De strafrechtketen in een gedigitaliseerde samenleving

Een onderzoek naar de strafrechtelijke afhandeling van cybercrime

Rutger Leukfeldt
Sander Veenstra
Miranda Domenie
Wouter Stol

Lectoraat Cybersafety
NHL Hogeschool / Politieacademie
Open Universiteit

November 2012

Voorwoord

Dit rapport bevat een weergave van de werking van de strafrechtketen in een gedigitaliseerde samenleving. Met de digitalisering van de samenleving is ook de criminaliteit gedigitaliseerd. Delicten met een digitale component noemen we ook wel cybercrimedelicten of kortweg cybercrime. Dit onderzoek bekijkt hoe de afhandeling van degelijke delicten in de praktijk loopt en wat beslismomenten en afwegingen binnen de strafrechtketen zijn. Het onderzoek is uitgevoerd in opdracht van het Programma Aanpak Cybercrime van de politie en het Intensiveringsprogramma Cybercrime van het Openbaar Ministerie.

Een onderzoek als dit kan alleen tot stand komen dankzij de medewerking van velen. Onze dank gaat uit naar de politiekorpsen, de Arrondisementsparketten en het Parket Generaal van het Openbaar Ministerie voor hun medewerking bij het in kaart brengen van de zaakstroom van cybercrimedelicten. Daarnaast bedanken we alle geïnterviewde medewerkers van de politie, het Openbaar Ministerie en de Zittende Magistratuur voor hun tijd en de informatie die zij ons hebben verschaft.

Rutger Leukfeldt
Sander Veenstra
Miranda Domenie
Wouter Stol

Samenvatting

Inleiding
De samenleving digitaliseert en daarmee het werkaanbod van politie en justitie. Klassieke vormen van criminaliteit, zoals oplichting en smaad, worden nu ook via internet gepleegd. Daarnaast zijn nieuwe criminaliteitsvormen ontstaan, zoals hacken en het verspreiden van virussen. Criminaliteit waarbij ICT een wezenlijke rol speelt in de uitvoering van het delict wordt ook wel cybercrime genoemd. Binnen de strafrechtketen bestaat discussie of cybercrime in ruime zin wel of niet gedefinieerd moet worden als cybercriminaliteit. De vraag is namelijk of sprake is van nieuwe vormen van criminaliteit die ook een nieuwe strafrechtelijke aanpak vereist - zoals bij cybercrimes in enge zin niet zelden het geval is - of dat het gaat om oude criminaliteitsvormen die slechts met nieuwe middelen worden gepleegd. In dat laatste geval bestaat geen noodzaak om in de strafrechtketen veel te veranderen. De discussie over de te hanteren definitie is nog niet afgerond. Wij doen daarover in dit onderzoek geen uitspraken en kiezen er daarom voor om het in de literatuur gangbare onderscheid te behouden. In dit rapport hanteren we dus de term cybercrime voor delicten waarbij ICT een wezenlijke rol heeft speelt bij de realisatie van dat delict. Daarnaast hanteren we de termen cybercrime in ruime zin voor de in de regel klassieke delicten die nu deels of geheeld via digitale middelen gepleegd worden en de term cybercrime in enge zin voor de nieuwe delicten waarbij ICT niet alleen het middel, maar ook het doel is.

De overheid geeft prioriteit aan de bestrijding van cybercrime en neemt verschillende juridische en organisatorische maatregelen. In 2008 gaat bij de politie het Programma Aanpak Cybercrime van start en wordt binnen het Openbaar Ministerie het Intensiveringsprogramma Cybercrime opgericht. Ook is het Kenniscentrum Cybercrime voor de rechtspraak ingesteld. Het regeerakkoord ‘Vrijheid en Verantwoordelijkheid’ van kabinet Rutte spreekt van een ‘integrale aanpak van cybercrime’ (Regeerakkoord, 2010: 42). Dat is een aanpak waaraan tal van partijen bijdragen en waarin de bestrijding van cybercrime zeker niet een zaak is van de strafrechtketen alléén. Maar ook in die benadering is het zaak dat de strafrechtketen in staat is effectief uitvoering te geven aan haar aandeel in de bestrijding van cybercrime.

Over de werking van de strafrechtketen wordt regelmatig geschreven. Zo biedt de publicatiereeks ‘Criminaliteit en Rechtshandhaving’ inzicht in ontwikkelingen in en samenhangen tussen criminaliteit en rechtshandhaving (Kalidien & de Heer-de Lange, 2011) en verscheen onlangs een rapport van de Algemene Rekenkamer (2012) over de afhandeling van geweld en vermogensmisdrijven door de politie. In bestaand onderzoek blijft de strafrechtelijke afhandeling van cybercrime tot dusver echter buiten beschouwing. Het gebrek aan inzicht in de wijze waarop in de strafrechtketen cybercrimezaken worden afgehandeld, vormt dan ook de aanleiding voor onderhavig onderzoek.

Onderzoeksverantwoording
Het doel van dit onderzoek is het verschaffen van inzicht in de wijze waarop politie, Openbaar Ministerie (OM) en de Zittende Magistratuur (ZM) cybercrimezaken afhandelen, zodanig dat zicht ontstaat op mogelijkheden tot verbetering. Uiteindelijk moet het onderzoek daarmee bijdragen aan de bestrijding van cybercrime. De doelstelling van dit onderzoek is vertaald naar vijf hoofdvragen:

1. Waar in de strafrechtketen worden de door de politie in een aangifte opgenomen cybercrimezaken afgedaan?
2. Welke overwegingen spelen bij de politie een rol bij het nemen van beslissingen over de opsporing?
3. Welke overwegingen spelen bij het Openbaar Ministerie een rol bij het nemen van beslissingen over de opsporing en vervolging?
4. Welke overwegingen spelen bij rechters een rol bij het nemen van een beslissing over het opleggen van een straf?
5. Wat zijn knelpunten en best practices binnen het proces van afhandeling?

Om deze onderzoeksvragen te beantwoorden, zijn verschillende onderzoeksmethoden gehanteerd. Allereerst is literatuuronderzoek uitgevoerd naar de wijze waarop strafzaken (in het algemeen) worden afgehandeld in de strafrechtketen. Daarnaast is van 665 cybercrime aangiften geprobeerd in kaart te brengen hoeveel aangiften cybercrime hebben geleid tot een strafzaak. Van de aangiften die niet leidden tot een strafzaak, is getracht na te gaan waar in de strafrechtketen de zaak is blijven 'hangen'. Tot slot is door middel van interviews in kaart gebracht welke overwegingen een rol spelen bij de afhandeling van cybercrimezaken en welke knelpunten er zijn. In totaal zijn met 30 personen binnen de strafrechtketen semigestructureerde interviews gehouden.

De zaakstroom van aangiften cybercrime
Het is niet mogelijk gebleken om een sluitend antwoord te geven op de vraag waar in de strafrechtketen de 665 aangiften worden afgedaan. Van een te groot aantal aangiften ontbreekt daarvoor de benodigde informatie. Dat komt doordat de administraties van de afzonderlijke partners in de strafketen onvolkomen zijn en onvoldoende op elkaar aansluiten, waardoor zicht op aangiften verdwijnt. Uiteindelijk is alleen de wijze waarop de politie aangiften cybercrime afhandelt, voor zover mogelijk, in kaart gebracht. Volgens de politie is aan 43,6 procent van de zaken geen verder gevolg gegeven: die zaken heeft ze naar eigen zeggen zelfstandig afgedaan. Van 30,1 procent van de zaken geeft de politie aan dat ze zijn doorgestuurd naar het OM.

Van ruim een kwart van de aangiften (26,3 procent) is binnen de politie onbekend hoe ze zijn afgehandeld. Dat wordt deels veroorzaakt doordat aangiften die worden doorgestuurd naar een ander korps veelal niet traceerbaar zijn. Het feit dat korpsen die een aangifte toegestuurd krijgen daaraan een nieuw PV-nummer koppelen en/of het oude PV-nummer niet registreren, biedt daarvoor een mogelijke verklaring. Dat de afhandeling van aangiften cybercrime door de politie deels onbekend blijft, heeft tot gevolg dat geen exacte cijfers over de wijze van afhandeling gepresenteerd kunnen worden. Het percentage zaken dat is afgedaan door de politie is vermoedelijk groter dan het percentage naar het OM doorgestuurde zaken en ligt tussen de 43,6 en 69,9. Het percentage naar het OM doorgestuurde zaken ligt vermoedelijk tussen de 30,1 en de 56,3.

Overwegingen bij beslissingen over opsporing, vervolging en berechting
De strafrechtelijke afhandeling van cybercrimezaken is afhankelijk van beslissingen die actoren in het proces van slachtofferschap tot en met veroordeling nemen. Aan die beslissingen liggen verschillende overwegingen ten grondslag.

Allereerst moet sprake zijn van waargenomen slachtofferschap. Als slachtofferschap van een misdrijf niet wordt waargenomen, stroomt de zaak immers per definitie niet de strafketen in. Als sprake is van waargenomen slachtofferschap zijn er vier mogelijke vervolgacties.

Slachtoffers kunnen ten eerste geen actie ondernemen, bijvoorbeeld bij minder ernstige delicten. Ten tweede kan sprake zijn van schadeloosstelling: het slachtoffer ontvangt dan bijvoorbeeld een schadevergoeding van de verzekeraar en daarmee is de kous af. Ook kan het slachtoffer ervoor kiezen om zonder hulp van buitenaf een oplossing te zoeken, bijvoorbeeld door eigenrichting. Tot slot kan het slachtoffer overwegen om aangifte te doen bij de politie.

Als een slachtoffer aangifte wil doen, overweegt een intakemedewerker van de politie in hoeverre het verzoek van de burger tot de kerntaken van de politie behoort. Als de politiemedewerker vindt dat daarvan geen sprake is, wordt geen aangifte opgenomen. Zaken vallen daardoor soms ten onrechte buiten het geregistreerde werkaanbod in de strafrechtketen. De intakemedewerker kan bijvoorbeeld van mening zijn dat sprake is van een civiele zaak terwijl sprake is van een misdrijf. Hoewel ook van klassieke delicten soms ten onrechte geen aangifte wordt opgenomen, ligt het percentage bij de politie gemelde cybercrimezaken waarvan geen document wordt opgemaakt een stuk hoger (Domenie e.a. 2012).

Case screeners beoordelen of de door de politie opgenomen aangiften in behandeling worden genomen. Zij overwegen voornamelijk of een aangifte voldoende aanknopingspunten bevat om tot opsporing over te gaan. Ook beleidsindicatoren, de juridische haalbaarheid en de mate waarin het slachtoffer zelf verantwoordelijk is voor hetgeen hem of haar is overkomen worden overwogen. Hoewel deze beoordelingscriteria grotendeels overeenkomen met voor case screening geldende richtlijnen, maken case screeners daarvan naar eigen zeggen geen gebruik. Beslissingen over het wel of niet in behandeling nemen van een zaak nemen case screeners zelfstandig, zo zeggen zij. Zij roepen daarbij zelden hulp in van anderen, zoals een politiechef of het OM.

Aangiften die door de casescreening komen, worden ten behoeve van het opsporingsonderzoek verrijkt met opsporingsinformatie. Soms doen case screeners dat zelf, maar er zijn in sommige korpsen speciale teams voor ingericht. Tijdens dergelijk vooronderzoek wordt zoveel mogelijk bewijsmateriaal verzameld, zodat de recherche de zaak snel af kan handelen. Mocht het verzamelen van bewijsmateriaal onvoldoende resultaat opleveren, dan kan de zaak alsnog worden opgelegd. Als het wel gelukt is om de aangifte naar tevredenheid te verrijken, dan wordt de aangifte doorgestuurd aan een opsporingsteam. Het werkaanbod is voor opsporingsteams te groot om alle zaken op te pakken. Ook zij maken daarom opnieuw een afweging om een zaak al dan niet in behandeling te maken. De prioriteit van een zaak, de beschikbare capaciteit om een zaak op te pakken en de werkbelasting worden daarbij overwogen. Zaken die niet in behandeling worden genomen, stromen na verloop van tijd de strafrechtketen uit.

Afgehandelde opsporingsonderzoeken worden doorgestuurd naar het OM. De parketsecretaris van het OM toetst zaken vervolgens op juridische haalbaarheid. Hij kan besluiten een zaak voor aanvullingen terug te sturen naar de politie of hij overweegt de voor het OM beschikbare afdoeningswijzen voor strafzaken. Om te besluiten hoe het OM een zaak afhandelt, kan de parketsecretaris gebruik maken van daarvoor opgestelde beleidsregels. Daarin zijn richtlijnen voor strafvordering opgenomen. Het OM kan een zaak seponeren, een strafbeschikking opleggen, een transactie aanbieden of een zaak voor de rechter brengen middels een dagvaarding. Bij dagvaarding bereidt de parketsecretaris de zaak voor op het onderzoek ter zitting. De Officier van Justitie brengt de zaak vervolgens voor de rechter. Hij bepaalt daarbij een strafeis op basis van delictspecifieke richtlijnen voor strafvordering. Dergelijke richtlijnen zijn er nog niet om de strafmaat bij cybercrimes in enge zin vast te stellen.

Als een zaak voor de strafrechter wordt gebracht, toetst de rechter of de verdachte schuldig is aan het ten laste gelegde misdrijf. Er zijn geen rechters speciaal voor de afhandeling van cybercrimezaken. Rechters moeten namelijk alle typen strafzaken kunnen behandelen, dus ook cybercrime, aldus onze respondenten. Om ervoor te zorgen dat rechters eenduidig straffen in vergelijkbare zaken, zijn oriëntatiepunten opgesteld die rechters helpen bij het vaststellen van een straf. Dergelijke richtlijnen bestaan echter, met uizondering van skimmen, nog niet voor cyberdelicten in enge zin.

Knelpunten
Voor zowel klassieke delicten als voor cybercrime geldt dat een aanzienlijk deel van de gepleegde criminaliteit de strafrechtketen niet instroomt.Niet alle (cyber) delicten worden waargenomen en zo wel dan wordt daarvan lang niet altijd aangifte en/of melding gedaan. Volgens recent onderzoek is het aangiftepercentage bij cybercrime nog lager dan bij klassieke delicten (Domenie e.a 2012). Burgers en bedrijven betwijfelen of de politie effectief uitvoering kan geven aan de bestrijding van cybercrime en kiezen er mede daardoor voor om geen aangifte te doen.

Als wel aangifte wordt gedaan, leidt de ontoereikende kennis van intakemedewerkers er toe dat een deel van het werkaanbod cybercrime ten onrechte niet wordt geregistreerd. Er wordt in sommige gevallen bijvoorbeeld geen aangifte opgenomen, terwijl wel sprake is van een strafbaar feit. Bovendien is de kwaliteit van wel opgenomen aangiften door het kennistekort van intakemedewerkers soms te laag, waardoor belangrijke (opsporings)informatie in aangiften ontbreekt. Dat heeft tot gevolg dat dergelijke aangiften al tijdens de casescreening worden opgelegd en dat opsporing, vervolging en berechting dus uitblijft.

Het verrijken van aangiften cybercrime wordt door respondenten als lastiger ervaren dan het verrijken van reguliere aangiften. Dat wordt veroorzaakt door een gebrek aan kennis en een gebrek aan ervaring met het afhandelen van aangiften cybercrime. Daarbij is de politie bij cyberzaken veelal afhankelijk van derden voor de verzameling van bewijsmateriaal: voor het opvragen van NAW gegevens op basis van IP adressen moeten bijvoorbeeld officiële verzoeken bij internetserviceproviders worden ingediend en om op basis van een rekeningnummer persoonsgegevens op te vragen bij een bank moet soms worden betaald. De daarvoor vereiste inspanning en het gebrek aan ervaring met dergelijk opsporingswerk werpen een drempel op om cyberzaken in behandeling te nemen.

Ook binnen opsporingsteams worden klassieke delicten eerder opgepakt dan cyberzaken. Allereerst is sprake van een gebrek aan prioriteit: vaak gaan andere zaken voor. Landelijke doelstellingen op het gebied van cybercrime worden onvoldoende vertaald naar regionale targets waardoor andere zaken voorrang krijgen. Bovendien vergt de afhandeling van cyberzaken volgens respondenten veel tijd, terwijl er (te) weinig capaciteit voorhanden is. Het regio overstijgende of soms zelfs internationale karakter van cyberzaken vraagt bijvoorbeeld om onderzoeksinspanningen in samenwerking met andere korpsen en/of landen. Daarvoor is te weinig menskracht beschikbaar. Opsporingsteams, die in de regel uitsluitend bestaan uit politiemedewerkers zonder digitale expertise, hebben bovendien te weinig kennis om cyberzaken effectief op te pakken. Over de hele linie lijkt een deel van de vroegtijdige uitstroom van cyberzaken bij de politie ongewenst: dergelijke zaken worden wegens voornoemde knelpunten eerder opgelegd dan klassieke delicten. Hierop bestaat geen controle door het OM

Verder is sprake van discontinuïteit in de wijze waarop de aanpak van cybercrime binnen de verschillende organisaties in de strafrechtketen is georganiseerd. Allereerst wordt ketenbreed geen eenduidige definitie van cybercrime gehanteerd. Alleen bij het OM is het merendeel van de medewerkers die we spraken expliciet van mening dat cybercrime in ruime zin geen cybercrime is. Het betreft in essentie klassieke delicten, zoals fraude of stalking, in een digitaal jasje. Alleen cybercrime in enge zin, hardcore vormen van digitale criminaliteit zoals hacken en het platleggen van websites, typeren de OM medewerkers als cybercrime. Opvallend is dat voor de afhandeling van cyberzaken binnen het OM specialisten zijn aangewezen. Zo zijn er cyberparketsecretarissen en cyber Officieren van Justitie. Wat knelt bij het OM is dat deze cyber-specialisten, doordat zij alleen de naar verhouding in kleine mate geregistreerde cybercrimes in enge zin afhandelen, weinig of in een enkel geval soms zelfs geen cyberzaken te behandelen krijgen. Binnen de politie en de rechterlijke macht wordt een dergelijk onderscheid tussen cybercrime in ruime zin en cybercrime in enge zin en de aanpak daarvan niet gemaakt. Er zijn op politiekorpsniveau geen specialistische teams die zich uitsluitend bezig houden met opsporingsonderzoeken naar cybercrime in enge zin en ook zijn er bij de ZM formeel geen cybercrimespecialisten.

Rechters ervaren naar eigen zeggen geen knelpunten in de afhandeling van cyberzaken. Wel merken rechters op dat cybercrimezaken door het geringe werkaanbod minder routine zijn waardoor het ze meer tijd kost om de materie te doorgronden. Ook is er nog weinig jurisprudentie en zijn er in beperkte mate richtlijnen voor straftoemeting bij cyberzaken voorhanden (bij cybercrimes in ruime zin kunnen dezelfde straftoemetingsprinicpes gebruikt worden als bij de offline variant van het delict, bij cybercrimes in ruime zin zijn – behalve voor skimmen – geen richtlijnen voorhanden).Voorgaande leidt er echter niet toe, zo zeggen rechters, dat cyberzaken anders worden afgehandeld dan klassieke delicten. Strafrechters zijn afhankelijk van het door de politie, het OM en de advocatuur aangedragen en begrijpelijk uitgewerkte informatie. Op basis daarvan moeten zij, ongeacht het type delict, in staat zijn om te toetsen of een verdachte schuldig is. Het is daarbij wel de taak van de rechter om te beoordelen of het opsporingsonderzoek deugdelijk is verricht (art 359a Sv). Dat kan lastig zijn bij cyberzaken, maar dat geldt volgens rechters evengoed voor reguliere zaken. Bovendien bestaan over het opsporingsonderzoek in de praktijk lang niet altijd vragen of twijfels. Daardoor kunnen rechters naar eigen zeggen volstaan met de hen aangeleverde informatie bij het vellen van hun oordeel.

Dat rechters naar eigen zeggen geen problemen ervaren met de afhandeling van cybercrimes, betekent niet automatisch dat zij hun onafhankelijke toetsende taak bij cyberzaken al optimaal vervullen. Bij de afhandeling van klassieke zaken hebben rechters vermoedelijk doorgaans wel een beeld van eventuele lacunes in het verrichtte opsporingsonderzoek. Of dergelijke kennis, die nodig is om de kwaliteit van het verrichtte opsporingsonderzoek te beoordelen, onder rechters ook bij cyberzaken al tot gemeengoed is geworden is een vraag voor vervolgonderzoek. Het is immers denkbaar dat rechters, door een gebrek aan ervaring met en kennis over cyberzaken, bepaalde tekortkomingen in opsporingsonderzoek bij cyberzaken niet herkennen en er daardoor onterecht van uit gaan dat zij hun uitspraak kunnen baseren op het aangeleverde en begrijpelijk uitgewerkte bewijsmateriaal. Dat hebben wij echter niet specifiek onderzocht.

Tabel S1: knelpunten in het proces van slachtofferschap tot veroordeling

Knelpunten per procesdeel	Procesdeel	Zie §
Slachtofferschap wordt niet waargenomen en/of gemeld bij de politie	Slachtofferschap aangifte	6.2
Ongewenste uitstroom van cyberzaken bij de politie door: - het gebrek aan kennis tijdens het opnemen van aangiften cybercrime; - het gebrek aan kwaliteit van opgenomen aangiften; - het gebrek aan kennis en ervaring die vereist is om aangiften cybercrime te verrijken met opsporingsinformatie; - hindernissen in de samenwerking tussen politie en private instellingen (providers en banken); - het gebrek aan zicht van het OM op de uitstroom tijdens intake en case screening.	Intake en casescreening door politie	6.3
Knelpunten in de opsporing: - gebrek aan prioriteit voor de opsporing van cybercrime; - gebrek aan gekwalificeerde (kennis) politiecapaciteit voor de opsporing van cybercrime.	Opsporing door politie	6.4
Gespecialiseerde cyber-OvJ's krijgen weinig of geen cyberzaken	Openbaar Ministerie	6.5
Rechters ervaren geen problemen met het beoordelen van cybercrime omdat politie en OM begrijpelijk uitgewerkte dossiers aanleveren. Onduidelijk is gebleven in hoeverre rechters hun onafhankelijke, toetsende taak ook wat cybercrime betreft al optimaal (kunnen) vervullen.	Zittende Magistratuur	6.6
Discontinuïteit in de aanpak van cybercrime binnen de strafrechtketen.	Ketenbreed	6.3 – 6.6

Conclusies

Allereerst is het niet mogelijk gebleken om op een kwalitatieve manier een sluitend antwoord te geven op de vraag waar in de strafrechtketen de door de politie in een aangifte opgenomen cyberzaken worden afgedaan. Dat wordt veroorzaakt doordat de administraties van de afzonderlijke partners in de strafrechtketen onvolkomen zijn en onvoldoende op elkaar aansluiten. Dat is overigens geen nieuwe conclusie: in eerder onderzoek werd ook al geconcludeerd dat de adminstratieve processen van de politie en het OM niet optimaal op elkaar zijn afgestemd (Algemene Rekenkamer, 2012; Brug, 2009; Leertouwer & Kalidien, 2011).

Uit het kwantitatieve onderzoeksdeel naar de zaakstroom van aangiften cybercrime blijkt wel dat de wijze waarop de politie cybercrimezaken afhandelt verschilt per delictsoort. De wijze van afhandeling hangt af van de mate van complexiteit en prioriteit van een zaak. De relatief complexe hackenzaken worden bijvoorbeeld relatief vaak afgedaan door de politie, hetgeen betekent dat ze worden opgelegd en geen vervolg krijgen. Aan e-fraude zaken, die door politiemedewerkers veelal worden getypeerd als 'eigen schuld, dikke bult' zaken, wordt geen prioriteit gegeven en ook dergelijke zaken worden dus relatief vaak door de politie opgelegd.

Kinderpornozaken daarentegen, waaraan prioriteit wordt gegeven, worden relatief vaak doorgestuurd naar het OM.

Slachtofferschap van cybercrime wordt niet altijd waargenomen. Daarnaast wordt van een aanzienlijk deel van de wel waargenomen cybercrimes geen aangifte gedaan. En als wel aangifte wordt gedaan dan zorgt de ontoereikende kennis van intakemedewerkers ervoor dat meldingen/aangiften soms ten onrechte niet worden geregistreerd. Kortom, een aanzienlijk deel van de cyber delicten komt nooit in de strafrechtketen terecht.

Als cyberzaken wel de strafrechtketen instromen, dan zorgt een gebrek aan kennis, prioriteit en capaciteit voor de aanpak van cybercrime voor een ongewenste uitstroom van cyberzaken. In opgenomen aangiften ontbreekt relevante opsporingsinformatie, omdat de kennis van intakemedewerkers om dergelijke informatie te verzamelen ontoereikend is. Vervolgens leggen case screeners aangiften cybercrime door het gebrek aan opsporingsinformatie al in een vroegtijdig stadium op, waardoor opsporing, vervolging en berechting uitblijven. Cyberzaken die wel door de screening komen, verliezen het in prioritering van klassieke delicten bij de politie. Dat komt doordat andere zaken voor gaan (zaken met bloed, bijvoorbeeld) en ook doordat politiemedewerkers weinig ervaring hebben met de afhandeling van zaken met een digitale component. Zij beschouwen cyberzaken als arbeidsintensief en lastig. Er is binnen opsporingsteams te weinig kennis voorhanden om cybercrime op te pakken

Rechters ervaren naar eigen zeggen geen problemen met de afhandeling van cyberzaken. Dat komt, zo zeggen zij, doordat zij doorgaans op basis van het door de politie, het OM en de verdediging aangeleverde bewijsmateriaal een uitspraak kunnen doen. Hoewel het formeel een taak van de rechter is om een oordeel te vellen over de kwaliteit van het verrichtte opsporingsonderzoek, bestaan daarover volgens rechters in de praktijk lang niet altijd vragen of twijfels. Aangezien cyberzaken en de opsporingsmethoden die worden gebruikt om de bewijsvoering bij dergelijke zaken rond te krijgen relatief nieuw zijn, is het denkbaar dat de politie en het OM wel degelijk steken laten vallen in opsporingsonderzoeken, maar dat rechters dergelijke lacunes (nog) niet herkennen. Of de kennis van rechters in de praktijk toereikend is om verichtte opsporingsonderzoeken in cyberzaken op waarde te schatten is een vraag voor vervolgonderzoek. Wij hebben dat niet specifiek onderzocht.

Tot slot ontbreekt het aan continuïteit in de wijze waarop de aanpak van cybercrime binnen de verschillende organisaties in de strafrechtketen is georganiseerd. De politie probeert de aanpak van cybercrime te integreren in haar alledaagse werkzaamheden en ondervindt daarin, wegens het gebrek aan kennis, prioriteit en geschikte capaciteit problemen. Het OM heeft maatregelen getroffen om cybercrime in enge zin aan te kunnen pakken, door cyber secretarissen en cyber officieren aan te stellen en de ZM heeft weer geen cyber-specialisten. Er is aldus geen sprake van een eenduidige op elkaar afgestemde ketenbrede aanpak. In plaats daarvan werken politie, OM en ZM op uiteenlopende wijze aan de bestrijding van cybercrime.

Inhoudsopgave

1. Inleiding

Digitalisering en criminaliteit
Onze samenleving digitaliseert in een rap tempo. Burgers, bedrijven en overheden maken volop gebruik van nieuwe technologie, bijvoorbeeld om met elkaar te communiceren, sociale contacten te onderhouden en handel te drijven. De digitalisering heeft er echter ook voor gezorgd dat er nieuwe manieren zijn om criminaliteit te plegen. Om te beginnen zijn er 'klassieke' vormen van criminaliteit die nu (ook) via internet gepleegd worden. Voorbeelden zijn fraudeurs die via websites mensen oplichten, pedofielen die via cybernetwerken kinderporno verspreiden, en stalkers die ook via internet methoden vinden om hun slachtoffer lastig te vallen. Het gaat bij deze voorbeelden als het ware om oude wijn in nieuwe zakken – oude criminaliteit die wordt gepleegd met nieuwe (digitale) middelen. Dit heet ook wel cybercrime in ruime zin. Daarnaast zijn nieuwe criminaliteitsvormen ontstaan zoals hacken en het verspreiden van computervirussen. Het betreft delicten waarbij ICT niet alleen het middel maar ook het doelwit is. Dit wordt ook wel cybercrime in enge zin genoemd. Beide vormen van criminaliteit worden in dit rapport gedefinieerd als cybercrime: criminaliteit waarbij ICT een wezenlijke rol speelt in de realisatie van het delict.

Binnen de strafrechtketen is in discussie of cybercrime in ruime zin wel gedefinieerd moet worden als cybercriminaliteit. De vraag is of sprake is van nieuwe criminaliteit die ook een nieuwe strafrechtelijke aanpak vereist - zoals bij cybercrimes in enge zin het geval is - of dat het gaat om oude criminaliteit die slechts met nieuwe middelen wordt gepleegd. In dat laatste geval bestaat niet direct een noodzaak om in de strafrechtketen veel te veranderen. De strafrechtketen is van oudsher namelijk al ingericht op veranderende werkwijzen van criminelen. De politie werkt bijvoorbeeld sinds de jaren vijftig van de vorige eeuw met een 'modus operandi systeem' (MO-systeem, later Herkenningsdienstsysteem HKS) waarin zij bijhoudt op welke wijze delicten worden gepleegd (Stol, 1996; Rademaker 1996). Ontstaan er onder criminelen nieuwe werkwijzen, al dan niet op basis van nieuwe technologie, dan vergaart de politie kennis daarover en ontwikkelt contra-strategieën, maar ze ontwikkelt geen nieuwe afdelingen en procedures. Een nieuwe MO pareert de politie van oudsher dus binnen bestaande structuren.

De discussie over de te hanteren definitie is nog niet afgerond. Wij doen daarover in dit onderzoek geen uitspraken en kiezen er daarom in dit onderzoek voor om het in de literatuur gehanteerde onderscheid te behouden (zie voor een uitvoerige beschrijving Domenie e.a., 2012). In dit rapport hanteren we dus de term cybercrime voor delicten waarbij ICT een wezenlijke rol speelt in de realisatie van dat delict. Daarnaast hanteren we de term 'cybercrime in ruime zin' voor de in de regel klassieke delicten die nu deels of geheel via digitale middelen gepleegd worden, en de term 'cybercrime in enge zin' voor de delicten waarbij ICT niet alleen het middel, maar ook het doel is.

Digitalisering en de strafrechtketen
Criminaliteitsbestrijding vereist kennis over de aard en omvang van criminaliteit. Bij herhaling wordt echter geconstateerd dat het gebrek aan kennis het primaire probleem vormt bij de bestrijding van cybercrime (zie Stol, 2004; Van der Hulst & Neve, 2008). Toutenhoofd e.a. (2009) constateren bijvoorbeeld dat het kennisniveau van intakemedewerkers bij de politie onvoldoende is om aangiften van delicten met een digitale component op te nemen. Niet zelden wordt een aangever van cybercrime door de politie onverrichter zake weggestuurd en 'panklare zaken' worden volgens aangevers niet afgehandeld door de politie.

Dat was de situatie in 2009. Inmiddels zijn we drie jaar verder en zijn er inspanningen verricht om deze situatie te verbeteren. In het themanummer 'Veiligheid in cyberspace' van Justitiële Verkenningen (2012) maken Stol, Leukfeldt en Klap de balans op en zij concluderen: 'Het totaalbeeld dat oprijst anno 2012 is dat van een politie die nog flink wat heeft in te halen op de samenleving die haar omringt, niet zozeer omdat er geen actie wordt ondernomen maar wel omdat de acties nog pril zijn en nog te veel het karakter hebben van pionierswerk van enkelen, zoals de mensen verbonden aan de PAC-projecten (Programma Aanpak Cybercrime). "Digitaal" is ten onrechte nog geen normaal en integraal onderdeel van de politieorganisatie in de volle breedte.' (2012:37). Eenzelfde conclusie is te lezen in het rapport 'De organisatie van de opsporing van cybercrime door de Nederlandse politie' (Struiksma e.a., 2012).

Aandacht voor de kwaliteit van politiewerk is één ding, maar de strafrechtelijke aanpak van cybercrime is niet alleen afhankelijk van hoe adequaat de politie met de materie omgaat. Het functioneren van de gehele strafrechtketen is daarbij aan de orde: in het proces van opsporing, vervolging en berechting hebben naast de Politie ook het Openbaar Ministerie (OM) en de Zittende Magistratuur (ZM) een rol[1].

De overheid geeft sinds 2007-2008 nadrukkelijk prioriteit aan de bestrijding van cybercrime In 2008 gaat bij de politie het Programma Aanpak Cybercrime (PAC) van start (Programmaplan PAC, 2008) en wordt binnen het Openbaar Ministerie (OM) het Intensiveringsprogramma Cybercrime opgericht (OM, 2008/2009). Daarnaast is het Kenniscentrum Cybercrime voor de rechtspraak ingesteld (www.rechtspraak.nl[2]). Het regeerakkoord 'Vrijheid en Verantwoordelijkheid' van kabinet Rutte (2010-2012) spreekt van een 'integrale aanpak van cybercrime' (Regeerakkoord, 2010: 42). Dat is een aanpak waaraan tal van partijen bijdragen en waarin de bestrijding van cybercrime zeker niet een zaak is van de strafrechtketen alléén. Maar ook in die benadering is het zaak dat de strafrechtketen in staat is effectief uitvoering te geven aan haar aandeel in de bestrijding van cybercrime.

Over de werking van de strafrechtketen is recentelijk nog geschreven. De publicatiereeks 'Criminaliteit en Rechtshandhaving' van het WODC, biedt inzicht in ontwikkelingen in en samenhangen tussen criminaliteit en rechtshandhaving. De recentste rapportage geeft onder andere een overzicht van de zaakstroom van misdrijven in de strafrechtketen (Kalidien & De Heer-de Lange, 2011). Daarnaast geeft de Algemene Rekenkamer (2012) een beeld van de afhandeling van geweld- en vermogensmisdrijven (ruim tweederde van alle misdrijven binnen de strafrechtketen). De rapportages wijzen op tal van verbeterpunten maar bieden geen inzicht in de strafrechtelijke afhandeling van cybercrime.

