramma stelde vast dat grote investeringen nodig zijn in mensen en middelen.

> 'Hoewel in grote lijnen de inhoud van het eerste actieprogramma uit 1998 nu vandaag de dag nog overeind staat, zijn er door voortschrijdend inzicht en de actualiteit wel enkele gewijzigde inzichten te benoemen. De hoofddoelstelling om basiskennis over digitaal rechercheren tot in alle haarvaten van de Nederlandse politie- en justitieorganisatie over te brengen en bij de uitvoering van activiteiten aansluiting te vinden bij de primaire operationele processen binnen de regiokorpsen is ongewijzigd gebleven.'

9 Zie http://www.iusmentis.com/beveiliging/hacken/opsporing-politie/.

Er wordt een 'kennislagenmodel' voorgesteld, bestaande uit vijf kennislagen.

Tabel 2.1: Kennislagenmodel

Kennislaag 1	Algemeen deskundigheidsniveau, dat aanwezig moet zijn binnen de basispolitiezorg en recherche, het strategisch en tactisch/operationeel management op het gebied van digitaal rechercheren.
Kennislaag 2	Deskundigheid op het niveau van de taakaccenthouder binnen de basispolitiezorg of recherche. Afhankelijk van de schaalgrootte kunnen dergelijke functionarissen op het niveau van een lokale unit, een district of op regionaal niveau worden aangetroffen.
Kennislaag 3	De digitaal-rechercheurs, internet-rechercheurs en ICT-specialisten op mbo-niveau binnen dit werkveld. Afhankelijk van de schaalgrootte en de problematiek zouden deze deskundigen aangetroffen kunnen worden op verschillende (geconcentreerde) niveaus in de politieorganisatie.
Kennislaag 4	De forensische ICT-specialisten/ontwikkelaars en deskundigen op minimaal hbo- en academisch niveau, alsmede recherche-, beleids- en juridische adviseurs binnen de politie op dit onderwerp. Kern van de activiteiten ligt bij het ontwikkelen van innovatieve (digitale) recherche- en opsporingsmethoden, het (doen) opzetten, uitvoeren en/of begeleiden van research & development-trajecten en het leveren van kwalitatief hoogwaardige expertise en advisering.
Kennislaag 5	Externe deskundigheid, waarvan zo weinig gebruik hoeft te worden gemaakt dat het om bedrijfseconomische redenen niet zinvol is die binnen de politieorganisatie permanent aanwezig te hebben.

In de nota *Digitaal opsporen – beleid inzake de bestrijding van criminaliteit in een gedigitaliseerde maatschappij* van het Landelijk Project Digitaal Opsporen (LPDO), die in juli 2005 het licht zag, wordt geconstateerd dat cybercrime een onderdeel is van het gehele spectrum van crimineel gedrag en dat digitale opsporing onderdeel moet zijn van het gehele spectrum van de opsporing, als een normaal aspect van de dagelijkse politiepraktijk. Dit vormde een breuk met het verleden, waarin digitaal rechercheren vooral als een specialisme werd gezien. De politie moest niet langer uitsluitend investeren in specialistische functies. Ook van de opleiding moest digitale opsporing een natuurlijk onderdeel vormen. Deze aanbevelingen zijn overgenomen door de Raad van Hoofdcommissarissen.

In april 2007 verscheen het document *Programma aanpak cybercrime* (PAC). Het PAC is een van de vijf intensiveringsprogramma's van de RHC en is erop gericht de korpsen te ondersteunen in de technologische (digitale) ontwikkelingen die zich in de maatschappij voordoen. Het beleid uit 2005 is leidend voor het PAC. Het PAC beperkt zich niet tot opsporen maar richt zich op alle processen. Een van de doelstellingen van het PAC is dat de Nederlandse samenleving met succes een beroep kan doen op de politie bij de bestrijding van cybercrime.

In het Regeerakkoord van het kabinet-Rutte (2010) wordt een integrale aanpak van cybercrime aangekondigd. Die is uitgewerkt in de *Nationale Cyber Security Strategie* (2011) waarin sprake is van de intensivering van de opsporing en vervolging van cybercrime.

> 'De zich snel ontwikkelende cybercriminaliteit vereist effectieve bestrijding om het vertrouwen in de digitale samenleving hoog te houden. Hiertoe moeten de uitvoeringsorganisaties in de strafrechtelijke keten (voornamelijk de politie en andere opsporingsdiensten maar ook het Openbaar Ministerie en de rechterlijke macht) die belast zijn met de bestrijding van cybercrime, beschikken over voldoende specialisten. Het gaat hierbij om de zeer specialistische behandeling van complexe zaken (hightech crime) en om behandeling van de meer eenvoudige (high volume) zaken die het vertrouwen in ICT van burgers, MKB en het overig bedrijfsleven aantasten. Doel is dat de aangiftebereidheid en de pakkans stijgen en dat overtreders steviger worden aangepakt. Ook met internationale samenwerking wordt grensoverschrijdende criminaliteit beter aangepakt.'[10]

Binnen het huidige budgettaire kader van de politie, zo wordt gesteld, vindt de komende jaren een verschuiving plaats naar meer recherchecapaciteit en daarbinnen ook richting opsporing en vervolging van cybercriminaliteit. Het gaat hierbij om internetsurveillanten en -specialisten binnen de regio's en bij het team hightech crime van het KLPD.

Medio augustus 2011 is het rapport *De inrichting van Digitale Expertise bij de Nederlandse politie* uitgebracht in opdracht van het Programma Aanpak Cybercrime en de Expertgroep Digitaal Opereren. De huidige inrichting van de opsporing van cybercrime wordt daarin beschreven evenals een drietal scenario's voor de toekomstige inrichting ervan.

Scenario 1: Gedecentraliseerd en gedeconcentreerd

Op tien locaties wordt een unit DE (Digitale Expertise) gestationeerd. Een unit is te beschouwen als een afdeling van een territoriale eenheid of meervoud daarvan. De inzet is vooral reactief, op basis van door de tactiek gestelde vraag. Het komt voor dat DE-medewerkers ad hoc worden toegevoegd aan tactische teams bij een tekort aan capaciteit. Er is geen (landelijke) centrale aansturing van DE. Er is geen onderlinge personele uitwisseling tussen de units in het land; de units werken betrekkelijk eigenstandig. Het uitvoering geven aan werkzaamheden in het teken van innovatie is de verantwoordelijkheid van iedere unit; er is alleen beperkt landelijk beleid op nationaal niveau. Er is geen zeggenschap vanaf het nationale niveau over de units.

10 Pagina 8.

Scenario 2: Gecentraliseerd en gedeconcentreerd

Bij dit scenario – dat voortbouwt op scenario 1 – wordt een landelijke expertiseorganisatie voor Digitale Expertise opgericht, van waaruit naar rato DE wordt uitgezet naar tien politiekorpsen dan wel samenwerkingsverbanden. Deze landelijke entiteit krijgt tevens de beschikking over een forensisch computerlaboratorium. Afhankelijk van de vraag kan extra (inhoudelijke) capaciteit worden toegedeeld vanuit de landelijke expertiseorganisatie. Op deze manier is er aansluiting bij de cyberaanpak van de regiokorpsen en (gedeeltelijk) bij de compacte rijksdienst en de integrale aanpak van cybercrime. De tien territoriale eenheden worden door de landelijke expertiseorganisatie bediend, van daaruit krijgt elk de beschikking over een substantieel aantal medewerkers van de landelijke entiteit om de regio bij te staan in het kader van Digitale Expertise. Medewerkers van de unit maken echter deel uit van de landelijke expertiseorganisatie, niet van de regio.

Scenario 3: Gecentraliseerd en geconcentreerd

Een landelijke expertiseorganisatie voor alle expertise wordt in het leven geroepen als een centraal geleid onderdeel van de politie. De oriëntatie van deze landelijke entiteit is echter breder en de opzet en invulling van de landelijke expertiseorganisatie gaat verder dan in het vorige scenario. Ook hier wordt de landelijke organisatie zo georganiseerd dat elk van de tien territoriale eenheden wordt voorzien van een unit DE. Elk politiekorps of samenwerkingsverband beschikt zo over basiscapaciteiten ten behoeve van ondersteuning van de opsporing. Belangrijke verschillen ten opzichte van de eerste twee scenario's zijn ten eerste de nadrukkelijke nevengeschiktheid van DE ten opzichte van de territoriale eenheden en ten tweede de samenvoeging van alle 'ondersteunende' entiteiten (operationele expertises) in deze ene organisatie. Een derde verschil is dat de interactie tussen de landelijke expertiseorganisatie en de territoriale eenheden in het teken staat van een primair proces van DE zelf.

2.4 Conclusie

In dit hoofdstuk is gebleken dat de voorloper van het begrip cybercrime al sinds eind jaren tachtig onderwerp van onderzoek en discussie is. Internet en cyberspace bestonden nog nauwelijks, en daarmee cybercrime ook niet, maar de eerste computers waren al wel onderwerp van misbruik. De commissie-Franken bracht er het rapport *Informatietechniek en strafrecht* over uit. Vooral sinds begin jaren negentig kwam de digitale revolutie in een stroomversnelling en volgden rapporten elkaar op. Er werden Nationale Actieprogramma's over opgesteld, waarvan vooral het programma uit 2001 nog lang invloed had, onder meer door het daarin geïntroduceerde kennislagenmodel. In de loop van de tijd zijn ook de opsporingsbevoegdheden toegenomen. In 2004 is de Wet vordering gegevens telecommunicatie van kracht geworden. Ook op grond van het Wetboek van Strafvordering zijn de bevoegdheden uitgebreid.

De in dit hoofdstuk geschetste context vormt de opmaat naar een beschrijving van de huidige organisatie van de opsporing van cybercrime. Dit wordt in het volgende hoofdstuk uitgewerkt.

3 De huidige opsporing van cybercrime

3.1 Inleiding

In dit hoofdstuk wordt de praktijk van de opsporing van cybercrime door de politie beschreven. Daarbij gaan we achtereenvolgens in op de organisatie-inrichting, de formatie, de taakprofielen, de prioriteiten, de expertise, de kwaliteit en de bevoegdheden.

3.2 Organisatie-inrichting

3.2.1 Centraal

Binnen de Dienst Nationale Recherche (DNR), onderdeel van het KLPD, houden twee teams zich bezig met de bestrijding van cybercrime. Dat gebeurt door het team High Tech Crime (THTC) en door het team Digitaal & Internet (D&I).

D&I doet enerzijds aan research & development (R&D, 70-80% van de tijd/capaciteit) en biedt daarnaast ondersteuning aan regio's, aan THTC en aan de negentien onderzoeksteams van DNR. De negentien onderzoeksteams van DNR hebben alle een digitale expert. D&I kent de volgende typen functies.

- Internetrechercheurs (kunnen scripts schrijven, alle ruwe data analyseren, enzovoort). Ze worden ingeschakeld om andere teams te ondersteunen.
- Programmeurs. Ze ontwikkelen tools en doen aan R&D. Ze adviseren soms ook in speciale zaken.
- Facilitaire digitale rechercheurs. Kunnen IP-data analyseren, dringen binnen in systemen, enzovoort.
- Overig: beleidsadviseurs, juristen (die bijvoorbeeld jurisprudentie bijhouden), interceptiecoördinatoren.

Als een regionaal digitaal team niet over voldoende expertise beschikt, kan het D&I inschakelen, dat zowel van afstand als op locatie ondersteuning kan bieden. Dat gebeurt echter niet vaak, jaarlijks ongeveer vijftien keer. Volgens responden-

ten komt dit doordat men doorgaans zelf over de benodigde expertise beschikt en anderzijds omdat er een drempel zou kunnen zijn om D&I in te schakelen, omdat dit als een brevet van onvermogen beschouwd zou kunnen worden.

D&I houdt zich niet bezig met vervolging, het ondersteunt alleen. Alleen zaken waarin sprake is van 'cybercrime in enge zin', worden in principe zelfstandig door D&I afgedaan. Hierbij gaat het bijvoorbeeld om gevoelige of complexe hack-zaken en te kraken USB-sticks.