De hierboven gememoreerde bevindingen omtrent de behandeling van cybercrime door de politie roepen de vraag op hoe het zit met de aanpak van cybercrime in de gehele strafrechtketen. Het gebrek aan inzicht in de wijze waarop in de gehele strafrechtketen cybercrimezaken worden afgehandeld, vormt de aanleiding tot onderhavig onderzoek. Op basis van literatuuronderzoek, een kwantitatieve analyse over 665 cybercrimezaken en diepte-

[1] Tot de strafrechtketen behoren ook de Justitiële Inrichtingen en de Reclassering. Zij zijn belast met de tenuitvoerlegging van opgelegde straffen. In deze rapportage staat het proces van opsporing tot en met berechting centraal. De tenuitvoerlegging van straffen wordt buiten beschouwing gelaten. Als wordt gesproken over de strafrechtketen wordt daarmee dus het proces van opsporing (Politie), vervolging (OM) en berechting (ZM) bedoeld.

[2] http://www.rechtspraak.nl/Organisatie/Gerechtshoven/DenHaag/OverHetGerechtshof/Organisatie/Pages/Kenniscentrum-Cybercrime.aspx, laatst geraadpleegd op: 2012-02-23

interviews met actoren uit de strafrechtketen, biedt dit onderzoek inzicht in het strafrechtelijke afhandelproces van cybercrimezaken en de overwegingen die daarbij een rol spelen.

Leeswijzer
In hoofdstuk 2 wordt de methodische verantwoording van dit onderzoek beschreven. Aan bod komen onderzoeksdoel en -vragen en gebruikte methoden. Hoofdstuk 3 bevat een beschrijving van het proces van slachtofferschap tot veroordeling. Hierin beschrijven we welke actoren een rol spelen en wat hun keuzemogelijkheden zijn. Ook beschrijven we op basis van de literatuur de doorstroom van zaken binnen de strafrechtketen, in algemene zin. In hoofdstuk 4 bespreken we vervolgens de doorstroom van *cybercrime* in de strafrechtketen. In hoofdstuk 5 schetsen we de overwegingen die ten grondslag liggen aan de keuzes van actoren bij beslissingen over de opsporing, vervolging en berechting van (cybercrime)zaken. Hoofdstuk 6 bevat een weergave van de knelpunten in de doorstroom van cybercrimezaken. In hoofdstuk 7 staan de conclusies van dit onderzoek..

2. Onderzoeksopzet en methodische verantwoording

2.1 Onderzoeksopzet

Onderwerp en definitie
De samenleving digitaliseert en daarmee het werkaanbod van politie en justitie. Steeds meer zaken kennen een digitale component. Dit onderzoek gaat over de wijze waarop de strafrechtketen cybercrime afhandelt. In de literatuur worden verschillende definities van cybercrime gehanteerd (zie PAC, 2008; Van der Hulst en Neve, 2008). In hoofdstuk 1 is ingegaan op de discussie omtrent het begrip cybercrime (zie voor een uitbebreidere beschrijving Domenie e.a., 2012). In dit onderzoek wordt cybercrime gedefinieerd als alle vormen van criminaliteit waarbij ICT een wezenlijke rol speelt in de realisatie van het delict. Daarbij worden twee subcategorieën onderscheiden. Voor delicten waarbij ICT zowel instrument als doelwit is, hanteren we de term 'cybercrime in enge zin'. Voorbeelden zijn hacken en de verspreiding van virussen. Het zijn delicten die voor de komst van cyberspace nog niet bestonden. De tweede subcategorie, 'cybercrime in ruime zin', omvat klassieke vormen van criminaliteit die nu (ook) via internet gepleegd worden. Het betreft delicten waarbij ICT van wezenlijk belang is voor de uitvoering maar waarbij ICT geen doelwit is. Voorbeelden daarvan zijn fraude via veiling/verkoopsites, diefstal in virtuele werelden of de verspreiding van kinderpornografie.

Figuur 2.1: definitie van cybercrime

Cybercrime	
Alle vormen van criminaliteit waarbij ICT een wezenlijke rol speelt in de realisatie van het delict	
In ruime zin (cybercriminaliteit)	**In enge zin (computercriminaliteit)**
Dit omvat alle (traditionele) criminele activiteiten waarbij ICT van wezenlijk belang is voor de uitvoering zonder dat ICT expliciet doelwit is van de criminele activiteiten (E-fraude, smaad of laster via internet).	*Dit omvat alle criminele activiteiten waarbij ICT als instrument wordt gebruikt én waarbij ICT expliciet doelwit is van de criminele activiteiten (hacken, wijzigen of vernietigen van digitale gegevens).*

We zijn ons er van bewust dat het begrip cybercrime daarmee weliswaar is ingeperkt, maar nog niet van een scherpe grens is voorzien. De vraag blijft namelijk wanneer ICT van wezenlijk belang is en wanneer ICT alleen als een hulpmiddel is gebruikt en we dus niet spreken van cybercrime (bijvoorbeeld de inbreker die met Google-maps een vluchtroute uitstippelt). In dit onderzoeksrapport spelen dergelijke grensgevallen echter geen rol.

Doel van onderzoek
Het doel van dit onderzoek is het leveren van een bijdrage aan de bestrijding van cybercrime. Het dichterbij gelegen doel is het verschaffen van inzicht in de wijze waarop politie, OM en ZM cybercrimezaken afhandelen, zodanig dat zicht ontstaat op mogelijkheden tot verbetering.

Onderzoekvragen
Voornoemde doelstelling is vertaald naar vijf hoofdvragen:

1. Waar in de strafrechtketen worden de door de politie in een aangifte opgenomen cybercrimezaken afgedaan? (Hoeveel zaken gaan door naar het OM? Hoeveel zaken komen voor de rechter? In hoeveel zaken volgt een veroordeling?)
2. Welke overwegingen spelen bij de politie een rol bij het nemen van beslissingen over de opsporing?
3. Welke overwegingen spelen bij het Openbaar Ministerie een rol bij het nemen van beslissingen over de opsporing en vervolging?
4. Welke overwegingen spelen bij rechters een rol bij het nemen van een beslissing over het opleggen van een straf?
5. Wat zijn knelpunten en *best practices*?

Met de beantwoording van vraag 1 wordt de zaakstroom van aangiften cybercrime in kaart gebracht. We schetsen een beeld van welke weg een aangifte cybercrime bewandelt. Daarnaast is het van belang om te weten welke overwegingen van politie, justitie en de rechtbank ten grondslag liggen aan het nemen van beslissingen. Deze beslissingen bepalen immers het procesverloop van een zaak. Hiertoe zijn onderzoeksvraag 2 t/m 4 geformuleerd. De laatste onderzoeksvraag is gericht op het signaleren van verbetermogelijkheden.

We maken onderscheid tussen hoe de afhandeling volgens de regels zou moeten verlopen en hoe het werk in de praktijk verloopt. Als er niets op papier staat aangaande de afhandeling van aangiften cybercrime, luidt de conclusie dat deze afhandeling niet specifiek is geregeld. Het kan dan nog zijn dat de afhandeling van aangiften in het algemeen wel is vastgelegd. In dat geval worden de algemene regels aangenomen als de regels die ook gelden voor cybercrime. Immers, als er regels zijn gesteld voor de afhandeling van ‘een strafbaar feit’ zonder uitzondering, dan gelden die regels ook voor cybercrime. Tijdens interviews is gevraagd hoe de afhandeling van cybercrime in de praktijk verloopt en wat daarbinnen eventuele good practices of verbeterpunten zijn.

De hoofdvragen uitgewerkt
De onderzoeksvragen zijn als volgt in deelvragen uitgewerkt.

1. Waar in de strafrechtketen worden aangiften cybercrime afgedaan?
   a) Hoeveel procent van de opgenomen aangiften wordt door de politie afgedaan? Hoe? Wat is de aard van de zaken (per afdoeningswijze)?
   b) Hoeveel procent van de zaken wordt door politie naar het OM gestuurd? Wat is de aard van deze zaken?
   c) Hoeveel procent van de aangiften cybercrime die bij het OM komen, worden door het OM afgedaan? Hoe? Wat is de aard van deze zaken (per afdoeningwijze)?
   d) Hoeveel procent van de zaken wordt door het OM voor de rechter gebracht? Wat is de aard van de zaken?
   e) Hoeveel procent van de aangiften cybercrime die voor de rechter komen, worden door de rechter afgedaan? Hoe? Wat is de aard van deze zaken (per afdoeningswijze)? Wat is de (eventueel) opgelegde straf?

2. Welke overwegingen spelen bij de politie een rol bij het nemen van beslissingen over de opsporing?

   Op papier
   a) Wat zijn de procedures voor de afhandeling van aangiften cybercrime bij de politie?
   b) Zijn er procedures vastgelegd voor case-screening van aangiften cybercrime? Hoe luiden ze?
   c) Zijn criteria vastgelegd op grond waarvan de politie aangiften cybercrime doorstuurt naar het OM? Zijn hiervoor afspraken gemaakt met het OM?

   In de praktijk
   d) Gebruikt de politie procedures voor case-screening van aangiften cybercrime?
   e) Hoe verloopt case-screening van aangiften cybercrime?
   f) Op grond van welke criteria stuurt de politie aangiften cybercrime door naar het OM?
   g) Welke problemen inzake opsporing hebben politiemensen met de opgemaakte processen-verbaal?
   h) Welke overwegingen spelen een rol bij het wel of niet doorsturen van aangiften naar het OM? Waarom worden aangiften wel of niet doorgestuurd? Wat was het alternatief?

3. Welke overwegingen spelen bij het *openbaar ministerie* een rol bij het nemen van beslissingen over de opsporing en vervolging?

   Op papier
   a) Zijn er procedures voor in 'welke gevallen van cybercrime' verder onderzoek wordt gedaan?
   b) Zijn er procedures voor wanneer men overgaat tot vervolging van een cybercrime-zaak?

   In de praktijk
   c) Gebruikt het OM procedures voor wanneer men overgaat tot verder onderzoek?
   d) Gebruikt het OM procedures voor wanneer men overgaat tot vervolging van een cybercrime zaak?
   e) Welke overwegingen spelen een rol bij de beslissing tot verder onderzoek en/of vervolging? Wat zijn de alternatieven?
   f) Welke juridische problemen hebben parketsecretarissen en officieren met de wel ingestuurde processen verbaal?
   g) Hoe beoordelen parket secretarissen en officieren van justitie de kwaliteit van processen-verbaal cybercrime?

4. Welke overwegingen spelen bij *rechters* een rol bij het nemen van beslissingen over het opleggen van een straf?

   Op papier
   a) Zijn er procedures voor het opleggen van een straf voor het plegen van een cybercrime?

   In de praktijk
   b) Welke factoren spelen een rol bij het opleggen van een straf? Welke factoren spelen een rol bij de wijze waarop een dader gestraft wordt?

5. Wat zijn knelpunten en *best practices*?
   a) Welke knelpunten en best practices zien respondenten bij het opsporen en vervolgen van cybercrimezaken?
   b) Welke knelpunten en best practices volgen uit de overige onderzoeksbevindingen?
   c) Hoe kunnen knelpunten worden opgelost en *best practices* worden benut?
   d) Welke aanbevelingen kunnen op basis van het onderzoek worden gedaan? Welke mogelijkheden zien respondenten? Welke mogelijkheden voor verbetering volgen uit de onderzoeksbevindingen?

Onderzoeksontwerp en methoden
Het onderzoek is een casestudy met een mix van kwantitatieve en kwalitatieve methoden, met nadruk op die laatste. Het kwantitatieve deel betreft een analyse van de strafrechtelijke afhandeling van 665 processen-verbaal van aangiften cybercrime over heel Nederland. Het kwalitatieve deel omvat een literatuurstudie, een analyse van beleidsdocumenten en een serie interviews. De interviews zijn afgenomen bij de parketten Groningen, Rotterdam, Utrecht en Haarlem en de daarbij horende regiokorpsen van de politie. Hierna wordt verantwoord hoe de onderzoeksmethoden zijn ingezet.

2.2 Methodische verantwoording

1) Literatuurstudie/documentenanalyse
Er is een literatuurstudie uitgevoerd naar de wijze waarop strafzaken in het algemeen worden afgehandeld in de keten (zie hoofdstuk 3). Daarvoor is gebruik gemaakt van literatuur over de werking van de strafrechtketen en van specifieke beleids- en visiedocumenten van politie en justitie over de afhandeling van strafzaken. Gezocht is zowel naar cybercrime-specifieke als algemene documenten. Beleids- en visiedocumenten van politie en justitie zijn verzameld via PolitieKennisNet, het Intensiveringsprogramma Cybercrime van het OM en het Programma Aanpak Cybercrime van de politie. Daarnaast is tijdens de interviews steeds gevraagd of er beleidsstukken beschikbaar waren voor analyse. Specifiek beleid omtrent cybercrime is echter schaars.

2) *Kwantitatieve dossieranalyse*
Het doel van de kwantitatieve analyse was om de (cijfermatige) zaakstroom van aangiften cybercrime in de strafrechtketen in kaart te brengen. Voor het onderzoek is gebruik gemaakt van dossiers uit de *Verkenning Cybercrime in Nederland 2009* (Leukfeldt, e.a., 2010). De Verkenning Cybercrime Nederland (VCN) bestond uit een analyse van 665 politiedossiers naar de aard, omvang en kenmerken van daders van vijf cybercrimes. Deze dossiers cybercrime omvatten:

- 139 aangiften hacken (2007);
- 314 aangiften e-fraude (2006-2007);
- 13 aangiften cyberafpersen (2003-2007);
- 40 aangiften haatzaaien (2003-2007);
- 159 aangiften kinderporno (2007).

Van deze aangiften is geprobeerd in kaart te brengen hoeveel hebben geleid tot een strafzaak. Van de aangiften die niet leidden tot een strafzaak, is getracht na te gaan waar in de strafrechtketen de zaak is blijven ‘hangen’. 18 van de 665 dossiers uit de VCN bleken ongeschikt voor het onderzoek naar de afhandeling van aangiften cybercrime. Dat komt doordat de PV-nummers van deze dossiers tijdens de fase van dataverzameling voor de VCN foutief geregistreerd en dus per definitie niet terug te vinden zijn in de systemen van politie en

justitie. Daardoor is de afhandeling van 647 aangiften cybercrime onderzocht. Het bieden van inzicht in de zaakstroom van aangiften cybercrime bleek echter geen sinecure en is dan ook slechts voor een deel geslaagd. Hierna is uiteengezet hoe de kwantitatieve dossieranalyse is uitgevoerd en tegen welke knelpunten we daarbij zijn aangelopen.

Om de afhandeling van aangiften cybercrime binnen de strafrechtketen in kaart te brengen, moest allereerst inzicht worden verkregen in de afhandeling bij de politie. Voor de VCN is gebruik gemaakt van aangiften cybercrime uit alle politiekorpsen in Nederland. Alle politiekorpsen is daarom verzocht om aan te geven hoe de in dat korps opgenomen aangiften zijn afgehandeld[3]. Van 73,7 procent van de zaken weet de politie aan te geven hoe zij zijn afgehandeld (paragraaf 4.2). De politie vindt over 26,3 procent van de aangiften geen informatie terug over de afhandeling. Dat wordt (deels) veroorzaakt doordat zaken die worden doorgestuurd naar een ander korps, vaak niet meer te traceren zijn. Dat dergelijke zaken niet worden teruggevonden is mogelijkerwijs te wijten aan het feit dat korpsen die een dossier toegestuurd krijgen, daaraan een nieuw PV-nummer koppelen (zonder het originele PV-nummer te registreren).

Volgens de politie is 30,1 procent (n=195) van de zaken naar het OM doorgestuurd. Bij het OM zochten we naar informatie over de strafrechtelijke afhandeling van deze zaken. Er is gezocht in OM Data. Dat is een systeem waarin de afhandeling van alle bij het OM binnengekomen zaken wordt geregistreerd. In OM Data kan (onder andere) gezocht worden op PV-nummers (die door de politie worden gebruikt om zaken te registreren) en op parketnummers (registratienummers van het OM). Van beide mogelijkheden is gebruik gemaakt. Van alle zaken was een PV-nummer bekend. Daarbij moet worden opgemerkt dat de door de politie gebruikte PV-nummers niet altijd door het OM worden geregistreerd. Het had dus de voorkeur om in de systemen van het OM te zoeken op parketnummers. Van 67,2 procent (n=131) van de naar het OM gestuurde zaken is een parketnummer bekend. Desondanks vonden we met behulp van OM Data slechts over 41,5 procent (n=81) van deze zaken informatie over de strafrechtelijke afhandeling. Dat betekent dat we meer dan de helft van de zaken die volgens de politie doorgestuurd zijn naar het OM, daar niet hebben teruggevonden. Volgens de Algemene Rekenkamer wordt het niet terug kunnen vinden van door de politie naar het OM gestuurde dossiers deels veroorzaakt doordat de politie en het OM ingekomen zaken op uiteenlopende wijze registreren. De politie werkt met zaaksgebonden dossiers en het OM hanteert persoonsgebonden dossiers. Iedere aangifte is een zaak, maar bij een zaak kunnen meerdere verdachte personen betrokken zijn en bovendien kan een persoon verdacht worden van verschillende misdrijven (Algemene Rekenkamer, 2012). Van de wel bij het OM teruggevonden zaken is bovendien niet met honderd procent zekerheid te zeggen dat we de juiste zaak hebben teruggevonden. Soms vonden we bij een PV-nummer dat bij ons hoorde bij een e-fraude, bij het OM een zaak die als verkeersdelict staat geregistreerd. Dus: ook al klopten de nummers, uit de bij de zaak opgenomen codes inzake de aard van het delict bleek dan dat het ging om een ander soort zaak. Hoe dat mogelijk was, hebben we niet kunnen achterhalen. Om zeker te weten of de afhandeling van de juiste zaak in kaart is gebracht, zouden alle dossiers ingezien moeten worden. Dat ging het bestek van dit onderzoek te buiten.

Omdat op basis van PV- en parketnummers te weinig zaken werden teruggevonden, is ook geprobeerd om in OM Data zaken terug te vinden op basis van kenmerken van verdachten (naam, geboortedatum en –plaats) uit de politiedossiers. De resultaten bevatten echter te veel

[3] Deze vraag is uitgezet bij de Regiogebonden Informatie Knooppunten van de politie

ruis: alle zaken waarbij verdachten met soortgelijke kenmerken (bijvoorbeeld dezelfde achternaam en/of woonplaats) betrokken waren kwamen uit die zoekslag naar voren. Het betrof dus niet per se dezelfde verdachten en/of dezelfde zaken als die voor de VCN werden geregistreerd. Een zoekslag in OM Data op basis van verdachtenkenmerken leverde 12.108 hits op. Vervolgens stonden we voor de vraag welke van deze zaken overeen kwamen met de zaken waarvan we het spoor zochten. Om dat vast te stellen, zouden we alle 12.108 gevonden dossiers handmatig moeten beoordelen. Ook dat viel buiten het bereik van dit onderzoek.

De bevinding dat de administratieve processen van de politie en het OM niet optimaal op elkaar zijn afgestemd is niet nieuw (Algemene Rekenkamer, 2012; Brug, 2009; Leertouwer & Kalidien, 2011). De Algemene Rekenkamer concludeert daarover bijvoorbeeld dat de betrokken organisaties '*zich niet sluitend (in kwantitatieve zin) kunnen verantwoorden over hun zaakafhandeling: instroom-, uitstroom- en voorraadgegevens sluiten niet op elkaar aan of zijn onbekend*' (2012:9). Van een te groot aantal aangiften ontbreekt daardoor de benodigde informatie om betrouwbare uitspraken te doen over de strafrechtelijke afhandeling van cybercrime door het Openbaar Ministerie en de Zittende Magistratuur. Om die reden is in overleg met de opdrachtgever besloten om het kwantitatieve deel van het onderzoek te staken. Uiteindelijk is dus alleen in kaart gebracht de wijze waarop de politie aangiften cybercrime heeft afgehandeld. In hoofdstuk 4 wordt de afhandeling van aangiften cybercrime door de politie voor zover mogelijk beschreven.

Toestemming
Voor de inzage in politiegegevens en informatie over de tenlastelegging, afdoeningsbeslissing en het eventuele vonnis in de zaken die horen bij de 665 aangiften heeft het College van procureurs-generaal namens de Minister van Justitie toestemming verleend.

3) *Interviews*
Met behulp van interviews is in kaart gebracht welke overwegingen een rol spelen bij de afhandeling van cybercrimezaken en welke knelpunten en best practices er zijn. In totaal zijn met dertig sleutelfiguren binnen de strafrechtketen semigestructureerde interviews gehouden. Het betreft medewerkers van politie en justitie die aan de basis staan van keuzes over de opsporing en vervolging van zaken. Tabel 2.1 geeft een overzicht van het type en aantal respondenten binnen de strafrechtketen.

Tabel 2.1: Overzicht respondenten

	Functie	Aantal
Politie	Case screener	9
	Operationeel leidinggevende	2
Openbaar Ministerie	Parketsecretaris	5
	Officier van Justitie	2
	Rechercheofficier	3
	Kwaliteitsofficier	3
	Cyberofficier van Justitie	3
Zittende Magistratuur	Rechter	3
Totaal		30

Een beperking van het onderzoek is dat het niet meer dan vier korpsen / parketten omvat. Binnen het tijdsbestek van dit onderzoek bleek het niet mogelijk om meer korpsen / parketten bij het onderzoek te betrekken. Verder is in totaal met dertig personen binnen de strafrechtketen gesproken, maar zijn die dertig niet evenredig verdeeld over de verschillende organisaties binnen de strafrechtketen. De sleutelfiguren zijn geselecteerd op basis van de beslismomenten binnen de keten en binnen politie en OM zijn nu eenmaal meer beslismomenten dan bij de ZM. Al met al geeft het onderzoek een goede inkijk in de beslismomenten binnen de strafrechtketen, maar is enige voorzichtigheid geboden bij het interpreteren en generaliseren van de resultaten.

3. Het proces van slachtofferschap tot veroordeling

3.1 Inleiding

Dit onderzoek gaat over de doorstroom van cybercrimezaken in de strafrechtketen. De strafrechtketen omvat het geheel van instellingen die belast zijn met de handhaving van het strafrecht in Nederland. De keten bestaat uit de fasen opsporing, vervolging, berechting en tenuitvoerlegging van opgelegde straffen en maatregelen (Van der Leij, 2011). De strafrechtketen bestaat uit vijf organisaties: de politie, het OM, de rechter, de justitiële inrichtingen en de reclassering (De Vries, 2011). Voor dit onderzoek zijn alleen de eerste drie fasen en organisaties van belang. Wat er na een eventuele berechting met de veroordeelde gebeurt, valt buiten het bestek van dit onderzoek. Wel voegen we een eerste stap aan het proces toe: waargenomen slachtofferschap. Voordat een delict de strafrechtketen in kan stromen moet er immers een strafbaar feit worden waargenomen.

We geven in dit hoofdstuk op basis van de literatuur en interviews een schets van het proces van slachtofferschap tot veroordeling. Het betreft een theoretische beschrijving van het proces: hoe het proces van slachtofferschap tot veroordeling in de praktijk verloopt hoeft hiermee dus niet overeen te komen. In hoofdstuk 5 wordt beschreven welke overwegingen in de praktijk een rol spelen bij de afhandeling van cyberzaken.

3.2 Waargenomen slachtofferschap

Het overgrote deel van de door de politie geregistreerde delicten zijn door burgers aangegeven en zijn niet het resultaat van zelfstandig opsporingswerk (University of Leicester, 2007; Van de Bunt en Rademaker, 1992; In 't Velt, 1996, 1999; De Poot e.a., 2004). Overigens is het voor een slachtoffer of getuige niet per definitie verplicht om aangifte te doen. Volgens artikel 161 Sv is iedereen die kennis draagt van een strafbaar feit *bevoegd* om aangifte te doen, maar dus niet *verplicht*. Uitzondering zijn in artikel 160 Sv genoemde misdrijven, waaronder:

- misdrijven tegen de veiligheid van de Staat of Koninklijke waardigheid voor zover daardoor levensgevaar is veroorzaakt;
- misdrijven tegen het leven gericht;
- mensenroof;
- verkrachting.

De politie is daarmee dus in sterke mate afhankelijk van de aangiftebereidheid van slachtoffers, of van de ogen en oren van omstanders (getuigen) die de politie op de hoogte brengen van een strafbare gebeurtenis.

3.3 Politie

Intake en registratie

Indien het slachtoffer, een getuige of andere betrokkene ervoor kiest om aangifte te doen moet er contact worden opgenomen met de politie. Het proces van het opnemen en registreren van een aangifte binnen de politie heet de intake. Voor de intake zijn landelijke protocollen opgesteld. Toutenhoofd e.a. (2009) beschrijven op basis van landelijke beleidsdocumenten de wegen waarop burgers contact met de politie kunnen opnemen[4]. Dat zijn de volgende kanalen:

- aan de balie / het bureau;

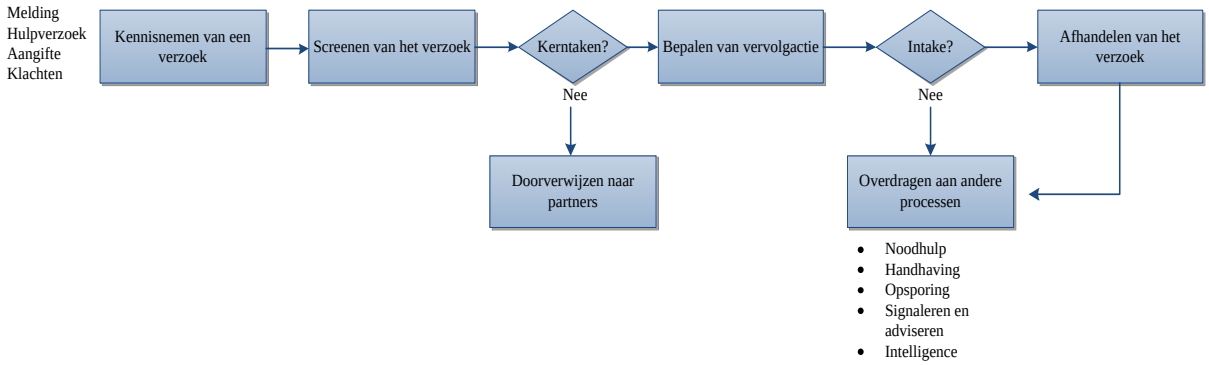
[4] Herijking Visie op Dienstverlening (2007), de Visie op Intake (2008) en het Programmaplan 2008-2012 van de Board Intake en Noodhulp (2009)

- met de agent op straat / op locatie;
- via de telefoon;
- via internet.

In 2010 is binnen de politie afgesproken dat vanuit het oogpunt van voorspelbaarheid en betrouwbaarheid voor burgers, er meer landelijke eenheid moet zijn in het aanbieden van de verschillende kanalen. Dit omdat bleek dat korpsen de kanalen op verschillende manieren aanbieden (Van Uden e.a., 2012). De voorkeursvolgorde is volgens Van Uden e.a. (2012) internet – telefonie – aan de balie – op locatie.

In de landelijke politiedocumenten 'Herijking Visie op Dienstverlening (2007) en de Visie op Intake (2008)' wordt het intakeproces en de beslismomenten beschreven (zie figuur 3.1).

Figuur 3.1: Het intakeproces[5]



Intakemedewerkers zijn belast met het opnemen van alle aangiften, dus ook aangiften cybercrime. Voor cybercrime is geen speciaal team ingericht.

Case screening
Nadat de intaker de aangifte heeft opgenomen komt deze terecht bij de casescreening. Dit zou in alle korpsen moeten gebeuren middels het geautomatiseerde systeem BOSZ (Betere Opsporing door Sturing op Zaken) (Kruijer, 2012), maar uit onze interviews blijkt dit in de praktijk ook nog op papier te gebeuren. De case screeners krijgen dan een bak met uitgeprinte aangiften. BOSZ was tijdens onze interviews nog niet in alle korpsen in gebuik. In de loop van 2012 zou dat wel overal zo moeten zijn (Kruijer, 2012).

BOSZ is een landelijk zaakvolgsysteem voor politiedossiers met als doel zicht te krijgen op de status van opsporingsonderzoeken en de daarin genomen kernbeslissingen. Er staat zowel informatie van de politie als het OM in, en het systeem is ook door beide organisaties te raadplegen. Overigens werkt ook het OM nog niet overal met dit systeem, maar enkel binnen het parket Amsterdam en Haarlem. Dit moet in 2012 landelijk gaan gebeuren (Kruijer, 2012).

Alle aangiften die intakers vastleggen in het bedrijfsprocessensysteem BVH worden iedere nacht ingelezen door BOSZ en verschijnen automatisch in een digitale bak van de case

[5] Bron: Herijking Visie op Dienstverlening (2007)

screeners. Er bestaan uitzonderingen op het automatisch doorzetten van aangiften, bijvoorbeeld zedenzaken, milieuzaken en verkeerszaken. Die gaan meteen door naar de afdelingen die daar verantwoordelijk voor zijn. Cybercrimezaken behoren tot het reguliere werkaanbod van case screeners. De case screener behandelt alleen aangiften die te maken hebben met het eigen district. Indien het een aangifte betreft van een ander district dan stuurt hij/zij de aangifte daar naar de betreffende case screener. Indien het om een andere politieregio gaat dan stuurt de case screener de aangifte naar de betreffende regio.

In alle onderzochte korpsen is een vaste groep medewerkers belast met de casescreening.[6] Het is niet zo dat alle agenten uit een district meedraaien in de casescreening. Volgens de respondenten is er geen cursus of opleiding voor case screeners. Wel hebben ze in de regel, maar niet altijd dus, 'een blauwe achtergrond' (als executieve politiemedewerker). Dat is volgens enkele respondenten ook wel nodig omdat de case screener alleen dan een goede afweging kan maken omtrent welke zaken wel en niet moeten worden opgepakt.

De case screener leest en beoordeelt iedere dag alle nieuwe aangiften die in zijn digitale (of papieren) bak zitten. Bij deze 'weging' van de aangiften kijken de case screeners alleen naar opsporingsindicatie[7] (de mate waarin een aangifte aanknopingspunten biedt om de verdachte op te sporen: zijn er getuigen, videobeelden, een IP-adres, e-mailadres, etc.) en niet naar juridische haalbaarheid ('één getuige is geen getuige', zegt het OM, maar als er een opsporingsindicatie is, gaat de zaak dus wel door). Indien de intakers onvoldoende informatie in de aangifte hebben opgenomen, dan stuurt de case screener de aangifte weer terug naar de intaker. Bijvoorbeeld om een telefoonnummer, IP-adres of imei-nummer toe te voegen. Bij onvoldoende opsporingsindicatie wordt de zaak opgelegd.

Er zijn landelijk vastgelegde criteria op basis waarvan een case screener kan bepalen of een zaak wel of niet wordt doorgestuurd naar een opsporingsteam. Dit is op basis van de Aanwijzing voor de opsporing. Hierin is vastgelegd op basis waarvan een aangifte wel of niet wordt opgepakt. Volgens de Aanwijzing moeten alle zaken met opsporingsindicatie in behandeling worden genomen.

Aangifte verrijken

De aangiften die door de screening zijn gekomen, worden verrijkt met daderinformatie. Dit kan door de case screeners zelf gebeuren, maar er zijn ook aparte afdelingen voor. De afdeling die de aangifte verrijkt, doet het onderzoek tot aan de verdachte. Er bestaat geen procedureel verschil tussen het verrijken van aangiften cybercrime en het verrijken van reguliere aangiften: dat wordt door dezelfde politiemedewerkers gedaan. Videobeelden worden gecheckt, gegevens die leiden tot de verdachten worden gevorderd en eventueel worden verdachten verhoord (maar dat laatste is in principe de taak van een opsporingsteam). Het doel van dergelijk vooronderzoek is te komen tot een verdachte zodat de recherche die meteen kan verhoren. Zodra de aangifte is verrijkt, gaat de zaak door naar een opsporingsteam. Mocht blijken dat er op deze manier toch niet tot een verdachte kan worden gekomen, dan kan worden besloten de zaak alsnog op te leggen.

[6] Overigens lijkt er geen landelijke uniformiteit in de benaming van de afdeling te zijn die belast is met de case screening. In de regio's die we bezochten voor dit onderzoek kwamen we namen als Bureau Wegen Kiezen en Monitoren, Vakspecialist procesondersteuning en Afdeling Coördinatie Operationele Werkprocessen tegen.

[7] Repondenten gebruiken de termen opsporingsindicatie en daderindicatie door elkaar. In de onderzoek spreken we alleen van opsporingsindicatie.

Bij twijfel of er wel vooronderzoek naar een zaak moet worden gedaan, is er (sporadisch) overleg met andere collega's van de casescreening, een teamleider van de politie of met het OM. Bijvoorbeeld als er twijfel is of het wel zin heeft om tijd te investeren in een verdachte omdat de kans op veroordeling klein is. Overleg met het OM lijkt er vooral te zijn in de korpsen waarbij het OM nadrukkelijk aanwezig is bij de politie. In een aantal korpsen heeft het OM bijvoorbeeld een zogenaamd ZSM-loket op een politiebureau. Het ZSM-loket handelt zaken die bij de politie binnenkomen zo snel mogelijk af[8]. Het loket richt zich voornamelijk op eenvoudige zaken die zonder rechter kunnen worden afgedaan. Dat is mogelijk op basis van de Wet OM-afdoening (i.w.tr. 1 mei 2012). Bij complexere zaken krijgt de verdachte een dagvaarding mee, waarna hij of zij alsnog voor de rechter moet verschijnen. Politie, de (hulp)Officier van Justitie, de parketsecretaris en de reclassering zijn vertegenwoordigd binnen het loket. Het ZSM-loket wordt niet of nauwelijks gebruikt voor cybercrimezaken, omdat voor dergelijke zaken veelal meer onderzoek vereist is om tot een verdachte te komen. De aanwezigheid van OM-functionarissen in het bureau brengt echter wel voordelen met zich mee als zich cybercrimezaken aandienen, omdat daardoor gemakkelijker overlegd kan worden over de afhandeling van zo'n zaak. Casescreeners en werkvoorbereiders in deze korpsen geven aan dat ze door de korte lijn die er met het OM is, sneller checken bij het OM wat ze met een zaak moeten doen waarover twijfel is. Overleg tussen de case screening en het OM is er ook bij bijzondere zaken. Bijvoorbeeld een huiselijk geweld zaak. De man zegt dat er niets aan de hand is, de vrouw zegt dat hij haar slaat. Dergelijke zaken zijn moeilijk te bewijzen, maar hebben wel beleidsprioriteit. Het OM kan dan ook zorgen dat deze mensen in hulpverleningstrajecten worden opgenomen. Ook indien een zaak, om wat voor reden dan ook, (te) lang is blijven liggen is er overleg met het OM. De regel is dat een aangifte binnen negentig dagen een onderzoeksdossier is geworden, of is afgedaan.