Anders dan D&I, neemt het THTC een onderzoek volledig over van een regio als een zaak de expertise of omvang van de regio te boven gaat. Het team behandelt in principe complexe (hightech) cybercrimezaken van nationaal en internationaal belang. In veel gevallen blijkt overigens niet de complexiteit van de cybercrimezaken de doorslag te geven, maar vooral het nationale of internationale belang van een zaak. Een voorbeeld van een recente zaak van nationaal belang die door THTC is opgepakt, betreft de zaak DigiNotar. Hierbij was de betrouwbaarheid van een groot deel van de digitale communicatie tussen burgers en overheid in het geding (zie kader). De technische complexiteit van deze zaak lijkt echter niet bijzonder hoog te zijn. De door DigiNotar toegepaste methode en techniek van het uitgeven van certificaten is niet complex en is op zichzelf betrouwbaar. Het probleem bij DigiNotar lag dan ook niet in de complexiteit of de onbetrouwbaarheid van de toegepaste techniek, maar in de onbetrouwbaarheid van de eigen organisatie. Ook bij de vraag of de opsporing in dit geval een nationaal belang dient, kan een vraagteken worden gezet. De betrouwbaarheid van de digitale communicatie tussen overheid en burger wordt in dit geval namelijk vooral gediend door het inschakelen van een betrouwbare organisatie (het vervangen van DigiNotar door een andere betrouwbare certificatieautoriteit) en niet door de opsporing van criminelen die misbruik hebben gemaakt van DigiNotars onbetrouwbare organisatie. Het THTC ondersteunt daarnaast de regionale recherche met cybercrime-

DigiNotar was een Nederlandse commerciële certificatieautoriteit. Het bedrijf verzorgde de PKIoverheid-certificaten voor grote delen van de Nederlandse overheid, waaronder die van DigiD en de RDW. In juni 2011 lukte het een hacker in te breken bij DigiNotar. Als gevolg van deze hack gaf DigiNotar op 10 juli 2011 een certificaat voor het Google-domein google.com uit aan onbekende personen in Iran. Dit certificaat zou mogelijk gebruikt kunnen zijn voor een cyberaanval tegen Gmail. Eind juli 2011 raakte DigiNotar bekend met de uitgifte van dit certificaat, maar

maakte daar geen melding van. Een rapport van het bedrijf Fox-IT bracht diverse fouten in de procedures en systemen van DigiNotar aan het licht. De uitkomsten van dit onderzoek hadden als gevolg dat het aanvankelijke standpunt van de overheid dat de PKIoverheid-certificaten veilig waren, werd ingetrokken en dat de overheid uiteindelijk het vertrouwen in DigiNotar volledig opzegde.

expertise (niet alleen ad hoc, maar ook door het aangeven van methoden en technieken (tooling)). Ook verricht het team algemeen, op kennisvermeerdering gericht onderzoek. De taakafbakening met de regionale digitale expertiseteams wordt bepaald door het hightech karakter van het informatieverzoek van de regionale recherche. Er is geen duidelijke taakafbakening met andere R&D-afdelingen binnen en buiten de politie (o.a. D&I, IPOL, NFI). Het team doet aan onderzoek op basis van de door de aangeboden zaken bepaalde algemene kennisbehoefte.

Jaarlijks voert het THTC ongeveer twee grote zaken en vier kleinere zaken uit. Uit het NCSS blijkt dat in 2014 door het team twintig grote zaken moeten worden gedaan. Volgens betrokkenen is dat een reëel aantal. Het is momenteel niet zo dat er allemaal zaken op de plank liggen, maar op dit moment wordt er ook niet veel tijd en moeite gestoken in het verwerven van meer zaken.

3.2.2 *Decentraal*

De feitelijke opsporing van cybercrime binnen de regio's is gestoeld op twee principes: integratie en concentratie van expertise. Er zijn bij regionale korpsen geen rechercheteams die zich alleen maar richten op cybercrime. Opsporingsonderzoeken worden verricht door reguliere rechercheteams (al dan niet door Teams Grootschalige Opsporing, TGO's).

Regio's hebben daarnaast de beschikking over (meer of minder specialistische) digitale expertise. Dit is binnen regio's op verschillende wijzen ingevuld, al dan niet in bovenregionaal verband.

Het oorspronkelijke idee was dat bij zeven Bureaus Digitale Expertise, BDE's, (vooral) digitale specialisten op hbo-niveau werkzaam waren, terwijl Bureaus Digitale Recherche (BDR's) gevormd werden door experts op mbo-niveau. De BDE's deden de complexere digitale klussen en de BDR's de minder complexe (zoals het uitlezen van mobiele telefoons en het veiligstellen van computers). Vaak (maar niet altijd) waren de BDE's bovenregionaal georganiseerd. Bij sommige BDE's werden ook minder complexe zaken opgepakt en zij vormden daarmee een combinatie van BDE en BDR. De namen 'BDE' en 'BDR' worden in sommige regio's nog wel gehanteerd, maar het zuivere onderscheid tussen beide is verwaterd.

Lange tijd is in de praktijk het onderscheid tussen BDE en BDR gehanteerd. Het onderscheid tussen BDR's en BDE's is in de loop van de tijd vervlakt. Voor de zuiverheid gebruiken we in dit rapport daarom de verzamelnaam Team Digitale Opsporing (TDO).

Uit de naamgeving blijkt al dat deze teams zich niet alleen met 'cybercrime' bezighielden, maar met digitale zaken in bredere zin. In het eerder aangehaalde rapport *De inrichting van Digitale Expertise bij de Nederlandse politie* worden vijf vakgebieden binnen de digitale expertise onderscheiden:[11]

1 data op gegevensdragers als telefoons en computers;
2 multimedia (beeld en geluid);
3 mobiele apparatuur (robots, autonavigatie, domotica);
4 interceptie (onderscheppen en opvangen van telecommunicatie);
5 internet.

Op elk van de vakgebieden gaat het om drie hoofdtaken: veiligstellen (van bewijs in een digitale omgeving), veredelen (het maken van digitale kopieën en het bewerken van data, zodanig dat daar bewijs uit kan worden verkregen) en analyseren (het beschikbaar stellen van data voor tactische doeleinden).

Een aantal regio's heeft geen TDO maar (een bescheiden aantal) digitale experts ondergebracht binnen de recherchedivisie, bijvoorbeeld in de afdeling Forensische Opsporing.

11 PAC 2011, p. 21.

Sommige regio's kennen behalve de centraal (binnen de regio of bovenregionaal) georganiseerde digitale expertise ook taakaccenthouders binnen districten. De taakaccenthouders zijn verantwoordelijk voor het bulkwerk, zoals het uitlezen van mobiele telefoons en het veiligstellen van camerabeelden. Als hun expertise niet volstaat, wordt opgeschaald naar een TDO. De taakaccenthouders zijn alleen in hun eigen district actief. Ze worden soms ook ingeschakeld voor andere typen zaken, bijvoorbeeld zaken van het Team Grootschalige Opsporing (TGO), maar in principe houden ze zich met digitale kwesties bezig.

Sommige respondenten vinden de aanwezigheid van dergelijke taakaccenthouders binnen districten van meerwaarde omdat daarmee het contact met de 'basis' (reguliere rechercheteams, basispolitiezorg) beter is. Het TDO vormt daardoor minder een eiland, de lijnen zijn korter en taakaccenthouders kunnen proactiever werken. Een nadeel van taakaccenthouders is dat ze hiërarchisch onder een lijnchef vallen en niet onder de chef van het TDO, waardoor ze ook niet door de chef van het TDO zijn aan te sturen.

3.3 *Formatie*

In deze paragraaf gaan we in op de invulling van de digitale expertise per regio en op de daarmee gepaard gaande formatieplaatsen. We sluiten aan bij het kennislagenmodel dat weergegeven is in §2.3 van dit rapport. Een TDO waarin (ook) een substantiële deskundigheid op hbo-niveau aanwezig is, duiden we aan als *TDO kennislaag* 4 (afgekort TDO4). Is dat niet het geval en heeft het team (vrijwel) alleen de beschikking over deskundigheid op mbo-niveau, dan benoemen we dat als *TDO kennislaag* 3 (TDO3).

Negentien regio's beschikken over een TDO4, meestal in bovenregionaal verband. De vier grootste korpsen (Amsterdam-Amstelland, Rotterdam-Rijnmond, Haaglanden en Utrecht) hebben een eigen TDO4. Daarnaast zijn er bovenregionale teams in Noord- en Oost-Nederland. Zuid-Nederland heeft een TDO dat vooral als beheerseenheid fungeert en zorg draagt voor bijvoorbeeld gezamenlijke inkoop, cursussen en opleidingen. De meeste van deze teams hebben een omvang van rond de tien fte. Haaglanden (18) en Rotterdam (37) hebben er duidelijk meer.

In Oost- en Zuid-Nederland hebben alle regio's daarnaast ook nog een 'eigen' TDO3. De omvang hiervan is gemiddeld ongeveer vijf fte. Verder zijn er nog enkele regio's die uitsluitend een TDO4 of een TDO3 hebben of binnen de divisie recherche enkele cybercrime-experts binnen de forensische

opsporing hebben. De aantallen zijn gebaseerd op informatie van gesprekspartners.

In onderstaande tabel is het bovenstaande samengevat. Hieruit blijkt dat de totale formatieomvang voor de opsporing van cybercrime door de politie per 2011 iets minder dan 300 fte bedraagt.

Tabel 3.1: Formatieomvang bij de politie voor de opsporing van cybercrime

Regio	Aantal regio's[12]	Formatie
Centraal (KLPD)		63
TDO4, bovenregionaal	15	26,5
TDO4, regionaal	4	74
TDO3	13	58
Onderdeel FO, kennislaag 3	5	29
Taakaccenthouders, kennislaag 2	6	42
Totaal		**292,5**

3.4 Taakprofielen

TDO's zijn faciliterend aan de 'reguliere' rechercheteams. Ze worden op verzoek van een TGO of regulier rechercheteam ingeschakeld. Het is dus niet aan de TDO's om te bepalen of digitale expertise in concrete zaken nuttig of noodzakelijk is. Soms maakt een digitale expert actief deel uit van een TGO of regulier rechercheonderzoek, waarbij hij aangeeft welke gegevens veiliggesteld moeten worden en hoe die veredeld en vervolgens geanalyseerd zouden moeten worden. Vaker wordt aan het TDO een 'zoekvraag' voorgelegd, waarna het TDO in de vorm van een rapportage een antwoord hierop formuleert. Het is voor de digitale expert dan van belang om de context van een zaak te kennen, zodat hij gerichter kan zoeken. Deze contextinformatie wordt echter niet altijd gegeven. Vaak is het volgens een respondent van een TDO een kwestie van 'dit is de computer, red je er maar mee'.

De inschakeling of raadpleging van een digitale expert maakt in veruit de meeste regio's geen deel uit van de protocollen die van kracht zijn bij de vorming van TGO's. Een TGO start, zo blijkt uit het Programma Versterking Opsporing (PVO), zodra er sprake blijkt te zijn van een kapitaal misdrijf. Dit is een – moge-

12 Opgeteld bevat deze kolom (fors) meer dan het totale aantal van 25 politieregio's. Dat komt doordat zich in veel regio's een combinatie van de verschillende varianten voordoet.

lijk – opzettelijk levensdelict, zeer ernstig zedendelict, brandstichting met ernstige gevolgen, gijzeling, ontvoering en andere misdrijven tegen de lichamelijke integriteit waarop een strafbedreiging van twaalf jaar gevangenisstraf of meer staat – met een (te verwachten) grote maatschappelijke impact en waarbij geen ondubbelzinnig daderschap kan worden vastgesteld. TGO's worden bemenst vanuit een Vaste Kern Leidinggevenden (VKL) en Vaste Kern Uitvoerenden (VKU). In een zeer beperkt aantal regio's maakt een digitale rechercheur van een TDO deel uit van de VKU. Digitale experts zijn in geen enkele VKL vertegenwoordigd. Volgens een respondent is het in zijn regio altijd 'vechten' om een digitale expert in een TGO te krijgen. Idealiter gaat een digitale expert mee naar zoekingen om gegevens veilig te stellen, teneinde deze te kunnen veredelen en analyseren. Dit gebeurt in de praktijk slechts sporadisch. In slechts een enkel TDO is een lid van het TDO standaard aanwezig bij het eerste werkoverleg in een nieuw TGO.

Het feit dat de TDO's worden ingeschakeld naar aanleiding van ondersteuningsverzoeken heeft tot gevolg dat het risico bestaat dat niet in alle zaken waarin digitale expertise gewenst of vereist is, deze ook daadwerkelijk wordt ingeroepen. Onbekendheid met (de taken en werkzaamheden van) het TDO maakt dat hiervan sprake kan zijn, net als onbekendheid met digitale fenomenen. Onbekend maakt ook in dit geval onbemind, hetgeen ertoe kan leiden dat digitale expertise ten onrechte niet wordt ingeschakeld. Om dit te ondervangen doen veel TDO's aan actieve voorlichting binnen hun regio('s) over hun taken en mogelijke ondersteuning.

Late inschakeling van digitale expertise kan funest zijn. Zoals een respondent verwoordde: 'Een lijk blijft wel liggen maar digitale gegevens zijn zo weg.' Als een rechercheur in alle onschuld een computer uitzet, kan dit betekenen dat relevante data als het werkgeheugen van een computer onherroepelijk verdwenen zijn. Zeker voor de eerste taak van digitale experts, het veiligstellen van gegevens op bijvoorbeeld computers, geldt dat fouten of niet uitgevoerde handelingen niet meer hersteld of uitgevoerd kunnen worden.

3.5 Prioriteit

De aanpak van cybercrime heeft binnen de politie steeds meer prioriteit. Dat blijkt onder meer uit het cybercrimeprogramma van de politie en uit de forse uitbreiding van de formatie voor de opsporing van cybercrime. Desondanks hoeven niet veel TDO's prioriteiten te stellen om de werk- en zaakdruk aan te kunnen. Eén TDO heeft een (structurele) achterstand van drie maanden. Als een

TDO in verband met het aanbod van zaken wel prioriteiten moet stellen, dan sluiten deze prioriteiten grotendeels aan bij de algemene korpsprioriteiten. Een zaak van een TGO heeft altijd prioriteit. Daarnaast heeft een enkel TDO aanvullende eigen prioriteiten, zoals de vermissing van minderjarigen en het belang van een snelle ondersteuning (bijvoorbeeld omdat anders data verloren gaan of omdat een verdachte anders in vrijheid wordt gesteld).

Bovenstaande heeft betrekking op cybercrime in ruime zin, oftewel een commuun delict met digitale componenten. Cybercrimezaken in enge zin hebben een lage prioriteit bij de besluitvormende organen (stuurgroep Recherche, Openbaar Ministerie). De cybercrime-officieren van justitie in de arrondissementen hebben niet of nauwelijks zaken. Soms tot frustratie van TDO's worden zaken met betrekking tot skimming ('zaak voor de banken', aldus een respondent van een TDO), ddos-aanvallen, digitale stalking en hacking niet of nauwelijks opgepakt. Hieraan wordt door de besluitvormende organen geen prioriteit gegeven. 'Bloed gaat voor bytes,' aldus een respondent. Het Landelijk Parket, dat in de persoon van de landelijke cybercrime-officier de onderzoeken van het THTC leidt en voorbrengt, heeft – zoals eerder aangegeven – wel voldoende zaken van cybercrime in enge zin. Het team heeft geen last van concurrerende prioriteiten, omdat het zich uitsluitend bezighoudt met hightech crime.

Het THTC heeft capaciteit om circa drie grote zaken te behandelen. Er moeten daarom regelmatig keuzes worden gemaakt en tussentijds (op grond van politieke keuzes) nieuwe prioriteiten worden gesteld waardoor lopende zaken blijven liggen. De DigiNotar-zaak is hiervan een voorbeeld: toen deze zaak zich aandiende, vormde de maatschappelijke onrust reden om er prioriteit aan te geven zodat andere zaken (tijdelijk) stil kwamen te liggen. In algemene zin worden prioriteiten gesteld op basis van de actualiteit, maatschappelijke onrust of wanneer het een nieuw onderwerp betreft waarvan het nuttig is om er ervaring mee op te doen. Of een cybercrimeonderzoek wordt opgepakt ligt ook aan de beschikbare capaciteit. Als zich een nieuwe zaak aandient, kan deze bij onvoldoende capaciteit niet worden onderzocht. Tenzij er, zoals aangegeven, sprake is van maatschappelijke onrust of politieke gevoeligheid.

3.6 *Expertise en kwaliteit*

De drie hoofdtaken van een digitale expert, te weten veiligstellen, veredelen en analyseren van digitale gegevens, stellen verschillende eisen aan de benodigde expertise. In algemene zin kan gesteld worden dat voor het veiligstellen in kwali-

tatief opzicht de minste expertise nodig is. Mbo-niveau volstaat doorgaans. Voor het veredelen en analyseren van digitale gegevens kan hbo-niveau gewenst zijn.

Uit de vorige paragraaf blijkt dat de aanwezige expertise binnen regio's varieert, hetgeen zich bijvoorbeeld manifesteert in TDO3 en TDO4. Ook tussen de verschillende TDO4's bestaat verschil in kwaliteit, zo wordt door diverse respondenten aangegeven. Er zijn innoverende teams met hooggekwalificeerde ICT'ers en er zijn teams met vooral 'om- en bijgeschoolde dienders'.

Als een TDO niet zelf over de benodigde expertise beschikt, kan – zoals aangegeven – de hulp van het team D&I van het KLPD worden ingeroepen. Dit gebeurt echter weinig. Daarnaast kan het NFI worden ingeschakeld. Het betreft hier zaken die zijn te classificeren binnen kennislaag 5, waarin sprake is van dermate specialistische kennis, *tools* of apparatuur dat het bedrijfseconomisch niet uit kan dat de politie deze kennis zelf in huis heeft. Van een computer die lang in het water heeft gelegen, kunnen door het NFI bijvoorbeeld nog data worden gehaald. Een pdf-bestand dat onvindbaar is op een computersysteem, kan door het NFI – mogelijk – worden teruggevonden.

Voor elk forensisch onderzoek waarbij het NFI door de politie wordt ingeschakeld, geldt dat er een Service Level Agreement (SLA) is afgesloten tussen het NFI en de politie over het beroep dat op het NFI kan worden gedaan. Voor deze SLA's is een lumpsumfinanciering van toepassing van het ministerie van Justitie aan het NFI. Producten en diensten die binnen de SLA vallen, hoeven door politieregio's daardoor niet afzonderlijk betaald te worden. Voor veel producten is een maximum aantal zaken afgesproken (bijvoorbeeld maximaal 200 DNA-onderzoeken per maand), voor de afdeling Digitale Biometrie bestaat de SLA uit een maximaal aantal arbeidsuren. Net als voor D&I geldt ook voor het NFI dat men niet aan opsporing doet maar alleen technische ondersteuning biedt, vooral voor het onttrekken van data aan systemen (computers, telefoons, camerabeelden). Ook particuliere instituten behoren tot kennislaag 5. Voor de diensten van deze instituten moet echter wel afzonderlijk betaald worden.[13]

13 In 2010 en 2011 liep er een pilot 'Uitbesteding forensisch onderzoek aan particuliere instituten' in het kader waarvan ook de kosten van particuliere instituten gefinancierd kunnen worden indien voldaan wordt aan bepaalde criteria. De pilot wordt geevalueerd door Pro Facto. Het evaluatieonderzoek, dat verricht is in opdracht van het WODC (ministerie van Veiligheid en Justitie), is medio 2012 verschenen onder de titel *Bekend maakt bemind*.

Uit de gevoerde gesprekken en onze eigen analyse blijkt dat er wat betreft de digitale expertise binnen de politie niet zozeer een probleem is gelegen in de kwaliteit van de meeste van de gespecialiseerde TDO's, maar in de korpsbrede digitale expertise. Wouter Stol, lector Cybersafety aan de Noordelijke Hogeschool Leeuwarden en bijzonder hoogleraar Politiestudies aan de Open Universiteit, zegt hierover in het *Tijdschrift voor de Politie:*

> 'Het zit met name in de breedte van politie en justitie. Er zijn natuurlijk specialisten in de bestrijding van cybercrime in het land, bij het KLPD, de bureaus Digitale Expertise, het NFI en het OM. Ook de specialisten zitten met vragen omtrent bijvoorbeeld de aard van cybercrime, maar het grootste probleem is dat digitale criminaliteit niet meer iets voor specialisten alleen is, maar zich in de volle breedte van de samenleving voordoet. Iedere politieman of politievrouw kan ermee te maken krijgen, maar die ontbreekt het vaak aan de benodigde kennis. Als iemand aangifte komt doen van een cybercrime dan blijkt het al een enorme opgave om zo'n aangifte goed op papier te krijgen. En daar begint het mee.'[14]

In 2007 is op de Politieacademie als pilot de afstudeerrichting Digitale Recherche gestart. Daarnaast hebben ruim 2000 tactische rechercheurs een vijfdaagse training digitaal rechercheren gevolgd. Door middel van e-learning worden (intake)medewerkers in de basispolitiezorg geschoold. Desondanks blijft het volgens respondenten een probleem om digitale kennis binnen de politie breed te borgen.

Ook het vervullen van vacatures is bij diverse TDO's een probleem. Hooggekwalificeerde (hbo of wetenschappelijk onderwijs) ICT-experts met bij voorkeur een politieachtergrond zijn moeilijk te vinden. Meerdere TDO's hebben te kampen met onderbezetting door moeilijk vervulbare vacatures.

3.7 Bevoegdheden

Uit de gevoerde gesprekken blijkt dat er geen sprake is van een belemmering voor de opsporing van cybercrime doordat de verleende bevoegdheden tekort zouden schieten. De enige bevoegdheid die door sommige respondenten

14 Jaargang 72, nr. 9/10, p. 19.

gemist wordt, is dat van afstand een computer binnen kan worden gedrongen om zo *real time* de handelingen te kunnen volgen. Dat is effectiever dan het naderhand analyseren van een computer omdat dan het risico bestaat dat deze versleuteld is. Technisch is het voor de politie geen probleem om een computer van afstand binnen te dringen, maar het is niet toegestaan.

4

De ideale organisatie

4.1 Inleiding

Binnen de organisatiekunde en het kennismanagement is veel praktijkonderzoek gedaan naar het effectief organiseren van kennisintensieve organisaties. Zo is bijvoorbeeld de huidige rechterlijke organisatie in fasen tot stand gekomen, waarbij vanaf het rapport van de commissie-Wiersma in 1972[15] tot in de voorbereiding van de Wet organisatie en bestuur gerechten (WOBG, 2002) en de Wet Raad voor de rechtspraak (2002) steeds de vigerende inzichten uit de organisatiekunde zijn toegepast.[16] Dit type praktijkonderzoek in verschillende sectoren van overheid en bedrijfsleven heeft zich vertaald naar een aantal ideaalmodellen van effectieve organisaties en een aantal normen voor effectief kennismanagement. In dit hoofdstuk worden deze modellen en normen beschreven.

De opsporing van cybercrime vindt plaats binnen de bestaande politieorganisatie, zoals beschreven in het vorige hoofdstuk. De regionale korpsen hebben taken die van regionaal belang zijn. Het KLPD heeft taken die van landelijk of internationaal belang zijn. De regionale korpsen en het KLPD vallen onder het ministerie van Veiligheid en Justitie. De organisatie wordt zodoende gekenmerkt door:

- een centrale strategische aansturing (bepalen van het doel en de middelen, organisatie, bevoegdheden, begroting);
- een decentrale tactische aansturing (deels geografisch en deels taakgeoriënteerd);
- een decentrale uitvoering (realiseren van het opgedragen doel met de beschikbaar gestelde middelen).

15 Commissie Wiersma (1972). *Rapport van de werkgroep herziening rechterlijke organisatie, gedachten over de toekomst van de rechtspleging*. Den Haag: Staatsuitgeverij.

16 Zie onder andere KPMG BAS (2006). *Het functioneren van de rechterlijke organisatie in beeld. Breedtestudie Wet organisatie en bestuur gerechten en Wet Raad voor de rechtspraak*. Den Haag: WODC.

De strategische besluitvorming vindt hierbij plaats op het ministerie en de tactische besluitvorming door de korpsleiding.

De kennis die wordt toegepast bij de opsporing van cybercrime is hoofdzakelijk algemeen (niet regionaal bepaald), complex en dynamisch. Het over verschillende afdelingen verspreid verwerven en beschikbaar stellen van dit type kennis heeft in algemene zin een aantal nadelen. Het leidt tot:

- doublures (meerdere malen uitvinden van het wiel, via meerdere kanalen beschikbaar stellen van dezelfde kennis);
- het ontbreken van vereiste kennis (als deze bijvoorbeeld slechts landelijk in een bepaalde afdeling of in een regio aanwezig is, terwijl er ook landelijk bij andere afdelingen en in andere regio's behoefte is aan deze kennis);
- inconsistenties (als opsporingsmethoden en technieken voor dezelfde opsporingsvraag op meerdere plaatsen worden ontwikkeld, maar niet in alle gevallen de best practice wordt gevonden).

Kennis van dit type zou daarom idealiter niet op operationeel niveau moeten worden ingebed.

Naar de organisatie van effectieve (kennisintensieve) organisaties is veel onderzoek gedaan. In de literatuur wordt een beschrijving gegeven van voorkomende organisatietypes en een verklarend verband gelegd tussen bepaalde kenmerken van deze types en de effectiviteit van deze organisaties. In §4.2 worden de belangrijkste organisatietypes, hun kenmerken en hun invloed op de effectiviteit van de organisatie beschreven.

In §4.3 wordt deze algemene kennis over de effectiviteit van kennisintensieve organisaties toegepast op de gegeven kenmerken van de huidige organisatie van de opsporing van cybercrime. Dit mondt in §4.4 uit in een voorkeursvariant voor de organisatie van de opsporing van cybercrime.

4.2 Mogelijke organisatie-inrichtingen: de theorie

4.2.1 Organisatie

In de literatuur worden overheids- en bedrijfsorganisaties veelal beschreven aan de hand van de volgende organisatieonderdelen:[17]

- strategische onderdelen (bepalen van doel en middelen);
- tactische onderdelen (toekennen van middelen aan kerntaken);

- operationele onderdelen (uitvoeren van de kerntaken);
- technische onderdelen (ontwerpen van methoden en technieken voor de uitvoering van kerntaken);
- ondersteunende onderdelen (ondersteunen van de uitvoering van kerntaken).

De effectiviteit van de organisatie wordt enerzijds bepaald door de *coördinatie van de organisatieonderdelen en activiteiten* (meer hierover in §4.2.2), dat wil zeggen de wijze van aansturing van de organisatieonderdelen en hun onderlinge taakverdeling, en anderzijds door de *reductie van onzekerheid* (§4.2.3) in de organisatie, dat wil zeggen het hebben van duidelijke en stabiele taken en het beschikken over de juiste kennis en vaardigheden voor de uitvoering daarvan. Coördinatie en reductie van onzekerheid zijn dan ook de instrumenten waarmee de effectiviteit van een organisatie kan worden verhoogd.