Opsporing

De politie kan op twee manieren kennis nemen van een (vermoedelijk) strafbaar feit. Dat kan omdat een burger (slachtoffer of getuige) of bedrijf dat meldt of door zelfstandig opsporingsonderzoek door de politie (door ontdekking op heterdaad of door zelf gericht onderzoek te doen) (In 't Velt, 1996, 1999; De Poot e.a., 2004, Van der Leij, 2011). De eerste categorie zaken zijn brengzaken, de tweede categorie haalzaken.

De zaken waarvan aangifte is gedaan, komen via de case screening bij een opsporingsteam terecht. Dit kan bij de Basis Politie Zorg (BPZ), een crime team (ook wel administratieve recherche genoemd: een team BPZ'ers onder leiding van een rechercheur), of een rechercheteam. Er zijn op korpsniveau geen teams die specifiek belast zijn met het afhandelen van cybercrimezaken. Wel vinden we op regio (overstijgend) niveau teams 'digitale expertise'[9] die weliswaar niet zelfstandig zaken oppakken en afhandelen, maar wel een ondersteunende rol hebben in opsporingsonderzoeken naar complexere cybercrimezaken (PAC, 2008; Stol, Leukfeldt en Klap, 2012). De ondersteunende digitale experts lezen bijvoorbeeld in beslag genomen computers of GSM's uit. Op nationaal niveau is er het zelfstandig opererende Team High Tech Crime (THTC) van het KLPD. De BPZ pakt de kleine ofwel 6-uurszaken[10] op die binnen aan dag kunnen worden opgelost, de crimeteams

[8] Op dit moment is het ZSM-loket alleen aanwezig in Amsterdam, Utrecht, Rotterdam, Den Haag en Den Bosch. Bron: http://www.om.nl/onderwerpen/zsm/@155732/versnelde-afdoening/ Laatst geraadpleegd 23 maart 2012.

[9] Voor dit team worden in verschillende korpsen verschillende benamingen gebruikt. Zo kwamen we bijvoorbeeld ook de term Team Digitale Ondersteuning en Forensische Ondersteuning tegen. Wij hanteren in dit rapport de term Team Digitale Expertise.

[10] De 6 uur verwijst naar de tijd die de politie een aangehouden verdachte buiten de voor de nachtrust bedoelde tijd aan het bureau mag houden. Is het nodig dat de verdachte langer ingesloten blijft, dan is een inverzekering-stelling vereist.

doen de zaken die groter zijn dan de 6-uurszaken. In de regel zijn de 6-uurszaken de high-volume crimes ofwel veel voorkomende criminaliteit. De districtsrecherche doet de grotere zaken. Het THTC handelt zaken af die de nationale infrastructuur bedreigen of een internationaal karakter hebben.

Binnen opsporingsteams, of het nu de BPZ, een crimeteam of de (districts)recherche betreft, wordt opnieuw een afweging gemaakt om een (cybercrime)zaak al dan niet in behandeling te nemen. De overwegingen die daarbij een rol spelen worden besproken in hoofdstuk 5. Opsporingsambtenaren zoeken vervolgens naar sporen, horen getuigen en slachtoffers, houden verdachten aan en leggen alle gegevens schriftelijk vast in een proces-verbaal, waarbij de eindverantwoordelijkheid ligt bij het OM (Van der Leij, 2011). De Officier van Justitie geeft officieel leiding aan het opsporingsonderzoek, maar in de praktijk is het eerste contact tussen een opsporingsteam en het OM bij de veelvoorkomende brengzaken vaak pas het aanvragen van Bijzondere Opsporingsbevoegdheden (BOB). Dat zijn bevoegdheden waarmee inbreuk wordt gemaakt op de vrijheden van personen en waartoe de toestemming van de Officier van Justitie en in bepaalde gevallen van de rechter-commissaris nodig is (Van der Leij, 2011). De bevoegdheden van de Wet bijzondere opsporingsbevoegdheden uit 2000 (BOB) zijn opgenomen in het eerste boek van het Wetboek van Strafvordering onder 'bijzondere bevoegdheden tot opsporing'. Voorbeelden zijn: het stelselmatig observeren van een verdachte van een misdrijf (126g Sv), het stelselmatig inwinnen van informatie over zo'n verdachte (126j Sv) en pseudokoop (126i Sv).

De opsporingsteams leggen zelf ook zaken op. Als een zaak niet binnen negentig dagen is opgepakt dan krijgt de aangever een brief waarin staat dat de zaak verder niet in behandeling wordt genomen.[11]

Het besluit van de politie om een zaak op te pakken en bijvoorbeeld een verdachte te gaan horen of bijzondere opsporingsbevoegdheden in te zetten leidt niet in alle gevallen tot verdere vervolging (Van der Leij, 2011). Er is een aantal redenen op basis waarvan de politie kan besluiten om zaken op te leggen, bijvoorbeeld als er (alsnog) geen zicht op een dader is of bij gebrek aan politiecapaciteit (Kruijer, 2012). De politie hanteert de volgende wijzen van afdoening (Van der Leij, 2011:30-32):

- *Politiesepot*. Dit sepot heeft geen strafrechtelijke consequenties. De politie maakt geen proces-verbaal op en maakt de zaak dus niet kenbaar aan het OM. De politie kan wel een mutatie in het bedrijfsprocessensysteem maken. Die mutatie kan volgens Van der Leij (2011) een rol spelen in de besluitvorming bij een nieuw contact van de persoon met de politie. De politie kan een (jeugdige) pleger vermanend toespreken, waarna hij of zij weer vrijuit gaat. Deze handelwijze valt in de praktijk ook onder het 'politiesepot', omdat aan de vermaning geen strafrechtelijke consequenties verbonden zijn.

- *Politie strafbeschikking*. Naast de Officier van Justitie kunnen ook (buitengewoon) opsporingsambtenaren (zie art. 275b Sv) en sommige bestuursorganen strafbeschikkingen opleggen (van der Leij, 2011). De politiestrafbeschikking is een gevolg van de Wet OM-afdoening die in 2008 is ingevoerd en ervoor moet zorgen dat de rechtshandhaving in Nederland efficiënter verloopt. Eenvoudige zaken worden niet langer door de rechter afgedaan, maar door opsporingsambtenaren en het openbaar ministerie. In het geval van een politiestrafbeschikking kan de politie een geldboete geven. De strafbeschikking die

[11] Voor de goede orde: het gaat hier dus niet om alle aangiften, maar alleen om aangiften die door de casescreening zijn gekomen en door opsporingsteam worden opgepakt.

wordt uitgevaardigd door (buitengewoon) opsporingsambtenaren heeft de politietransactie vervangen.

- *Halt-afdoening*. 'Het ALTernatief'. De politie kan een jeugdige dader ter afhandeling verwijzen naar een Halt-bureau. Voorwaarden zijn dat het moet gaan om een bekennende verdachte en een zogeheten 'first offender', die instemt met de verwijzing. Verder gaat het volgens Van der Leij (2011) om minder zware delicten zoals vernieling, brandstichting met geringe schade en winkeldiefstal met geringe buit.

- *Bureau Jeugdzorg-verwijzing*. Kinderen onder de 12 jaar kunnen niet worden vervolgd, het stafrecht is niet op hen van toepassing. Deze jongeren worden doorverwezen naar Bureau Jeugdzorg.

Zaken waarin de politie opsporingsonderzoek heeft verricht en waarop voornoemde voornoemde afdoeningswijzen niet van toepassing zijn, worden voor vervolging doorgestuurd naar het OM.

3.4 Openbaar Ministerie

Als de politie een zaak heeft afgerond en (naar eigen oordeel) voldoende bewijs heeft verzameld om over te gaan tot vervolging, dan wordt de zaak doorgestuurd naar het OM. Zaken die zijn doorgestuurd naar het OM worden door een administratieve afdeling in de bedrijfsprocessensystemen GPS en COMPAS van het OM ingevoerd. De parketsecretaris beoordeelt de juridische haalbaarheid van de zaak en kan besluiten de zaak terug te sturen naar de politie voor aanvullingen (Kruijer, 2012). Cyberzaken in enge zin, worden beoordeeld door een daar speciaal voor aangewezen cybersecretaris. Cyberzaken in ruime zin zijn in essentie klassieke delicten (zoals fraude of stalking) en worden door 'reguliere' secretarissen afgehandeld.

Op grond van de resultaten van het opsporingsonderzoek besluit het OM of een verdachte al dan niet wordt vervolgd. Het OM heeft een recht tot vervolgen, niet de plicht daartoe (het zogenaamde *opportuniteitsbeginsel*). Het OM bepaalt dus wie voor de strafrechter moet verschijnen, en voor welk strafbaar feit.[12] Als een zaak dagvaarding vereist, dan bereidt de parketsecretaris de zaak voor op het onderzoek ter zitting. De Officier van Justitie brengt de zaak uiteindelijk voor de rechter. Dagvaardingen bij cyberzaken in enge zin worden afgehandeld door een speciaal daarvoor aangewezen cyberofficier. Cyberzaken in ruime zin worden afgehandeld door andere OvJ's. Internetfraude wordt bijvoorbeeld ondergebracht bij een fraudeofficier omdat het in essentie een klassiek delict betreft. Het OM beslist op grond van daarvoor opgestelde beleidsregels hoe een zaak wordt afgehandeld. Als dagvaarding niet aan de orde is, heeft het OM de volgende mogelijkheden om zaken af te handelen (Van der Leij, 2011: 35-36):

- *Technisch sepot*[13]. Vervolging is volgens het OM niet haalbaar. Er kan bijvoorbeeld sprake zijn van een verdachte die onterecht als verdachte is aangemerkt, een gebrek

[12] Het OM is georganiseerd in parketten: negentien arrondissementsparketten (bij alle rechtbanken), vijf ressortparketten (bij alle gerechtshoven), één Landelijk Parket, één Functioneel Parket en het parket bij de Hoge Raad (Van der Leij, 2011). Er wordt gewerkt aan een voorstel tot herziening van de gerechtelijke kaart. De hier besproken indeling zou daarmee wijzigen. Het achterliggende idee is dat de gerechten en parketten door schaalvergroting minder kwetsbaar worden en er meer ruimte bestaat voor specialisatie.

[13] Personen die het oneens zijn met de beslissing dat een zaak wordt geseponeerd, kunnen hiertegen bezwaar maken door een klacht in te dienen bij het gerechtshof. Als het hof de klacht gegrond verklaart, moet het OM alsnog tot (verdere) vervolging overgaan.

aan wettig bewijs, niet ontvankelijkheid van het OM, een onbevoegde rechter of een niet strafbaar feit en/of niet strafbare dader.

- *Beleidssepot*[14]. Als het OM besluit tot een beleidssepot, dan is vervolging wel haalbaar, maar acht het OM vervolging niet wenselijk. Er is bijvoorbeeld voldoende bewijs, maar sprake van een gering feit of het geschil tussen de dader en het slachtoffer is al opgelost.

- *OM strafbeschikking*. Het OM heeft de mogelijkheid om buiten de rechter om een straf op te leggen. De strafbeschikking omvat uiteenlopende straffen, maatregelen en aanwijzingen zoals een geldboete, een taakstraf of een ontzegging van de rijbevoegdheid. De strafbeschikking kan alleen worden opgelegd bij overtredingen en misdrijven waarop een maximale gevangenisstraf van 6 jaar is gesteld. Verdachten kunnen verzet instellen tegen een strafbeschikking. De zaak wordt dan alsnog door de rechter behandeld.

- *Transactie*. Als een zaak niet voldoet aan de in de Aanwijzing OM-afdoening opgenomen beleidsmatige criteria voor het uitvaardigen van een strafbeschikking, kan het OM voorlopig nog een transactie aanbieden. Op den duur vervangt de OM-strafbeschikking de transactiemogelijkheid. Het verschil van de transactie ten opzichte van de strafbeschikking is dat de verdachte door het accepteren van het transactievoorstel voorkomt dat hij wordt vervolgd en bestraft. De strafbeschikking komt meer overeen met een uitspraak van de rechter: het biedt het OM de mogelijkheid om zelfstandig te vervolgen en bestraffen.

- *Voeging ter berechting*. Het samenvoegen van ingeschreven strafzaken om de rechter deze zaken tegelijk te laten beoordelen. Een voeging kan efficiënt zijn bij zaken met dezelfde verdachte.

- *Voeging ad informandum*. Het OM kan belastend materiaal over de verdachte uit een andere strafzaak ‘ad informandum’ aan de rechter voorleggen. De rechter kan bij de bepaling van de strafmaat rekening houden met de feiten in de gevoegde zaak.

3.5 Zittende Magistratuur

Van der Leij (2011) beschrijft op hoofdlijnen hoe de Zittende Magistratuur functioneert. Als het OM besluit te dagvaarden, vindt er een onderzoek ter zitting plaats. Dat betekent dat een rechter uitspraak moet doen over het aan een verdachte ten laste gelegde. Vrijwel alle strafzaken beginnen in eerste aanleg bij een rechtbank. De enkelvoudige kamer van de rechtbank bestaat uit één rechter en behandelt eenvoudige zaken. De meervoudige kamer bestaat uit drie rechters en behandelt ingewikkeldere zaken. Of een zaak door de enkelvoudige of de meervoudige kamer wordt behandeld, besluit de Officier van Justitie. Het is echter mogelijk dat de alleensprekende rechter een zaak verwijst naar de meervoudige kamer en vice versa. Welke rechter een zaak toebedeeld krijgt is willekeurig. Iedere rechter kan dus cyberzaken krijgen. Rechters moeten in principe dan ook alle zaken kunnen afhandelen. Er zijn wel uitzonderingen, zo zijn er bijvoorbeeld kinderrechters die alleen zaken

[14]Rechtstreeks belanghebbenden die het oneens zijn met de beslissing dat een zaak wordt geseponeerd kunnen hiertegen op grond van artikel 12 Sv bezwaar maken door een schriftelijke klacht in te dienen bij het betreffende gerechtshof. Als het hof de klacht gegrond verklaart, moet het OM alsnog tot (verdere) vervolging overgaan (de zgn. ‘artikel 12 procedure’).

van minderjarige verdachten behandelen. Bij cybercrime is er niet zo'n strikte toedeling, maar- zo meldden respondenten - rechters die affiniteit hebben met cybercrime worden voor zover de planning dat toelaat zoveel mogelijk ingeschakeld bij cyberzaken.

De alleensprekende rechter of de voorzitter van de meervoudige kamer leidt het onderzoek ter zitting. De rechter vraagt allereerst naar de personalia en feitelijke verblijfplaats van de verdachte. Vervolgens wijst de rechter de verdachte er op dat hij niet tot antwoorden verplicht is. Daarna draagt de Officier van Justitie de zaak voor en wordt de verdachte door de rechter ondervraagd. De vragen van de rechter hebben meestal eerst betrekking op het ten laste gelegde feit en vervolgens op de persoonlijke omstandigheden van de verdachte. Daarna worden eventueel getuigen, deskundigen en/of slachtoffer(s) gehoord.

Vervolgens vindt het requisitoir plaats. In het requisitoir vat de Officier van Justitie het bewijs samen en vordert hij (indien van toepassing) een straf en/of maatregel. Bij het bepalen van de strafmaat wordt gebruik gemaakt van delictspecifieke strafvorderingsrichtlijnen. Voor iedere strafvorderingsrichtlijn gelden in beginsel de uitgangspunten en rekenmethode van de Aanwijzing Kader voor Strafvordering (2010A032).

De verdachte of diens advocaat kan reageren op het requisitoir door een pleidooi te voeren. De Officier van Justitie wordt vervolgens de mogelijkheid geboden om daarop te reageren. Tot slot heeft de verdachte recht op het laatste woord.

Na afloop van het onderzoek beoordeelt de enkel-/ meervoudige kamer vier *formele* vragen: 'de geldigheid van de dagvaarding, haar bevoegdheid te oordelen over het ten laste gelegde feit of de ten laste gelegde feiten, de ontvankelijkheid van de Officier van Justitie en of er redenen zijn voor schorsing van de vervolging' (Van der Leij, 2011:39). Als de dagvaarding nietig is, de rechtbank onbevoegd, de Officier van Justitie niet-ontvankelijk of als aanleiding bestaat tot schorsing van vervolging, dan zal de rechter dat uitspreken. Er is dan sprake van een formele einduitspraak.

Als wordt overgegaan tot berechting, dan buigt de kamer zich over vier *materiële* vragen: (1) is het feit wettig en overtuigend bewezen, (2) is het bewezen verklaarde feit strafbaar, (3) is de dader strafbaar en (4) welke straf en/of maatregel moet worden opgelegd? Volgend op vraag 1 t/m 3 zijn de volgende uitspraken mogelijk:

- *Vrijspraak.* Het feit is niet wettig en overtuigend bewezen.

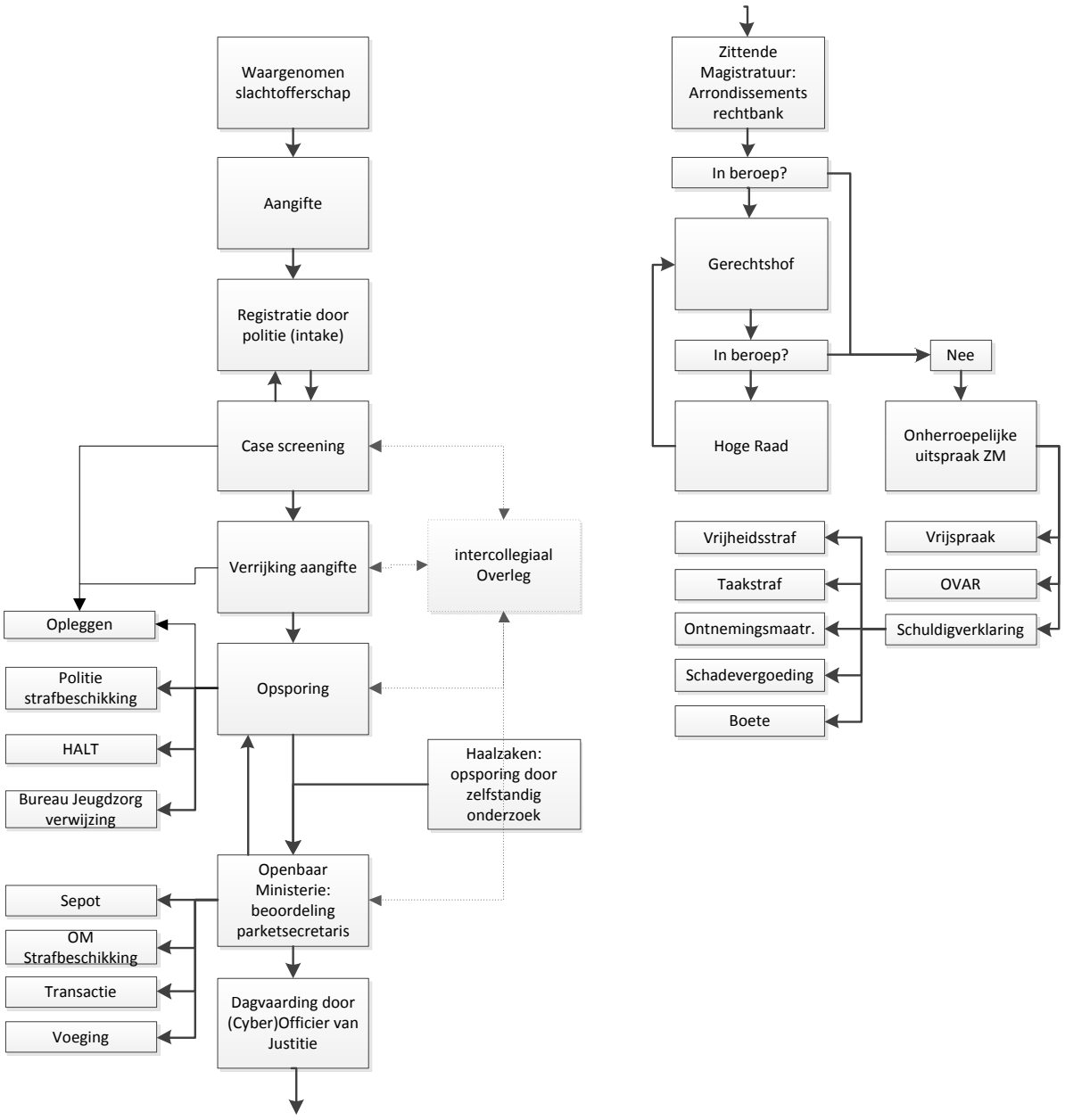
- *Ontslag van alle rechtsvervolging*. Het omschreven feit is wel wettig en overtuigend bewezen, maar het bewezen verklaarde feit levert géén strafbaar feit op. Of het bewezen verklaarde feit levert wél een strafbaar feit op, maar de dader is niet strafbaar.

- *Schuldigverklaring*. Het feit is wettig en overtuigend bewezen, het bewezen verklaarde feit is strafbaar en de dader is strafbaar.

Indien de dader strafbaar is, dan moet de rechter bepalen welke sanctie (straf en/of maatregel) moet worden opgelegd en hoe hoog die sanctie moet zijn. Er zijn hoofdstraffen, bijkomende straffen en maatregelen. De hoofdstraffen zijn gevangenisstraf, hechtenis, geldboete en de taakstraf. Een maatregel is bijvoorbeeld de ontneming van het wederrechtelijk verkregen voordeel of een terbeschikkingstelling (TBS). Een bijkomende straf is volgens Van der Leij

(2011) de openbaarmaking van de rechterlijke uitspraak, de ontzetting uit bepaalde rechten, zoals de ontzetting uit een ambt of beroep, en de verbeurdverklaring. De uiteindelijke uitspraak van de rechtbank heet een vonnis.

Figuur 3.2: Het proces van slachtofferschap tot veroordeling[15] [16]



[15] Gebaseerd op Leertouwer & Kalidien (2011b), Algemene Rekenkamer (2012) en eigen interviews met respondenten van de politie, het OM en de ZM. Dit schema geeft het proces weer van de manier waarop het gros van de zaken de strafrechtketen doorstroomt. Het gaat hier om de zogenoemde brengzaken. Zaken die door slachtoffers, benadeelden of getuigen worden aangedragen aan de politie. Naast brengzaken zijn er ook haalzaken. Dit zijn zaken die politie oppakt op basis van intelligence, Bijvoorbeeld restinformatie uit een afgerond onderzoek naar een hennepkwekerij die aanleiding geeft tot een nieuw opsporingsonderzoek naar een bende de zich bezig houdt met witwassen.

[16] De ondoorbrokenlijn staat voor de mogelijke stappen in het proces, de stippellijn staat voor de overlegmomenten.

Indien een van de partijen het oneens is met het vonnis, dan kan in beroep worden gegaan. Een zaak in hoger beroep wordt behandeld door een gerechtshof. Bij een uitspraak van een gerechtshof zijn drie rechters betrokken. De uitspraak heet een arrest. De procedure bij het gerechtshof is vergelijkbaar met de procedure bij de rechtbank. Zowel de Officier van Justitie als de verdachte krijgen opnieuw de gelegenheid om de zaak toe te lichten. Het gerechtshof beoordeelt de zaak nogmaals en komt tot zijn eigen uitspraak.

Ook tegen een arrest van een gerechtshof kan in beroep worden gaan: het beroep in cassatie. De zaak komt dan bij de Hoge Raad terecht. De Hoge Raad is het hoogste nationale rechtscollege op het gebied van het strafrecht. De Hoge Raad gaat niet meer feitelijk inhoudelijk in op de zaak, maar beoordeelt slechts of is gehandeld volgens de voorschriften uit de wet. Het bevorderen van uniformiteit in rechtstoepassing is dan ook de belangrijkste functie van de Hoge Raad. Zaken waarin de Hoge Raad oordeelt dat het recht niet juist is toegepast, worden terugverwezen naar het gerechtshof. De zaak moet daar dan opnieuw inhoudelijk worden behandeld.

3.6 Het proces van slachtofferschap tot vervolging in cijfers

Deze paragraaf is gebaseerd op de publicaties *Criminaliteit en rechtshandhaving 2010* van het WODC (Kalidien & De Heer-de Lange, 2011) en *Prestaties in de strafrechtketen* van de Algemene Rekenkamer (2012). We beschrijven op basis van voornoemde publicaties de cijfermatige doorstroom van zaken in de strafrechtketen. De zojuist door ons aangehaalde onderzoekers hebben voor het schrijven van hun rapportages gebruik gemaakt van verschillende informatiebronnen, zoals slachtofferonderzoek, systemen van de politie en systemen van het OM. Volgens Leertouwer & Kalidien sluiten cijfers van de verschillende ketenpartners daardoor niet één-op-één op elkaar aan. Desondanks bieden voornoemde rapportages inzicht in de doorstroom van zaken in strafrechtketen. Het betreft hier dus niet specifiek de doorstroom van aangiften cybercrime. Daarover wordt gerapporteerd in hoofdstuk 4.

Slachtofferschap en aangifte

Huys en Smit (2011) brengen op basis van slachtofferonderzoek naar voren dat 8,2 miljoen burgers en/of bedrijven in 2010 slachtoffer zijn geworden van een misdrijf. Het gros van de misdrijven, 5,7 miljoen, heeft volgens Huys en Smit betrekking op burgers en 2,5 miljoen op bedrijven. Burgers meldden ruim een derde van de door hen ondervonden misdrijven. Bedrijven deden dat in grotere mate: zo'n 60 procent van de bedrijven die slachtoffer werden van criminaliteit, maakte daarvan melding bij de politie. Zowel burgers als bedrijven doen in slechts ongeveer een kwart van de gevallen daadwerkelijk aangifte. Een groot deel van de door burgers en bedrijven ondervonden delicten blijft dus buiten het zichtveld van politie en justitie.

Politie

Volgens de rapportage criminaliteit en rechtshandhaving registreerde de politie in 2010 ruim 1 miljoen misdrijven[17]. 287.000 misdrijven werden opgelost: een ophelderingspercentage van 24 procent (Eggen & Kessels, 2011). In criminaliteit en rechtshandhaving is de wijze waarop de politie de door haar geregistreerde zaken afhandelt niet verder uitgesplitst. Een recente

[17] We beschreven dat 8,2 miljoen burgers en/of bedrijven in 2010 slachtoffer werden van een misdrijf. Als, zoals Huys en Smit (2011) beschrijven, een kwart daarvan aangifte doet, zou dat betekenen dat de politie ruim 2 miljoen misdrijven zou moeten hebben geregistreerd. De politie registreerde echter 1 miljoen misdrijven. Het gevonden verschil wordt veroorzaakt doordat de cijfers afkomstig zijn uit verschillende bronnen (respectievelijk slachtofferonderzoek en politieregistratie).

publicatie over de strafrechtelijke afhandeling van gewelds en vermogensmisdrijven van de Algemene Rekenkamer (2012) biedt wel inzicht in de wijze van afdoening van de politie (tabel 3.1). Het gros van de door de Algemene Rekenkamer bestudeerde zaken, 656.650 van de 725.328 bij de politie binnengekomen gewelds en vermogensmisdrijven, leidt niet tot opsporing en/of vervolging (90,5%). 503.036 van de bij de politie binnengekomen gewelds- en vermogensmisdrijven kwam niet door de case screening (69,4%). Bij de zaken die in eerste aanleg wel door de screening komen, volgen opsporingshandelingen. Het is mogelijk dat geen verdachte wordt gevonden. Deze zaken worden gearchiveerd als afgerond zonder verdachte en krijgen geen verder vervolg. Dat zijn 123.641 zaken (17%). Zaken met voldoende opsporingsindicatie worden in behandeling genomen. 25.295 gewelds- en vermogenszaken met opsporingsindicatie hebben wegens gebrek aan bewijs uiteindelijk alsnog geleid tot politiesepot (3,5%). Tot slot zijn 4.678 (0,6%) reprimandes opgelegd. Ook deze zaken stromen zonder tussenkomst van een andere organisatie, zoals het OM, uit bij de politie.

Tabel 3.1: De uitstroom van gewelds- en vermogensmisdrijven bij de politie (Algemene Rekenkamer, 2012)

	Omvang	
Uitstroom als	Aantal	Percentage
Beëindigd na case screening	503 036	69,4
Beëindigd zonder verdachte	123 641	17,0
Politiesepot	25 295	3,5
Reprimande	4 678	0,6
Subtotaal uitstroom bij de politie	656 650	90,5
Transactie (CJIB)	4 832	0,7
HALT	5 516	0,8
Doorgestuurd naar OM	58 330	8,0
Subtotaal doorstroom ketenpartner	68 678	9,5
Totaal	725 328	100

Van de overige zaken zijn 4.832 transacties opgelegd (0,7%) en is 5.516 keer verwezen naar Halt (0,8%). Niet meer dan 8 procent van alle bij de politie binnengekomen gewelds en vermogensmisdrijven wordt voor vervolging doorgestuurd naar het OM.

Openbaar Ministerie

In 2010 werden 208.600 strafzaken bij het Openbaar Ministerie (OM) ingeschreven (Leertouwer & Kalidien, 2011). Het aantal afdoeningen in dat jaar bedroeg 83.600 (40,1%). In ruim de helft van alle strafzaken die het OM zelf afdeed is een transactie aangeboden (n=42.300). Het OM seponeerde bijna een derde van de strafzaken (n=25.000). Het merendeel daarvan (n=14.700) betrof beleidssepots en in 10.300 zaken was sprake van een technisch sepot. Bij een vijfde van de zaken (n=16.300) is sprake van een andere wijze van afdoening, zoals een voeging, een opgelegde strafbeschikking of een overdracht naar een ander parket. Zaken die niet door het OM zelf zijn afgehandeld hebben geleid tot een dagvaarding. Dat betreft 59,9 procent van alle bij het Openbaar Ministerie ingeschreven strafzaken (Brouwers & Eggen, 2011).

Zittende Magistratuur
In 2010 deed de rechter 106.000 strafzaken tegen verdachten van misdrijven af. De rechter kan een strafzaak op verschillende manieren afdoen. Meestal verklaart de rechter een verdachte schuldig. 90 procent van de in 2010 voor de rechter gebrachte zaken hebben geleid tot een schuldigverklaring (n=95.800). In nagenoeg 9 procent van de overige zaken werd de verdachte vrijgesproken of ontslagen van rechtsvervolging (n=9500). Bij 1 procent van de zaken was sprake van een andere afdoeningswijze.

De keten in cijfers
Kortom, in iedere stap in het proces van slachtofferschap tot veroordeling vindt een selectie plaats. Sommige zaken vallen in een vroegtijdig stadium af, terwijl andere een vervolg krijgen. Het begint bij het doen van een aangifte door een slachtoffer of getuige en de daaropvolgende registratie van de politie. Dan is er een selectieproces binnen de politie, een aanzienlijk deel van de aangiften wordt afgedaan zonder opsporingsonderzoek, of omdat het opsporingsonderzoek niet het gewenste resultaat oplevert. Vervolgens kan de politie een transactie opleggen, een doorverwijzing geven naar Halt of de zaak insturen bij het OM. Bij het OM komt op die manier maar een fractie van de zaken binnen waarvan aangifte is gedaan.

Ook bij het OM vindt een selectie plaats. Ten eerste kunnen zaken bij elkaar worden gevoegd (ad informandum of ter berechting). Tevens kan het OM besluiten een zaak te seponeren, omdat een veroordeling door een rechter niet haalbaar lijkt (technisch sepot) of omdat een beoordeling door een rechter niet wenselijk lijkt (beleidssepot). Ook kan het OM de verdachte een transactie aanbieden, of zelf de schuld vaststellen van en straf opleggen aan een verdachte middels een OM-strafbeschikking. De overgebleven zaken brengt het OM via een dagvaarding voor de rechter. Deze kan de verdachte vrijspreken of schuldig verklaren, de verdachte ontslaan van rechtsvervolging of het OM niet-ontvankelijk verklaren.

In tabel 3.2 staat het proces van slachtofferschap tot veroordeling op hoofdlijnen in cijfers weergegeven, op basis van gegevens ontleend aan Leertouwer en Kalidien (2011). Omdat gebruik is gemaakt van verschillende informatiebronnen (slachtofferonderzoek, politieregistratie, OM-registratie en ZM-registratie) en de gepresenteerde cijfers daardoor beperkt vergelijkbaar zijn en/of op elkaar aansluiten, tellen de percentages in de tabel niet over de hele linie, maar per processtap (slachtofferschap, politie, OM, ZM) op tot honderd procent. Met name de gegevens uit slachtofferonderzoek laten zich moeilijk vergelijken met gegevens uit officiële registraties binnen de strafrechtketen omdat slachtofferonderzoek geen zicht biedt op zogenoemde slachtofferloze delicten (illegale wapen- en drugshandel bijvoorbeeld) en omdat slachtofferonderzoek doorgaans niet alle mogelijke vormen van criminaliteit bevraagt.

Binnen de strafrechtketen geven de cijfers op hoofdlijnen wel enige indicatie over de doorstroom van zaken. De politie registreert in een jaar 1.185.000 zaken en in een jaar zijn er 95.800 schuldigverklaringen. Het gaat daarbij niet om het aantal schuldigverklaringen uit precies die 1.185.000 zaken maar om zaken die (deels) eerder al door de politie werden geregistreerd. Echter, als we op hoofdlijnen weten dat de politie ongeveer 1,2 miljoen zaken per jaar registreert en dat rechters per jaar zo'n 95.800 schuldigverklaringen uitspreken, dan wijst dat, over alle soorten delicten gemeten, op een gemiddeld 'schuldigverklaringspercentage' van bij de politie geregistreerde zaken van ongeveer 8 procent.

Tabel 3.2: Van slachtofferschap tot veroordeling, cijfers over 2010[18]

			Aantal	Percentage
Slachtofferschap totaal (zelfrapportage)			8.200.000	100,0
	Slachtofferschap burgers		5.700.000	69,5
	Slachtofferschap bedrijven		2.500.000	30,5
Zaken geregistreerd door politie			1.185.000	100,0
Zaken geregistreerd door OM			208.600	100,0
	Dagvaardingen		125.000	60,0
	Afdoeningen door het OM		83.600	40,0
		Afdoeningen OM, uitgesplitst:	83.600	100,0
		Transactie	42.300	50,1
		Sepot	25.500	30,1
		Overige afdoeningen	16.300	19,5
Zaken geregistreerd door ZM			106.800	100,0
	Schuldigverklaring		95.800	89,7
	OVAR & vrijspraak		9.500	8,9
	Overige afdoeningen		700	0,7

[18] Bron: Leertouwer & Kalidien (2011:211)

4. De zaakstroom van aangiften cybercrime

4.1 Inleiding

In dit hoofdstuk wordt de doorstroom van aangiften cybercrime in de strafrechtketen beschreven. Het in kaart brengen van de zaakstroom van aangiften cybercrime in de strafrechtketen is slechts ten dele geslaagd (zie paragraaf 2.2). Alleen de wijze waarop de politie aangiften cybercrime heeft afgehandeld kon uiteindelijk in kaart worden gebracht. Van een te groot aantal aangiften ontbreekt namelijk informatie om betrouwbare uitspraken te doen over de strafrechtelijke afhandeling van cybercrime door het Openbaar Ministerie en de Zittende Magistratuur. Deze paragraaf beperkt zich dan ook tot het beschrijven van de afhandeling van aangiften cybercrime door de politie.

4.2 De afhandeling van aangiften cybercrime door de politie

De afhandeling van 647 aangiften cybercrime bij de politie is in kaart gebracht. Zoals in de methodische verantwoording staat beschreven, is voor het onderzoek gebruik gemaakt van dossiers uit de Verkenning Cybercrime in Nederland 2009 (Leukfeldt e.a., 2010). Alle politiekorpsen is op basis van PV-nummers van die dossiers verzocht om aan te geven hoe deze aangiften cybercrime zijn afgehandeld. Tabel 4.1 geeft weer hoe die afhandeling er op basis van de verzamelde data in eerste aanleg uit zag.

Tabel 4.1: afhandeling door de politie

	Aantal	Percentage
Afgedaan door de politie	274	42,3
Doorgestuurd naar het OM	189	29,2
Doorgestuurd naar ander korps	87	13,4
Onbekend	97	15,0
Totaal	647	100,0

De afhandeling van 15 procent van de zaken is volgens de politie onbekend. In het gros van de gevallen gaf de politie aan dat de afhandeling onbekend is, maar werd niet toegelicht waarom de wijze van afdoening niet kon worden achterhaald (n=75). In een aantal gevallen was sprake van een andere wijze van afhandeling: de aangifte werd bijvoorbeeld ingetrokken, er werd een internationaal rechtshulpverzoek gedaan of er was sprake van een reeds opgelost geschil (n=12). Ook van dergelijke zaken is onbekend of de politie ze uiteindelijk zelf heeft afgedaan of alsnog heeft opgestuurd naar het OM, bijvoorbeeld omdat de verdachte ambtshalve is vervolgd. Tot slot was volgens de politie een aantal keer sprake van een onbekend PV-nummer (n=10). PV-nummers die tijdens de fase van dataverzameling voor de VCN foutief geregistreerd werden, zijn op voorhand zoveel mogelijk uit de in het onderhavige onderzoek gebruikte dataset verwijderd. Dat een PV-nummer fout was, konden we bijvoorbeeld zien wanneer het nummer niet het juiste aantal karakters had. Desondanks kan het zijn dat ons verzoek aan de politiekorpsen foutief geregistreerde PV-nummers bevatte, bijvoorbeeld door tikfouten die werden gemaakt tijdens het onderzoek waaraan wij de data ontleenden of tijdens ons onderzoek.

Om in kaart te brengen hoe de politie de overige 85 procent van de dossiers heeft afgehandeld, is het van belang om inzicht te krijgen in de wijze waarop zaken die naar een ander korps zijn toegestuurd, zijn afgehandeld. Aan alle korpsen aan wie dossiers zijn

doorgestuurd is daarom gevraagd om aan te geven hoe zij de bij hen binnengekomen dossiers afhandelden (tabel 4.2).

Tabel 4.2: Afhandeling door het korps waarnaar een dossier is doorgestuurd

	Aantal	Percentage
Onbekend	73	83,9
Afgedaan door politie	8	9,2
Doorgestuurd naar het OM	6	6,9
Totaal	87	100,0

Van de naar een ander korps doorgestuurde zaken is de afhandeling in 83,9 procent van de gevallen onbekend, 9,2 procent wordt afgedaan door de politie en 6,9 procent van dergelijke zaken wordt doorgestuurd naar het OM. We weten nu dus van nog eens 14 zaken hoe ze zijn afgehandeld. Die gegevens voegen we bij het overzicht in tabel 4.1 en zo ontstaat tabel 4.3.

Tabel 4.3: afhandeling door de politie, inclusief afhandeling van doorgestuurde zaken.

	Aantal	Percentage
Afgedaan door de politie	282	43,6
Doorgestuurd naar het OM	195	30,1
Onbekend	170	26,3
Totaal	647	100

Van 73,7 procent van de zaken is de afhandeling bekend: afgedaan door de politie of doorgestuurd naar het OM. Van ruim een kwart van de door ons onderzochte aangiften cybercrime is de afhandeling echter niet in kaart te brengen. In theorie zouden alle zaken waarvan we de afhandeling niet hebben achterhaald, afgedaan kunnen zijn door de politie. Het percentage zaken dat is afgedaan door de politie ligt dus tussen de 43,6 en 69,9 procent (percentage afgedaan politie + percentage onbekend). Ook is het in theorie mogelijk dat alle zaken waarvan de afhandeling onbekend is, zijn doorgestuurd naar het OM. Het percentage naar het OM doorgestuurde zaken ligt dus tussen de 30,1 en de 56,4 procent (percentage doorgestuurd OM + percentage onbekend).

Het lijkt daarmee waarschijnlijk dat het percentage zaken die de politie zelf afdoet hoger is dan het percentage zaken dat wordt doorgestuurd naar het OM. Niet alleen onze bevindingen wijzen in die richting, maar ook in eerder onderzoek wordt geconcludeerd dat het merendeel van alle bij de politie geregistreerde zaken niet doorstroomt in het proces van vervolging en berechting (Algemene Rekenkamer, 2012; Leertouwer en Kalidien, 2011). Ook de bevinding dat de wijze waarop een deel van de aangiften zijn afgehandeld onbekend blijft, is niet nieuw. De Algemene Rekenkamer (2012) concludeerde eerder bijvoorbeeld al dat de politie haar zaakstroom niet sluitend kan verantwoorden: van 8,7 procent van de onderzochte geweld- en vermogensmisdrijven is onbekend hoe de politie ze heeft afgehandeld. Het percentage geweld- en vermogensmisdrijven waarvan de afhandeling onbekend is ligt aanzienlijk lager dan het percentage cyberzaken waarbij de afhandeling onbekend is. De aard van de onderzochte cyberzaken biedt daarvoor een mogelijke verklaring: nagenoeg de helft van de cyberzaken betreft e-fraude. E-fraudedossiers worden relatief vaak doorgestuurd naar een ander politiekorps omdat de dader buiten het gebied van dat korps opereert, waarna de afhandeling veelal niet meer in kaart te brengen is.

Er is onderzocht in hoeverre verschillen bestaan in de afhandeling per soort cybercrime (tabel 4.4). Afpersen laten we hierbij buiten beschouwing omdat we daarvan een te gering aantal zaken in de analyse hebben (n=13). Hacken en e-fraude dossiers worden relatief vaak afgedaan door de politie.[19] Mogelijk speelt de complexiteit van hackenzaken en het gebrek aan prioriteit bij e-fraude zaken – die tijdens de interviews veelal worden getypeerd als 'eigen schuld, dikke bult zaken' – daarbij een rol. Van kinderpornodossiers wordt een groter deel dan van andere cybercrimes doorgestuurd naar het OM.[20] Een mogelijke verklaring daarvoor is dat, deels vanwege de maatschappelijke verontwaardiging ten aanzien van dit delict, aan de bestrijding van kinderporno hoge prioriteit wordt gegeven (Stol e.a., 2008). De afhandeling van e-fraude zaken is voor een groot deel onbekend.[21] Bij fraudezaken wordt dat (deels) veroorzaakt doordat een aanzienlijk deel (26,5%) van de dossiers wordt doorgestuurd naar een ander korps en vervolgens ontraceerbaar is.

Tabel 4.4: afhandeling per soort cybercrime

			Definitieve afhandeling			
			Afgedaan door politie	Doorgestuurd naar OM	Onbekend	Totaal
	E-fraude	n	141	55	108	304
		%	46,4	18,1	35,5	100,0
	Haatzaaien	n	7	16	16	39
		%	17,9	41,0	41,0	100,0
	Hacken	n	108	8	19	135
		%	80,0	5,9	14,1	100,0
	Kinderporno	n	22	109	25	156
		%	14,1	69,9	16,0	100,0

Op basis van de verzamelde data kunnen geen exacte uitspraken worden gedaan over de wijze waarop aangiften cybercrime worden afgehandeld. Het percentage zaken waarvan de afhandeling onbekend blijft is daarvoor te hoog. Bovendien betrof onze steekproef niet alle soorten cybercrime maar een selectie van vijf soorten. Het percentage zaken in onze steekproef dat wordt afgedaan door de politie ligt tussen de 43,6 en 69,9 procent. Het percentage zaken die voor verdere vervolging naar het OM zijn doorgestuurd ligt tussen de 30,1 en de 56,4 procent. Het onderzoek geeft aanleiding om te veronderstellen dat de wijze van afhandeling verschilt per soort cybercrime, afhankelijk van complexiteit en prioriteit. E-fraude zaken worden bijvoorbeeld relatief vaak afgedaan door de politie omdat politiemedewerkers daaraan geen prioriteit toekennen. Het slachtoffer is volgens hen zelf bijvoorbeeld deels verantwoordelijk voor de oplichting. Aan de bestrijding van kinderpornozaken, waarbij sprake is van grote maatschappelijke verontwaardiging, wordt hoge prioriteit gegeven. Dergelijke zaken worden dan ook relatief vaak doorgestuurd naar het OM.

[19] Het percentage 'afgedaan door de politie' is bij hacken significant hoger dan bij e-fraude, haatzaaien en kinderporno, en bij e-fraude significant hoger dan bij haatzaaien en kinderporno ($p<0.01$; z-skore voor proporties).

[20] Het percentage 'doorgestuurd naar het OM' is bij kinderporno significant hoger dan bij de andere drie cybercrimes in deze analyse ($p<0,01$; z-skore voor proporties).

[21] Het percentage 'onbekend' bij e-fraude en bij haatzaaien is significant hoger dan bij hacken en kinderporno ($p<0,01$; z-skore voor proporties).

5. Overwegingen bij de strafrechtelijke afhandeling van cybercrime

5.1 Inleiding

Hoofdstuk drie laat zien dat actoren op verschillende plaatsen binnen het proces van aangifte tot veroordeling kunnen kiezen tussen een aantal mogelijkheden. Die keuzes zijn bepalend voor het verloop van dit proces. In dit hoofdstuk laten we zien welke overwegingen ten grondslag liggen aan de keuzes van actoren bij beslissingen over de opsporing en vervolging van (cybercrime)zaken. Per processtap beschrijven we op basis van de literatuur en interviews de overwegingen en laten we zien wat dat in de praktijk betekent voor de afhandeling van cybercrimedelicten.

5.2 Waargenomen slachtofferschap

Figuur 5.1: Waargenomen slachtofferschap

Niet alle strafbare feiten komen in de strafrechtketen terecht. Voordat überhaupt melding gemaakt kan worden van een strafbaar delict moet dat delict eerst door iemand worden gezien of ervaren. Vervolgens moet diegene het delict als strafbaar beoordelen. Dat geldt ook voor cybercrimes. Slachtofferschap van cybercrime is lastig vast te stellen omdat mensen niet altijd weten dat zij slachtoffer zijn (Domenie e.a., 2012). Wat als iemands computer is gehackt en onderdeel is gemaakt van een botnet waarmee spam wordt verstuurd en de eigenaar van de computer dat niet in de gaten heeft? Hetzelfde geldt voor malware (kwaadaardige software zoals virussen en spyware). Het is voor een gebruiker niet altijd duidelijk of dit wel of niet op de computer zit. Er is in dergelijke gevallen dus sprake van slachtofferschap, maar doordat het slachtoffer dat niet weet kan er ook geen aangifte worden gedaan bij de politie. In een Amerikaans onderzoek uit 2005 (America Online e.a., 2005), gehouden onder internetgebruikers, geeft 46 procent van de respondenten aan dat de computer spyware bevat. Na een scan op spyware door de onderzoekers blijkt dat 61 procent van de respondenten spyware op de computer heeft.

Daarnaast zijn er zogenaamde slachtofferloze delicten. Voorbeelden hiervan in de offline wereld zijn heling, rijden onder invloed, drugs- en wapenhandel, maar ook milieuovertredingen. Dergelijke delicten kunnen worden gepleegd zonder dat een voor de hand liggend ‘slachtoffer’ het delict zal melden. Ook bij cybercrime is er sprake van slachtofferloze delicten. Voorbeelden hiervan zijn de illegale handel van medicijnen en heling via internet. Het is onbekend wat de omvang van dergelijke cyberdelicten is en dus is ook onbekend hoeveel van deze delicten niet bij politie en justitie terechtkomen.

Uit recent slachtofferonderzoek naar cybercrime blijkt dat 8,5 procent van de ondervraagde burgers slachtoffer is geworden van een of meer vormen van cybercrime. 4,3 procent werd het slachtoffer van hacken, 3,5 procent is slachtoffer van financiele cyberdelicten en 1,5 procent is slachtoffer geworden van stalking en/of bedreiging (Domenie e.a. 2012). Naast burgers worden ook bedrijven slachtoffer. Dijk (2007) vindt dat 22,8 procent van de Midden en Klein

Bedrijven slachtoffer is van een ernstige vorm van computercriminaliteit. Daaronder schaart hij hacken met of zonder diefstal van gegevens, dDos aanvallen, en defacement van websites.

Als mensen weten dat zij of hun bedrijf slachtoffer zijn van een misdrijf, zijn er vier mogelijke vervolgacties (Goudriaan e.a. 2004). Ten eerste kan iemand besluiten om helemaal niets te doen, volgens Wittebrood (2006) een voor de hand liggende optie bij minder ernstige delicten. Een tweede optie is schadeloosstellen zonder de dader te benaderen, bijvoorbeeld door ontvreemde goederen terug te halen of een schadevergoeding (van de verzekering) te ontvangen. Als derde mogelijkheid kan een slachtoffer zonder hulp van buitenaf een oplossing zoeken. Bijvoorbeeld door via eigenrichting de dader zelf te straffen, of door het nemen van extra veiligheidsmaatregelen om herhaling te voorkomen (Wittebrood, 2006). Een vierde mogelijkheid is het doen van aangifte bij de politie. De politie kan dan de dader opsporen, de ontvreemde goederen achterhalen of de politiebemoeienis kan er toe leiden dat dader en slachtoffer de zaak onderling regelen.

Uit onderzoek blijkt dat slachtoffers van cybercrime soms inderdaad niets doen (Domenie e.a., 2012). Bij financiële delicten onderneemt grofweg een op de tien slachtoffers geen actie. Bij oplichtingen via veiling- of verkoopsites is dat 11,8 procent en bij identiteitsfraude en/of diefstal is dat 11,1 procent. Bij voorschotfraude zijn de slachtofferaantallen te laag om te percenteren, maar deden vier van de achttien slachtoffers niets. Bij cybercrimes in de persoonlijke sfeer ligt het percentage van slachtoffers dat niets doet hoger dan bij de financiële delicten. Bij stalking is dat bijvoorbeeld 58,7 procent en bij bedreiging 38,9 procent. Het merendeel van de slachtoffers van financiële delicten deed wel iets: zij probeerden hun geld terug te krijgen (Domenie e.a., 2012). Manieren waarop slachtoffers proberen geld terug te krijgen, zijn het blijven benaderen van de verkoper, via de eigen bank of de bank van de oplichter. Ook zochten de slachtoffers na de oplichting informatie over de oplichter via internet.

De vierde optie die Wittebrood (2006) noemt is het doen van een aangifte. Uit bovenstaande blijkt al dat slachtoffers van cybercrimes niet in alle gevallen aangifte doen. In het geval van cybercrime is het dan ook de vraag of, indien er sprake is van slachtofferschap, burgers vinden dat de politie verantwoordelijk is voor hun veiligheid in de digitale wereld. Domenie e.a. (2012) vroegen in hun onderzoek aan internetters wie de veiligheid op internet moet waarborgen. Volgens internetters zijn vooral de financiële instellingen (93.4%), de eigenaren van websites (79.9%) en zij zelf (85.1%) verantwoordelijk voor de veiligheid op internet. Ruim een kwart van de internetters (27.1%) acht zichzelf echter niet goed in staat de eigen veiligheid te waarborgen. Bijna drie op de tien internetters (29.0%) vindt dat (ook) de politie een verantwoordelijkheid heeft in het waarborgen van de veiligheid op internet. In lang niet alle gevallen denkt een burger dus meteen aan de politie in het geval van slachtofferschap. Een deel van de cyberzaken waarvan burgers slachtoffer worden, stroomt de strafrechtketen dus niet in. Meer over aangiftepercentages in de volgende paragraaf.

5.3 Aangifte door het slachtoffer

Figuur 5.2: Aangifte

Indien een slachtoffer (of een omstander) ervoor kiest om aangifte te doen bij de politie kan een zaak de strafrechtketen instromen. Volgens het CBS werd in 2010 één op de vier ondervonden delicten via internet of een ondertekend Proces Verbaal aangegeven bij de politie (CBS, 2011). Het aangiftepercentage hangt sterk af van het soort delict. Met name bij vermogensdelicten ligt het aangiftepercentage hoog: 42 procent (met uitschieters voor inbraak en diefstal met respectievelijk 80 en 61 procent). Van mishandeling deed 20 procent van de slachtoffers aangifte. Bedreiging werd door 10 procent aangegeven en seksuele delicten door 5 procent. Ook omstanders blijken vaak terughoudend te zijn in het doen van aangifte over een strafbare gebeurtenis waarvan zij getuige waren (University of Leicester, 2007).

Domenie e.a. (2012) bevinden dat het percentage burgers dat contact op neemt met de politie bij cybercrimedelicten gemiddeld 13,4 procent is. Het aangiftepercentage verschilt per delictsoort. Het is relatief hoog bij stalking en bedreiging (respectievelijk 30,4 en 27,8%). Daarna volgt oplichting op een veiling- of verkoopsite (19,6%). Het aandeel slachtoffers dat contact met de politie opneemt is klein bij een hack (in dit geval hacken van een computer of e-mailaccount of defacing) en voorschotfraude (respectievelijk 4,1 en 5,6%). In het empirische onderzoek *Aangiftebereidheid van computercriminaliteit bij bedrijven* vindt Dijk (2007) voor de delicten hacken, dDos-aanvallen en website defacement een gemiddeld aangiftepercentage van 3,4 procent. Deze cijfers laten zien dat het aangiftepercentage van verschillende financiële cybercrimes aanzienlijk lager ligt dan de 42 procent bij vermogensdelicten in de IVM. Ook het aangiftepercentage van delicten als hacken is erg laag vergeleken met het gemiddelde aangiftepercentage van delicten in de IVM.

Een enigszins uitgewerkt voorbeeld van een laag aangiftepercentage geven we aan de hand van malware. In onderzoek naar het geregistreerde werkaanbod cybercrime vinden de onderzoekers in twee korpsen geen enkele aangifte inzake malware (Domenie e.a., 2009)[22]. Dit terwijl 16,7 procent van de internetters in de afgelopen 12 maanden malware heeft opgemerkt op de computer thuis (Domenie e.a., 2012). Van die groep had 16,1% financiële schade geleden, bijvoorbeeld omdat de PC moest worden gerepareerd, wat neerkomt op 2,7 procent van alle internetters. Dit is dus een duidelijk voorbeeld van criminaliteit met financiële gevolgen voor het slachtoffer, waarvoor het slachtoffer geen contact opneemt met de politie.

Slachtoffers geven verschillende redenen om geen aangifte te doen bij de politie (CBS, 2011): het helpt toch niet (36 procent), de zaak is niet belangrijk genoeg (26 procent), het is geen zaak voor de politie (17 procent), de zaak is al opgelost (8 procent) of er werd gevreesd voor represailles (1 procent). Bij 13 procent speelden andere, niet nader bekende, redenen een rol om geen aangifte te doen. Meest genoemde reden om wel aangifte te doen zijn volgens het

[22] Dat betekent overigens niet altijd dat slachtoffers nooit aangifte doen, maar wel dat de politie deze delicten niet heeft geregistreerd.

CBS (2011) dat het slachtoffer vond dat de politie het moest weten (24 procent) of vanwege een verzekering (23 procent). Andere redenen zijn: om het gestolen goed terug te krijgen (18 procent), omdat de dader moet worden gepakt (16 procent). 'Ik vond het mijn plicht' werd met 9 procent het minst als reden genoemd.

Er is voor zover wij weten nog maar weinig onderzoek gedaan naar de redenen van slachtoffers van cybercrime om wel of geen aangifte te doen. Om te beginnen vindt een aanzienlijk deel van de slachtoffers dat in eerste instantie niet de politie maar anderen verantwoordelijk zijn voor hun veiligheid in de digitale wereld (zie paragraaf 5.2). Volgens geïnterviewden in ons onderzoek doen slachtoffers om meerdere redenen geen aangifte van cybercrime. De zwaardere high-tech crime zaken bij *bedrijven* komen vaak niet bij politie en justitie binnen, omdat met name grotere bedrijven eigen afdelingen hebben die aanvallen afweren. Deze bedrijven proberen problemen eerst zoveel mogelijk intern op te lossen. Datzelfde is volgens een respondent overigens te zien bij fraudezaken binnen bedrijven. Grootschalige interne fraudes willen bedrijven liever zelf oplossen. Dat bedrijven de politie veelal niet inschakelen heeft volgens onze respondenten te maken met angst voor imagoschade. Die veronderstelling zien we ook elders bij de politie. Over cyberafpersen schrijft het KLPD (2007) bijvoorbeeld dat de daadwerkelijke omvang van het probleem in Nederland groter kan zijn dan uit de registraties naar voren komt, bijvoorbeeld omdat bedrijven bang zijn voor imagoschade en niet in het nieuws willen brengen dat zij ingaan op de eisen van een afperser. Dijk (2007:58) vindt echter geen verband tussen door het bedrijf verwachte imagoschade en het al dan niet doen van aangifte. Als belangrijkste motivaties van bedrijven om geen aangifte te doen vindt Dijk: 'heeft toch geen zin' (29,0%), 'weegt niet op tegen de tijd die een aangifte kost' (27,4%), en 'incident was niet ernstig genoeg' (19,4%).

Een ander probleem, dat volgens respondenten zowel bij burgers als bedrijven speelt, is dat het aangiftepercentage laag is doordat het imago van politie en OM op het gebied van cybercrime voor verbetering vatbaar is. Bedrijven hebben veel meer technische kennis in huis om zaken zelf op te lossen en/of zien de politie niet als competent in dergelijke zaken. Dijk treft deze reden ook aan: 9,7 procent van de bedrijven die slachtoffer werden van cybercrime deed geen aangifte daarvan vanwege 'geen vetrouwen in de politie' (ibidem). Een van onze respondenten zei in dit verband dat 'als een bedrijf al aangifte doet en de politie pakt de zaak vervolgens niet goed op, dan doet dat bedrijf de volgende keer geen aangifte meer'. Dijk rapporteert dat 3,2 procent van de eerder genoemde bedrijven geen aangifte deed vanwege 'slechte eerdere ervaringen met politie' (ibidem).

Kortom, net zoals bij reguliere vormen van criminaliteit, is het aangiftepercentage bij cybercrime laag. Dat betekent dat het grootste deel van de cybercriminaliteit buiten het zicht van politie en justitie blijft. Helemaal vergelijkbaar zijn de cijfers die we hebben over aangiftepercentages van offline en online delicten niet, maar ze maken wel aannemelijk dat het aangiftepercentage bij cyberdelicten (nog) lager ligt dan bij klassieke offline delicten. Er zijn verschillende oorzaken voor het lage aangiftepercentage. Burgers en bedrijven betwijfelen bijvoorbeeld of de politie effectief in staat is om cybercrime te bestrijden en ze zien de politie niet als de instantie die in eerste instantie verantwoordelijk is voor de veiligheid in de digitale wereld.

5.4 Politie: registratie

Figuur 5.3: Registratie door politie

De burger neemt contact op met de politie om een melding van een strafbaar feit te maken. De intake kan op verschillende manieren: op het bureau of op lokatie, via de telefoon of internet. De manier waarop burgers melding of aangifte kunnen doen, is niet in alle korpsen gelijk. Zo kan niet in alle korpsen telefonisch een aangifte worden opgenomen, in een aantal korpsen kan een aangifte alleen op afspraak worden gedaan en in andere korpsen is het maken van een afspraak niet nodig (Toutenhoofd e.a. 2009).

De stap om naar een bureau te gaan om aangifte te doen kan drempelverhogend zijn, daarom is het sinds enige jaren mogelijk om bijvoorbeeld via internet aangifte te doen van een aantal delictsoorten. Intakers zelf geven echter aan dat een aangifte cybercrime aan de balie moet worden opgenomen (Toutenhoofd e.a., 2009). De reden hiervoor is dat de aangever alleen in face-to-face contact bewijsstukken kan overleggen (bijvoorbeeld prints van e-mail contact, uitdraaien van internetpagina's, uitdraaien van MSN verkeer en IP-adressen).

Uit de landelijke politiële beleidsdocumenten 'Herijking visie op dienstverlening' (2007) en 'Visie op intake' (2008) blijkt dat de politiemedewerker die de intake verzorgt, bepaalt of een aangifte moet worden opgenomen. Hij of zij weegt daarbij af of de aangedragen zaak tot de kerntaken van de politie behoort. De kerntaken van de politie staan beschreven in de Politiewet van 1993. De politie is belast met de handhaving van de openbare orde, het opsporen van strafbare feiten, hulpverlening bij nood en signalering van en advisering bij (on)veiligheidssituaties. Alleen als de door de burger aangedragen zaak tot deze kerntaken behoort neemt de intaker de aangifte op. Is dat niet het geval, dan verwijst de politiemedewerker de burger door naar een andere instantie. Het officiële beslismoment is dus de afweging of een melding betrekking heeft op de kerntaken van de politie. Maar er blijken meer redenen te zijn om een aangifte niet te registreren[23] (Wittebrood, 2006; University of Leicester, 2007; Toutenhoofd e.a., 2009):

- de agent beoordeelt het feit als zijnde niet strafbaar;
- de agent vindt dat er te weinig bewijs is;
- het delict is te licht of geniet geen prioriteit binnen het korps;
- er is sprake van 'blameworthiness' van de klager (eigen-schuld-dikke-bult zaken);
- de verdachte is nog geen 12 jaar en kan niet strafrechtelijk worden vervolgt.

Een eenmaal opgenomen aangifte kan door de aangever nog weer worden ingetrokken, bijvoorbeeld omdat het vermiste goed weer terecht is en dus toch niet gestolen was, of omdat de aangever angst krijgt voor represailles. Intrekken hoeft niet te betekenen dat de aangifte uit de politieregistratie wordt verwijderd, maar in de regel zal het wel betekenen dat de politie verder geen actie meer onderneemt, tenzij het gaat om een ernstige zaak die de politie vanwege die ernst ambtshalve in behandeling neemt.

[23] Wanneer de aangever er op staat dat een aangifte wordt opgemaakt en de politie weigert dit, dan kan de aangever een klacht indienen bij de politie of de Officier van Justitie (artikel 12 WvSv).

Uit de literatuur blijkt dat de politie niet alle aangiften van slachtoffers registreert. Volgens Wittebrood (2006:95) wordt 'van ongeveer 20 procent van de delicten die bij de politie worden gemeld geen document zoals een proces-verbaal ondertekend. Deze delicten worden dus ook niet opgenomen in de politieregistraties.' Het is onbekend hoe hoog dit percentage is bij cybercrimedelicten. We weten wel dat intakers, onder andere door een kennistekort waardoor ze de strafbaarheid verkeerd inschatten, niet altijd een aangifte opnemen en soms slachtoffers naar huis sturen (Toutenhoofd e.a., 2009; Ministerie van Justitie, 2010). Zie casus 5.1.

Casus 5.1: Niet herkennen van een delict

Volgens het Ministerie van Justitie (2010) komt het voor dat intakers indentiteitsdiefstal of -misbruik niet herkennen en dat ze weigeren om een aangifte op te nemen. Hiertoe voert de politie verschillende argumenten aan. Een argument is dat het gebruik maken van de identiteit van een ander persoon op zich geen strafbaar feit is. Een ander argument is dat de persoon die aangifte wil doen, niet de benadeelde is van de fraude. Dit kan bijvoorbeeld als op naam van een persoon goederen bij een bedrijf zijn besteld en deze persoon wordt aangesproken voor de kosten, terwijl hij of zij de goederen nooit heeft ontvangen. Sommige bedrijven nemen de schade hiervan voor eigen rekening als blijkt dat de goederen bij een fraudeur zijn afgeleverd. Enkele politiekorpsen hanteren in dat geval de regel dat niet de klant, maar het betrokken bedrijf de benadeelde is en dat dit bedrijf aangifte zou moeten doen. Het komt echter ook voor dat bedrijven geen aangifte willen doen. Echter de klant is ook slachtoffer, er is misbruik gemaakt van zijn/haar gegevens. Hoewel er geen apart wetsartikel is voor identiteitsmisbruik, kan de benadeelde klant bijvoorbeeld op basis van artikel 326 Sr wel aangifte doen. Daarin wordt 'het iemand bewegen tot afgifte van enig goed door het aannemen van een valse naam of een valse hoedanigheid' strafbaar gesteld. Het feit dat niet de persoon in kwestie, maar het bedrijf financiële schade heeft geleden vormt geen belemmering om de aangifte op te nemen. Artikel 161 van het Wetboek van Strafvordering bepaalt namelijk dat iedereen die kennis draagt van een strafbaar feit daarvan aangifte mag doen. Artikel 163 lid 6 van het Wetboek van Strafvordering verplicht de politie vervolgens om een dergelijke aangifte op te nemen.

Domenie e.a. (2012) laten zien wat de politie volgens slachtoffers van cybercrime doet nadat zij contact opnemen (tabel 5.1). De reactie van de politie is grofweg te verdelen in drie categorieën: de politie nam een aangifte op, de politie nam een melding op of gaf advies, de politie deed niets.

Tabel 5.1: Reactie van de politie op cybercrimes

Reactie	Aangifte opgenomen		Melding of advies		Geen strafrechtelijke actie	
	Aantal	%	Aantal	%	Aantal	%
Fraude via veiling- of verkoopsites, voorschotfraude en identiteitsfraude (n=58)	33	56,9	10	17,2	15	25,9
Stalking, bedreiging, belediging, defacing, pc gehackt of mail gehackt (n=63)	18	28,6	33	52,4	12	19,0

De tabel laat zien dat wanneer een respondent contact opnam met de politie vanwege fraude via veiling- of verkoopsites, voorschotfraude of identiteitsfraude, de politie in 56,9 procent van de gevallen een aangifte opnam. Bij hacken of een op de persoon gericht delict (stalking, bedreiging, belediging) in 28,6 procent van de gevallen. In het laatste geval wordt vaker een melding opgenomen of advies gegeven (52,4%).

De politie neemt dus lang niet in alle gevallen een aangifte op. Bij de niet-financiële delicten ligt het percentage slachtoffers dat zegt dat de politie geen aangifte opnam het hoogst. Het is geen verrassend verschil, want bij delicten in de persoonlijke sfeer is voor de politie niet altijd duidelijk wie welk aandeel had in het gerezen conflict en kan de vraag rijzen of een strafrechtelijke route wel de beste aanpak is. Derhalve zijn politiemensen dan terughoudender met het opnemen van een aangifte.

Volgens Wittebrood (2006) wordt van bijna 80 procent van de gemelde (offline) delicten een aangifte opgemaakt. In geval van finec-cybercrime neemt de politie van 56,9 procent van de gevallen een aangifte op en in geval van interpersoonlijke cybercrimes in 28,6 procent. Beide percentages zijn significant lager dan het door Wittebrood genoemde gemiddelde percentage voor (offline) criminaliteit.[24] Of de aangiftepercentages voor cybercrime ook lager zijn dan de aangiftepercentages voor vergelijkbare (financieel-economische) offline criminaliteit, is uit deze gegevens niet af te leiden.

Casus 5.2: Geen strafrechtelijke actie / niet serieus nemen van een aangever (bron: Toutenhoofd e.a. 2009)

Een slachtoffer van diefstal van virtuele goederen in het virtuele habbo hotel heeft aangifte gedaan bij de politie in korps E. Zij heeft eerst de politie gebeld om te vragen of zij aangifte kon doen. De politiemedewerker met wie zij sprak, had twijfels over het doen van aangifte. De aangever heeft doorgezet en moest zeuren om toch aangifte te kunnen doen. Ze is hierover ontevreden. Tijdens het opnemen van haar aangifte hoorde de aangever andere politiemedewerkers lachen om haar verhaal. Ze voelde zich dus niet serieus genomen. De verbalisant snapte niet waarover het ging maar kon haar verhaal toch redelijk op papier zetten. De aangifte is eind 2007 opgenomen. Begin 2009 is zij gebeld om te melden dat er

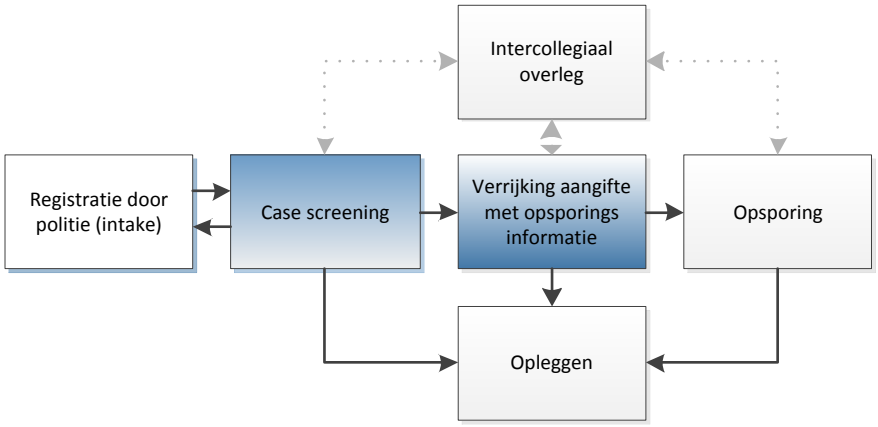
[24] P<0,01; z-skore voor proporties. De n in het onderzoek van Wittebrood (2006) was 1.631.000

waarschijnlijk een onderzoek wordt gestart omdat er meer meldingen/aangiften binnen zijn gekomen van diefstal uit het habbo hotel. De aangever kreeg het advies van de politie om een goede virusscanner te instaleren. Dit is wederom een teken voor de aangeefster dat de agent niet snapte waar het over gaat: 'het gaat hier om hacken dus zou je advies moeten krijgen over beveiliging van een pc!' Al met al is de aangeefster niet tevreden over de intake.