De wijze waarop de coördinatie en de reductie van onzekerheid moeten worden aangepakt is afhankelijk van de actuele effectiviteit van de organisatie. Deze kan worden bepaald aan de hand van *effectiviteitscriteria* (§4.2.4). In de politieorganisatie vormt het ministerie van Veiligheid en Justitie het strategische onderdeel, terwijl de korpsleidingen van het KLPD en de regionale korpsen het tactische onderdeel vormen. Op het gebied van de opsporing zijn de rechercheafdelingen van het KLPD en de regionale korpsen de operationele afdelingen, die de kerntaken uitvoeren. Algemene methoden en technieken voor de uitvoering van de opsporing worden verspreid over de strategische (proces- en productstandaards)[18] en operationele (kennisstandaards) afdelingen (in het bijzonder het KLPD en zijn onderafdelingen) ontwikkeld. Hetzelfde geldt voor de ondersteunende afdelingen; deze zijn verspreid over de centrale en regionale operationele afdelingen (er zijn zelfs ondersteunende afdelingen die enkele regio's bedienen).

17 Deze indeling is gebaseerd op Mintzbergs originele analyse (Mintzberg 1979) en wordt nog steeds door de meeste auteurs gevolgd.

18 Processtandaards (normen voor de wijze waarop de politietaak moet worden uitgevoerd) zijn bijvoorbeeld neergelegd in de Politiewet (aansturing van de opsporing), in het Wetboek van Strafvordering (opsporingsbevoegdheden) en in de Wet Politiegegevens (normen voor de omgang met opsporingsgegevens). Productstandaards vinden we in de beleidsplannen van het ministerie, die worden vertaald naar beleidsafspraken met de operationele diensten (bijvoorbeeld de opeenvolgende Landelijke Kaders Nederlandse Politie en de regionale convenanten waarin prestatieafspraken zijn opgenomen).

4.2.2 Coördinatie van de organisatie

De coördinatie van de organisatieonderdelen (de wijze van aansturing van de organisatieonderdelen en hun onderlinge taakverdeling) wordt door de volgende kenmerken bepaald:

C1 door *de wijze van inhoudelijke aansturing* van activiteiten (de mate van operationele autonomie). Hierbij kan sprake zijn van:
- a directe aansturing: het geven van directe opdrachten;
- b aansturing door proces-, kennis- of productstandaardisatie: aansturing door het stellen van normen (voor de taakuitvoering, de toe te passen kennis en de te gebruiken vaardigheden en de te boeken resultaten) en niet door het geven van directe opdrachten;
- c geen aansturing (evt. horizontale coördinatie tussen operationele afdelingen): het organiseren van de taakuitvoering door ad hoc overleg tussen de uitvoerders.

C2 door het *organisatieonderdeel waar het zwaartepunt van de beslissingsbevoegdheden* ligt (mate van specialisatie en daaruit voortvloeiende hiërarchische structuren).

C3 door *centralisatie of decentralisatie van beslissingsbevoegdheden*.

Op grond van de organisatieonderdelen en de verschillende kenmerken van coördinatie kunnen vijf *prototypische organisatievormen* worden onderscheiden. Deze prototypen zijn beschrijvend van aard. Zij beschrijven typische (veelvoorkomende) feitelijke organisatievormen. In combinatie met de effectiviteitscriteria verkrijgen zij ook een normatieve waarde.

1 **Ondernemingsorganisatie** (*simple structure*, bijv. kleine ondernemingen)
   C1 directe aansturing;
   C2 door het *strategische* onderdeel (zwaartepunt beslissingsbevoegdheden);
   C3 centralisatie van beslissingsbevoegdheden.
2 **Bureaucratische organisatie** (bijv. grote bedrijven en ministeries)
   C1 aansturing door standaardisatie van processen (formeel omschreven taken en bevoegdheden);
   C2 door de technische afdeling die methoden en technieken ontwikkelt (zwaartepunt beslissingsbevoegdheden);
   C3 strategische centralisatie, tactische en operationele decentralisatie van beslissingsbevoegdheden.

3 **Professionele organisatie** (bijv. advocatenkantoren, wetenschappelijk onderwijs)
C1 aansturing door standaardisatie van kennis;
C2 door de operationele afdeling (zwaartepunt beslissingsbevoegdheden);
C3 decentralisatie van beslissingsbevoegdheden.
4 **Divisieorganisatie** (bijv. nationale, regionale en lokale overheden, conglomeraten)
C1 aansturing door standaardisatie van producten (bijv. prestatieafspraken);
C2 door het tactische onderdeel (zwaartepunt beslissingsbevoegdheden);
C3 tactische decentralisatie van beslissingsbevoegdheden.
5 **Innovatieve organisatie** (*adhocracy*, bijv. projectgeoriënteerde ondernemingen en instellingen (consultancy en wetenschappelijk onderzoek))
C1 geen inhoudelijke aansturing;
C2 zwaartepunt bij de ondersteunende afdelingen (leveren kennis aan de operationele onderdelen) of bij de operationele afdelingen zelf;
C3 centralisatie van ondersteuning, decentralisatie van operationele beslissingen.

De toepassing van de effectiviteitscriteria kan blootleggen dat voor de uitvoering van bepaalde taken een verkeerd (minder effectief) organisatietype is gekozen, dan wel dat bepaalde kenmerken van een bepaald organisatietype moeten worden versterkt. De hiervoor in algemene termen omschreven politieorganisatie is bijvoorbeeld een bureaucratische divisieorganisatie. Een organisatie die moet opereren in een dynamische kennisomgeving, zoals die van de opsporing van cybercrime, zou op grond van toepassing van de effectiviteitscriteria mogelijk gericht moeten zijn op professionalisering en innovatie en zou derhalve vooral moeten lijken op organisatietypen 3 (professionele organisatie) en/of 5 (innovatieve organisatie).

4.2.3 *Reductie van onzekerheid*

Reductie van onzekerheid is naast de coördinatie van organisatieonderdelen bepalend voor de effectiviteit van de organisatie. Er kunnen twee vormen van reductie van onzekerheid worden onderscheiden: interne en externe.

De *interne* onzekerheid wordt bepaald door de mate waarin de kennis en vaardigheden die noodzakelijk zijn voor de uitvoering van activiteiten, door de operationele afdelingen worden verworven en feitelijk beschikbaar zijn. Een

organisatie die in een eenvoudige en stabiele kennisomgeving opereert kan bijvoorbeeld volstaan met het aannemen van personeel dat over voldoende standaardkennis en -vaardigheden beschikt (een bepaalde opleiding heeft genoten). Een organisatie waarin complexe en voortdurend wijzigende kennis moet worden toegepast, zoals die van de opsporing van cybercrime, kan zijn kennisonzekerheid alleen reduceren door de instelling van ondersteunende en technische afdelingen. Deze afdelingen ondersteunen de opsporing in specifieke gevallen met gerichte kennis of leveren standaards voor het opsporen van bepaalde categorieën van gevallen. Reductie van de interne onzekerheid kan plaatsvinden door een effectief kennismanagement (§4.3).

De *externe* onzekerheid wordt bepaald door de complexiteit en de mate van veranderlijkheid van de politieke, economische en technische omgeving. In een eenvoudige en stabiele omgeving kan worden volstaan met een statische vorm van aansturing, zoals die door standaardisatie van processen in bureaucratische organisaties. In complexe dynamische omgevingen waarin zowel strategische doelen (politieke doelstellingen) als operationele doelen (gebaseerd op de concrete vraag naar dienstverlening, bijvoorbeeld opsporing op basis van concrete aangiftes) voortdurend wijzigen en soms strijdig zijn, moeten de beslissingen worden genomen door de tactische en operationele afdelingen waar de strategische en operationele doelen samenkomen. Reductie van de externe onzekerheid kan derhalve plaatsvinden door het kiezen van de juiste vorm van coördinatie (§4.2.2).

4.2.4 *Effectiviteitscriteria*

Effectiviteit wordt veelal vereenzelvigd met doeltreffendheid. Complexe organisaties worden echter gekenmerkt door een veelheid van, soms strijdige, doelen. Bij de opsporing van cybercrime is bijvoorbeeld sprake van een veelheid van zowel structurele als ad hoc politieke doelen (de reorganisatie van de politieorganisatie, het bezuinigingsbeleid, het opsporingsbeleid en politieke incidenten zoals DigiNotar) en van operationele doelen (feitelijke aangiftes). Effectiviteit wordt daarom in de organisatiekunde veelal gedefinieerd als het vinden van een optimale balans tussen het realiseren van deze verschillende doelen. Voor het bepalen van dit optimum worden effectiviteitscriteria gehanteerd. Effectiviteitscriteria bepalen welke vorm van coördinatie en welke vorm van onzekerheidsreductie moeten worden gekozen om de organisatie effectiever te maken.

In de literatuur worden drie effectiviteitscriteria het meest genoemd:

1 flexibiliteit;
2 efficiency;
3 belangenbehartiging.

De samenhang tussen de effectiviteitscriteria en de organisatietypen (de wijze van coördinatie) en de reductie van onzekerheid kan als volgt worden beschreven.

Ad 1. Flexibiliteit

Flexibiliteit heeft te maken met het structurele aanpassingsvermogen van de organisatie aan een veranderende omgeving. Er kan hierbij een onderscheid worden gemaakt tussen strategische, tactische, operationele, technische en ondersteunende flexibiliteit.

Strategische flexibiliteit heeft betrekking op het vermogen om beleidsdoelstellingen aan te passen aan nieuwe inzichten. Op het gebied van cybercrime betekent dit het vertalen van nieuwe technologische realiteiten in het stellen van prioriteiten in de opsporing. Strategische flexibiliteit moet overigens worden onderscheiden van de mogelijkheid om de organisatie ad hoc in te zetten voor politieke doeleinden, zoals bijvoorbeeld in het geval van de DigiNotar-zaak is gebeurd. Het acute probleem van bedreiging van de veiligheid van de digitale overheidscommunicatie wordt natuurlijk niet opgelost door (bespoediging van) de aanvang (en overigens evenmin door de voltooiing) van de opsporing, maar door de organisatorische en technische veiligheidsmaatregelen die de overheid neemt.

Tactische flexibiliteit heeft voornamelijk te maken met het vermogen om, gegeven beperkte middelen, prioriteiten te stellen in de afhandeling van concrete zaken, c.q. aangiftes. Het gaat hier bijvoorbeeld om het vermogen om als er zich een te groot aantal landelijke cybercrimezaken aandient, toch regionale capaciteit in te schakelen, bijvoorbeeld door de Amsterdamse kinderpornozaak toch regionaal af te handelen in plaats van hiervoor ook een groot deel van de landelijke capaciteit in te zetten.

Operationele flexibiliteit heeft betrekking op het vermogen om een veranderende kennisbehoefte te herkennen in geval van veranderende technische realiteiten. Bijvoorbeeld de noodzaak om de juridische en technische kennis te verwerven die nodig is om rechtmatig en effectief

in digitale criminele organisaties te infiltreren als deze organisaties in toenemende mate van de technische mogelijkheden gebruikmaken.

Technische en ondersteunende flexibiliteit betreft het vermogen om de standaard en specifieke kennis te genereren die vereist is om de opsporing in geval van een veranderde technische realiteit effectief te laten verlopen. Technische en ondersteunende flexibiliteit hangen sterk samen met het type kennis dat vereist is. Complexe en dynamische kennis vereisen bijvoorbeeld gespecialiseerde technische en ondersteunende afdelingen.

Flexibiliteit op strategisch niveau heeft derhalve te maken met het aanpassingsvermogen van de organisatie aan veranderende (politieke) doelstellingen en beschikbare middelen. Flexibiliteit op tactisch niveau met de vertaling daarvan in nieuwe kerntaken en de daaraan toegewezen middelen. Flexibiliteit op operationeel niveau heeft te maken met het vermogen om de uitvoering van kerntaken te wijzigen en in het bijzonder de vereiste kennis en vaardigheden daarvoor te verwerven.

Het eerste organisatietype (de ondernemingsorganisatie) is het effectiefst bij kleine kennisintensieve innoverende organisaties. Het tweede organisatietype (de bureaucratische organisatie) is het meest effectief bij gestructureerde statische kennis, het derde (de professionele organisatie) bij gestructureerde dynamische kennis, het vierde (de divisieorganisatie) bij ongestructureerde statische kennis en het vijfde (de innovatieve organisatie) bij ongestructureerde dynamische kennis.

In het geval van de opsporing van cybercrime is er enerzijds sprake van gestructureerde dynamische kennis (methodische en technische standaards voor de opsporing van cybercrime/best practices) die systematisch en structureel zou moeten worden ontwikkeld door een technische afdeling en worden toegepast door de operationele afdelingen om maximale flexibiliteit te bereiken. Anderzijds is er sprake van ongestructureerde dynamische kennis (steeds nieuwe vormen van cybercrime) waarop de operationele afdelingen niet zelfstandig kunnen anticiperen, waarvoor de kennis zou moeten worden aangeleverd door een ondersteunende afdeling die voortdurend gevoed wordt door de veranderende technische realiteit.

Ad 2. Efficiency

Efficiency (doelmatigheid) heeft te maken met het bereiken van een optimale verhouding tussen kosten en baten, c.q. het opsporen van het grootste aantal gevallen van cybercrime met behulp van de beperkte beschikbare middelen. De efficiëntie van de opsporing kan worden geschat door veranderingen in de kosten per zaak over de tijd te vergelijken of door vergelijking met de kosten voor de uitvoering van dezelfde taken in andere organisaties (bijvoorbeeld bedrijven die digitale beveiliging aanbieden).