Samengevat zien we het volgende: conform landelijk politiebeleidsdocumenten beoordeelt de intakemedewerker bij de politie of een aangifte tot de kerntaken van de politie behoort en naar aanleiding daarvan of al dan niet een aangifte moet worden opgenomen. Niet alle meldingen of aangiften worden geregistreerd: de politiemedewerker kan bijvoorbeeld van mening zijn dat er geen sprake is van een strafbaar feit. Het is mogelijk dat zaken daardoor ten onrechte buiten het geregistreerde werkaanbod van de politie vallen. Deze problematiek speelt niet alleen bij cybercrime. Wittebrood (2006) gaf al aan dat van ongeveer 20 procent van de delicten die bij de politie worden gemeld geen document zoals een proces-verbaal wordt ondertekend. Domenie e.a. (2012) laten echter zien dat in het geval van cybercrime het aantal zaken waarvan de politie geen proces verbaal opmaakt nog een stuk hoger is.

5.5 Politie: casescreening

Figuur 5.4: Case screening door politie[25]



De Inspectie Openbare Orde en Veiligheid (IOOV) (2009) laat zien dat de gehanteerde criteria voor het stoppen of doorgaan met een zaak divers zijn. De meest genoemde criteria zijn: juridische haalbaarheid (de kans op vervolging en/of veroordeling), beleidsindicatoren (waaronder landelijke-, regionale-, lokale beleidsprioriteiten en korpsprioriteiten) en opsporingsindicatie (de mate waarin een aangifte aanknopingspunten biedt om de verdachte op te sporen). Minder vaak, maar nog wel regelmatig, wordt volgens de IOOV (2009) als criterium genoemd: 'ernst feit/zwaarte incident' en 'beschikbare capaciteit in relatie tot slagingskans'. Ook criteria als 'instructie sepotgronden', 'OM-aanwijzingen, landelijke aanwijzingen voor de opsporing' en 'wegingsfactoren dan wel puntensysteem' worden genoemd. Het merendeel van de korpsen (negentien van de vijfentwintig) zeggen volgens de IOOV wel eens af te wijken van de te hanteren criteria. Redenen om af te wijken van deze

[25] De ondoorbrokenlijn staat voor de mogelijke stappen in het proces, de stippellijn staat voor de overlegmomenten.

criteria zijn de ernst en maatschappelijke impact van een delict (dit schuift aspecten van efficiëntie terzijde), schrijnende gevallen, onderbuikgevoel of kosten-baten afwegingen.

De criteria juridische haalbaarheid, beleidsindicatoren en opsporingsindicatie die door het IOOV benoemd werden als belangrijkste criteria voor het stoppen of doorgaan met een zaak worden ook door het merendeel van de respondenten in dit onderzoek genoemd. Uit interviews blijkt wel dat de weging per persoon verschillend is. Case screeners maken geen gebruik van richtlijnen bij het bepalen of een zaak wel of niet door de screening komt. Een aantal case screeners weet van de Aanwijzing voor de Opsporing, maar geen van de case screeners zegt daar mee te werken. Overigens zegt dat niet dat case screeners niet een afweging maken die in lijn is met de Aanwijzing voor de opsporing. Alle respondenten geven namelijk aan dat de afweging gemaakt wordt op basis van aanwezigheid van opsporingsindicatie. Het gaat dan om de aanwezigheid van informatie die tot de verdachte kan leiden, bijvoorbeeld getuigen en videobeelden, maar ook een ip-adres of een e-mailadres.

Ook de beleidsprioriteiten spelen volgens case screeners een rol. Als er prioriteit zit op een bepaald delict dan laten case screeners dergelijke zaken in de regel doorgaan, ook al is er geen sprake van opsporingsindicatie. Op cybercrime zit volgens de case screeners geen prioriteit. Wel kan het zo zijn dat een cybercrime in brede zin valt onder één van de beleidsprioriteiten. Bijvoorbeeld een zaak waarin een minderjarige wordt afgeperst met de verspreiding van naaktbeelden. Het is volgens de respondenten niet zo dat zaken waar geen prioriteit aan gegeven is per definitie niet door de screening heen komen.

De juridische haalbaarheid noemt maar een enkele case screener als belangrijke factor in de afweging. Over de hele linie vinden respondenten het beoordelen van de kans op vervolging en veroordeling een verantwoordelijkheid van het OM en niet van de case screening. Indien het in de ogen van de case screener om een grote zaak gaat met een hoge maatschappelijke impact, maar de kans op vervolging en/of veroordeling klein lijkt, dan wordt overlegd met het OM. Het OM kan dan beslissen om het onderzoek wel of niet op te zetten. De verantwoordelijkheid daarvoor willen de case screeners niet op zich nemen.

Naast opsporingsindicatie, beleidsprioriteit en juridische haalbaarheid speelt volgens enkele respondenten de mate waarin het slachtoffer zelf verantwoordelijk is voor hetgeen hem of haar is overkomen een rol. Case screeners noemen dit het ‘eigen-schuld-dikke-bult’ principe. Voorbeelden worden genoemd van oplichtingen via internet waarbij mensen geld overmaken en het bestelde goed niet krijgen. ‘Je kunt toch ook niet verwachten dat je voor zo’n laag bedrag dat product kunt kopen’, aldus een respondent.

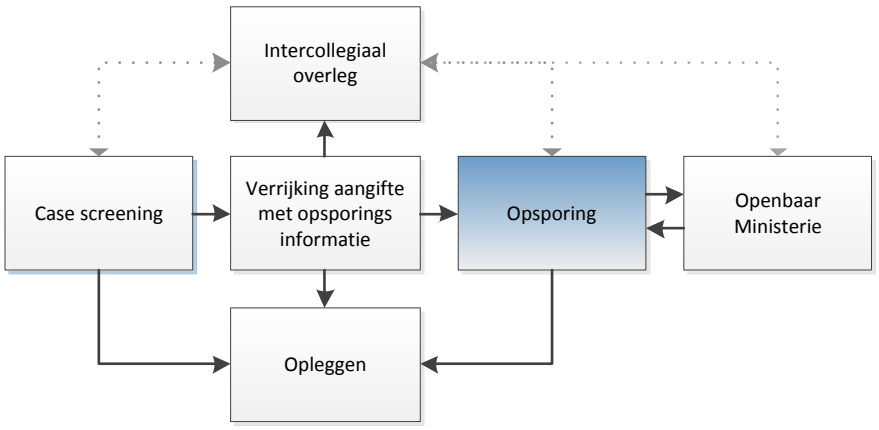
Samengevat blijkt uit de interviews dat case screeners naar eigen inzicht beoordelen of een zaak in behandeling wordt genomen: zij maken volgens eigen zeggen geen gebruik van richtlijnen (zoals de Aanwijzing voor de Opsporing) bij het bepalen of een zaak wel of niet door de screening komt. Wel geven alle case screeners aan dat aangiften voornamelijk worden gescreend op opsporingsindicatie. Ook beleidsindicatoren en – in beperkte mate – de juridische haalbaarheid van een zaak spelen een rol. Volgens enkele respondenten speelt daarnaast de mate waarin het slachtoffer zelf verantwoordelijk is voor het geen hem of haar is overkomen een rol. Case screeners noemen dit het ‘eigen-schuld-dikke-bult’ principe.

Eerder beschreven De Poot e.a. het proces van case screening op basis van een uitvoerige bestudering van recherchedossiers en aanvullende interviews. Aan het vorenstaande voegen zij toe dat zaken waarin reeds een verdachte is aangehouden ‘praktisch allemaal’ in opsporing

genomen worden (2004:55). De aanwezigheid van een direct op of nabij de plaats van het delict aangehouden verdachte geeft een zaak dus de hoogste prioriteit. De Poot e.a. spreken dan van 'klip-en-klaarzaken'. In geval van cybercrime zal zelden of nooit meteen bij de aangifte al een verdachte zijn aangehouden. Cybercrimezaken hoeven in de fase van case screening dus niet alleen te concurreren met zaken met een hoge maatschappelijke impact maar ook met zaken met een lagere maatschappelijke impact waarbij meteen al een verdachte is aangehouden.

5.6 Politie: opsporing

Figuur 5.5: Opsporing door politie[26]



De casescreening stuurt de aangifte door naar een opsporingsteam. Niet alle zaken die door de case screening komen worden daadwerkelijk in behandeling genomen door opsporingsteams (IOOV, 2009; Kalidien de Heer-de Lange, 2011; Algemene Rekenkamer, 2012). Deze teams hebben over het algemeen een groot werkaanbod en kunnen niet alle zaken (meteen) in behandeling nemen. Tijdens de opsporing worden daarom nieuwe prioriteiten gesteld. Cybercrime heeft in veel gevallen volgens respondenten een lage prioriteit. Er komt in geen geval bloed bij kijken. Dergelijke zaken verliezen het daardoor van de 'waan van de dag' zaken: als er een moord of gewelddadige overval is gepleegd dan is het volgens respondenten 'alle hens aan dek'. De benodigde capaciteit om zo'n zaak te draaien wordt vrijgemaakt en de andere zaken blijven liggen. Meer over capaciteit en prioriteit in hoofdstuk 6.

Respondenten geven aan dat alleen zaken die qua omvang van het recherchewerk 'behapbaar' zijn, binnen de regionale opsporingsteams worden afgehandeld. Als een zaak door de BPZ of een crimeteam wordt opgepakt, dan bepaalt de betreffende chef lokale prioriteiten. Volgens respondenten is dit een belangrijke schakel wat betreft het oppakken van het werkaanbod dat buiten de landelijke prioriteiten en 'waan van de dag' zaken valt. 'Als daar iemand zit die niets met digitale onderzoeken heeft, dan is de kans erg klein dat zo'n zaak wordt opgepakt', aldus een respondent. Cybercrimezaken blijven dan liggen en worden na verloop van tijd (90 dagen) opgelegd: de zaak wordt dan afgehandeld zonder dat opsporingsonderzoek is vericht. Omvangrijke en / of zware zaken worden door een districtelijk rechercheteam opgepakt. Ook binnen deze rechercheteams worden prioriteiten gesteld. Dat wordt gedaan op basis van een

[26] De ondoorbrokenlijn staat voor de mogelijke stappen in het proces, de stippellijn staat voor de overlegmomenten.

‘weegdocument’. Dat weegdocument is opgesteld op basis van korpsspecifieke doelstellingen. Hoe de resultaten van de weging vervolgens worden geïnterpreteerd is afhankelijk van een disctrictelijk overleg. In dat overleg, waarbij de hoofden van alle politieprocessen en de Districts Officier van Justitie aanwezig zijn, wordt vervolgens definitief besloten of een zaak in behandeling wordt genomen.

Naast beleidsprioriteit is in de fase van de opsporing nog steeds ook de opsporingsindicatie van belang. Het is volgens respondenten nu niet alleen van belang dat er een opsporingsindicatie is maar ook hoe *snel* een verdachte kan worden geïdentificeerd, gelokaliseerd en aangehouden. Hoe makkelijker dat kan, hoe eerder een zaak wordt opgepakt. Deze afweging wordt gemaakt in combinatie met de prioriteiten. Volgens respondenten is bij cybercrimedelicten vaak aanvullend onderzoek nodig om tot een verdachte te komen. Er is misschien wel een IP-adres bekend, maar dan moet nog worden onderzocht welke verdachte daar precies bij hoort: wie zit er bijvoorbeeld achter het e-mailadres onbekend@onbekend.com? Respondenten zien dit als een drempel om dergelijke zaken op te pakken. Meer hierover in hoofdstuk 6.

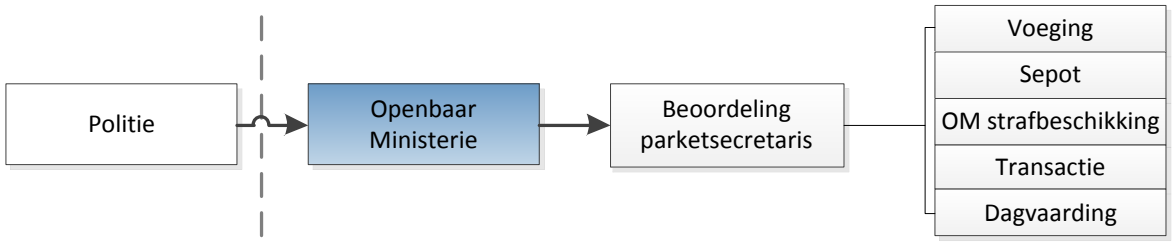
Volgens Huys & Smit (2011) varieert het percentage door de politie opgehelderde misdrijven voor de verschillende delictgroepen. Misdrijven die door eigen opsporingsactiviteiten worden geconstateerd, zoals (vuur)wapen- en drugsmisdrijven, kennen een relatief hoog opheldering-spercentage, dat ruim boven 80 procent uitkomt. Gewelds- en seksuele misdrijven hebben ook een relatief hoog ophelderingspercentage van 63 procent. Hierbij speelt volgens de onderzoekers een rol dat slachtoffer en dader elkaar vaak kennen, wat het opsporen van de dader voor de politie vergemakkelijkt. Van twee veel voorkomende delictsgroepen ligt het ophelderingspercentage juist een stuk lager: van vernielingen wordt een vijfde deel opgehelderd en van vermogensmisdrijven een tiende deel.

Over cybercrime weten we dat bepaalde cybercrimesoorten vaker dan andere cybercrimesoorten door de politie worden doorgestuurd naar het OM. Bij de gevallen die de politie doorstuurt, heeft zij een verdachte op het oog en lijkt vervolging haalbaar (zie ook hoofdstuk 4). De kwantitatieve analyse van de zaakstroom die we deden voor dit onderzoek laat zien dat het percentage zaken dat de politie doorstuurt naar het OM bij kinderpornografiezaken het hoogst is (69,9%). Bij de e-fraudezaken en hackenzaken ligt dat percentage een stuk lager (respectievelijk 18,1% en 5,9%). We hebben dit lang niet van alle mogelijke vormen van cybercrime in kaart kunnen brengen, maar wel is te zien dat ook bij cybercrimezaken per delictsgroep verschil bestaat in het percentage misdrijven dat de politie naar het OM doorstuurt. Uit de interviews blijkt dat daaraan verschillende overwegingen ten grondslag liggen: prioriteit, de mate waarin capaciteit beschikbaar is om een zaak op te pakken en de mate waarin een aangifte aanknopingspunten voor de opsporing bevat.

Samengevat zien we dat ook binnen opsporingsteams keuzes worden gemaakt om bepaalde zaken wel of niet op te pakken. Er vallen ook in deze fase dus zaken uit de strafrechtketen. Volgens respondenten leidt het gebrek aan prioriteit, beschikbare en of vrijgemaakte capaciteit en de ervaren moeite om bij cyberzaken opsporingsonderzoek te verrichten ertoe dat dergelijke zaken minder snel worden opgepakt dan aangiften van traditionele delicten.

5.7 Openbaar Ministerie

Figuur 5.6: Openbaar Ministerie



Indien de politie optreedt ter strafrechtelijke handhaving van de rechtsorde, verricht zij haar werk onder het gezag van de Officier van Justitie (art. 13 Politiewet 1993). Een zaak die de politie naar het OM heeft gestuurd, wordt beoordeeld door een parketsecretaris. Deze kan besluiten de zaak terug te sturen naar de politie voor aanvullingen (Kruijer, 2012). Daarbij is sprake van kwaliteitscontrole: de parketsecretaris beoordeelt of alle relevante stukken aanwezig zijn en toetst de zaak op juridische haalbaarheid.

Deze controle door het OM wordt alleen uitgevoerd op zaken die de politie instuurt. Er is geen zicht op de zaken waar de politie nog niets mee heeft gedaan of waar al wel opsporingswerk voor is verricht, maar waarover nog geen contact is geweest met het OM. Er is volgens respondenten vanuit het OM bijvoorbeeld geen systematische manier om de kwaliteit en inhoud van de intake te beoordelen. Het kan dus zijn dat panklare zaken al verloren gaan bij de intake, zonder dat het OM daar zicht op heeft. De IOOV (2009) komt tot eenzelfde conclusie. Bijna tweederde van de parketten heeft volgens de Inspectie geen of onvoldoende zicht op de zaken die de politie als werkvoorraad heeft.

Als de zaak niet wordt teruggestuurd naar de politie, dan overweegt het OM de haar beschikbare afdoeningswijzen voor strafzaken. Daarbij wordt doorgaans gebruik gemaakt van zogenaamde beleidsregels. Daarin zijn richtlijnen opgenomen over de wijze waarop het OM zaken af dient te handelen. Zij heeft de volgende mogelijkheden (zie figuur 5.6):

- Allereerst kan het OM strafzaken ‘voegen’, dat wil zeggen bijeen brengen zodat de zaken in samenhang kunnen worden beoordeeld. Daarvan zijn twee varianten. (1)_Een zaak kan ter berechting worden gevoegd. De rechter beoordeelt verschillende zaken met dezelfde verdachte dan tegelijkertijd. (2) Een zaak kan ad informandum worden gevoegd: belastend materiaal over de verdachte uit een andere lopende strafzaak kan dan door de rechter ter informatie worden meegenomen in het bepalen van de strafmaat.
- Het OM kan een zaak seponeren. Er vindt dan geen verdere vervolging plaats. De ‘Aanwijzing gebruik sepotgronden’ bevat een overzicht van de gronden die aan de basis liggen van een sepot. Er zijn verschillende soorten sepots. Als onvoldoende uitzicht bestaat op veroordeling omdat daarvoor bijvoorbeeld het bewijs ontbreekt, zal gekozen worden voor een technisch sepot. Als op grond van het algemeen belang wordt afgezien van vervolging, bijvoorbeeld als strafrechtelijk ingrijpen een hulpverleningstraject van de reclassering ongewenst doorkruist, dan kan worden gekozen voor een beleidssepot. Sepots kunnen zowel voorwaardelijk, als onvoorwaardelijk van aard zijn.
- Ook kan het OM zonder tussenkomst van een rechter zelfstandig een strafbeschikking opleggen. Een strafbeschikking kan uiteenlopend van aard zijn. Het OM kan onder meer

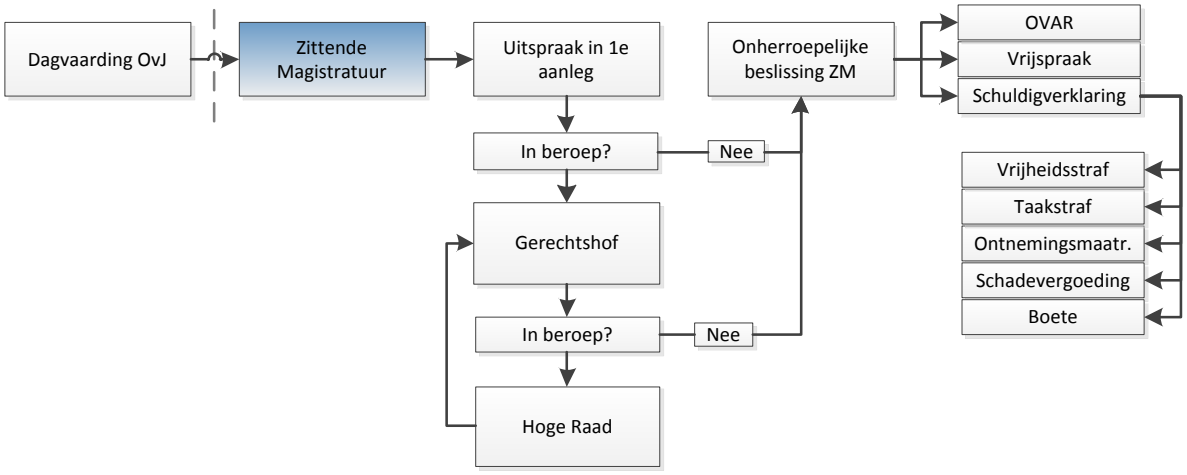
opleggen: een geldboete, een taakstraf of een schadevergoedingsmaatregel voor het slachtoffer. In de ‘aanwijzing OM-afdoening’ zijn beleidsmatige criteria opgenomen op basis waarvan een strafbeschikking kan worden opgelegd. Het opleggen van een strafbeschikking berust op schuldvaststelling: als niet kan worden vastgesteld dat de verdachte het ten laste gelegde feit heeft gepleegd, wordt de strafbeschikking niet uitgevaardigd.

- Als een zaak niet voldoet aan de in de Aanwijzing OM-afdoening uitgewerkte criteria voor het uitvaardigen van een strafbeschikking kan een transactie worden aangeboden. De ‘aanwijzing kader voor strafvordering’ biedt richtlijnen voor (de hoogte van) het transactieaanbod.
- Als een zaak dagvaarding vereist bereidt de parketsecretaris de zaak voor op het onderzoek ter zitting. De Officier van Justitie brengt de zaak uiteindelijk voor de rechter. De strafeis wordt bepaald op basis van daarvoor opgestelde delictspecifieke richtlijnen voor strafvordering. Deze richtlijnen zijn verwerkt in het Beslissing Ondersteunend Systeem (BOS) dat door het OM gebruikt wordt om de strafeis te bepalen. Het systeem bepaalt de strafeis op basis van een rekensom. Aan ieder misdrijf waarvoor delictspecifieke richtlijnen zijn opgesteld is een vast aantal strafpunten toegekend. Het aantal punten kan, afhankelijk van de omstandigheden waarin het delict is gepleegd, worden verhoogd of verlaagd. Afhankelijk van de aard van- en omstandigheden waarin het delict is gepleegd, wordt dus het definitieve aantal strafpunten vastgesteld. Op basis daarvan berekent het systeem vervolgens de strafeis. De bestaande richtlijnen bieden weliswaar richtlijnen voor de afhandeling van (sommige) cybercrimes in ruime zin, zoals oplichting, bedreiging en/of smaadschrift, maar bieden (nog) geen houvast om de strafmaat bij cybercrimes in enge zin vast te stellen. Daarvoor zijn er nog te weinig zaken geweest.

Kortom, zaken die de politie doorstuurt naar het OM worden in eerste aanleg beoordeeld door een parketsecretaris. Hij toetst binnengekomen zaken voornamelijk op juridische haalbaarheid. De parketofficier heeft de mogelijkheid om zaken voor aanvullend onderzoek terug te sturen naar de politie. Gebeurt dat niet, dan overweegt het OM de tot haar beschikking staande afdoeningswijzen. Op basis van zogenaamde beleidsregels wordt overwogen of een zaak wordt geseponeerd, er een strafbeschikking of transactie wordt opgelegd of dat de zaak voor de rechter wordt gebracht. In de richtlijnen voor het bepalen van de strafmaat komt cybercrime in enge zin niet voor.

5.8 Zittende Magistratuur

Figuur 5.7: Zittende Magistratuur



De Officier van Justitie bepaalt of een zaak voor de rechter wordt gebracht. Hij beslist ook of de zaak wordt voorgelegd aan een enkelvoudige of meervoudige kamer. De rechter beoordeeld vervolgens of de dagvaarding in orde is, de rechter bevoegd is en de Officier van Justitie ontvankelijk.

Voor delicten die relatief veel voorkomen zijn in een Landelijk Overleg van Voorzitters van Strafsectoren zogenaamde 'oriëntatiepunten voor straftoemeting' opgesteld (Stafbureau LOVS, 2012). De oriëntatiepunten bieden richtlijnen voor rechters om de hoogte van een straf te bepalen. Volgens respondenten zijn de richtlijnen ontleend aan jurisprudentie en onderzoek. Rechters zijn niet verplicht om die uitgangspunten te hanteren. Dergelijke richtlijnen zijn er, met uitzondering van skimmen, niet voor de afhandeling van cybercrimezaken in enge zin. Dat komt volgens respondenten doordat daarover weinig jurisprudentie voorhanden is.

De opgelegde straf wordt doorgaans bepaald op basis van het wettelijke strafmaximum in combinatie met zaakgerelateerde- en persoonlijke omstandigheden van de verdachte. Zaakgerelateerde omstandigheden zijn:
- de aard en gevolgen van het delict;
- opzet / voorbedachte rade (hoe geraffineerder het plan, hoe hoger de strafmaat);
- de termijn waarbinnen de zaak voor de rechter is gebracht (hoe langer de termijn, hoe beperkter de straf);
- de tijdsduur waarbinnen het delict zich heeft afgespeeld (heeft de verdachte zich eenmalig schuldig gemaakt aan het delict, of gedurende langere tijd/herhaaldelijk);
- of er sprake is van een criminele organisatie en de positie van de verdachte binnen die organisatie.

Persoonlijke omstandigheden zijn bijvoorbeeld eventuele justitiële documentatie van de verdachte en persoonlijkheidsstoornissen.

Volgens respondenten kan het van belang zijn om de waardering van de gevolgen van cybercrimezaken te herijken ten opzichte van reguliere zaken. De gevolgen van een

cybercrime kunnen immers een geheel andere dimensie hebben dan de gevolgen van een regulier misdrijf: het delict, zoals smaad, kan mogelijk worden geopenbaard aan een in beginsel onbeperkt grote groep mensen én gedurende een onbeperkte tijd. Dat kan de gevolgen ernstiger maken.

Bij het vellen van zijn oordeel, is de rechter afhankelijk van de informatie uit het verrichte opsporingsonderzoek en de informatie uit het verweer van de (advocaat) van de verdachte. Volgens de respondenten maakt het geen verschil of de in het opsporingsonderzoek aangedragen informatie betrekking heeft op een cyberzaak en dus bijvoorbeeld afkomstig is uit internettaps of betrekking heeft op een reguliere zaak en afkomstig is uit rapportages van bijvoorbeeld een observatieteam. Het gaat erom dat de politie en het OM hun bevindingen helder rapporteren, zodat rechters de bewijsbaarheid van een zaak kunnen toetsen. Hoewel het formeel de taak van rechters is om te beoordelen of het opsporingsonderzoek deugdelijk is verricht (art. 359a Sv) en dat volgens rechters zowel bij reguliere, als bij cyberzaken best lastig kan zijn, bestaan daarover in de praktijk lang niet altijd twijfels. Rechters zijn het er dan ook over eens dat cyberzaken niet lastiger zijn af te handelen dan reguliere zaken.

Samengevat toetsen strafrechters in hoeverre een verdachte schuldig is aan het ten laste gelegde misdrijf. Voor delicten die relatief veel voorkomen zijn richtlijnen opgesteld om de strafmaat te bepalen. Voor cybercrimezaken (in enge zin) bestaan dergelijke richtlijnen niet. Wel gelden algemene overwegingen, zoals de persoonlijke omstandigheden van de verdachte. Rechters ervaren cyberzaken niet per definitie als lastiger dan reguliere zaken: zij zijn afhankelijk van het begrijpelijk uitgeschreven bewijsmateriaal dat door de politie en het OM is aangeleverd en het verweer van de (advocaat) van de verdachte. Hoewel ook van ze wordt verwacht dat ze een oordeel vellen over (de kwaliteit van) het opsporingsonderzoek en dat niet altijd een gemakkelijke opgave is, bestaan daarover doorgaans weinig tot geen twijfels. Daardoor kunnen zij in de praktijk naar eigen zeggen volstaan met de door de politie, het OM en de verdediging aangeleverde informatie. Wel merken respondenten op dat de digitale component aan cyberzaken er toe kan leiden dat de gevolgen voor het slachtoffer anders zijn dan bij reguliere strafzaken: een smadelijke tekst of foto kan bijvoorbeeld voor een onbeperkt grote groep mensen toegankelijk gemaakt worden via internet. Dergelijke overwegingen spelen een rol bij het bepalen van de uiteindelijke straf.

5.9 Het proces samengevat

Hoofdstuk 3 en 5 maken duidelijk dat slachtofferschap in veel gevallen niet leidt tot een veroordeling van de dader. Zaken komen nooit terecht in de strafrechtketen of vallen daar om verschillende redenen en op verschillende momenten weer uit voordat het tot een rechterlijke uitspraak komt. Er is dus sprake van selectiviteit. Dat is logisch, er is te weinig capaciteit om alle zaken op te pakken en daardoor moeten politie en justitie keuzes maken. Hierna volgt een korte schets van het gehele proces.

Niet alle vormen van cybercrime zijn direct zichtbaar voor slachtoffers. Daarnaast is het percentage slachtoffers van cybercrime dat aangifte doet laag, naar het zich laat aanzien lager dan bij offline criminaliteit. Dat betekent dat een groot deel van de cybercriminaliteit buiten de politieregistratie blijft. Er zijn verschillende oorzaken voor het lage aangiftepercentage. Burgers en bedrijven betwijfelen bijvoorbeeld of de politie effectief in staat is om cybercrime te bestrijden en ze zien de politie niet als de instantie die primair verantwoordelijk is voor de veiligheid in de digitale wereld. Al met al kunnen we constateren dat burgers en bedrijven zich met een aanzienlijk deel van de delicten nooit tot de strafrechtketen wenden.

Ook al doen ze dat wel, dan wil dat nog niet zeggen dat die zaak in de strafrechtketen belandt. Ook bij de intake en registratie van cybercrime vallen zaken af. De intakemedewerker bij de politie beoordeelt of een aangifte moet worden opgenomen. Niet alle meldingen of aangiften worden geregistreerd: de politiemedewerker kan bijvoorbeeld (al dan niet terecht) van mening zijn dat er geen sprake is van een strafbaar feit. Het is mogelijk dat zaken daardoor ten onrechte buiten het geregistreerde werkaanbod van de politie vallen. Van de traditionele delicten die bij de politie worden gemeld eindigt ruim 20 procent niet in een aangifte (Wittebrood, 2006). Domenie e.a. (2012) laten zien dat in het geval van cybercrime het percentage zaken waarvan de politie geen aangifte opneemt significant hoger is: 43,1 procent bij finec cybercrime en 71,4 procent bij interpersoonlijke delicten.[27]

De Aanwijzing voor de Opsporing schrijft richtlijnen voor op basis waarvan een case screener kan bepalen of een zaak wel of niet moet worden doorgestuurd naar een opsporingsteam. De stelregel is dat alle zaken met opsporingsindicatie worden opgepakt. Case screeners maken naar eigen zeggen niet bewust gebruik van deze of andere richtlijnen bij het bepalen of een zaak wel of niet door de screening komt. Wel hanteren zij vergelijkbare criteria voor de screening van zaken. Aangiften worden door case screeners voornamelijk getoetst op opsporingsindicatie en in mindere mate ook op beleidsindicatoren en juridische haalbaarheid. Op cybercrime zit volgens de case screeners geen prioriteit. Wel kan het zo zijn dat een cybercrime in brede zin valt onder één van de beleidsprioriteiten. Naast opsporingsindicatie, beleidsprioriteit en juridische haalbaarheid speelt volgens enkele respondenten de mate waarin het slachtoffer zelf verantwoordelijk is voor hetgeen hem of haar is overkomen een rol. Case screeners noemen dit het 'eigen-schuld-dikke-bult' principe. Volgens respondenten stromen cyberzaken in verhouding tot traditionele zaken eerder uit. Zaken die niet afvallen, gaan door naar een opsporingsteam.

Vervolgens worden binnen de opsporingsteams weer keuzes gemaakt om bepaalde zaken wel of niet op te pakken en vallen er dus weer nieuwe zaken uit de strafrechtketen. Cybercrime heeft in veel gevallen volgens respondenten een lage prioriteit. Dergelijke zaken verliezen het dus van de 'waan van de dag' zaken. Gevolg is dat cybercrimezaken blijven liggen en na verloop van tijd (90 dagen) automatisch worden afgedaan. Indien zaken wel worden opgepakt dan is er volgens respondenten bij cybercrimedelicten veelal aanvullend onderzoek nodig om tot een verdachte te komen. Respondenten zien dit als een drempel om dergelijke zaken op te pakken.

Zaken die de politie doorstuurt naar het OM worden in eerste aanleg beoordeeld door een parketsecretaris. Hij voert als het ware een kwaliteitscontrole uit. Bij onvoldoende kwaliteit van het dossier kan de parketsecretaris zaken voor aanvullend onderzoek terugsturen naar de politie. Gebeurt dat niet dan overweegt het OM op basis van zogenaamde beleidsregels of een zaak wordt geseponeerd, of er een strafbeschikking of transactie wordt opgelegd of dat de zaak voor de rechter wordt gebracht. Er bestaan richtlijnen om de strafmaat te bepalen, maar niet voor cybercrime in enge zin.

Ten slotte toetsen strafrechters in hoeverre een verdachte schuldig is aan het ten laste gelegde misdrijf. Voor delicten die relatief veel voorkomen zijn richtlijnen opgesteld om de strafmaat te bepalen. Voor cybercrimezaken in enge zin bestaan dergelijke richtlijnen, met uitzondering van skimmen, niet. Wel gelden algemene overwegingen, zoals de persoonlijke omstandigheden van de verdachte. Bij het vellen van zijn oordeel is het volgens artikel 359a

[27] $P<0,01$; z-skore voor proporties.

van het wetboek van Strafvordering de taak van de rechter om te beoordelen of het opsporingsonderzoek deugdelijk is verricht. In de praktijk bestaan volgens rechters echter lang niet altijd twijfels over het verrichte opsporingsonderzoek, waardoor rechters naar eigen zeggen uitspraak kunnen doen over de zaak op basis van de door de politie, het OM en de verdediging aangeleverde en begrijpelijk uitgeschreven informatie. Zij ervaren het afhandelen van cyberzaken niet als lastiger dan het afhandelen van reguliere zaken.

6. Knelpunten binnen het proces van slachtofferschap tot veroordeling

6.1 Inleiding

In dit hoofdstuk beschrijven we de knelpunten die respondenten van de politie, het OM en de ZM signaleren met betrekking tot de doorstroom van cybercrimezaken. We beschrijven deze knelpunten per stap binnen het proces van slachtofferschap tot veroordeling.

Een aantal respondenten geeft aan dat er voor cybercrime geen specifieke knelpunten zijn, maar dat de knelpunten die in het algemeen gelden voor de afhandeling van zaken ook gelden voor cybercrime. Het merendeel van de respondenten geeft echter aan dat er wel degelijk specifieke problemen zijn omtrent de afhandeling van cybercrime. In elk geval menen respondenten unaniem dat er knelpunten zijn in het proces.

6.2 Waargenomen slachtofferschap en aangifte

Figuur 6.1 waargenomen slachtofferschap en aangifte

Allereerst blijkt dat het gros van de misdrijven niet de strafrechtketen instromen omdat daarvan geen melding en/of aangifte wordt gedaan bij de politie. Of slachtofferschap wordt waargenomen (door slachtoffers zelf of door omstanders) is van invloed op het werkaanbod cybercrime. Burgers nemen niet altijd waar dat zij digitaal slachtoffer zijn geworden (bijvoorbeeld dat een computer gehackt is en onderdeel is gemaakt van een botnet of dat een computer geïnfecteerd is met malware). Bovendien wordt van lang niet alle waargenomen misdrijven aangifte gedaan bij de politie. Dat geldt ook voor cybercrime. Respondenten stellen dat geen aangifte wordt gedaan, omdat door burgers en bedrijven wordt betwijfeld of de politie effectief uitvoering kan geven aan de bestrijding van cybercrime. In een ander onderzoek (Domenie e.a., 2012) hebben we gezien dat burgers bij de vraag wie verantwoordelijk is voor de veiligheid op internet, niet primair aan de politie denken maar eerder aan financiële instellingen, eigenaren van websites en aan zichzelf. Wellicht speelt bij het lage aangiftepercentage voor cybercrime dus ook een rol dat burgers bij online criminaliteit niet direct denken aan een politietaak.

Of we het geringe aangiftepercentage van cybercrime een knelpunt moeten noemen, is een kwestie van perspectief. Het is zonder meer een knelpunt voor wie meent dat de politie er is om elk strafbaar feit aan te pakken. De politie wordt dan immers onterecht buiten spel gezet door burgers die geen aangifte doen. Het geringe aangiftepercentage is minder – of misschien zelfs wel niet – een knelpunt voor wie meent dat niet per definitie de politie de door een strafbaar feit geschonden maatschappelijke orde moet herstellen. Wellicht kunnen anderen dat ook en voorkomen zij daarmee de inzet van schaarse politie-capaciteit. Zo gezien is het niet altijd alleen maar slecht dat burgers en bedrijven zaken oplossen zonder de bemoeienis van de politie. Als burgers en bedrijven *alle* strafbare feiten zouden aangeven, dan zou zelfs al snel blijken dat de politieorganisatie daarop niet is ingericht. Het komt er aldus op aan dat in de samenleving een zekere consensus bestaat over waarvan aangifte moet worden gedaan, waarvan niet, en over wat daar tussenin ligt.

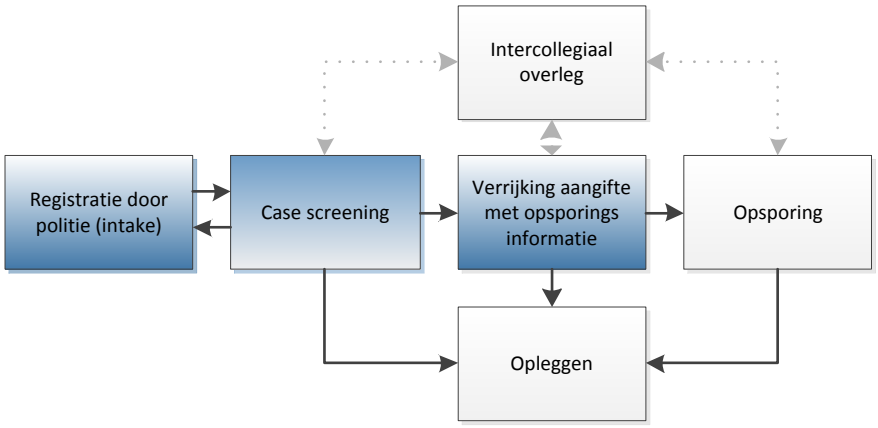
Het knelpunt bij cybercrime in de slachtofferschap- en aangiftefase zouden we zo gezien liever niet kortweg willen omschrijven als 'burgers doen vaak geen aangifte'. Het ligt genuanceerder. Er is ook een gebrek aan maatschappelijke concensus over wie in de bestrijding van cybercrime welke verantwoordelijkheid heeft en welke inzet dat van wie vraagt. 'Maatschappelijke concensus' hebben we niet onderzocht, dus met zekerheid kunnen we hierover hier geen uitspraken doen. We zien echter dat burgers niet altijd allereerst aan de politie denken wanneer zij denken aan hun veiligheid in de digitale wereld (Domenie e.a, 2012). We zien tegelijkertijd ook dat de politie investeringen doet om aangiften te verzamelen en te analyseren, bijvoorbeeld in de vorm van het Meldpunt Internetoplichting (www.mijnpolitie.nl/if.shtml) en het Digitaal Bedrijvenloket Cybercrime (www.mijnpolitie.nl/ondernemer/index.shtml; waar bedrijven aangifte kunnen doen).

Een van de kenmerken van cybercrime is dat daders geografisch gesproken eenvoudig op geheel verschillende plaatsen slachtoffers kunnen maken, bijvoorbeeld door oplichting via internet. Een internetcrimineel kan met vele kleine oplichtingen de dader zijn van een omvangrijke criminaliteit. Het vergt van de politie een nieuwe (informatie)strategie om dergelijke criminelen met de juiste prioriteit te kunnen beoordelen: geografisch sterk verspreide aangiften moeten bijeen kunnen worden gebracht en aan elkaar gerelateerd. De politie is zich daarvan bewust en onderneemt stappen, bijvoorbeeld middels het genoemde Meldpunt Internetoplichting, maar ook door het ontwikkelen van analysestrategieën en bijbehorende instrumenten (vgl. Elzinga, 2011). Als de politie zich inricht op het via vele kleine zaken achterhalen van grote boeven, dan is het wel zaak dat burgers van kleine zaken aangifte doen, ook al lijken ze nu daartoe niet geneigd – en dat de politie al die kleine zaken efficiënt en effectief in haar informatiebestanden weet op te nemen.

Resumé knelpunten in waargenomen slachtofferschap en aangifte
Burgers nemen niet altijd waar dat zij slachtoffer zijn van cybercrime. Doen zij dat wel, dan is de vraag in welke gevallen aangifte zou moeten worden gedaan. De nieuwe criminaliteit vraagt om nieuwe informatiestrategieën van de politie. Voor het realiseren daarvan is het onvoldoende dat de politie haar organisatie en informatiesystemen aanpast: ook moet de maatschappelijke concensus omtrent van welk feit burgers/bedrijven aangifte dienen te doen, opnieuw tot stand worden gebracht.

6.3 Politie: intake en case screening

Figuur 6.2: Intake en case screening door politie[28]



Zoals gezegd, is het overgrote deel van de door de politie geregistreerde delicten door burgers aangegeven en niet het resultaat van zelfstandig opsporingswerk (University of Leicester, 2007). Aan de basis van het gros van de zaken in de justitiële keten staat dus een aangifte. Het goed opnemen van een aangifte is daarom essentieel voor de verdere afhandeling van een zaak. Respondenten van zowel de politie als het OM noemen het gebrek aan kennis over cybercrime bij intakemedewerkers en de kwaliteit van de opgenomen aangiften als een knelpunt.

Burgers of bedrijven die aangifte doen, worden volgens respondenten soms ten onrechte weggestuurd door intakemedewerkers. Herhaaldelijk vertellen respondenten dat burgers geen aangifte konden doen van fraude via veiling- en verkoopsites (ook wel marktplaatsfraudes genoemd), omdat het volgens de intaker om een civiele zaak ging (zie ook Toutenhoofd e.a., 2009). Verder zijn er voorbeelden van politiemedewerkers die weigeren om aangifte op te nemen van feiten die wel bij wet strafbaar zijn gesteld (zie ook Ministerie van Justitie, 2010). De ontoereikende kennis van intakemedewerkers leidt er toe dat misdrijven niet worden geregistreerd en dus ook niet de strafrechtketen instromen.

Ook op het moment dat intakemedewerkers besluiten om wel een aangifte op te nemen kan het kennistekort de verdere afhandeling van cybercrimezaken belemmeren. De kwaliteit van opgenomen aangiften blijkt in sommige gevallen te laag. Belangrijke (opsporings)informatie ontbreekt bijvoorbeeld in de aangifte. Intakers hebben dan niet de juiste vragen gesteld en/of geen relevant bewijsmateriaal verzameld. Het probleem met aangiften waarbij belangrijke informatie mist, bijvoorbeeld opsporingsindicatie, is dat die zaken de case screening al niet door komen. In sommige gevallen stuurt de case screening de aangifte terug naar de intakemedewerker met het verzoek de ontbrekende informatie toe te voegen, maar respondenten geven aan dat dit lang niet altijd het geval is. Als de aangifte niet terug gaat naar de intake dan komt de aangifte, doordat opsporingsindicatie ontbreekt, niet door de screening en doet de politie de zaak op dat moment af. Een opsporingsteam en/of het OM krijgen de

[28] De ondoorbrokenlijn staat voor de mogelijke stappen in het proces, de stippellijn staat voor de overlegmomenten.

zaak dan nooit te zien. Volgens een respondent worden aangiften cybercrime vaker dan reguliere aangiften opgelegd als OD: een zaak met een onbekende dader en/of te weinig opsporingsindicatie. Een deel van de uitstroom van cybercrimezaken lijkt dan ook ongewenst: op grond van de Aanwijzing voor de Opsporing zou immers iedere zaak met voldoende opsporingsindicatie een vervolg moeten krijgen. In cybercrimezaken wordt tijdens het opnemen van aangiften echter niet altijd voldoende opsporingsinformatie verzameld, waardoor dergelijke zaken al in een vroeg stadium worden opgelegd.

Dat intakemedewerkers onvoldoende kennis hebben om aangiften cybercrime op te nemen komt volgens respondenten doordat zij daarvoor onvoldoende zijn opgeleid. Er wordt van intakemedewerkers verwacht dat zij van alle delicten een aangifte kunnen opnemen. Die verwachting is irreëel vinden onze respondenten: 'Er zijn intakers die alleen de basisschool hebben afgemaakt.' Respondenten nemen het intakers niet kwalijk als zij fouten maken: 'dan moeten ze maar niet de laagst opgeleiden op zo'n belangrijke post zetten', aldus een case screener. Er wordt opgemerkt dat de ontoereikende kwaliteit van opgenomen aangiften geen specifiek aan cybercrime gelieerd probleem is: ook de kwaliteit van opgenomen aangiften van reguliere misdrijven is niet altijd toereikend.

De bevinding dat de kennis van intakemedewerkers ontoereikend is om een aangifte cybercrime op te nemen is niet nieuw. Naar de intake van cybercrimedelicten is eerder onderzoek gedaan door Toutenhoofd e.a. (2009). De belangrijkste conclusies uit het onderzoek naar intake was dat het kennisniveau over cybercrime bij de intake te laag is (zie ook casus 6.1). Er was tot voor kort in politieopleidingen en aanvullende cursussen geen specifieke aandacht voor cybercrime en de kennis die er is, is fragmentarisch. Dat fragmentarische karakter is volgens de onderzoekers ontstaan doordat intakers hun kennis overwegend ontlenen aan de praktijk: eigen ervaringen en verhalen van anderen. Er is geen systematiek in de kennisopbouw en -voorraad: de één weet iets van deze en de ander weet iets van een andere cybercrime.

Casus 6.1: Onvoldoende kennis van een intakermedewerker[29]

Een aangever van hacken in korps D is ontevreden over het aangifteproces en de wijze waarop ze is ontvangen op het politiebureau. De intaker toonde wel interesse en leek de zaak serieus te nemen, maar achteraf gezien heeft de aangever zijn twijfels over die interesse. Ze heeft het idee dat ze niet serieus is genomen. De aangever had de toezegging gekregen dat ze aangifte kon doen bij iemand met veel kennis van zaken, terwijl dit absoluut niet het geval was. De verbalisant zei zelf dat ze geen kennis had van cybercrime en snapte de zaak niet. De aangever is niet op de hoogte gesteld van wat er met de aangifte is gedaan. Al met al heeft aangever geen vertrouwen in de politie als het om cybercrime gaat. Ze zou niet nogmaals aangifte doen bij de politie maar direct een advocaat inschakelen. De aangeefster is gewezen op de mogelijkheid van slachtofferhulp maar heeft hiervan geen gebruik gemaakt. Aangever kreeg geen advies van de politie. Dit is logisch, zo zegt zij, want de verbalisant had geen kennis van zaken.

Naar aanleiding van het onderzoek van Toutenhoofd e.a. (2009) is door het Programma Aanpak Cybercrime een cursus ontwikkeld voor intakemedewerkers op het gebied van cybercrime. In enkele regiokorpsen hebben intakers de cursus gevolgd en vanaf 2012 moet

[29] Bron: Toutenhoofd e.a. (2009).

het project landelijk worden geïmplementeerd. Inmiddels is er in opdracht van het PAC ook een handreiking voor delicten met een digitale component ontwikkeld die onder andere door intakers gebruikt kan worden (Leukfeldt e.a., 2012). Deze handreiking is in druk verschenen en is tevens digitaal beschikbaar via het politie-intranet PolitieKennisNet (PKN) onder de titel Cybertoolkit. Cursus en handreiking worden door het PAC in combinatie binnen de politie verspreid.

Daar hier sprake is van een kennisachterstand bij de politie, ligt er ook een taak voor de Politieacademie. In 2009 was er volgens het politiële Programma Aanpak Cybercrime (PAC) nauwelijks sprake van 'een opleidingsaanbod waarin digitale componenten verweven zijn; gemiddeld 2 procent van alle leeropdrachten bevatten een digitale component.'(PAC, 2009:38). Inmiddels zijn er wel verschillende ontwikkelingen in het politieonderwijs te melden, niet in de laatste plaats gestimuleerd door het PAC (Stol e.a., 2012). Maar: 'De stap naar "digitaal als integraal onderdeel van het politieonderwijs" moet de komende periode nog worden gezet.' (ibidem:36).

Case screening en het verrijken van aangiften
Nadat intakemedewerkers aangiften hebben opgenomen, komen deze bij de case screening. Case screeners bepalen met name op basis van de aanwezige opsporingsindicatie of een zaak wordt opgelegd of wordt doorgestuurd naar een opsporingsteam. Verschillende respondenten geven aan dat ze moeite hebben om cybercrimezaken te snappen en het daardoor lastig vinden om in te schatten of een dergelijke zaak voldoende opsporingsindicatie bevat. In de praktijk leidt dat echter niet per definitie tot problemen. In één korps geven respondenten bijvoorbeeld aan dat een van de collega's aan het bureau erg ICT-smart is en veel weet van cybercrime. Zijn hulp wordt dan ook ingeroepen bij het beoordelen van de opsporingsindicatie bij (complexere) cybercrimezaken.

Het doen van een aangifte via internet is een nieuwe manier om slachtoffers op een laagdrempelige wijze aangifte te laten doen. Internetaangiften geven volgens respondenten echter nieuwe problemen. Dergelijke aangiften bevatten doorgaans weinig tot geen opsporingsindicatie. Mocht een internetaangifte wel opsporingsindicatie bevatten, dan moet de aangever alsnog naar het bureau komen om de politie van aanvullende informatie (bewijsmiddelen e.d.) te voorzien. Uitzondering hierop vormen internetaangiften van oplichting via veiling- of verkoopsites. Dat kan bij het politiemeldpunt voor internetgerelateerde fraude (https://www.mijnpolitie.nl/if.shtml). Via een elektronisch aangifteformulier kan de aangever alle voor een eventueel opsporingsonderzoek benodigde informatie doorgeven. Aangiften die bij het meldpunt gedaan worden, komen niet meer als aangifte binnen bij de politieregio's, maar worden centraal gebundeld en geanalyseerd. Als de politie en het OM besluiten om naar aanleiding van een of meerdere aangiften een zaak op te pakken, dan krijgt de aangever per post het verzoek om zijn proces verbaal te ondertekenen. De aangever hoeft niet meer aan het bureau te verschijnen. Meer hierover in de bijlage over best practices.

Voordat een aangifte met voldoende opsporingsindicatie naar een opsporingsteam gaat, wordt de aangifte verrijkt met daderinformatie. In sommige korpsen is daarvoor een speciaal team ingericht, in andere korpsen worden aangiften verrijkt door case screeners zelf. Respondenten zeggen dat het in het geval van cybercrimezaken soms lastiger is dan bij reguliere zaken om aangiften te verrijken. Eigenlijk weten alleen enkele hobbyisten hoe NAW-gegevens op basis van IP-adressen kunnen worden achterhaald of hoe informatie uit een e-mailheader kan worden verkregen. Voor technische ondersteuning kunnen medewerkers weliswaar terecht bij het ondersteunende Team Digitale Expertise (TDE), maar het TDE is in de praktijk erg druk

met het bieden van ondersteuning aan lopende onderzoeken ('uitlezen' computers en telefoons, etc) waardoor ondersteuning bij het verrijken van aangiften weinig prioriteit heeft. Ook 'krijg je van het TDE antwoorden terug waar je niet veel wijzer van wordt'.

Daarnaast geven case screeners uit een korps aan dat er soms verhoudingsgewijs veel inspanning is vereist en/of hoge kosten zijn verbonden aan het verkrijgen van aanvullende daderinformatie. Om NAW gegevens bij IP-adressen te krijgen moeten officiële verzoeken bij providers worden ingediend. Ook brengen (sommige) banken volgens respondenten kosten in rekening voor het opvragen van gegevens[30]. Als het dan om een eenvoudige oplichting van een paar tientjes op een veilingsite gaat 'kan je je afvragen of het wel zin heeft om dat te doen'. Daarnaast geven de case screeners aan dat het vaak een hele administratieve rompslomp is om informatie van bedrijven te krijgen. Er moet dan een officieel verzoek in worden gediend (ondertekend door een OvJ) en als de bedrijfsjurist dan ook maar één foutje ontdekt (bijvoorbeeld dat het niet bankafko.x, maar bankafkorting.x is) dan moet de aanvraag weer helemaal opnieuw gedaan worden.

Gewenste en ongewenste uitstroom

De politie moet keuzes maken in welke zaken ze wel en niet oppakt. Aangiften die op voorhand kansloos zijn, bijvoorbeeld omdat er geen opsporingsindicatie aanwezig is, moeten dan ook meteen weer uitstromen. Dit is de gewenste uitstroom. Volgens de Algemene Rekenkamer (2012) is echter ook een deel van die uitstroom onterecht en dus ongewenst. Het blijkt dat zaken 'uitgescreend' worden, terwijl die zaken op grond van de *Aanwijzing voor de opsporing* van het OM (i.w.tr. 1 maart 2003) wel opvolging zouden moeten krijgen. Dat is ongewenste uitstroom. De politie maakt de afweging om dergelijke zaken uit te laten stromen zelf en heeft in de regel geen overleg met het OM. Dit is volgens de Algemene Rekenkamer (2012) met name het geval bij veel voorkomende criminaliteit. Bij zware en middelzware criminaliteit is de kans kleiner omdat het OM dan eerder bij de zaak betrokken is (bijvoorbeeld doordat het gaat om haalzaken, of omdat er BOB-verzoeken worden gedaan). Onduidelijk is om hoeveel zaken het gaat.

De Algemene Rekenkamer (2012:14) concludeert dat: 'De ongewenste uitstroom bij casescreening wordt veroorzaakt doordat regelgeving en beleid te veel ruimte en te weinig richting geven in de dagelijkse praktijk: te veel zaken zouden tot opsporingsactiviteit moeten leiden, terwijl de capaciteit daarvoor ontbreekt.' Door een tekort aan capaciteit blijven dus aangiften liggen die eigenlijk gewoon moeten worden opgepakt. Volgens de Algemene Rekenkamer (2012) zijn er korpsen die aangiften van internetfraude meteen terzijde leggen en die oude aangiften (plankzaken) alsnog bij casescreening laten uitstromen.

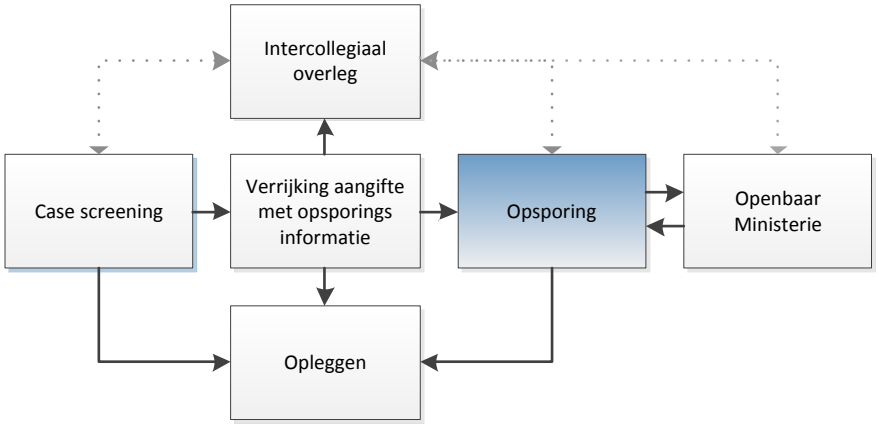
In hoofdstuk 4 lieten we zien dat de uitstroom van cybercrimezaken bij de politie aanzienlijk is. Het percentage zaken dat is afgedaan door de politie, ligt tussen de 43,7 en 69,9 procent. Het percentage zaken dat naar het OM wordt doorgestuurd ligt waarschijnlijk lager: tussen de 30,1 en de 56,3 procent. Onbekend is wat de verhouding tussen gewenste en ongewenste uitstroom bij cybercrime is. We horen in ons onderzoek echter dezelfde geluiden als de onderzoekers van de Algemene Rekenkamer: door een gebrek aan capaciteit en kennis worden cybercrimezaken minder snel opgepakt en blijven dergelijke zaken langer op de plank liggen. Bovendien geven case screeners aan dat cybercrime geen prioriteit heeft. Deze bevindingen hebben tot gevolg dat dergelijke aangiften vaker dan reguliere aangiften al in een vroeg stadium worden opgelegd zonder dat het OM daar zicht op heeft.

[30] Banken hebben daartoe het recht op grond van de wet vorderen gegevens financiele sector.

Resumé knelpunten in intake en casescreening
Uit de interviews blijkt dat ontoereikende kennis op het gebied van cybercrime bij intakemedewerkers ertoe leidt dat aangiften niet worden opgenomen of dat de kwaliteit van aangiften te laag is door ontbrekende informatie. Verder wordt aangegeven dat de opsporingsindicatie in cybercrimezaken soms lastiger is vast te stellen dan de opsporingsindicatie bij reguliere aangiften. Dat heeft te maken met de complexiteit van sommige cyberzaken – of weer met een gebrek aan kennis bij politiemensen. Ook het verrijken van aangiften met opsporingsindicatie wordt bij cybercrimes als lastig ervaren. De meeste politiemedewerkers zijn bijvoorbeeld nog onvoldoende in staat om op basis van een IP adres NAW gegevens op te vragen. Daarnaast ervaart de politie hindernissen in de samenwerking met providers en banken. Het verkrijgen van informatie gaat dan gepaard met relatief hoge kosten en administratieve rompslomp, hetgeen er toe kan leiden dat bij bepaalde aangiften geen extra daderinformatie wordt toegevoegd. Als een dossier wel voldoende compleet is, dan leidt gebrek aan capaciteit er toe dat in sommige cyberzaken alsnog niet wordt overgegaan tot opsporing. Over de hele linie lijkt een deel van de vroegtijdige uitstroom van cyberzaken ongewenst: dergelijke zaken worden wegens voornoemde knelpunten eerder opgelegd dan klassieke delicten. Hierop bestaat geen controle door het OM.

6.4 Politie: opsporing

Figuur 6.3: Opsporing door de politie[31]



De zaken die wel door intakemedewerkers worden opgenomen en die vervolgens door de casescreening komen, moeten in behandeling worden genomen door opsporingsteams. Binnen deze teams wordt opnieuw een afweging gemaakt om een (cybercrime)zaak al dan niet in behandeling te nemen. Respondenten benoemen drie cybercrimespecifieke knelpunten die ertoe leiden dat cyberzaken minder snel worden opgepakt dan klassieke delicten: er wordt geen prioriteit gegeven aan cybercrime, er is te weinig capaciteit in het algemeen en op digitaal gebied in het bijzonder en - daarmee samenhangend - het ontbreekt aan kennis en kunde om het complexe(re) werkaanbod op te pakken. Deze problemen bespreken we hierna.

Geen prioriteit

[31] De ondoorbrokenlijn staat voor de mogelijke stappen in het proces, de stippellijn staat voor de overlegmomenten.

De politie krijgt veel meer zaken dan ze aan kan. Er moeten dus keuzes worden gemaakt. Cybercrime valt volgens de respondenten vaak af in de prioriteitsstelling. Zij stellen dat kinderpornografie-, zeden-, geweld-, drugs- en jeugdzaken landelijke prioriteiten zijn. Uit verschillende landelijke beleidsdocumenten blijkt echter dat ook cybercrime landelijke prioriteit geniet (bijvoorbeeld: Regeerakkoord, 2010). Op landelijk niveau geformuleerde doelstellingen op het gebied van cybercrime worden volgens respondenten niet in alle korpsen vertaald naar regionale targets.

In korpsen waar cybercrime wel als prioriteit is benoemd (in beleidsplannen en regioplannen), blijkt dat sturing op het oppakken van cyberzaken ontbreekt. In de praktijk worden eerst zaken opgepakt 'waar bloed bij komt kijken' (moord, gewelddadige overval). Daardoor verliezen cyberzaken het in de prioritering van klassieke delicten. Politiewerk is volgens respondenten dus grotendeels afhankelijk van 'de waan van de dag'. 'Wij kunnen onze criminelen niet sturen', aldus een respondent. Als veel capaciteit zit in teams voor grootschalige onderzoeken (TGO's), dan is er minder capaciteit voor andere zaken – en vallen cybercrimezaken als een van de eersten af.

Enkele respondenten merken op dat de politiekorpsen (in ieder geval deels) worden afgerekend op tagets die behaald moeten worden. Zij moeten bijvoorbeeld een x aantal zaken van een bepaald delict afhandelen of een vooraf vastgesteld aantal verdachten aanleveren bij het OM. Enkele respondenten binnen de politie ervaren daardoor grote druk om targets te halen. Een door een van de respondenten beschreven voorbeeld illustreert dat een dergelijk prestatiestelsel zijn doel voorbij schiet: 'kwantiteit gaat voor kwaliteit'. Het aanleveren van verdachten staat centraal: de politie lost daardoor liever meerdere enkelvoudige internetoplichtingen met verschillende daders op, dan dat zij een grootschalig en arbeidsintensief onderzoek start naar een notoire internetoplichter die verschillende slachtoffers in verscheidene regio's heeft gemaakt. Het oplossen van eenvoudige oplichtingen kost simpelweg minder tijd en draagt in grotere mate bij aan het behalen van targets (verdachten aanleveren). Over het algemeen geldt volgens respondenten overigens dat cyberzaken eerder niet in behandeling worden genomen dan traditionele zaken, omdat ze gecompliceerder zijn en er meer tijd nodig is om ze af te handelen.

In één politiekorps geven respondenten aan dat cybercrime ook binnen het OM weinig prioriteit heeft. Het is, aldus respondenten, zonde als de politie veel inspanning levert, een panklare cyberzaak naar het OM stuurt en het OM de zaak vervolgens alsnog oplegt. Daarbij merkt een respondent op dat de politie 'een beetje klaar is' met cybercrimezaken, omdat het OM geen richtlijnen opstelt over wanneer cybercrimezaken wel of niet in behandeling moeten worden genomen. Overigens is er met de komst van de cyber OvJ's een aantal jaar geleden wel een en ander veranderd: die hebben volgens respondenten wel affiniteit met cybercrime en de verwachting is dat zij dergelijke zaken wel in behandeling nemen.

Tot slot vindt in sommige regio's een periodiek overleg plaats tussen het OM (de Districtsofficier) en de politie (operationeel leidinggevenden). Daarin wordt besproken wat gedaan dient te worden met de zaken die bij de politie blijven liggen. Dat wordt bepaald op basis van prioriteiten en de beschikbare politiecapaciteit om zaken af te handelen. Het prioriteren van zaken gebeurt aan de hand van een drietrapssysteem: (1) zaken met een hoge maatschappelijke impact hebben de eerste prioriteit (bijvoorbeeld geweldszaken, overvallen en inbraken), (2) veelvoorkomende zaken (high volume) worden afgehandeld als daarvoor de middelen beschikbaar zijn, (3) zaken in de restcategorie worden meestal meteen opgelegd. In die laatste categorie vallen kleine zaken met weinig opsporingsindicatie of zaken die volgens

het overleg eigenlijk als civielrechtelijk zouden moeten worden bestempeld. Volgens respondenten vallen cybercrimezaken veelal in de laatste categorie. Dergelijke plankzaken worden doorgaans dus niet opgepakt. Overlegstructuren of afspraken tussen de politie en het OM zijn niet op (boven)regionaal niveau vastgelegd. Of overleggen plaatsvinden en of afspraken gemaakt zijn, is per Districtsofficier verschillend. Respondenten zeggen dat te weinig eenduidigheid bestaat in de werkwijze hieromtrent.

Te weinig capaciteit
Verschillende respondenten geven aan dat het als een probleem wordt ervaren dat één aangifte cybercrime een grote hoeveelheid werk op kan leveren. Het afhandelen van dergelijke zaken kan in verhouding tot reguliere zaken erg arbeidsintensief zijn en legt daardoor (te) veel beslag op de schaarse politiecapaciteit.

Tijdens de interviews wordt een aantal voorbeelden gegeven over de hoeveelheid extra werk die een cyberzaak met zich mee kan brengen. Bij een phishingzaak, waarvan in een bepaald korps vijf aangiften waren (en een onbekend aantal in andere korspen), bleken veertig zogenaamde geldezels betrokken te zijn. De geldezels woonden verspreid over heel Nederland. Om een opsporingsonderzoek naar deze phisingzaak uit te voeren zouden alle geldezels verhoord moeten worden. ‘Dan moet je dus het hele land door om verdachten aan te houden en te verhoren’, aldus een respondent. Daarvoor is hulp van andere politieregio’s nodig. Als dan was gebleken dat in andere politieregio’s ook aangiften van phising gedaan waren die tot dezelfde zaak behoorden, dan had de zaak nooit gedraaid kunnen worden, omdat daarvoor de capaciteit ontbreekt. Zelfs simpele oplichting via een verkoopsite kan tot heel veel werk leiden. Als er maar één aangifte is in een bepaalde regio dan is het een makkelijke zaak, maar als blijkt dat er nog twintig aangiften met dezelfde verdachte in andere regio’s zijn, dan wordt een dergelijke zaak toch niet op regioniveau opgepakt omdat daarvoor te weinig menskracht beschikbaar is.

Ook geven respondenten voorbeelden op kinderpornografiegebied. Om kinderpornozaken op te sporen kan volgens hen gebruik worden gemaakt van een technische tool die losgelaten wordt in een p2p-netwerk. De tool spoort dan gebruikers op die in het bezit zijn van kinderpornografisch materiaal. Een nacht die tool laten draaien levert zo maar een paar honderd mogelijke zaken op. Die kunnen dan echter niet gedraaid worden omdat daarvoor geen capaciteit is. Ook de inzet van internetrechecheurs (op nationaal niveau) die actief opzoek zijn naar kinderpornografie levert veel zaken op. Het is volgens respondenten echter nog maar de vraag wat de regiokorpsen die deze zaken op hun bordje krijgen er vervolgens mee doen. Er zijn in alle korpsen zedenrechercheurs maar die hebben vaak al een drukke agenda, en zijn dus niet volledig inzetbaar. Ondanks landelijk beleid over de aanpak van kinderpornografie, kunnen korpsen feitelijk zelf bepalen of ze zaken wel of niet oppakken. Dat is deels afhankelijk van de mate waarin daarvoor capaciteit beschikbaar is.

Cybercrimezaken hebben in grotere mate dan klassieke zaken een regio-overstijgend of zelfs internationaal karakter (zie bijvoorbeeld Leukfelkdt e.a., 2010). Over zaken met een internationale component zeggen meerdere respondenten binnen de politie dat die bijna altijd worden opgelegd. ‘Ook al is iemand voor 30.000 euro opgelicht, zodra een buitenlands rekeningnummer in het spel komt, houdt het onderzoek voor een regio op.’ Zaken waarbij internationale rechtshulpverzoeken nodig zijn lopen in de praktijk eigenlijk altijd stuk. Daarin zit teveel recherchewerk, waarvoor te weinig menskracht beschikbaar is en/of wordt vrijgemaakt. Overleg met het OM lost dat probleem niet op. Bovendien is het eenvoudiger om een zaak op te lossen die niet regio-overstijgend of zelfs internationaal is. Als dus sprake is

van een verdachte in een andere regio of in een ander land wordt eerder besloten om een zaak niet op te pakken. In geval van cybercrime heeft de politie nogal eens te maken met zaken waarbij verdachten vanuit het buitenland opereren. De voor de VCN uitgevoerde analyse van politiedossiers laat bijvoorbeeld zien dat in 23,3 procent van de hackenzaken sprake was van een vanuit het buitenland opererende dader. Dat betekent dat een kwart van de hackenzaken om die reden dus al afvalt. Bij e-fraude is dat 14,5 procent (Leukfeldt e.a., 2010).

Naast het feit dat cyberzaken dus relatief arbeidsintensief zijn, geven respondenten aan dat digitaal experts te beperkt inzetbaar zijn om bij te dragen aan de afhandeling van cybercrimezaken. Digitaal experts hebben een ondersteunende rol in opsporingsonderzoeken. Dat betekent dat zij niet zelfstandig onderzoek uitvoeren, maar in het kader van een lopend onderzoek bijvoorbeeld worden ingezet om harde schijven uit te lezen. Het probleem is dat digitaal experts niet alleen worden ingezet bij cyberzaken, maar ook bij klassieke zaken. Bij bijvoorbeeld een moordzaak kan het namelijk relevant zijn om de computer van de verdachte te bekijken of om zijn chatgeschiedenis in kaart te brengen. Een deel van de capaciteit van ondersteunende technische teams gaat dus naar klassieke ernstige delicten: die genieten immers prioriteit. Er is te weinig capaciteit om digitaal experts actief te betrekken bij complexe cyberzaken.[32]

Door het gebrek aan inzetbare capaciteit en kennis komt het voor dat een cyberzaak te omvangrijk (en te complex) is voor een lokaal of regionaal rechercheteam, maar nog steeds te klein om door het THTC van het KLPD te worden afgehandeld. In eerste instantie kan een cyberzaak bijvoorbeeld aan een crimeteam worden toegewezen. Als na enig speurwerk blijkt dat de zaak te complex, regio overschrijdend of internationaal is, dan zal het crimeteam de zaak weer moeten doorspelen naar een geschikter team, zoals de regionale recherche. Daar komt de zaak weer op de stapel te liggen en moet de zaak opnieuw door de prioritering heenkomen. De zaak kan dan alsnog worden opgelegd. Dat kan tevens worden veroorzaakt doordat de doorlooptijd van de zaak inmiddels is verstreken.