Eenvoudigere coördinatiemechanismen zoals die van directe aansturing in de ondernemingsorganisatie brengen lagere kosten met zich mee dan ingewikkeldere coördinatiemechanismen zoals aansturing via standaardisatie of zelfs het ontbreken van (centrale) aansturing (zie §4.2.2). Hoe minder communicatie en besluitvorming tussen verschillende organisatieonderdelen nodig is, des te eenvoudiger de coördinatie. Standaardisatie van de taakuitvoering, specialisatie van operationele afdelingen (minder hiërarchie door decentrale beslissingen) en decentralisatie (meer autonomie door zelfvoorziening) vergroten de eenvoud en daarmee de efficiency van een organisatie. Complexe dynamische kennis kan niet met behulp van standaardisatie, specialisatie of decentralisatie worden geaccommodeerd. Organisaties die complexe dynamische kennis verwerken zullen daarom in het algemeen minder effectief worden als de efficiency wordt verhoogd (bijvoorbeeld door bezuinigingen).

Verhoging van de efficiency heeft veelal een negatief effect op de reductie van onzekerheid, omdat het verlagen van de investeringen veelal ook een lager kennisniveau met zich meebrengt. Flexibiliteit brengt gewoonlijk hogere kosten met zich mee. Het centraliseren van technische en ondersteunende diensten kan echter zowel een verhoging van de efficiency als van de flexibiliteit met zich meebrengen. De voorwaarden hiervoor zijn dat de centrale ondersteuning een grotere kenniscapaciteit en -diversiteit heeft dan de afzonderlijke decentrale ondersteuning had, en dat de ondersteuning betrekking heeft op algemene kennis, anders gezegd kennis waaraan de verschillende decentrale eenheden behoefte hebben.

Ad 3. Belangenbehartiging

Belangenbehartiging betreft de mate waarin de doelstellingen van de interne en externe belanghebbenden worden gerealiseerd. Het gaat hierbij ook om een optimum, omdat deze belangen strijdig kunnen zijn. In het geval van de opspo-

ring van cybercrime gaat het om politieke belangen (vertaald in wetgeving, beleid of ad hoc opdrachten van de minister), interne belangen van de organisatie (het op een redelijke wijze inzetten van beperkte middelen, arbeidsomstandigheden, enzovoort) en om externe belangen (onder meer van slachtoffers en van het publiek).

De interne belangenbehartiging is sterk afhankelijk van de juiste combinatie van organisatietype en taken. Kleine concurrerende organisaties worden in het algemeen effectiever als de interne belangen worden overvleugeld door de externe belangen. Dat wil zeggen dat de belangen van afnemers een hogere prioriteit krijgen dan de belangen van de deelnemers aan de organisatie. In een grote politiek aangestuurde, bureaucratische organisatie bestaat een sterke cesuur tussen politieke (strategische) belangen en tactische belangen. Aan de ene kant worden de strategische doelen en middelen van de organisatie vrijwel uitsluitend bepaald op grond van politieke overwegingen en spelen overwegingen vanuit het operationele niveau hierbij een kleine rol. Aan de andere kant hebben het tactische en operationele niveau een grote mate van autonomie, omdat ze worden afgerekend op basis van hun output en niet op basis van de effectiviteit van hun werkprocessen of de kennisvoorziening. De externe belangenbehartiging kan in een dergelijke organisatie samenvallen met het strategische belang als deze een directe vertaling van de politieke opdrachten (de wensen van het electoraat, de publieke opinie) betreft.

Professionele organisaties worden in het algemeen effectiever als de externe belangenbehartiging wordt overvleugeld door de interne belangenbehartiging. De redenen hiervoor zijn de standaardisatie van kennis die hierdoor mogelijk wordt, een gebrek aan concurrentie (het monopolie van het verlenen van publieke diensten) en/of de bijzondere (wettelijk exclusieve) status van de experts in de organisatie. Voor divisieorganisaties die concurreren om schaarse middelen geldt hetzelfde als voor kleine concurrerende organisaties, waarbij de externe belangen net als bij de bureaucratische organisaties samenhangen met de strategische opdrachten. Als de divisies niet of weinig concurreren, geldt hetzelfde als voor professionele organisaties. Innovatieve organisaties worden effectiever als zij zich specialiseren. Hoe groter het verschil in kennisniveau tussen organisatie en opdrachtgever, des te afhankelijker deze laatste wordt.

Hoe duidelijker de interne en externe belangen kunnen worden vastgesteld, des te effectiever zal de organisatie zijn vanuit het oogpunt van onzekerheidsreductie. Kleine concurrerende organisaties kunnen bijvoorbeeld door specialisatie de concurrentie en daarmee de onzekerheid reduceren. Grote politiek (strategisch) aangestuurde bureaucratische organisaties hebben per definitie te

maken met duidelijke (zij het wisselende) externe belangen. Er kan wel onzekerheid ontstaan als outputcriteria op operationeel niveau niet sporen met de strategische doelstellingen (zoals het uitschrijven van meer boetes tegenover het opsporen van meer politiek gevoelige zaken). Professionele organisaties hebben eveneens duidelijke, in dit geval interne, belangen, die de externe belangen veelal overvleugelen. Reorganisaties, bezuinigingen en privatisering kunnen hier onzekerheid met zich meebrengen. Divisieorganisaties kunnen als ze concurreren net als kleine concurrerende organisaties effectiever worden door specialisatie. Niet concurrerende divisieorganisaties hebben ook hier te maken met duidelijke strategische belangen. Innovatieve organisaties hebben net als professionele organisaties voornamelijk te maken met interne belangen. In dit geval voornamelijk omdat de doeleinden intern worden bepaald en vanwege de exclusieve status van de experts.

4.3 Effectiviteit en kennismanagement

Als de uitvoering van de taken van een organisatie een hoog niveau van complexe en dynamische kennis en vaardigheden vereist, dan is er naast de voorgaande algemene kennis over de effectiviteit van organisaties ook behoefte aan specifieke kennis over de effectiviteit van kennisintensieve organisaties. Ook op dit gebied bestaat er een omvangrijke literatuur.[19]

Kennismanagement heeft betrekking op:

- identificatie van de vereiste kennis, oftewel het bepalen van de voor de uitvoering van de kerntaken (bijv. de opsporing van cybercrime) vereiste kennis;
- verwerving of productie van de vereiste kennis (acquisitie en onderhoud);
- vastleggen en disseminatie van de vereiste kennis (representatie en communicatie);
- het gebruik van de vereiste kennis (vaardigheden, scholing).

De belangrijkste *strategieën van kennismanagement* zijn de volgende.

- Structureel vastleggen van kennis
  Complexe kennis is veelal impliciet in de organisatie aanwezig (in de hoofden van de experts). Structureel vastleggen van kennis kan plaatsvinden door codificatie, d.w.z. het bijeenbrengen en expliciteren van de impliciete

19 Ook hier geldt dat er een oeranalyse is die veel geciteerd wordt, namelijk die van Ikujiro Nonaka uit 1991.

kennis in geschrift of in digitale vorm. Deze strategie wordt ook wel push-strategie genoemd, omdat het primaire doel van deze wijze van kennis-management het vastleggen van kennis is.
- Ad hoc vastleggen van kennis
  Deze strategie is erop gericht de impliciet aanwezige kennis te ontsluiten door het gebruiken van (netwerken van) experts als bron. Deze strategie wordt ook wel pull strategie genoemd.

De eerste strategie is zonder meer geschikt voor minder complexe en statische kennis. Hoe complexer de kennis, des te hoger de kosten van de eerste strategie. Hoe dynamischer de kennis, des te minder haalbaar de eerste strategie is. Natuurlijk is niet alle kennis in een organisatie complex en/of dynamisch. Voor dit deel van de kennis kan voor standaardisatie worden gekozen. Het management van complexe dynamische kennis vereist menselijke experts en een (dynamische) projectorganisatie. Oplossingen voor het ad hoc karakter van kennismanagement van complexe en dynamische kennis zijn de lerende en de netwerkorganisatie. In een lerende organisatie wordt de kennis van experts verworven en vastgehouden door opleidingen, door het intern scheppen van meester-leerlingverhoudingen in de organisatie (interne stages en dergelijke) en door het extern opleiden van nieuwe experts. In een netwerkorganisatie wordt expertise gedeeld via een menselijk en/of IT-netwerk: direct door communicatie en samenwerking via het netwerk en indirect door het vastleggen van de processen en procedures van de communicatie en samenwerking in het netwerk (bijvoorbeeld in een wiki).

Methoden van kennismanagement: identificatie en verwerving of productie en onderhoud

De voor de uitvoering van taken vereiste kennis kan worden geïdentificeerd op strategisch, tactisch, operationeel, technisch of ondersteunend niveau. Op strategisch niveau, bij het bepalen van de organisatiedoelen, kan tevens worden bepaald welke kennis voor het realiseren hiervan vereist is. Het kan hierbij gaan om aanwijzing van een intern organisatieonderdeel (bijvoorbeeld een technische of een ondersteunende afdeling) of een externe organisatie die als kennisbron zal worden gebruikt (*outsourcing*). Een aangewezen technische afdeling zal systematisch methoden en technieken genereren (R&D gericht op standaardisatie), een ondersteunende afdeling zal de ontwikkelde methoden en technieken toepassen en ad hoc expertise beschikbaar stellen aan de operationele afdelingen. Op tac-

tisch niveau kan ten slotte vereiste kennis worden geïdentificeerd als er op operationeel niveau kennis wordt verworven en geproduceerd, waaraan middelen moeten worden toegewezen. De kwaliteit van de kennisvoorziening vereist dat er middelen worden gereserveerd om de continuïteit van de processen van identificatie en verwerving of productie van kennis te garanderen (onderhoud).

Technieken van kennismanagement: representatie en disseminatie

De geïdentificeerde en verworven of geproduceerde kennis kan worden vastgelegd en gecommuniceerd met behulp van een groot aantal technieken.

De belangrijkste categorieën zijn:

- knowledge and expert locators (bijvoorbeeld Yellow Pages);
- document management systems;
- groupware/collaborative technologies (bijvoorbeeld wiki's);
- information systems (storing and retrieving of data and knowledge);
- knowledge repositories;
- expert/knowledge systems (application of knowledge);
- e-learning systems.

Scholing

De toepassing van deze methoden en technieken vereist een permanent proces van scholing. Het kan effectief zijn om de scholing te laten plaatsvinden door of begeleid door de afdeling die de methoden en technieken verwerft dan wel produceert. De technische afdeling die de standaardmethoden en -technieken ontwikkelt voor de uitvoering van de opsporing van cybercrime zou bijvoorbeeld tevens verantwoordelijk moeten zijn voor de scholing van medewerkers in het toepassen van deze standaardmethoden en -technieken en hiervoor op elk niveau de nodige opleidingspakketten moeten ontwikkelen.

De diversiteit van taken die samenhangen met het kennismanagement brengt met zich mee dat er meerdere organisatieonderdelen bij betrokken moeten zijn. Bovendien zullen deze onderdelen over en weer over het kennismanagement moeten communiceren. Een vaak beschreven effectieve organisatie van dit meervoud aan taken en de bijbehorende communicatiebehoefte is de volgende.

1 In de eerste lijn is de kennis aanwezig die nodig is om de kerntaken te kunnen uitvoeren, in het bijzonder om de vraag van de klant te kunnen interpreteren

en het juiste werkproces te kunnen kiezen om het aanbod te kunnen genereren door de levering van een product of een dienst (operationele afdelingen).
2 In de tweede lijn is de ondersteuning met expertise belegd van de uitvoering van de kerntaken (ondersteunende afdelingen).
3 In de derde lijn zijn het onderwijs en het onderzoek en de ontwikkeling van methoden en technieken voor de uitvoering van de kerntaken (technische afdelingen, R&D) belegd.

4.4 *Voorkeursvariant*

In deze paragraaf wordt de algemene kennis over de effectiviteit van kennisintensieve organisaties uit de vorige paragrafen toegepast op de gegeven kenmerken van de huidige organisatie van de opsporing van cybercrime.

Organisatieonderdelen

Het eerste bijzondere kenmerk van de politieorganisatie is de sterke scheiding tussen het strategische niveau (het ministerie van Veiligheid en Justitie) en het tactische en operationele niveau (de regionale korpsen en het KLPD). Strategische beslissingen zijn daardoor sterk hiërarchisch georiënteerd en gecentraliseerd, terwijl de uitvoering juist sterk heterarchisch georiënteerd en gedecentraliseerd is. De strategische beslissingen kennen een sterk top-down karakter (door de politiek en niet door het werkveld bepaald). De tactische beslissingen worden in sterke mate bepaald door politieke outputeisen[20] ('meer blauw op straat', 'bonnenquota') en door politiek bepaalde gegevenheden van de organisatievorm (regionale divisies en taakgeoriënteerde nationale divisies, enzovoort). De operationele beslissingen kennen daarentegen juist een sterk bottom-up karakter (aangifte- en onderzoekbepaald). De taakafbakening tussen operationele, technische en ondersteunende afdelingen is door deze cesuur niet scherp.

De regionale afdelingen hebben niet alleen operationele, maar ook (zich per regio herhalende) ondersteunende taken. Dit is meteen het tweede bijzondere kenmerk van de politieorganisatie. De regionale indeling leidt in gevallen waarin de ondersteunende kennis geen regionaal karakter heeft, tot een duplicatie van dezelfde kennis in regionale ondersteunende afdelingen. Het ontwikkelen

20 Zie onder andere Fijnaut 2007, p. 297 e.v.

van nieuwe kennis lijdt aan hetzelfde euvel. Dit brengt niet alleen duplicatie met zich mee, maar ook kennisongelijkheid, omdat regio's waarin bepaalde vormen van criminaliteit zich meer voordoen, meer kennis ontwikkelen. Er zijn legio voorbeelden van de uitvoering van onderzoek naar algemene methoden en technieken in specifieke regio's (onder meer onderzoek naar de digitalisering van dossiers in de strafrechtketen, onderzoek naar monitoring van criminaliteit, onderzoek naar data mining, enzovoort).

Coördinatie van de organisatieonderdelen

De operationele autonomie bij de opsporing door de politie (ook van cybercrime) is hoog. Er is in de regionale korpsen geen sprake van directe aansturing en er is weinig kennisstandaardisatie. Binnen het KLPD is de aansturing directer omdat er een kleine gespecialiseerde afdeling hightech crime is. De hiërarchie binnen deze afdeling is echter zo sterk en de standaardisatie van de vereiste kennis zo gering dat het zwaartepunt toch op tactisch en operationeel niveau ligt.

Organisatievorm en effectiviteitscriteria

De hiervoor beschreven bijzondere kenmerken van de politieorganisatie bestempelen deze organisatie voor zover het om de opsporing van cybercrime gaat idealiter tot een professionele en innovatieve organisatie. Problematisch is dat de strategische aansturing van deze organisatie juist kenmerken van een bureaucratische en divisieorganisatie kent. Het gevolg hiervan is dat de strategische aansturing plaatsvindt door proces- en productstandaardisatie (output-standaardisatie), terwijl het complexe en dynamische karakter van de voor de taakuitvoering vereiste kennis juist om kennisstandaardisatie en sterke operationele autonomie vraagt. Daarbij verdient de terugkoppeling van kennis vanaf het tactisch-operationele niveau naar het strategische niveau (bottom-up) bijzondere aandacht, omdat de strategische beslissingen nu voornamelijk door de politiek en niet door tactisch-operationele behoeften en kennis worden bepaald. Zo kan de politiek wel bepalen wat de maatschappelijke behoefte is aan opsporing van cybercrime, maar niet of deze opsporing organisatorisch en technisch haalbaar is. Hierdoor worden ook taken als de ontwikkeling van methoden en technieken en de ondersteuning van de eerste lijn met expertise niet effectief en eenduidig aan organisatieonderdelen toegekend.

Kennismanagement

Het samenstel van taken van verschillende interne en externe organisatieonderdelen (zoals het THTC, het NFI, enzovoort) bij de verschillende onderdelen van het kennismanagement vertoont omissies, overlappingen en zelfs inconsistenties. Er wordt te weinig kennis vastgelegd, er wordt herhaaldelijk dezelfde kennis gegenereerd (regionale tweedelijnsondersteuning, versnippering van onderzoek over verschillende onderdelen van het KLPD, het NFI, enzovoort) en er worden inhoudelijk verschillende taken door dezelfde organisatieonderdelen uitgevoerd terwijl het effectiever zou zijn als deze alleen door gespecialiseerde afdelingen zouden worden uitgevoerd (rechercheafdelingen doen R&D).

Het zwaartepunt van de beslissingsbevoegdheid ligt in de politieorganisatie wel op het juiste niveau, namelijk het tactisch-operationele, maar de divisiestructuur (die regionaal en taakgeoriënteerd is) zorgt in combinatie met de overeenstemmende kennisbehoefte van alle divisies voor een suboptimaal kennisniveau (minder flexibiliteit door versnippering) en duplicatie van kennis (lage efficiency). Anders gezegd: alle divisies in deze organisatie hebben dezelfde taken en hebben daarvoor dezelfde algemene kennis nodig; zij hebben tevens alle dezelfde taak om deze algemene kennis binnen de eigen divisie (afdelingen van het KLPD, regio's of clusters van regio's) te verwerven en beschikbaar te stellen; de resources voor het verwerven en beschikbaar stellen van kennis van de gehele opsporingsorganisatie worden daarom niet flexibel en niet erg efficiënt gebruikt, namelijk herhaaldelijk voor hetzelfde doel. De politieorganisatie is ondanks dit alles redelijk effectief op het gebied van belangenbehartiging vanwege de aansturing op grond van politiek bepaalde outputnormen (eenvoudige kwantitatieve doelstellingen, weinig onzekerheid).

Onzekerheid en effectiviteitscriteria

De organisatie van de opsporing van cybercrime kent naast de hiervoor gesignaleerde coördinatieproblemen zowel interne als externe onzekerheid. De interne onzekerheid wordt veroorzaakt door de combinatie van complexe en veranderlijke juridische en technische kennis die vereist is, en door het grote aantal specialistische organisatieonderdelen die zich hiermee (vaak met overlappende taakomschrijvingen) bezighouden. De externe onzekerheid wordt veroorzaakt door de politieke dynamiek, de organisatievorm en het maatschappelijk werkveld (cybercrime). Er is sterke druk om tot een organisatieverande-

ring te komen (invoering nationale politie), er is een sterke scheiding tussen de strategische laag (het ministerie van Veiligheid en Justitie) en de tactische en operationele laag (de korpsen) en de digitale wereld is bijzonder complex en turbulent.

Conclusie betreffende de voorkeursvariant voor de opsporing van cybercrime

De oplossingsrichting voor de gesignaleerde tekortkomingen ligt in het verder uitbouwen van een meerlijnsorganisatie waarin de *beslissingsbevoegdheden* over de prioritering van de op te sporen zaken en over de daarvoor door andere gespecialiseerde afdelingen te verwerven en beschikbaar te stellen vereiste kennis verder *gedecentraliseerd* zijn (naar de tactische en operationele afdelingen). De volgende *taken* dienen daarentegen *gecentraliseerd* en duidelijk gescheiden en *per lijn geconcentreerd* te zijn. In verband hiermee moeten ondersteuning in individuele gevallen en ontwikkeling van algemene methoden en technieken uit elkaar worden gehaald:

1 eerstelijns recherche (tactische en operationele afdelingen) met decentrale beslissingsbevoegdheid over de prioritering van de opsporing en de bijbehorende kennisvraag;
2 tweedelijns technisch advies en ondersteunend onderzoek gecentraliseerd en geconcentreerd in een enkele ondersteunende afdeling;
3 derdelijns onderwijs en onderzoek, d.w.z. samenhangend ontwikkelen van algemene methoden en technieken voor de opsporing van cybercrime en het ontwikkelen van daarbij aansluitende opleidingen, gecentraliseerd en geconcentreerd in een enkele technische afdeling (samenbundeling van taken van de academie en de huidige technische onderdelen van de operationele afdelingen).

Deze oplossingrichting wijkt af van de drie in §2.3 beschreven scenario's uit het rapport *De inrichting van Digitale Expertise bij de Nederlandse Politie* (2011). Taakinhoudelijk sluit deze oplossingsrichting het meest aan bij het in het rapport voorgestelde scenario 3 (centralisatie en concentratie).

Het onderscheid is dat er in de hier voorgestelde voorkeursvariant geen sprake is van de centralisatie van beslissingsbevoegdheden. Er moet juist een eenduidiger aansturing vanuit het werkveld (aangiftes) plaatsvinden waarbij centrale (politieke) overwegingen slechts in uitzonderlijke gevallen de prioriteitstelling mogen beïnvloeden. De opsporingsorganisatie moet niet ad hoc

opdrachten krijgen om aan zaken van nationaal belang een hogere prioriteit te verlenen, maar ingericht zijn en de (reserve)capaciteit hebben om dergelijke zaken te behandelen, zonder dat dit afbreuk doet aan de uitvoering van de reguliere taken. Het ministerie is in dit scenario geen opdrachtgever, maar doet slechts aangifte van zaken van nationaal belang. De ondersteuning met en ontwikkeling van kennis op het gebied van (de opsporing van) cybercrime moeten bovendien in de hiervoor onderscheiden tweede en derde lijn gecentraliseerd en geconcentreerd worden om omissies, overlappen en inconsistenties te vermijden. Er is hierbij ten opzichte van de huidige situatie enerzijds sprake van *deconcentratie* (scheiden van de ondersteuning met kennis en de ontwikkeling van kennis, die nu vaak gecombineerd door dezelfde afdelingen plaatsvinden) en anderzijds van *concentratie* van alle ondersteunende taken in een enkele afdeling en concentratie van alle technische taken in een enkele afdeling.

Concentratie van taken kan worden gerealiseerd door de taken exclusief aan bepaalde organisatieonderdelen toe te wijzen. Het kan hierbij gaan om traditioneel georganiseerde onderdelen (lijn- of stafafdelingen), maar ook om gestructureerde netwerken van experts. Dit is een organisatievorm waarbij experts weliswaar bij verschillende organisatieonderdelen werkzaam blijven, maar met behulp van informatietechnologie samenwerken in een gemeenschappelijke taakruimte (een virtueel organisatieonderdeel).

Het voorgaande kan worden samengevat in het volgende schema.

Tabel 4.1: Voorkeursvariant voor de opsporing van cybercrime

	Organisatie	Taken	Expertise
eerste lijn	Decentraal	Operationeel[21] en tactisch[22]	Opleidingspakket 1
tweede lijn	Centraal	Ondersteunend[23]	Opleidingspakket 2
derde lijn	Centraal	Onderzoek en Onderwijs[24]	Opleidingspakket 3
	Centraal	Strategisch[25]	

21 Recherche.

22 Prioritering zaken, inzet operationele middelen.

23 Juridisch (bevoegdheden) en technisch (cybercrime) advies.

24 Research & development (methoden en technieken t.b.v. de opsporing).

25 Politieke prioriteitstelling (niet ad hoc), omvang en allocatie middelen en doelen eerste, tweede en derde lijn.

5 Conclusies en aanbevelingen

5.1 Inleiding

In dit rapport is vanuit verschillende invalshoeken gekeken naar de organisatie van de opsporing van cybercrime door de Nederlandse politie. Enerzijds is de praktijk beschreven (hoofdstuk 3) en anderzijds is vanuit een theoretisch, organisatiekundig perspectief gekeken naar de ideale organisatie van de opsporing van cybercrime (hoofdstuk 4). In dit hoofdstuk worden beide perspectieven samengebracht door de praktijk te toetsen aan de theorie.

5.2 Knelpunten

We identificeren op grond van het voorgaande de volgende knelpunten in de opsporing van cybercrime door de politie.

Aansturing

De sterke scheiding tussen enerzijds strategisch (ministerie van Veiligheid en Justitie) en anderzijds tactisch en operationeel beslissingsniveau (nationale en regionale korpsen) in de organisatie van de opsporing van strafbare feiten levert geen eenduidige aansturing van de opsporing van cybercrime op. Prioriteiten worden enerzijds op grond van centrale politieke overwegingen en opdrachten (top-down, ad hoc) en anderzijds aan de hand van concrete praktische behoeften (bottom-up, structureel, aangiftes) gesteld.

Kennisvoorziening

De divisionele indeling van de opsporing levert op het gebied van cybercrime een probleem in de kennisvoorziening op, omdat de vereiste kennis zich niet

onderscheidt langs de lijnen van de huidige centrale en regionale divisies. De voor het bepalen van de taken van de divisies gehanteerde onderscheiden – complex-niet complex en (inter)nationaal-regionaal, waarbij het KLPD de complexe en (inter)nationale zaken behandelt en de regio's de niet complexe en regionale zaken – sluiten niet goed aan bij de kennis die nodig is voor het effectief opsporen van cybercrime.

Prioriteitstelling

De opsporing van cybercrime heeft binnen de regio's een lage prioriteit. Strafrechtelijke opsporingsonderzoeken naar cybercrime in enge zin zijn er nauwelijks. Op centraal niveau is het het THTC dat wel opsporingsonderzoeken uitvoert die zich richten op cybercrime in enge zin. Het zijn niet zozeer inhoudelijke criteria die een rol spelen bij de selectie van zaken die door het THTC worden uitgevoerd, als wel 'omgevingsfactoren' zoals maatschappelijke onrust of politieke druk. De DigiNotar-zaak is hiervan een voorbeeld. Deze zaak is inhoudelijk niet van een dusdanige complexiteit dat die alleen op centraal niveau opgepakt zou kunnen worden.

Ondersteuning

Er wordt geen duidelijk onderscheid gemaakt tussen de ondersteuning *met* kennis en de ontwikkeling *van* kennis binnen de organisatie van de opsporing van cybercrime. Op regionaal niveau zijn de meeste medewerkers van de TDO's betrokken bij de ondersteuning van rechercheteams. Hun belangrijkste taak is het inbrengen van specifieke knowhow over het veiligstellen, veredelen en analyseren van digitale gegevens. Binnen sommige TDO's houden enkele medewerkers zich bezig met de ontwikkeling van kennis (research & development). Er geen sprake van een strikte functiescheiding.

Op centraal niveau is dit onderscheid wel nadrukkelijker aanwezig. Het team Digitaal & Internet van de KLPD houdt zich voor het grootste gedeelte bezig met research & development (R&D), terwijl het THTC zelf onderzoeken draait en ondersteuning geeft aan de rechercheteams van DNR. In strijd met dit onderscheid is echter dat er ook R&D plaatsvindt binnen het THTC, al is dit niet de hoofdtaak, en dat het team D&I desgewenst ook regionale rechercheteams ondersteunt met kennis.