Een respondent van het OM geeft aan dat de politie soms cyberzaken naar het OM doorstuurt die eigenlijk van onvoldoende kwaliteit zijn. Door het bij het OM bekende capaciteitsprobleem binnen de politie, worden dergelijke zaken vaak niet teruggestuurd voor aanvullend recherchewerk maar opgelegd. Het zou namelijk te veel schaarse capaciteit van de politie vergen als alle zaken van onvoldoende kwaliteit zouden worden teruggestuurd. Worden zaken wel teruggestuurd, dan komt het bovendien veelvuldig voor dat het OM zo'n zaak nooit weer terugziet, aldus deze respondent. In hoevere deze respondent wijst op een breed voorkomend verschijnsel, hebben we in dit onderzoek niet kunnen vaststellen.

Complexiteit en kennistekort

Alle respondenten vertellen dat over de volle breedte van de politieorganisatie meer kennis van cybercrime nodig is om effectief uitvoering te kunnen geven aan de bestrijding ervan. Het probleem zit hem volgens respondenten met name in de door politiemedewerkers ervaren complexiteit van cyberzaken. Politiemedewerkers hebben daar nog weinig ervaring mee. 'Dan moet je zaken uit gaan zoeken die je nog nooit gedaan hebt', aldus een respondent. Het kennistekort en gebrek aan ervaring met de afhandeling van cyberzaken werpen een drempel op om opsporingsonderzoek te verrichten.

[32] Een uitzondering zien we in een van de onderzochte korpsen, zie de paragraaf over best practices.

Vooral onwetendheid over de (juridische) (on)mogelijkheden om bewijzen te verzamelen bij cybercrimezaken bemoeilijkt opsporingsonderzoek. Respondenten geven aan dat voor veel politiemedewerkers onduidelijk is welke handelingen nodig en/mogelijk zijn om bewijzen te verzamelen. Politiemedewerkers weten bijvoorbeeld niet of en wanneer het nodig is om Bijzondere Opsporings Bevoegdheden (BOB) aan te vragen bij het OM. Als politiemedewerkers daar wel van op de hoogte zijn, dan wordt het aanvragen van dergelijke bevoegdheden als vervelend ervaren. Het 'kost klauwen met tijd en geld' om voor het verzamelen van digitaal bewijs vorderingen aan te vragen. Bovendien stellen respondenten dat het voor de bewijsvoering bij cybercrimezaken vaker dan bij klassieke delicten nodig is om 'een BOB aan te vragen' (vragen een bijzondere opsporingsbevoegdheid te mogen toepassen). Dat werpt een drempel op. Uit eerder onderzoek weten we dat die drempel deels bestaat uit het niet durven benaderen van een ander (in dit geval de OvJ), omdat die bijvoorbeeld een onbekende is of omdat men die persoon niet wil storen. De gesignaleerde drempel is dus, zo suggereert eerder onderzoek, niet (alleen maar) te wijten aan onwelwillendheid, maar heeft ook te maken met psychologische factoren (liever niet een onbekende een vraag stellen; een ander niet willen storen). Een oplossing om dat soort drempels te slechten is om te zorgen dat de betrokken personen bekend zijn met elkaar (zie bijvoorbeeld. Algemene Rekenkamer, 1998; Van Treeck en Stol, 2000; Leukfeldt e.a., 2007).

Vervolgens bestaat onduidelijkheid over de bruikbaarheid van digitale sporen. Het achterhalen van een IP-adres staat bijvoorbeeld niet garant voor succesvolle opsporing of vervolging. Het is immers onduidelijk wie toegang had tot de PC en/of internetverbinding waarmee het delict is gepleegd. Bovendien kunnen daders gebruik maken van wisselende IP adressen of van onbeveiligde netwerken van anderen. Als in dergelijke gevallen het fysieke huisadres van 'de dader' wordt opgevraagd, leidt dat spoor niet per definitie tot de dader, maar bijvoorbeeld tot een onschuldig gezin wiens (onbeveiligde) netwerk is misbruikt door criminelen. Om de bewijsvoering bij cyberzaken rond te krijgen is dus vaak aanvullend opsporingsonderzoek nodig. Volgens respondenten stranden zaken met een digitale component daardoor eerder dan klassieke zaken.

Bijkomend nadeel volgens respondenten is de vluchtigheid van gegevens. Een aantal respondenten geeft aan dat als een zaak na de aangifte te lang is blijven liggen, de kans op het achterhalen van digitale sporen wel eens lager zou kunnen zijn door de 'vluchtigheid' van die digitale gegevens. Of de gegevens daadwerkelijk zo vluchtig zijn, maakt overigens niet uit. Het gaat om de perceptie van de respondenten, indien zij *denken* dat de vluchtigheid van gegevens ervoor zorgt dat ze na een bepaalde tijd niet of moeilijker te achterhalen zijn, dan zorgt dat ervoor dat dergelijke zaken niet worden opgepakt.[33]

We beschreven al dat er te weinig capaciteit bestaat om digitaal experts in te zetten in lopende rechercheonderzoeken naar cybercrime. Daardoor, zo signaleren respondenten, is er een gebrek aan kruisbestuiving tussen tactische en technische rechercheurs. In relatief complexe cyberzaken doen tactisch rechercheurs bijvoorbeeld zelfstandig de verhoren met een verdachte. Door het ontbreken van technische kennis stellen zij echter niet altijd de juiste vragen. Als bij zo'n verhoor een digitaal expert betrokken wordt, kan die belangrijke aanvullende vragen stellen. Digitaal en tactisch rechercheurs werken volgens respondenten te weinig samen en hierdoor kan belangrijke informatie verborgen blijven. Een respondent zegt daarover 'er moet dus een goed contact zijn tussen de digitale jongens en de tactische recherche' – maar digitaal experts zijn daarvoor in te beperkte mate inzetbaar.

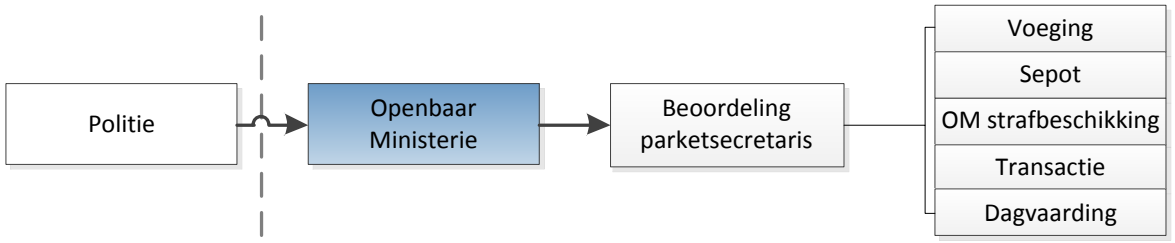
[33] Merton (1968:475) beschrijft dit als het Thomas theorema: 'If men define situations as real, they are real in their consequencces.'

Opvallend is dat enkele respondenten van het OM en de ZM, in tegenstelling tot respondenten van de politie, aangeven dat het kennistekort op het gebied van cybercrime geen knelpunt is. Sterker nog, de geïnterviewden vermoeden dat de politie 'cybercrime in ruime zin' eerder oppakt dan reguliere aangiften, omdat er meer bewijsmateriaal is (e-mails, berichten op profielsites e.d.) waardoor de dader eerder gepakt en bestraft kan worden. Was het bij een bedreiging eerder nog het woord van de aangever tegen het woord van de verdachte, nu is vaak vastgelegd wat er is gezegd. Bij deze zaken is weinig technische expertise nodig: de respondenten vermoeden dan ook niet dat de digitale component in dergelijke zaken een drempel opwerpt voor de politie. Wel zijn de respondenten zich er van bewust dat verzameld bewijsmateriaal, zoals IP adressen, niet altijd leiden tot de dader. Het is immers onduidelijk of een account of IP adres door de verdachte is gebruikt.

Resumé knelpunten in de opsporing
Het gebrek aan prioriteit, capaciteit en kennis over de aanpak van cybercrime leiden er volgens onze respondenten toe dat er eerder opsporingsonderzoek wordt verricht naar klassieke misdrijven, dan naar delicten met een digitale component. Daarbij zijn het gebrek aan prioriteit, capaciteit en kennis sterk met elkaar verweven: doordat cybercrime weinig prioriteit geniet wordt politiecapaciteit naar verhouding in grotere mate besteed aan opsporingsonderzoeken naar klassieke misdrijven. Het gebrek aan ervaring met cyberzaken blijft daardoor in stand. Bij cyberzaken die de politie wel in behandeling neemt, ervaart zij hindernissen in de samenwerking met private partijen: providers en banken werpen (procedurele en financiële) drempels op bij informatieverzoeken van de politie.

6.5 Openbaar Ministerie

Figuur 6.4: het Openbaar Ministerie



Welke OvJ bij welke zaak?
Respondenten binnen het OM merken op dat er onduidelijkheid bestaat over welke OvJ's welke cybercrimezaken moeten oppakken. Dat heeft te maken met onduidelijkheden over de definitie van cybercrime. Tot enkele jaren geleden constateerden onderzoekers dat er nog geen algemeen geaccepteerde definitie van cybercrime was (Van de Hulst en Neve, 2008; PAC, 2008; Leukfeldt e.a. 2010). Er werden verschillende definities met verschillende reikwijdtes gebruikt. De laatste jaren lijkt de definitie waarin twee categorieën van cybercrime onderscheiden worden algemeen geaccepteerd te zijn[34] (KLPD, 2010; NCSC, 2011; Leukfeldt e.a., 2012). De definitie luidt als volgt:

> Cybercrime is een overkoepelend begrip voor alle vormen van criminaliteit waarbij ICT een wezenlijke rol speelt in de realisatie van het delict. Daarbij kunnen twee

[34] De terminologie voor de categorieën verschilt, maar komt op het zelfde neer.

> subcategorieën worden onderscheiden. Voor delicten waarbij ICT zowel instrument als doelwit is, hanteren we de term ‘cybercrime in enge zin’. Voorbeelden zijn hacken en verspreiden van virussen. In de tweede subcategorie, ‘cybercrime in ruime zin’, vallen delicten waarbij ICT van wezenlijk belang is voor de uitvoering, maar waarbij ICT geen doelwit is, bijvoorbeeld fraude of verspreiden van kinderporno via internet.

Deze definitie wordt ook door de respondenten genoemd, al wordt soms gebruik gemaakt van andere terminologie. Er wordt dan bijvoorbeeld gesproken van high-tech crime in plaats van cybercrime in enge zin. Ondanks dat respondenten op de hoogte zijn van deze definitie, is onduidelijk welke zaken de cyber-OvJ wel en niet krijgt en/of oppakt. Omdat daarover geen eenduidige afspraken zijn gemaakt, kan per parket verschillen wat voor type cybercrimezaken een cyber-OvJ behandelt.

De meeste respondenten van het OM zijn van mening dat ‘cybercrime in ruime zin’ niet door cyberofficieren moeten worden afgehandeld. Het betreft in essentie immers klassieke delicten zoals fraude, stalking of kinderpornografie die ook door andere OvJ’s opgepakt kunnen worden. In het geval van internetfraude kan een fraudeofficier de zaak bijvoorbeeld afhandelen. Ook zijn respondenten het erover eens dat cybercrimezaken in enge zin, wel moeten worden behandeld door de cyber-OvJ. Echter, het geregistreerde werkaanbod van cyberzaken in enge zin is laag (Domenie e.a., 2009; Leukfeldt e.a., 2010). De geïnterviewde cyber OvJ’s geven allen dan ook aan het afgelopen jaar weinig tot geen cyberzaken in enge zin te hebben gedraaid. Bij de zaken die wel zijn voorgekomen was volgens respondenten veelal geen sprake van een ‘echte’ high tech crime zaak. Het gaat dan bijvoorbeeld om zaken waarbij een man de account van zijn ex-vrouw of -werkgever heeft gehackt om hem of haar dwars te zitten. Hoewel formeel sprake is van cybercrime in enge zin (hacken wordt gepleegd via ICT tegen ICT), ligt de achterliggende motivatie in de relationele sfeer.

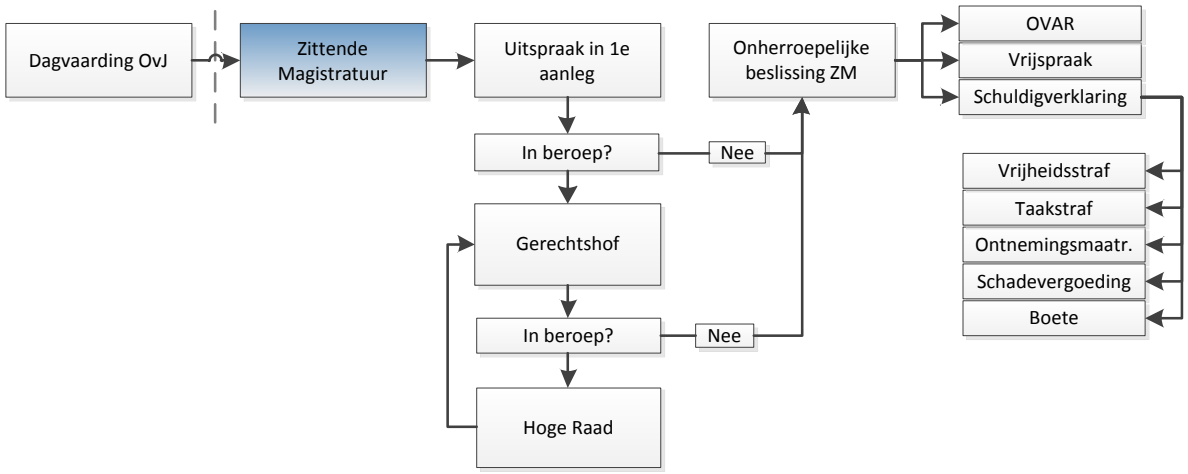
Deze redenering van respondenten is discutabel. Of iets high tech crime (of cybercrime in enge zin) is, wordt volgens de definitie van cybercrime in enge zin namelijk niet bepaald door de achterliggende motivatie van het gepleegde delict. Dat zou namelijk betekenen dat ook geen sprake is van cybercrime in enge zin als bijvoorbeeld een geavanceerd botnet is aangelegd omdat de dader zijn ex-werkgever te grazen wil nemen. De definitie van cybercrime stelt de aard van het delict, niet de achterliggende motivatie centraal. Zodra sprake is van een delict waarbij ICT van wezenlijk belang is voor de uitvoering ervan en het delict gericht is tegen ICT (bijvoorbeeld het platleggen van computers) wordt volgens de definitie gesproken van cybercrime in enge zin.

Volgens respondenten speelt bij het OM het kennistekort minder een rol dan bij de politie. Er zijn binnen het OM cyber-OvJ’s aangesteld die een opleiding hebben gevolgd en cybercrimezaken moeten afhandelen. Toch geldt ook voor de cyber OvJ’s dat de ontwikkelingen op het gebied van cybercrime snel gaan. Alle respondenten binnen het OM brengen naar voren dat de cyber OvJ’s nog weinig (soms zelfs geen) cyberzaken gedraaid hebben. De opgedane kennis kan dus niet in praktijk worden gebracht maar veroudert wel. Ook bestaan binnen het OM, net als binnen de politie, juridische onduidelijkheden door veranderende wetgeving, het gebrek aan jurisprudentie en een gebrek aan kennis over de inzet en de juridische (on)mogelijkheden van bijzondere opsporingsbevoegdheden op internet.

Resumé knelpunten Openbaar Ministerie
Het OM heeft zich anders georganiseerd op cybercrime dan de politie: er zijn speciale cyber-OvJ's, terwijl er geen speciale cyber-rechercheurs in de korpsen zijn. Wat knelt bij het OM is dat deze cyber-OvJ's onvoldoende, of wellicht soms zelfs geen, cyberzaken te behandelen krijgen.

6.6 Zittende Magistratuur

Figuur 6.5: De Zittende Magistratuur



Een rechter moet, aldus respondenten, in beginsel alle zaken kunnen afhandelen. Er zijn uitzonderingen, bijvoorbeeld de kinderrechter die zaken van jeugdigen afhandelt. In Den Haag is er een cyberkamer, waarin zaken met een cybercomponent worden behandeld. Verder zijn er informele 'teams' van rechters die vaker dan anderen de afhandeling van een bepaald type zaken, zoals cybercrime, op zich nemen. Het betreft rechters die affiniteit en/of ervaring hebben met dergelijke zaken. Of deze rechters daadwerkelijk een cyberzaak behandelen, hangt af van het werkrooster: er is niets formeel vastgelegd.

Het is volgens respondenten niet zo dat rechters met de komst van cybercriminaliteit ineens veel meer complexe zaken krijgen. Complexe zaken zijn er altijd al geweest, ook bij traditionele delicten. Maar doordat er nog weinig cybercrimezaken voor de rechter zijn geweest is de behandeling van cybercrimezaken voor rechters minder routine dan de behandeling van reguliere zaken. Daardoor kost het rechters meer tijd om de materie te doorgronden. Er is ook nog weinig jurisprudentie. In die zin zijn dergelijke zaken dus wel ingewikkelder, maar het leidt volgens respondenten niet tot een verschil in afhandeling ten opzichte van andere zaken. De digitale component in cyberzaken wordt niet ervaren als knelpunt. Sterker nog, respondenten geven aan dat verdachten digitaal wellicht meer traceerbare sporen achterlaten, waardoor zaken beter bewijsbaar en dus vervolgbaar zijn.

De rechter toetst of strafbaarheid bewezen kan worden op basis van de informatie die hem wordt voorgelegd. Het is daarbij formeel de taak van de rechter om te beoordelen of het opsporingsonderzoek deugdelijk is verricht (art 359a Sv). Hoewel dat volgens rechters zowel bij reguliere-, als bij cyberzaken lastig kan zijn ervaren zij daarin geen knelpunten. Dat komt, zo geven rechters aan, doordat over opsporingsonderzoek in de praktijk lang niet altijd vragen of twijfels bestaan. Veelal kunnen rechters dus volstaan met de hen aangeleverde informatie

bij het vellen van hun oordeel. Als er wel onduidelijkheden bestaan over het bewijsmateriaal, dan vraagt de rechter daarover om opheldering. Rechters kunnen daarbij bijvoorbeeld getuigen-deskundigen inschakelen.

De ZM dient dus in staat te zijn om een zaak die zich bevindt achter een begrijpelijk uitgewerkt dossier tot op zekere hoogte zelfstandig te beoordelen en wordt geacht in staat te zijn om vragen te stellen over bijvoorbeeld hetgeen niet in het dossier staat vermeld maar mogelijk wel aan de orde was, of over de (techniek van de) gehanteerde opsporingsmethoden. Bij een klassieke zaak heeft een rechter vermoedelijk doorgaans wel een beeld over wat voor bijzonderheden er bij zo'n zaak aan de orde zouden kunnen zijn en welke valkuilen op de loer liggen, en hij kan dan daarover vragen stellen omdat veel kennis van professionals c.q. specialisten inmiddels ook is doorgedrongen tot een breder publiek (Kunnen sporen zijn versleept? Hoe betrouwbaar konden waarnemingen van getuigen zijn? Hoe betrouwbaar is het geheugen van het slachtoffer? Welke culturele aspecten spelen een rol? Et cetera.). Hier is een zekere parallel te zien met wat de socioloog De Swaan (2008) protoprofessionalisering heeft genoemd: het door ingewijde leken overnemen van basisbegrippen die door specialisten worden gebruikt om de werkelijkheid te duiden. Als we wetenschappers op forensisch/criminologisch gebied beschouwen als professionals dan zijn rechters de in die vakgebieden ingewijde leken die kennis van criminologen en forensische wetenschappers overnemen en gebruiken om de werkelijkheid die aan hen wordt voorgelegd te helpen duiden. Of rechters ook op het gebied van cybercrime al tot ingewijde leken zijn geworden en over voldoende kennis beschikken om een oordeel te vellen over de kwaliteit van in cyberzaken verricht opsporingsonderzoek is een vraag voor vervolgonderzoek. Dat rechters naar eigen zeggen geen problemen ervaren met de afhandeling van cybercrimes, betekent namelijk niet automatisch dat zij hun onafhankelijke toetsende taak bij cyberzaken al optimaal kunnen vervullen. Wij hebben dat in ons onderzoek niet kunnen nagaan.

Resumé knelpunten ZM
Dat rechters geen probleem zeggen te ervaren met het beoordelen van cybercrime omdat zij van politie en OM immers begrijpelijk uitgewerkte dossiers krijgen voorgelegd, mogen we in zekere zin opvatten als compliment aan politie en justitie, maar dit impliceert niet automatisch dat rechters hun onafhankelijke, toetsende taak ook wat cybercrime betreft al optimaal (kunnen) vervullen. Vervolgonderzoek kan inzicht bieden in de mate waarin rechters bij de afhandeling van cyberzaken daadwerkelijk beschikken over voldoende kennis om de kwaliteit van het verrichtte opsporingsonderzoek te beoordelen en eventuele lacunes daarin te herkennen.

6.7 Resumé van knelpunten in het proces van slachtofferschap tot veroordeling

Tabel 6.1 geeft een overzicht van de in dit hoofdstuk beschreven knelpunten in het proces van slachtofferschap tot veroordeling. Voor een nadere inhoudelijke behandeling van de knelpunten zij verwezen naar de voorgaande paragrafen.

Tabel 6.1: knelpunten in het proces van slachtofferschap tot veroordeling

Knelpunten per procesdeel	Procesdeel	Zie §
Slachtofferschap wordt niet waargenomen en/of gemeld bij de politie	Slachtofferschap aangifte	6.2
Ongewenste uitstroom van cyberzaken bij de politie door:	Intake en casescreening	6.3

- het gebrek aan kennis tijdens het opnemen van aangiften cybercrime; - het gebrek aan kwaliteit van opgenomen aangiften; - het gebrek aan kennis en ervaring die vereist is om aangiften cybercrime te verrijken met opsporingsinformatie; - hindernissen in de samenwerking tussen politie en private instellingen (providers en banken); - het gebrek aan zicht van het OM op de uitstroom tijdens intake en case screening.		
Knelpunten in de opsporing: - gebrek aan prioriteit voor de opsporing van cybercrime; - gebrek aan gekwalificeerde (kennis) politiecapaciteit voor de opsporing van cybercrime.	Opsporing	6.4
Gespecialiseerde cyber-OvJ's krijgen weinig of geen cyberzaken.	Openbaar Ministerie	6.5
Rechters ervaren geen problemen met het beoordelen van cybercrime omdat politie en OM begrijpelijk uitgewerkte dossiers aanleveren. Onduidelijk is gebleven in hoeverre rechters hun onafhankelijke, toetsende taak ook wat cybercrime betreft al optimaal (kunnen) vervullen.	Zittende Magistratuur	6.6
Discontinuïteit in de aanpak van cybercrime binnen de strafrechtketen.	Ketenbreed	6.3 – 6.6

7. Conclusies

In dit hoofdstuk wordt antwoord gegeven op de onderzoeksvragen. Allereerst wordt ingegaan op de vraag waar aangiften cybercrime in de strafrechtketen worden afgedaan. Vervolgens wordt de vraag beantwoord welke overwegingen in de strafrechtketen een rol spelen bij het nemen van beslissingen over de afhandeling van cybercrime. De conclusieparagraaf sluit af met een beschrijving van de uit het onderzoek voortkomende knelpuntenten bij de afhandeling van cybercrime.

Onderzoeksvraag 1: Waar in de strafrechtketen worden aangiften cybercrime afgedaan?

Er bestaat een gebrek aan inzicht in de doorstroom van aangiften cybercrime in de strafrechtketen, omdat de administraties van de ketenpartners onvolkomen zijn en onvoldoende op elkaar aansluiten

Ten eerste is onderzocht waar in de strafrechtketen de door de politie in een aangifte opgenomen cybercrimes worden afgedaan. Het is niet mogelijk gebleken om een sluitend antwoord te geven op deze vraag. De voornaamste oorzaak daarvoor is dat de administratieve processen van de politie en het OM onvolkomen zijn en onvoldoende op elkaar aansluiten, waardoor het zicht op aangiften verdwijnt.

Volgens de politie zijn 195 van de 647 door ons onderzochte aangiften doorgestuurd naar het OM (30,1%). In OM Data, een systeem waarin de afhandeling van alle bij het OM binnengekomen zaken wordt geregistreerd, is vervolgens gezocht naar informatie over de strafrechtelijke afhandeling van die zaken. Er is gezocht op zowel PV-nummers (die door de politie worden gebruikt om zaken te registreren) als parketnummers (registratienummers van het OM). Ondanks dat van alle zaken een PV-nummer en van 67,2 procent (n=131) van de naar het OM doorgestuurde zaken ook een parketnummer bekend was, vonden we slechts van 81 van de 195 doorgestuurde zaken informatie over de strafrechtelijke afhandeling (41,5%). Over meer dan de helft van de door de politie naar het OM doorgestuurde zaken vonden we dus geen informatie over de afhandeling.

Ook binnen de politie kan de zaakstroom van aangiften niet sluitend worden verantwoord. Van 73,7 procent van de cybercrime-aangiften weet de politie wat daarmee is gebeurd. Van ruim een kwart weet de politie dat dus niet. Dat wordt deels veroorzaakt doordat aangiften die worden doorgestuurd naar een ander korps daarna veelal niet meer traceerbaar zijn.

Al met al ontbreekt van een groot aantal zaken de informatie die nodig is om betrouwbare uitspraken te doen over de strafrechtelijke afhandeling van cybercrime. We kunnen dus concluderen dat er een gebrek aan inzicht bestaat in de zaakstroom van cybercrime in de strafrechtketen omdat de administratie van politie en OM onvolkomen zijn en onvoldoende op elkaar aansluiten.

Dit beeld is overigens niet nieuw. Ook in eerdere onderzoeken wordt geconcludeerd dat het niet mogelijk is om de complete zaakstroom van politie tot ZM in kaart te brengen omdat zaken zoek raken en registratiesystemen niet op elkaar aansluiten (Kalidien & Heer-de Lange, 2011; Algemene Rekenkamer, 2012).

De in- en doorstroom van cybercrimes verschilt per delictsoort

De wijze waarop aangiften cybercrime door de politie worden afgehandeld, verschilt per delictsoort. Of cybercrimes meteen worden opgelegd of in behandeling worden genomen, lijkt af te hangen van de mate van complexiteit en prioriteit. Hacken en e-fraude-zaken worden relatief vaak afgedaan door de politie. Hacken wordt als complex ervaren en bij e-fraude zaken (veelal 'marktplaatsoplichting') is sprake van een gebrek aan prioriteit. Volgens de geïnterviewden zijn slachtoffers van marktplaatsoplichting daar zelf vaak debet aan: zij spreken van 'eigen schuld, dikke bult' zaken. Aangiften van kinderporno daarentegen worden veel vaker dan andere cybercrimes doorgestuurd naar het OM. De maatschappelijke verontwaardiging en de prioriteit die bij politie en OM aan de bestrijding van deze cybercrime wordt gegeven bieden daarvoor een plausibele verklaring.

Onderzoeksvraag 2 t/m 4: Welke overwegingen spelen bij politie, OM en ZM een rol bij het nemen van beslissingen over de opsporing en vervolging?

Doorgaans is het een slachtoffer dat een delict bij de politie kenbaar maakt. Als een slachtoffer aangifte wil doen, beoordeelt een intakemedewerker van de politie vervolgens of al dan niet een aangifte moet worden opgenomen. In de praktijk worden niet alle meldingen of aangiften geregistreerd: de politiemedewerker kan bijvoorbeeld van mening zijn dat er geen sprake is van een strafbaar feit. Het is mogelijk dat zaken daardoor ten onrechte buiten het geregistreerde werkaanbod van de politie vallen. Deze problematiek is niet uitsluitend verbonden aan cybercrime. Wittebrood (2006) beschrijft dat de politie van ongeveer 20 procent van de gemelde delicten geen aangifte opmaakt. Uit recent slachtofferonderzoek blijkt echter dat het aantal bij de politie gemelde cybercrimes waarmee niets gedaan wordt hoger is.

Wanneer een aangifte is opgenomen, beoordeelt de case screener of een zaak in behandeling wordt genomen. Hoewel er richtlijnen zijn voor het screenen van zaken, maken case screeners daarvan in de praktijk naar zij zeggen niet bewust gebruik. Naar eigen inzicht beoordelen zij of een aangifte voldoende opsporingsindicatie bevat om over te gaan tot opsporing. Ook beleidsindicatoren, de juridische haalbaarheid en de mate waarin het slachtoffer zelf verantwoordelijk is voor hetgeen hem of haar is overkomen worden overwogen. Case screeners besluiten over het algemeen zonder tussenkomst van anderen om sommige aangiften niet verder in behandeling te nemen. Sporadisch wordt overlegd met een operationeel teamleider van de politie of met het OM.

Als tijdens de casescreening wordt besloten om over te gaan tot verdere opsporingsactiviteiten, wordt de aangifte doorgestuurd naar een opsporingsteam. Opsporingsteams pakken niet alle aan hen doorgestuurde zaken op: ook zij maken keuzes om bepaalde zaken wel of niet op te pakken. De prioriteit van een zaak, de beschikbare capaciteit om een zaak op te pakken en de werkbelasting worden daarbij overwogen. Ook in deze fase van het proces stromen cybercrimes uit.

Door de politie afgehandelde zaken worden doorgestuurd naar het OM. De zaken die bij het OM binnenkomen, worden door de parketsecretaris getoetst op juridische haalbaarheid. De secretaris voert als het ware een kwaliteitscontrole uit. Bij onvoldoende kwaliteit van het dossier, kan worden besloten om de zaak voor aanvullingen terug te sturen naar de politie. Als de zaak niet wordt teruggestuurd naar de politie, dan worden de verschillende afdoeningswijzen voor strafzaken overwogen. Daarvoor maakt het OM gebruik van

verschillende beleidsregels: daarin zijn aanwijzingen en richtlijnen voor strafvordering opgenomen. Het OM kan een zaak allereerst seponeren (aanwijzing gebruik sepotgronden). Ook kan het OM zonder tussenkomst van een rechter zelfstandig een strafbeschikking opleggen (Aanwijzing OM-afdoening) of, als een zaak niet voldoet aan de in de Aanwijzing OM-afdoening uitgewerkte criteria voor het uitvaardigen van een strafbeschikking, een transactie aanbieden. Als een zaak dagvaarding vereist, wordt de zaak door de Officier van Justitie voor de rechter gebracht. De strafeis wordt bepaald op basis van daarvoor opgestelde delictspecifieke richtlijnen voor strafvordering (Aanwijzing Kader voor Strafvordering). De bestaande richtlijnen bieden, met uitzondering van skimmen, (nog) geen houvast om de strafmaat bij cybercrimes in enge zin vast te stellen.

Als een zaak voor de strafrechter wordt gebracht, toetst de rechter of de verdachte schuldig is aan het ten laste gelegde misdrijf. Rechters moeten alle strafzaken kunnen behandelen, dus ook cybercrimes. In een Landelijk Overleg van Voorzitters van Strafsectoren zijn richtlijnen opgesteld waarop de rechter zich kan oriënteren bij het bepalen van de op te leggen straf. Doel van die richtlijnen is om te komen tot een consistent landelijk straftoemetingsbeleid. Voor delicten die relatief veel voorkomen zijn dergelijke richtlijnen opgesteld, maar voor cybercrime bestaan deze richtlijnen nog niet (met uitzondering van skimmen). Wel gelden algemene overwegingen, zoals de persoonlijke omstandigheden van de verdachte. De drie rechters die we spraken ervaren cybercrimes niet per definitie als lastiger dan reguliere zaken. Hoewel het een taak van de rechter is om een oordeel te vellen over (de kwaliteit van) het verrichte opsporingsonderzoek en dat in de praktijk lastig kan zijn, laat de dagelijkse praktijk zien dat daarover niet altijd vragen of twijfels bestaan. Vaak kunnen rechters hun oordeel naar eigen zeggen dan ook vellen op basis van het begrijpelijk uitgeschreven bewijsmateriaal dat door de politie en het OM is aangeleverd. Wel is opgemerkt dat de digitale component bij cybercrime er toe kan leiden dat de gevolgen voor het slachtoffer anders zijn dan bij reguliere strafzaken: een smadelijke tekst of foto kan bijvoorbeeld voor een onbeperkt grote groep mensen toegankelijk gemaakt worden via internet. Dergelijke overwegingen spelen een rol bij het bepalen van de uiteindelijke straf.

Onderzoeksvraag 5: Wat zijn knelpunten binnen het proces van afhandeling?[35]

Een aanzienlijk deel van de cybercrimes bereikt nooit de strafrechtketen

Slachtofferschap van cybercrime is lastig vast te stellen omdat mensen niet altijd weten dat zij slachtoffer zijn (bijvoorbeeld dat een computer onderdeel is van een botnet of dat de computer spyware bevat). Daarnaast zijn er slachtofferloze delicten. Voorbeelden hiervan in de offline wereld zijn heling, rijden onder invloed, drugs- en wapenhandel. Bij slachtofferloze cybercrimes valt te denken aan illegale handel van medicijnen en heling via internet. Het is onbekend hoeveel van deze delicten niet bij politie en justitie terechtkomen.

Van wel waargenomen slachtofferschap moet een melding of aangifte volgen voordat het delict de strafrechtketen instroomt. Bij klassieke misdrijven verschilt het percentage delicten waarvan aangifte wordt gedaan per delictsoort en is gemiddeld over alle delicten tussen de 25 en 30 procent. Het aangiftepercentage bij cybercrime is lager. Burgers en bedrijven betwijfelen of de politie effectief uitvoering kan geven aan de bestrijding van cybercrime en/of vinden dat andere partijen verantwoordelijk zijn voor hun veiligheid op internet en doen daarom geen aangifte.

[35] In de onderzoeksvraag staat ook dat we inventariseren welke best practices de respondenten kennen op dit gebied. Een overzicht van alle door respondenten aangedragen best practices is opgenomen in bijlage A.

Ten slotte zorgt ontoereikende kennis van intakemedewerkers op het gebied van cybercrime er voor dat meldingen/aangiften soms ten onrechte niet worden geregistreerd/opgenomen. Burgers of bedrijven die aangifte willen doen, worden dan weggestuurd door intakemedewerkers omdat zij de melding of aangifte niet zien als een politiezaak.

Kortom, het niet altijd zichtbare slachtofferschap, het lage aangiftepercentage, en de ontoereikende kennis van intakemedewerkers zorgen er voor dat een aanzienlijk deel van de delicten nooit in de strafrechtketen terecht komt.