Scheidslijn tussen complexe en niet complexe kennis

De voorbeelden van zaken die door het THTC worden behandeld wijzen erop dat er geen sprake is van zaken waarvoor bijzonder complexe kennis is vereist (althans niet significant complexer dan die voor regionale zaken vereist is). Wel is er sprake van zaken met een groter, veelal (inter)nationaal belang en gaat de vereiste kennis het niveau van de gemiddelde rechercheur te boven. De complexiteit van een zaak is dus geen (doorslaggevend) criterium voor de toewijzing van zaken aan het THTC of aan de regio. Binnen regio's waar zowel een TDO3 als een TDO4 actief is, is dat onderscheid er vaak wel.

Ondersteuning *mét* kennis

De ondersteuning *met* kennis vindt niet geconcentreerd plaats, maar versnipperd over meerdere organisatieonderdelen binnen een regio. Elke regio biedt z'n eigen ondersteuning met kennis: rechercheteams kunnen een hulp- of ondersteuningsvraag indienen bij het eigen TDO. Binnen sommige regio's zijn zowel een bovenregionaal als een regionaal TDO aanwezig. Daarnaast hebben een zestal regio's ook nog taakaccenthouders binnen de districten. Hun taakafbakening is vooral inhoudelijk: hoe complexer de ondersteuning, des te meer opgeschaald wordt.

Een bijkomend knelpunt bij de ondersteuning met kennis is dat de ondersteuning door TDO's van rechercheteams grotendeels vraagafhankelijk is. Men wordt alleen ingeschakeld als een rechercheteam daar expliciet om vraagt. Hierdoor bestaat het risico dat niet in alle zaken waarin digitale expertise gewenst of vereist is, deze ook daadwerkelijk wordt ingeroepen.

Ontwikkeling *ván* kennis

De ontwikkeling *van* kennis vindt niet geconcentreerd, maar versnipperd over meerdere onderdelen van de politie plaats (Research & Development). Het team D&I van het KLPD neemt een centrale positie in als het gaat om R&D. Het is een van de voornaamste taken van het team. In zoverre is R&D dus geconcentreerd. Daarnaast wordt ook door het THTC en een aantal TDO4's aan R&D gedaan. Er worden bijvoorbeeld tools ontwikkeld.

Binnen de politie wordt soms meerdere keren dezelfde kennis ontwikkeld. De (boven)regionale initiatieven waarvan bij de bevindingen uit het vorige knelpunt wordt gesproken, worden soms wel en soms niet gedeeld met andere teams. Er vindt geen coördinatie plaats van alle (boven)regionale initiatieven. Het risico is daarmee aanwezig dat het wiel vaker dan eens wordt uitgevonden.

De aanwezige expertise binnen regio's varieert, hetgeen zich bijvoorbeeld manifesteert in TDO3 en TDO4. Ook tussen de verschillende TDO4's bestaat verschil in kwaliteit, zo wordt door diverse respondenten aangegeven. Er zijn innoverende teams met hooggekwalificeerde ICT'ers en er zijn teams met minder gekwalificeerde medewerkers.

Onderhoud

Er is geen eenduidig centraal punt waar kennis met betrekking tot (de opsporing van) cybercrime wordt verzameld en ontsloten. D&I kan aangemerkt worden als een dergelijk centraal punt, maar de initiatieven die door andere centrale organisatieonderdelen zoals het THTC en in de regio's worden ontplooid, worden niet door D&I gecoördineerd en/of verzameld.

Bezetting

Een aantal van de huidige TDO's heeft te kampen met een (te) lage bezetting in relatie tot het zaakaanbod. Daar komt bij dat vacatures vaak moeilijk te vervullen zijn.

5.3 Conclusies en aanbevelingen

Het onderzoek geeft aanleiding tot de volgende aanbevelingen.

- De voor de opsporing van cybercrime vereiste expertise op operationeel niveau is niet complex en beperkt zich tot de kennis die nodig is om het cybercrimekarakter van een zaak te kunnen herkennen en de weg te weten naar de gespecialiseerde kennis die de ondersteunende afdelingen kunnen bieden. Dit geldt zowel voor zaken van (inter)nationaal belang als voor andere zaken.

- Er zijn op operationeel niveau (zowel nationaal als regionaal) slechts licht op het gebied van cybercrime geschoolde rechercheurs vereist (opleidingspakket niveau 1) en dus geen gespecialiseerde *eerstelijns* rechercheurs.
- De specialistische kennis op het gebied van cybercrime is algemeen van aard en kan daarom niet effectief langs de lijnen van (inter)nationale en regionale divisies worden georganiseerd. De ondersteuning moet worden geconcentreerd in één enkele landelijke *tweedelijns* afdeling die zowel nationale als regionale rechercheurs ondersteunt. De medewerkers van deze afdeling moeten beschikken over de in een opleidingspakket niveau 2 te definiëren expertise.
- Het ontwikkelen van methoden en technieken voor de opsporing van cybercrime vereist andere expertise dan de directe ondersteuning van de opsporing en dient daarom eveneens te worden geconcentreerd in één enkele landelijke *derdelijns* afdeling. De medewerkers van deze afdeling moeten beschikken over de in een opleidingspakket niveau 3 te definiëren expertise.
- Deze afdeling moet niet alleen nieuwe methoden en technieken ontwikkelen, maar tevens de opleidingspakketten en toelatingseisen ontwikkelen voor de toepassing daarvan.
- De vereiste tactische en strategische kennis op het gebied van cybercrime moet worden gebaseerd op kennis van de praktijk en van de vereiste expertise voor de opsporing van cybercrime en niet op politieke opportuniteit.
- Vervolgonderzoek waarbij specifiek en in detail wordt ingegaan op de vereiste kennis en opleidingen is essentieel voor de uitwerking en toepassing van bovenstaande aanbevelingen. Een internationale verkenning van de opsporing van cybercrime door de politie in landen als Engeland, Duitsland en de Verenigde Staten zou daarbij toegevoegde waarde (kunnen) hebben.

Literatuur

Beleidsadviesgroep Computercriminaliteit (1996). *Op weg naar digitaal rechercheren. Visienota*.

Balkin, J.M. (2007). *Cybercrime: digital cops in a networked environment*. New York: New York University Press.

Bekkers, V., M. Thaens, G. Straten & P. Siep (2009). *Informatiemanagement binnen de politie. Van praktijk tot normatief kader*. Apeldoorn/Den Haag: Reed Business.

Berg, M., G. Dean & J. Karisen (2008). 'Police management roles as determinants of knowledge sharing attitude in criminal investigations'. In: *International Journal of Public Sector Management*, 21-3, 271-284.

Boek, J.L.M. (2000). 'Hacken als opsporingsmethode onder de Wet BOB'. In: *Nederlands Juristenblad* 75-11, 589-593.

Broer, W. (2009). 'Grenzeloos kennisnetwerk'. In: *Het Tijdschrift voor de Politie* 71-9, 30.

Commissie Wiersma (1972). *Rapport van de werkgroep herziening rechterlijke organisatie, gedachten over de toekomst van de rechtspleging*. Den Haag: Staatsuitgeverij.

Dasselaar, A. (2008). *Handboek digitale criminaliteit – over daders, daden en opsporing*. Culemborg: Van Duuren Media (tweede druk).

Dienst Nationale Recherche (DNR) (2010). *Criminaliteitsbeeldanalyse 2009: High Tech Crime*. Driebergen: KLPD.

Houben, G. (2009-2010). *De rol van de digitale en financiële expertise binnen de opsporing en vervolging en de miskenning daarvan*. Scriptie: Benelux Universitair Centrum.

Fijnaut, C.J.C.F. (2007). *Politie: studies over haar werking en organisatie*. Deventer: Kluwer.

Geest, E. van (2006). *Van herkenning tot aangifte – handleiding cybercrime*. Den Haag: GOVCERT.NL.

Goold, M. & A. Campbell (2002). *Designing effective organizations: how to create structured networks*. San Francisco: Jossey Bass.

Hulst, R.C. van der & R.J.M. Neve (2008). *High-tech crime, soorten criminaliteit en hun daders: een literatuurinventarisatie*. Den Haag: Boom Juridische uitgevers.

Hunton, P. (2009). 'The growing phenomenon of crime and the internet: A cybercrime execution and analysis model'. In: *Computer Law & Security Review* 25-6, 528-535.

Hunton, P. (2011). 'The stages of cybercrime investigations: bridging the gap between technology examination and law enforcement investigation'. In: *Computer Law & Security Review* 27-1, 61-67.

Ius mentis (2007). *Digitale opsporingsmethoden voor de politie*. (www.iusmentis.com/beveiliging/hacken/opsporing-politie)

Jägers, H.P.M. & W. Jansen (1991). *Het ontwerpen van effectieve organisaties*. Leiden: Stenfert Kroese.

Jakobsson, M. & Z. Ramzan (2008). *Crimeware : understanding new attacks and defenses*. Boston: Addison-Wesley.

Jorna, R.J. & J.L. Simons (1992). *Kennis in organisaties: toepassingen en theorie van kennissystemen*. Muiderberg: Coutinho.

Klap, H. & D. van der Sluis (2009). 'Politiewerk na de digitale revolutie'. In: *Het Tijdschrift voor de Politie* 71-5, 6-10.

Kleve, P., R. de Mulder & K. van Noortwijk (2011). 'The definition of ICT Crime'. In: *Computer Law & Security Review* 27-2, 162-169.

Landelijk Project Digitaal Opsporen (LPDO) (2005). *Digitaal opsporen, beleid inzake de bestrijding van criminaliteit in een gedigitaliseerde maatschappij*. Zoetermeer: LPDO.

Leukfeldt, E.R., M.M.L. Domenie & W.Ph. Stol (2010). *Verkenning cybercrime in Nederland 2009*. Den Haag: Boom Juridische uitgevers.

Mintzberg, H. (1979). *The structuring of organizations*. Englewood Cliffs, N.J.: Prentice Hall.

Mintzberg, H. (2009). *Structure in fives: designing effective organizations*. Harlow: Pearson Education.

Nationale Cyber Security Strategie (NCSS) (2011). *Slagkracht door samenwerking*. (http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/02/22/nationale-cyber-security-strategie-slagkracht-door-samenwerking.html)

National High Tech Crime Center (2006). *Verantwoording Project High Tech Crime – bijlage bij Ontwerp 'Nationale Infrastructuur Bestrijding Cybercrime'*. Den Haag: z. uitg.

National High Tech Crime Center (2006). *Ontwerp 'Nationale Infrastructuur Bestrijding Cybercrime' – ervaringen en werkwijzen National High Tech Crime Center (NHTCC) en NPC-project aanpak Cybercrime*. Den Haag: z. uitg.

Nonaka, I. (1991). 'The knowledge creating company'. In: *Harvard Business Review* 69-6, 96-104.

Oerlemans, J-J. & B-J. Koops (2011). 'De Hoge Raad bewijst een slechte dienst in high-tech-crimezaak over botnets'. In: *Nederlands Juristenblad* 86-18, 914-919.

Prakken, H. (2010). *Notities over strafrecht, strafvordering en cybercrime.* Universiteit Utrecht.

Programma Aanpak Cybercrime, Expertgroep Digitaal Opsporen (2011). *De inrichting van Digitale Expertise bij de Nederlandse Politie.*

Raad van Hoofdcommissarissen (2001). *Digitaal blauw. Aan de slag met digitaal rechercheren. Herijking nationaal actieprogramma.*

Seba I. & J. Rowley (2010). 'Knowledge management in UK police forces'. In: *Journal of Knowledge Management* 14-4, 611-626.

Stol, W.Ph. (2004). 'Trends in cybercrime'. In: *Justitiële verkenningen* 30-8, 76-94.

Stol, W.Ph. (2010). 'Kennis cybercrime schiet tekort'. In: *Het Tijdschrift voor de Politie* 72-9, 19-20.

Vrijheid en Verantwoordelijkheid. Regeerakkoord VVD-CDA, 30 september 2011.

WODC, KPMG, Universiteit van Utrecht (2006). *Het functioneren van de rechterlijke organisatie in beeld. Breedtestudie Wet organisatie en bestuur gerechten en Wet Raad voor de rechtspraak*. Den Haag: WODC.

http://www.wodc.nl/onderzoeksdatabase/1477a-high-tech-crime.aspx?cp=44&cs=6836

Bijlage

1 Lijst van gebruikte afkortingen

AIVD	Algemene Inlichtingen- en Veiligheidsdienst
BDE	Bureau Digitale Expertise
BDR	Bureau Digitale Recherche
D&I	Digitaal & Internet (team bij KLPD)
DNR	Dienst Nationale Recherche
Fte	Fulltime-equivalent (volledige formatieplaatsen)
Hbo	Hoger Beroepsonderwijs
ICT	Informatie- en communicatietechnologie
KLPD	Korps Landelijke Politiediensten
LPDO	Landelijk Project Digitaal Opsporen
Mbo	Middelbaar Beroepsonderwijs
NFI	Nederlands Forensisch Instituut
OU	Open Universiteit
OvJ	Officier van Justitie
PAC	Programma Aanpak Cybercrime
PVO	Programma Versterking Opsporing
R&D	Research & Development
RHC	Raad van Hoofdcommissarissen
SLA	Service Level Agreement
Sv	Wetboek van Strafvordering
TDO	Team Digitale Opsporing
TGO	Team Grootschalige Opsporing
THTC	Team High Tech Crime
VKL	Vaste Kern Leidinggevenden
VKU	Vaste Kern Uitvoerenden

2 Over de auteurs

Het onderzoek is uitgevoerd door Pro Facto in samenwerking met Kees de Vey Mestdagh. Pro Facto is een bureau voor juridisch en bestuurskundig onderzoek, advies en onderwijs. Namens Pro Facto participeerden Heinrich Winter en Niko Struiksma in het onderzoek.

Dr. mr. C.N.J. (Kees) de Vey Mestdagh is hoofd van het Centrum voor Recht & ICT van de Faculteit der Rechtsgeleerdheid van de Rijksuniversiteit Groningen. Hij studeerde rechten en psychologie en promoveerde op het gebied van kunstmatige intelligentie en recht. Hij initieerde en implementeerde de unieke bachelor- en masteropleiding Recht & ICT bij de Rijksuniversiteit Groningen. Zijn huidige onderzoek concentreert zich op IT-recht (waaronder privacy en cybercrime), *internet governance* (het bestuur en de regulering van de informatiesamenleving), juridisch kennismanagement (de effectieve inrichting van kennisintensieve organisaties) en juridische kennissystemen. Hij deed eerder onderzoek in de politieorganisatie, onder meer op het gebied van de Wet politiegegevens en de automatisering van de gegevensuitwisseling binnen de politieorganisatie.

Mr. N. (Niko) Struiksma is directeur van Pro Facto. Hij studeerde juridische bestuurswetenschappen aan de Rijksuniversiteit Groningen. Hij is enige tijd als onderzoeker werkzaam geweest bij een regionaal politiekorps en voerde namens Pro Facto diverse onderzoeken uit over de politie, onder andere in opdracht van Politie & Wetenschap. Deze onderzoeken handelden onder meer over de democratische inbedding van de politie, delegatie en mandaat van beheersbevoegdheden, de toepassing van (wetenschappelijke) kennis door de politie, de inschakeling van particuliere forensische instituten door politie en justitie en de uitvoering van de milieutaak door (boven)regionale milieuteams.

Prof. dr. H.B. (Heinrich) Winter is directeur van Pro Facto. Hij studeerde juridische bestuurswetenschappen en sociologie aan de Rijksuniversiteit Groningen en promoveerde op een onderzoek naar de relatie tussen evaluatie en kwaliteit van wetgeving. Naast zijn werk bij Pro Facto is hij parttime werkzaam als bijzonder hoogleraar Toezicht bij de vakgroep Bestuursrecht en Bestuurskunde van de Faculteit Rechtsgeleerdheid van de Rijksuniversiteit Groningen. Hij geeft onderwijs in verschillende juridische en bestuurskundi-

ge mastervakken, waaronder het vak Toezicht en rechtshandhaving. Hij was projectleider van diverse grote empirische onderzoeken en wetsevaluaties (Wet bescherming persoonsgegevens, Embryowet e.a.) in opdracht van verschillende ministeries.

Leden Redactieraad Programma Politie & Wetenschap

Secretariaat Programmabureau Politie & Wetenschap
Politieacademie
Arnhemseweg 348
7334 AC Apeldoorn

Postbus 834
7301 BB Apeldoorn
www.politieenwetenschap.nl

Uitgaven in de reeks Politiekunde

1. ***Criminaliteit in de virtuele ruimte***
   P. van Amersfoort, L. Smit & M. Rietveld, DSP-groep, Amsterdam/ TNO-FEL, Den Haag, 2002

2. ***Cameratoezicht. Goed bekeken?***
   I. van Leiden & H.B. Ferwerda, Advies- en Onderzoeksgroep Beke, Arnhem, 2002

3. ***De 10 stappen van Publiek-Private Samenwerking (PPS)***
   J.C. Wever, A.A. van Pel & L. Smit, DSP-groep, Amsterdam/TNO-FEL, Den Haag, 2002

4. ***De opbrengst van projecten. Een verkennend onderzoek naar de bijdrage van projecten aan diefstalbestrijding***
   C.J.E. In 't Velt, e.a., NPA-Onderzoeksgroep, LSOP, Apeldoorn, 2003

5. ***Cameratoezicht. De menselijke factor***
   A. Weitenberg, E. Jansen, I. van Leiden, J. Kerstholt & H.B. Ferwerda, Advies- en Onderzoeksgroep Beke, Arnhem/TNO, Soesterberg, 2003

6. ***Jeugdgroepen in beeld. Stappenplan en randvoorwaarden voor de shortlist-methodiek***
   H.B. Ferwerda & A. Kloosterman, Advies- en Onderzoeksgroep Beke & Politieregio Gelderland-Midden, Arnhem, 2004 (vierde druk 2006)

7. ***Hooligans in beeld.Van informatie naar aanpak***
   H.B. Ferwerda & O. Adang, Advies- en Onderzoeksgroep Beke, Arnhem/ Onderzoeksgroep Politieacademie Apeldoorn, 2005

8. ***Richtlijnen auditieve confrontatie***
   J.H. Kerstholt, A.G. van Amelsfoort, E.J.M. Jansen & A.P.A. Broeders, TNO Defensie en Veiligheid, Soesterberg/Politieacademie, Apeldoorn/NFI, Den Haag, 2005

9. ***Niet verschenen***

10. ***De opsporingsfunctie binnen de gebiedsgebonden politiezorg***
O. Zoomer, IPIT, Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2006

11. **Inzoomen en uitzoomen op Zaandam**
I. van Leiden & H.B. Ferwerda, Advies- en onderzoeksgroep Beke, Arnhem 2006

12. ***Aansprakelijkheidsmanagement politie. Beschrijving, analyse en handreiking***
E.R. Muller, J.E.M. Polak, C.J.J.M. Stoker m.m.v. M.L. Diepenhorst & S.H.E. Janssen, COT, Instituut voor Veiligheids- en Crisismanagement, Den Haag/Faculteit der Rechtsgeleerdheid Universiteit Leiden, 2006

13. ***Cold cases – een hot issue***
I. van Leiden & H.B. Ferwerda, Advies- en onderzoeksgroep Beke, Arnhem, 2006

14. ***Adrenaline en reflectie. Hoe leren politiemensen op de werkplek?***
A. Beerepoot & G. Walraven e.a., DSP-groep BV, Amsterdam/Walraven onderzoek en advies, 2007

15. ***Tussen aangifte en zaak. Een referentiekader voor het aangifteproces***
W. Landman, L.A.J. Schoenmakers & F. van der Laan, Twynstra Gudde, adviseurs en managers, Amersfoort, 2007

16. ***Baat bij de politie. Een onderzoek naar de opbrengsten voor burgers van het optreden van de politie***
M. Goderie & B. Tierolf, m.m.v. H. Boutellier & F. Dekker, Verwey-Jonker Instituut, Utrecht, 2008

17. ***Hoeveel wordt het vandaag? Een studie naar de kans op voetbalgeweld en het veiligheidsbeleid bij voetbalwedstrijden***
E.J. van der Torre, R.F.J. Spaaij & E.D. Cachet, COT, Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2008

18. ***Overbelast? De administratieve belasting van politiemensen bij de afhandeling van jeugdzaken***
G. Brummelkamp & M. Linssen, EIM, Zoetermeer, 2008

19. ***Geografische daderprofilering. Een inventarisatie van randvoorwaarden en succesfactoren***
G. te Brake & A. Eikelboom, TNO Defensie en Veiligheid, Soesterberg, 2008

20. ***Solosurveillance. Kosten en baten***
S.H. Esselink, J. Broekhuizen & F.M.H.M. Driessen, Bureau Driessen, 2009

21. ***Onderzoek naar de mogelijke meerwaarde van AWARE voor de politie. Ervaringen met een nieuwe aanpak van belaging door ex-partners***
M.Y. Bruinsma, J. van Haaf, R. Römkens & L. Balogh, IVA Beleidsonderzoek en Advies, i.s.m. INTERVICT/Universiteit van Tilburg, 2008

22. ***Gebiedsscan criminaliteit en overlast. Een methodiekbeschrijving***
B. Beke, E. Klein Hofmeijer & P. Versteegh, Bureau Beke, Arnhem, 2008

23. ***Informatiemanagement binnen de politie. Van praktijk tot normatief kader***
V. Bekkers, M. Thaens, G. van Straten & P. Siep; m.m.v. A. Dijkshoorn, Center for Public Innovation, Erasmus Universiteit Rotterdam, 2009

24. ***Nodale praktijken. Empirisch onderzoek naar het nodale politieconcept***
H.B Ferwerda, E.J van der Torre & V. van Bolhuis, Bureau Beke, Arnhem/ COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2009

25. ***Rellen om te rellen. Een studie naar grootschalige openbare-ordeverstoringen en notoire ordeverstoorders***
I. van Leiden, N. Arts & H.B. Ferwerda, Bureau Beke, Arnhem, 2009

26a. ***Verbinden van politie- en veiligheidszorg. Politie en partners over signaleren & adviseren***
W. Landman, P. van Beers & F. van der Laan, Twynstra Gudde, Amersfoort, 2009

26b. ***Politiepolitiek. Een empirisch onderzoek naar politiële signalering & advisering***
E.J.A. Bervoets, E.J. van der Torre & J. Dobbelaar m.m.v. N. Koeman, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2009

27. ***De politie aan zet: de aanpak van veelplegers in Deventer***
I. Bakker & M. Krommendijk, IPIT, Enschede, 2009

28. ***Boven de pet? Een onderzoek naar grootschalige ordehandhaving in Nederland***
O.M.J. Adang (redactie), S.E. Bierman, K. Jagernath-Vermeulen, A. Melsen, M.C.J. Nogarede & W.A.J. van Oorschot, Politieacademie, Apeldoorn, 2009

29. ***Rellen in Ondiep. Ontstaan en afhandeling van grootschalige ordeverstoring in een Utrechtse achterstandswijk***
G.J.M. van den Brink, M.Y. Bruinsma (redactie), L.J. de Graaf, M.J. van Hulst, M.P.C.M. Jochoms, M. van de Klomp, S.R.F. Mali, H. Quint, M. Siesling, G.H. Vogel, Politieacademie, Apeldoorn, 2010

30. ***Burgerparticipatie in de opsporing. Een onderzoek naar aard, werkwijzen en opbrengsten***
A. Cornelissens & H. Ferwerda (redactie), met medewerking van I. van Leiden, N. Arts & T. van Ham, Bureau Beke, Arnhem, 2010

31. ***Poortwachters van de politie. Meldkamers in dagelijks perspectief***
J. Kuppens, E.J.A. Bervoets & H. Ferwerda, Bureau Beke, Arnhem & COT, Den Haag, 2010

32. ***Het integriteitsbeleid van de Nederlandse politie: wat er is en wat ertoe doet***
M.H.M. van Tankeren, Onderzoeksgroep Integriteit van Bestuur, Vrije Universiteit Amsterdam, 2010

33. ***Civiele politie op vredesmissie. Uitzendervaringen van Nederlandse politiefunctionarissen***
H. Sollie, Universiteit Twente, Enschede, 2010

34. ***Ten strijde tegen overlast. Jongerenoverlast op straat: is de Engelse aanpak geschikt voor Nederland?***
M.L. Koemans, Universteit Leiden, 2010

35. ***Het districtelijk opsporingsproces; de black box geopend***
R.M. Kouwenhoven, R.J. Morée &. P. van Beers, Twynstra Gudde, Amersfoort, 2010

36. ***Balanceren tussen alert maken en onrust voorkomen. Publiekscommunicatie over seriële schokkende incidenten (casestudy Lelystad)***
A.J.E. van Hoek, m.m.v. P.F. van Soomeren, M.D. Abraham & J. de Kleuver, DSP-groep, Amsterdam, 2011

37. ***Sturing van blauw. Een onderzoek naar operationele sturing in de basispolitiezorg***
W. Landman, m.m.v. M. Malipaard, Twynstra Gudde, Amersfoort, 2011

38. ***Onder het oppervlak. Een onderzoek naar ontwikkelingen en (a)select optreden rond preventief fouilleren***
J. Kuppens, B. Bremmers, E. van den Brink, K. Ammerlaan & H.B. Ferwerda, m.m.v. E.J. van der Torre, Bureau Beke, Arnhem/COT, Den Haag, 2011

39. ***Naar eigen inzicht? Een onderzoek naar beoordelingsruimte van en grenzen aan de identiteitscontrole***
J. Kuppens, B. Bremmers, K. Ammerlaan & E. van den Brink, Bureau Beke, Arnhem/COT, Den Haag, 2011

40. ***Toezicht op zedendelinquenten door de politie in samenwerking met de reclassering***
H.G. van de Bunt, N.L. Holvast & J. Plaisier, Erasmus Universiteit, Rotterdam/Impact R&D, Amsterdam, 2012

41. ***Daders over cameratoezicht***
H.G.A. van Schijndel, A. Schreijenberg, G.H.J. Homburg & S. Dekkers, Regioplan Beleidsonderzoek, Amsterdam, 2012

42. ***Aanspreken op straat. Het werk van de straatcoach in al zijn verschijningsvormen***
L. Loef, K. Schaafsma & N. Hilhorst, DSP-groep, Amsterdam, 2012