Het gebrek aan kennis van intakemedewerkers leidt tot het niet in behandeling nemen van cyberzaken

Als er wel een aangifte wordt opgenomen, leidt het kennistekort binnen de politie tot problemen: de kwaliteit van opgenomen aangiften is in sommige gevallen te laag omdat belangrijke (opsporings)informatie ontbreekt. Dat kan worden veroorzaakt doordat intakers niet de juiste vragen hebben gesteld en/of niet weten welk bewijsmateriaal relevant is. Zaken waarvan de informatie in een aangifte ontoereikend is, worden al in een vroeg stadium opgelegd door casescreeners en dus niet doorgestuurd naar opsporingsteams.

De politie ervaart hindernissen in de samenwerking met providers en banken

De aangiften die wel worden doorgestuurd naar opsporingsteams, worden eerst verrijkt met opsporingsinformatie door daarvoor speciaal ingerichte teams of door case screeners. Respondenten zeggen dat het bij cybercrimes soms lastiger is dan bij klassieke zaken om aangiften te verrijken. Door gebrek aan kennis en ervaring is bijvoorbeeld het achterhalen van NAW-gegevens op basis van IP-adressen voor veel politiemedewerkers lastig. Verder is de politie bij cyberzaken voor het verzamelen van bewijsmateriaal vaak afhankelijk van derden: voor het opvragen van gegevens over een rekeningnummer bij een bank moet volgens respondenten (soms) betaald worden en om gegevens bij IP-adressen te krijgen moeten officiële verzoeken bij providers worden ingediend. Dergelijke arbeidsintensieve klussen werpen volgens hen een drempel op om cybercrimes aan te pakken.

Het OM heeft volgens respondenten geen zicht op de uitstroom van zaken in de fase van intake en casescreening

Volgens respondenten heeft het OM geen zicht op welke zaken uitstromen in de fase van intake en casescreening. Aangezien opsporing plaats vindt onder het gezag van het OM en de uitstroom van cyberzaken in deze fase blijkens ons onderzoek al aanzienlijk is, kan dat als knelpunt worden aangemerkt.

Binnen opsporingsteams is sprake van een gebrek aan prioriteit, capaciteit en kennis om effectief uitvoering te kunnen geven aan de bestrijding van cybercrime

De lokaal-geografisch georganiseerde strafrechtketen inzetten tegen internationaal opererende cybercriminelen is een onvoldoende strategie

Binnen opsporingsteams leidt het gebrek aan prioriteit, capaciteit en kennis er toe dat cybercrimes minder snel worden opgepakt dan klassieke delicten. Landelijke ambities op het gebied van cybercrime vinden we niet altijd terug ín de korpsen. De in beperkte mate beschikbare capaciteit wordt ingezet op andere onderzoeken. Daarbij speelt een rol dat het afhandelen van cybercrimes in verhouding tot reguliere zaken arbeidsintensiever is. Er moet volgens respondenten relatief veel opsporingswerk verricht worden om een dader aan te kunnen houden. Als bekend is waar een klassieke winkeldief woont, wordt hij thuis opgepakt. Als bekend is via welk IP adres internetfraude is gepleegd kan het daaraan toebehorende adres worden achterhaald, maar daarmee is de dader nog niet bekend. Ook is cybercrime veelal regio-overstijgend of heeft het zelfs een internationaal karakter, waardoor aanvullend opsporingsonderzoek in samenwerking met andere korpsen of landen vereist is. Dat kost (te) veel tijd terwijl er (te) weinig menskracht beschikbaar is. Cybercrimes zijn dan soms te groot voor lokale of regionale rechercheteams, maar te klein voor het op nationaal niveau opererende THTC met als gevolg dat de zaak na verloop van tijd wordt opgelegd. Bovendien signaleren respondenten een gebrek aan kennis in reguliere rechercheteams om cybercrimes effectief aan te pakken. Opsporingsteams bestaan uit tactisch rechercheurs die veelal beperkt kennis hebben van cybercrime en/of de digitale wereld. Er is, aldus respondenten, te weinig kruisbestuiving tussen tactische en technische rechercheurs en de digitaal experts zijn te weinig (in hun ondersteunende rol op oproepbasis) inzetbaar.

Uit eerder onderzoek naar de strafrechtelijke afhandeling van aangiften van gewelds- en vermogensmisdrijven blijkt dat een deel van de vroegtijdige uitstroom ongewenst is (Algemene Rekenkamer, 2012). Case screeners besluiten (noodgedwongen) om zaken in een vroegtijdig stadium op te leggen, terwijl volgens het vigerende politiebeleid sprake is van zaken waarnaar opsporingsonderzoek zou moeten worden verricht. De exacte omvang van de ongewenste uitstroom van cybercrimes is onbekend: dat hebben we niet specifiek onderzocht, en als we het wel hadden onderzocht dan – zo volgt uit ons onderzoek – hadden we de omvang bij gebrek aan een goede administratie omtrent de zaakstroom niet kunnen vaststellen. We horen in ons onderzoek echter wel dezelfde geluiden als de onderzoekers van de Algemene Rekenkamer: door gebrek aan prioriteit, capaciteit en kennis worden cybercrimes minder snel opgepakt, blijven dergelijke zaken langer op de plank liggen en hebben cybercrimes uiteindelijk een verhoogde kans om (ongewenst) uit te stromen.

Over het ‘gebrek aan prioriteit’ nog het volgende. Bij de lezer kan de indruk ontstaan dat hier impliciet sprake is van verwijtbaarheid, dat het met de bestrijding van cybercrime beter zou zijn gesteld als politie en justitie daaraan maar meer prioriteit zouden geven, het probleem maar serieuzer zouden nemen. Zonder te willen zeggen dat de genoemde instanties het niet beter zouden kunnen doen (het gebrek aan kennis omtrent cybercrime is een voorbeeld van een serieus deficiet in deze tijd, en een lokaal-geografisch georganiseerde strafrechtketen inzetten tegen internationaal opererende cybercriminelen is een onvoldoende strategie) willen we er op wijzen dat respondenten terecht naar voren brengen dat ‘zaken met bloed’ en andere emotioneel beladen zaken, zoals beroven van bejaarden, nu eenmaal voorgaan. Dat moeten

we niet zien als een uitvinding van politie en justitie maar eerder als een sociaal feit dat voor politie en justitie maatschappelijk gesproken geen ruimte laat voor een andere keuze.[36] Daar staat tegenover onze bevinding dat politie en justitie niet altijd in staat zijn om patronen in cybercrime bloot te leggen en te laten zien dat er zaken zijn waarbij een dader op vele plaatsen slachtoffers maakt. Dat roept de vraag op of een lage prioriteit wel altijd terecht is.

De gespecialiseerde cyber-OvJ's krijgen weinig of geen cyberzaken

Het werkaanbod cybercrime is volgens het OM klein. Het OM is afhankelijk van door de politie aangedragen zaken. We concludeerden al dat het gros van de cybercrimes door de politie wordt afgedaan. Een deel van de door de politie afgedane cybercrimes lijkt, gezien voornoemde knelpunten, ongewenste uitstroom. Het werkaanbod cybercrime voor het OM zal dus stijgen naarmate de politie meer opsporingsonderzoeken op het gebied van cybercrime verricht en zaken voor vervolging doorstuurt naar het OM. Vervolgens is het van belang dat ook het OM prioriteit geeft aan de bestrijding van cybercrime. Volgens respondenten in een van de korpsen is dat niet het geval. Zij stellen dat het daardoor zonde is als de politie veel inspanning levert om een cyberzaak op te lossen, als het OM daar vervolgens niets mee doet.

Dat het werkaanbod cybercrime volgens het OM klein is, wordt daarnaast veroorzaakt doordat OM medewerkers cybercrimes in ruime zin beoordelen als klassieke delicten (zij het gepleegd met moderne middelen). Het merendeel van de OM-medewerkers die we spraken is van mening dat cybercrimes in ruime zin niet door cyber officieren moeten worden afgehandeld, omdat het in essentie klassieke delicten betreft zoals fraude, stalking of kinderpornografie die ook door andere OvJ's afgehandeld kunnen worden. Cybercriminaliteit in enge zin komt echter in de registratiesystemen minder voor dan cybercriminaliteit in ruime zin. Gevolg is dat cyberofficieren weinig tot geen zaken draaien, waardoor (in opleidingen opgedane) kennis niet in de praktijk wordt gebracht en dus verouderd, terwijl ontwikkelingen op het gebied van cybercrime snel gaan.

Er is vanwege verschil in visie op hoe cybercrime het beste kan worden aangepakt een discontinuïteit in de organisatie van de strafrechtketen: de politie heeft geen speciale cybercrime-rechercheurs, het OM heeft wel speciale cybercrime-OvJ's en de ZM heeft weer geen speciale cybercrime-rechters

Politie en de rechtelijke macht hebben geen specialisten aangewezen voor de behandeling van cybercrime, ook niet voor cybercrime in enge zin. Wanneer we nu de strafrechtketen als geheel beschouwen is hier dus op keten-niveau sprake van een discontinuïteit in de organisatie van de zaakstroom cybercrime: de politie kent geen cybercrimespecialisten, noch bij intake noch bij de recherche, bij het OM zijn speciale cybercrime-OvJ's voor cybercrime in enge zin en bij de ZM weer geen cybercrime-specialisten. Dit wijst op verschillende visies op hoe de strafrechtketen moet omgaan met criminaliteit in de huidige gedigitaliseerde samenleving: zet de strafrechtketen daarvoor specialisten in of dient ieder in de strafrechtketen over het vermogen te bezitten om deze nieuwe vormen van criminaliteit te behandelen. Dit onderzoek is er niet op gericht om vast te stellen welke van deze twee zienswijzen – of welke tussenvorm – de beste is. Wel kunnen we op basis van dit onderzoek vaststellen dat er binnen verschillende schakels van de strafrechtketen (politie-OM-ZM) kennelijk verschillend hierover wordt gedacht. Of dat op zichzelf tot problemen leidt, en of

[36] Zie ook Van Ham e.a. (2011) die over de online illegale handel van cultuurgoederen constateren dat dergelijke criminaliteit het qua maatschappelijke prioriteit aflegt tegen zaken als moord, mishandeling en roof.

we dus van een knelpunt moeten spreken, volgt niet uit ons onderzoek. We hebben immers vooral moeten constateren dat er nauwelijks of geen sprake is van een stroom zaken die loopt via de route politie - cyber-OvJ - rechter. En waar geen zaakstroom is, worden geen knelpunten in de zaakstroom zichtbaar (behalve dan de OM-interne constatering dat de cyber-OvJ weinig of geen zaken te behandelen krijgen).

We nemen aan dat het voor het functioneren van de strafrechtketen als geheel niet goed is als verschillende delen van de keten zich organiseren vanuit verschillende visies op hoe cybercrime moet worden aangepakt. Met dat in gedachte kunnen we hier spreken van een knelpunt.

Het is de vraag of rechters in staat zijn om te beoordelen of opsporingsonderzoeken bij cyberzaken deugdelijk zijn verricht

Ook voor rechters is het werkaanbod cybercrime laag. Rechters merken dan ook op dat cyberzaken door het geringe werkaanbod minder routine zijn dan klassieke zaken. Daardoor kost het ze meer tijd om de materie te doorgronden. Ook is er nog maar weinig jurisprudentie, waardoor het bepalen van een straf niet op basis van algemeen geldende richtlijnen gedaan kan worden. Het gebrek aan ervaring en jurisprudentie leiden er echter niet toe dat zaken met een digitale component anders worden afgehandeld dan klassieke delicten, aldus de rechters die wij spraken.

Rechters zijn van mening dat zij in staat moeten zijn alle zaken af te handelen, dus ook cybercrimes. Dat is volgens hen ook mogelijk, omdat zij afhankelijk zijn van de door de politie, het OM en de verdediging aangedragen en begrijpelijk uitgewerkte informatie. Hoewel het formeel weliswaar de taak is van de rechter om te beoordelen of het opsporingsonderzoek deugdelijk is verricht (art 359a Sv) en dat bij zowel reguliere zaken als bij cyberzaken best lastig kan zijn, bestaan daarover veelal geen vragen of twijfels. Als het aangeleverde bewijsmateriaal wel vragen oproept dan vraagt de rechter daarover – al dan niet met behulp van getuigen-deskundigen – om opheldering. Het behandelen van cyberzaken wordt door de rechters die wij spraken in de praktijk dan ook niet als lastiger ervaren dan het behandelen van reguliere zaken.

Dat rechters naar eigen zeggen geen problemen ervaren met de afhandeling van cybercrimes impliceert niet automatisch dat zij bij cyberzaken even goed in staat zijn om te beoordelen of opsporingsonderzoeken deugdelijk zijn verricht als bij reguliere zaken. Zij hebben daarmee immers minder ervaring. Bij reguliere zaken hebben rechters vermoedelijk inzicht in eventuele lacunes in het verrichtte opsporingsonderzoek en zijn zij goed in staat om vragen te stellen over al dan niet gehanteerde opsporingsmethoden. Dat rechters bij cyberzaken doorgaans een oordeel vellen op basis van het door de politie, het OM en de verdediging aangeleverde informatie kan betekenen dat daarover, zoals rechters ook aangeven, in de praktijk nauwelijks vragen of twijfels bestaan. Het kan echter ook zijn dat rechters over onvoldoende kennis beschikken om de kwaliteit van bij cyberzaken verrichte opsporingsonderzoeken op waarde te schatten. Of de kennis van rechters in de praktijk toereikend is om verichtte opsporingsonderzoeken in cyberzaken te beoordelen is een vraag voor vervolgonderzoek.

Literatuur

Algemene Rekenkamer (1998). *Uitwisseling van recherche-informatie tussen CRI en politieregio's*. Den Haag: SDU Uitgevers.

Algemene Rekenkamer (2012). *Prestaties in de strafrechtketen*. Den Haag: Sdu Uitgevers.

America Online & National Cyber Security Alliance (2005). *AOL/NCSA Online Safety Study.* www.staysafeonline.info/pdf/safety_study_2005.pdf. Laatst geraadpleegd 19 mei 2008.

Brouwers, M. en A.Th.J. Eggen (2011). Vervolging, in: Kalidien, S.N. & N.E. de Heer-de Lange (red) *Criminaliteit en rechtshandhaving 2010*. Ontwikkelingen en samenhangen. Den Haag: WODC.

Brug, G. (2009). *Internetoplichting via veiling- en advertentiesites (thesis).* Groningen: Rijksuniversiteit Groningen

Bunt, H.G. van de, en J. Rademaker (1992). *Recherchewerk in de praktijk, een case-study naar recherche en informatievoorziening.* Lochem: Van den Brink.

CBS (2011). *Integrale veiligheidsmonitor 2010. Landelijke Rapportage.* Den Haag/Heerlen: CBS.

Dijk, J.K.G. (2007). *Aangiftebereidheid van computercriminaliteit bij bedrijven.* Scriptie Technische Universiteit Eindhoven.

Domenie, M.M.L., E.R. Leukfeldt, M.H. Toutenhoofd-Visser en W.Ph. Stol (2009). *Werkaanbod cybercrime bij de politie. Een verkennend onderzoek naar de omvang van het geregistreerde werkaanbod cybercrime*. Leeuwarden: NHL Hogeschool.

Domenie, M.M.L., E.R. Leukfeldt, J. van Wilsem, J. Jansen en W.Ph. Stol (2012). *Slachtofferschap van delicten met een digitale component onder burgers. Hacken, malware, persoonlijke en financiële delicten in kaart gebracht.* De Bilt / Leeuwarden: PAC / NHL Hogeschool.

Eggen, A.Th.J. en R.J. Kessels (2011). Criminaliteit en opsporing, in: Kalidien, S.N. & N.E. de Heer-de Lange (red) *Criminaliteit en rechtshandhaving 2010. Ontwikkelingen en samenhangen.* Den Haag: WODC.

Elzinga, P.G. (2011). *Formalizing the concepts of crimes and criminals*. Proefschrift. Amsterdam: Universiteit van Amsterdam, Faculteit Economie en Bedrijfskunde.

Goudriaan, H., K. Wittebrood en P. Nieuwbeerta (2004). Buurtkenmerken en aangiftegedrag van slachtoffers van criminaliteit: de effecten van sociaal-economische achterstand, informele sociale controle en vertrouwen in de effectiviteit van de politie, In: *Mens en Maatschappij, 79* (3), 287 – 314.

Van Ham, T., E.R. Leukfeldt, B. Bremmers, W.Ph. Stol en A.Ph. van Wijk (2011). *De kunst van het internet. Een onderzoek naar de online illegale handel in cultuurgroederen.* Den Haag: Boom/Lemma Uitgevers.

Hulst, R.C. van der, en R. Neve (2008). *High-tech crime, soorten criminaliteit en hun daders.* Den Haag: BJU.

Huys, H.W.J.M. en P.R. Smit (2011). Criminaliteit en slachtofferschap, in: Kalidien, S.N. & N.E. de Heer-de Lange (red) *Criminaliteit en rechtshandhaving 2010. Ontwikkelingen en samenhangen.* Den Haag: WODC.

In 't Velt, C.J.E. (1996). Het oplossen van diefstaldelicten. *Tijdschrift voor de Politie*, *58* (3), 6-10.

In 't Velt, C.J.E. (1999). *Politie en omgevingsanalyse. De rol van computerbestanden bij het oplossen van diefstallen.* Den Haag: Elsevier.

Inspectie Openbare Orde en Veiligheid (IOOV) (2009). *Evenwichtige Opsporing? Een onderzoek naar zicht op zaken.* Den Haag: IOOV.
Kalidien, S.N. & N.E. de Heer-de Lange (2011) *Criminaliteit en rechtshandhaving 2010. Ontwikkelingen en samenhangen.* Den Haag: WODC.
KLPD (2007). *Cybercrime - Focus op High Tech Crime: Deelrapport Criminaliteitsbeeld 2007*. Rotterdam: Thieme MediaCenter.
KLPD (2010). *High Tech Crime, criminaliteitsbeeldanalyse 2009.* Driebergen: KLPD.
Kruijer, F. (2012). Zaken in Beeld, In: *Blauw*, 1 (2012) 24-25.
Leertouwer, E.C. en S.N. Kalidien (2011). De strafrechtketen in samenhang, in: Kalidien, S.N. & N.E. de Heer-de Lange (red) *Criminaliteit en rechtshandhaving 2010. Ontwikkelingen en samenhangen.* Den Haag: WODC.
Leij, J.B.J. van der (2011). Het Nederlandse strafrechtssysteem, In: Kalidien, S.N. & N.E. de Heer-de Lange (red) *Criminaliteit en rechtshandhaving 2010. Ontwikkelingen en samenhangen.* Den Haag: WODC.
Leukfeldt, E.R., K.W.C van der Straten, M.P. Kruis en W.Ph. Stol (2007). *Ter plaatse. Allegdaagse samenwerking tussen de primaire hulpdiensten.* Den Haag: BJU.
Leukfeldt, E.R., A. Kentgens, B. Frans, M. Toutenhoofd, W.Ph. Stol en E. Stamhuis (2012). *Alledaags politiewerk in een gedigitaliseerde wereld. Handreiking voor delicten met een digitale component*. Den Haag: Boom Lemma Uitgevers.
Leukfeldt, E.R., M.M.L. Domenie en W.Ph. Stol (2010). *Verkenning Cybercrime in Nederland 2009.* Den Haag: Boom Juridische Uitgevers.
Merton, R.K. (1968). *Social Theory and Social Structure*. New York: The Free Press.
Ministerie van Justitie (2010). *Handreiking Politie Identiteitsfraude*. Den Haag: Ministerie van Justitie
NCSC (2011). *Van herkenning tot aangifte. Handleiding cybercrime*. Den Haag: Govcert.nl.
PAC (2008). *Definities van Cybercrime. Een onderzoek naar- en toetsing van diverse bestaande definities van Cybercrime, om te komen tot één werkbare, herkenbare en gedragen definitie voor intern en extern gebruik door het PAC.* De Bilt: interne notitie.
PAC (2009). *Bestrijding van criminaliteit in de gedigitaliseerde maatschappij. Actualisatie van het RHC beleid.* De Bilt: PAC
Poot, C.J. de, R.J. Bokhorst, P.J. van Koppen en E.R. Muller (2004). *Rechercheportret. Over dilemma's in de opsporing.* Alphen aan den Rijn: Kluwer.
Poot,C.J. de, E.R. Muller en P.J. van Koppen (2004). *Rechercheportret. Over dilemma's in de opsporing*. Deventer: Kluwer.
Politie (2007). *Bouwen aan vertrouwen: Herijking van de Visie op Dienstverlening door de politie.* Interne notitie
Politie (2008). *Visie op Intake: Bouwen aan vertrouwen*. Interne notitie
Rademaker, J. (1996). *De digitale strafrechtpleging.* Zwolle: W.E.J. Tjeenk Willink.
Regeerakkoord (2010). *Vrijheid en verantwoordelijkheid: Regeerakkoord VVD-CDA.*
Stafbureau LOVS (2012).*Oriëntatiepunten voor straftoemeting en LOVS-afspraken*. De rechtspraak
Stol, W.Ph. (1996). *Politie-optreden en informatietechnologie.* Lelystad: Koninklijke Vermande.
Stol, W.Ph., Kaspersen, H.W.K., Kerstens, J., Leukfeldt, E.R. & Lodder, A.R. (2008). *Filteren van kinderporno op internet. Een verkenning van technieken en reguleringen in binnen- en buitenland.* Den Haag: Boom Juridische uitgevers.
Stol, W.Ph. (2004). Trends in cybercrime. In *Justitiële Verkenningen, 8*, 22-33.
Stol, W.Ph., E.R. Leukfeldt & H. Klap (2012). Cybercrime en politie. Een schets van de Nederlandse situatie anno 2012. In: *Justitiële Verkenningen, 38* (1), 25-39

Struiksma, N., C.N.J. de Vey Mestdagh en H.B. Winter (2012). *De organisatie van de opsporing van cybercrime door de Nederlandse politie.* Apeldoorn / Groningen: Politie & Wetenschap / Pro Facto.

Swaan, A. de (2008, oorspr. 1999). *De draagbare De Swaan*. Amsterdam: Uitgeverij Bert bakker.

Toutenhoofd-Visser, M.H., S. Veenstra, M.M.L. Domenie, E.R. Leukfeldt, W.Ph. Stol (2009). *Politie en Cybercrime. Intake en Eerste Opvolging. Een onderzoek naar de intake van het werkaanbod cybercrime door de politie.* Leeuwarden: NHL Hogeschool.

Treeck, R.J. van en W.Ph. Stol (2000). Betrouwbare open bronnen. *Algemeen Politieblad, 149* (20), 11-13.

University of Leicester (2007). The measurement and impact of crime, In: *Theories of crime and deviance*. Leicester: University of Leicester, department of criminology.

Van Uden, A., P. van Os, P. Tops en D. van Arkel (2012). *De 'tweede frontlijn' Over intake en service in de politie*. Apeldoorn: Politieacademie.

Vries, M. de (2011). De justitiële keten. In W. Stol, C. Tielenburg, W. Rodenhuis, S. Pleysier en J. Timmer, *Basisboek integrale veiligheid,* Den Haag: Boom/Lemma Uitgevers, pp. 169-182.

Wittebrood, K. (2006). *Slachtoffers van criminaliteit. Een inleiding in de victimologie*. Den Haag: BJU.

Bijlage A: Verbetersuggesties en best practices volgens respondenten

Tijdens de interviews is niet alleen gevraagd naar knelpunten in de afhandeling van cybercrimezaken, maar ook naar mogelijke best practices om deze knelpunten te ondervangen. In dit hoofdstuk geven we een beschrijving van de best practices *die respondenten hebben aangedragen*. Best practices zijn voorbeelden van bestaande praktische oplossingen om knelpunten aan te pakken. Lokale initiatieven spelen daarin een grote rol. Onder andere dankzij het Programma Aanpak Cybercrime van de politie en het intensiveringsprogramma Cybercrime van het OM zijn de afgelopen jaren op (boven)regionaal niveau verschillende proeftuinen omtrent (de aanpak van) cybercrime gelanceerd. In een aantal van deze proeftuinen wordt geëxperimenteerd met oplossingen voor problemen die we in dit onderzoek constateerden.[37]

De eerste drempel volgens respondenten: intake en registratie
Er zijn volgens de respondenten twee problemen bij de intake van cybercrimedelicten. Er komen er ten opzichte van het aantal slachtoffers weinig aangiften cybercrime binnen bij de politie. Zowel onder burgers als onder bedrijven vindt volgens verschillende respondenten waarschijnlijk veel cybercrime plaats waarvan politie en OM geen weet hebben. Volgens respondenten is een negatief imago van de politie daar debet aan. Respondenten zijn dan ook van mening dat er maatregelen moeten worden getroffen om ervoor te zorgen dat slachtoffers van cybercrime aangifte doen. Campagnes die slachtoffers ervan bewust maken dat het doen van aangiften wel degelijk zin heeft kunnen hier volgens respondenten aan bijdragen.

Ten tweede worden slachtoffers van cybercrime die aangifte willen doen volgens respondenten soms onverrichter zake naar huis gestuurd. De politie neemt dan niet altijd een aangifte op, terwijl wel sprake is van een strafbaar feit. Aangiften die wel worden opgenomen zijn bovendien niet altijd van voldoende kwaliteit. Een deel van de aangiften komt daardoor nooit in de strafrechtketen terecht en aangiften die wel zijn opgenomen stromen de strafrechtketen door een gebrek aan kwaliteit vroegtijdig uit. Het is volgens respondenten dan ook noodzakelijk om intakers te scholen in het opnemen van aangiften cybercrime. Indien nodig moeten digitaal experts bij het opnemen van een aangifte aanwezig zijn om ervoor te zorgen dat de juiste informatie in de aangifte komt en er juiste vervolgacties kunnen worden ondernomen.

Met het oog op voornoemde knelpunten in de intake en registratie van cybercrimedelicten, noemen respondenten een tweetal best practices die in onderstaande tekstbox worden beschreven.

[37] Alle in deze bijlage beschreven best practices zijn aangedragen door respondenten. In de tekstboxen worden de genoemde best practices beschreven. Naast de de door respondenten aangedragen informatie is voor die beschrijvingen gebruik gemaakt van via de opdrachtgevers verkregen documentatie over de projecten waarnaar is gerefereerd.

Best practices: kennisimpuls intake

E-Learning Cybercrime
Om de kennis van intakemedewerkers op het gebied van cybercrime een impuls te geven heeft het Programma Aanpak Cybercrime een een digitale leeromgeving (e-learning) ontwikkeld. Tweehonderd medewerkers in Brabant Noord en Limburg Noord hebben de module aangeboden gekregen. De resultaten van een eerste evaluatie zijn positief: intakemedewerkers zijn naar eigen zeggen beter in staat om een aangiften cybercrime op te nemen dan voorafgaand aan de cursus.

Handreiking voor delicten met een digitale component
Om ervoor te zorgen dat het kennisniveau van de intakemedewerkers ook na de cursus up-to-date blijft is door het Programma Aanpak Cybercrime een handreiking ontwikkeld. Met deze handreiking is voor politiemedewerkers te herkennen om welk delict het gaat, te bepalen welke wetsartikelen relevant zijn, hoe digitale sporen kunnen worden veiliggesteld en welke (algemene) adviezen aan de aangever kunnen worden geven. In totaal staan op deze manier in 28 delicten beschreven.

Een bijkomend probleem van het lage percentage slachtoffers dat aangifte doet en/of waarvan de aangifte wordt geregistreerd, is volgens respondenten dat hierdoor een slecht zicht ontstaat op de aard en omvang van cybercrime. Respondenten geven aan dat problematiek omtrent de afhandeling van cybercrime zichtbaar moet worden gemaakt voor beleidsmakers. Zolang niet duidelijk is dat er een probleem is met het percentage slachtoffers dat aangifte doet, bestaat de kans dat dit probleem alleen maar groter wordt. Immers, hoe meer slachtoffers worden weggestuurd bij de balie en hoe meer slachtoffers teleurgesteld zijn omdat de politie niets doet met hun melding, hoe minder slachtoffers er überhaupt nog aangifte gaan doen. Als het probleem inzichtelijk wordt gemaakt, kunnen beleidsmakers dit op de (politieke) agenda zetten en erop sturen dat dit probleem wordt aangepakt.

Organisatie van de aanpak van cybercrime
Om effectief uitvoering te geven aan de bestrijding van cybercrime, is het volgens respondenten van belang dat de verschillende onderdelen in de strafrechtketen goed op elkaar aansluiten. Op dit moment is dat, zo stellen zij, onvoldoende het geval. Met name de politie is hier onderwerp van kritiek. Als de politie niet in staat is om effectief uitvoering te geven aan het opsporen van cybercrime, worden dergelijke zaken ook niet vervolgd. ‘Als er geen onderzoeken worden gedraaid, dan verlies je de race’, aldus een respondent. Ontwikkelingen op het gebied van cybercrime gaan snel en om dat bij te houden moeten er wel zaken gedraaid worden. Daarbij komt, dat zolang er geen of weinig ervaring met het oppakken van cybercrimezaken is, er een drempel zal blijven bestaan om die zaken op te pakken wanneer ze zich aandienen. ‘Onbekend maakt onbemind’, aldus een respondent. Respondenten geven dan ook aan dat er simpelweg meer zaken moeten worden gedraaid om het kennisniveau bij politie en justitie omhoog te krijgen. Om dit te kunnen bereiken moet er capaciteit worden vrijgemaakt. Omdat er op dit moment nauwelijks op wordt gestuurd om cyberzaken op te pakken, is het volgens respondenten ook noodzakelijk om per politiekorps medewerkers aan te wijzen die zich primair bezig houden met het onder de aandacht brengen en prioriteren van cybercrimezaken.

Verder stellen enkele respondenten voor om aan reguliere tactische rechercheteams digitale experts toe te voegen, zodat in opsporingsteams altijd een fundament van digitale expertise

aanwezig is. Andere respondenten gaan nog verder en opperen dat op bovenregionaal niveau specialistische teams moeten worden geformeerd die zicht uitsluitend bezig houden met de aanpak van cybercrime. Ook dergelijke teams zouden dan moeten bestaan uit zowel tactisch rechercheurs als digitaal experts, omdat het (inter)nationaal opererende Team High Tech Crime (THTC) op soortgelijke wijze successen boekt. Om de voorgestelde aanpak op te zetten kan het THTC in het begin mensen uitlenen aan (boven)regionale teams om zo de kennis die ze hebben uit te leren. Volgens een respondent van het OM wordt een dergelijk voorstel geopperd in voorlopige plannen over de inrichting van de nationale politie, maar of er daadwerkelijk dergelijke teams komen is onbekend. Bekend is wel dat de politie op dit moment nog niet zo werkt. Respondenten stellen dus een ander model voor dan nu wordt gehanteerd. Hoewel het aantal digitaal specialisten in Nederland toeneemt, is het huidige principe in politieland dat tactisch rechercheurs alle voorkomende delicten behandelen en dat digitaal experts uitsluitend ondersteuning bieden bij de behandeling van delicten met een digitale component (Stol, Leukfeldt & Klap, 2012).

In het verlengde van voorgaande geven respondenten aan dat de politie zich in eerste instantie kan richten op een aantal specifieke vormen van cybercrime zodat daarover kennis ontstaat. Dit kan bijvoorbeeld door alle zaken waarbij artikel 138ab een rol speelt op te pakken. Op die manier wordt kennis opgedaan over de aard van die zaken, leert de politie met wat voor andere criminaliteitssoorten die delicten in verband staan en kan worden geëxperimenteerd met bijzondere opsporingsbevoegdheden. Zodra er genoeg kennis is verkregen kan dit worden uitgeleerd aan andere regio's. Dan kan weer worden overgegaan op een andere vorm van cybercrime die de aandacht verdient.

Respondenten noemen een aantal best practices die ertoe leiden dat de politie cyberzaken structureel aanpakt. In onderstaande tekstbox worden de door respondenten aangedragen projecten beknopt beschreven.

Best practices:opsporingsonderzoeken bij de politie

De aanpak van online kinderpornografie
In Rotterdam is capaciteit vrijgemaakt voor rechercheurs die zich uitsluitend bezig houden met de aanpak van online kinderpornografie. Als dat niet was gedaan, zouden online kinderpornozaken niet worden opgepakt, omdat ze binnen de zedenteams een lagere prioriteit hebben dan bijvoorbeeld een incest- of verkrachtingszaak, aldus een respondent. In het verleden waren er geen rechercheurs speciaal voor kinderpornografie vrijgesteld, maar moesten er wel een bepaald aantal zaken worden gedraaid. Dan moesten er dus soms verkrachtingszaken blijven liggen omdat er nog een aantal kinderpornografiezaken moesten worden opgestart. Door capaciteit vrij te maken voor kinderpornografie hoeft die keuze niet meer te worden gemaakt, aldus de respondent.

Virtueel flexibele netwerkteams
Bij politie Kennemerland bestaan zogeheten 'virtueel flexibele netwerkteams'. Daarbinnen wordt gewerkt met een team dat bestaat uit een vaste kern van 3 a 4 mensen, waarbij – afhankelijk van de aard van een zaak die zich aandient – tijdelijk specialisten (ook van buiten de politie) worden 'ingevlogen' om een zaak te behandelen. Bij cyberzaken kunnen bijvoorbeeld digitaal experts worden ingevlogen

Eén van de problemen van de aanpak van cybercrime is dat aangiften tegen verdachten niet allemaal in één regio binnenkomen. Dat is ook het geval bij de kleinere bulkzaken zoals oplichtingen via veiling- en verkoopsites. Voor de aanpak van cybercrime moet daarom ook volgens respondenten niet meer regionaal gedacht worden: 'Je kunt niet meer in regio's denken.'. Het centraal binnen laten komen, analyseren en bundelen van aangiften zorgt ervoor dat beter kan worden ingeschat welke zaken echt prioriteit behoeven omdat landelijk kan worden bekeken waar een verdachte allemaal bij betrokken is. De belangrijkste zaken kunnen dus als eerste worden aangepakt. Zo wordt voorkomen dat verschillende korpsen werken aan dezelfde zaak zonder dat ze dat van elkaar weten. Een bijkomend voordeel is dat er uiteindelijk een bundel zaken naar het korps wordt gestuurd waarin de verdachte woont. In dat korps moet de zaak vervolgens worden opgepakt. Daardoor leren politiemedewerkers hoe dergelijke zaken effectief aangepakt kunnen worden. Een dergelijke aanpak kan een uitkomst zijn bij bijvoorbeeld phishingzaken.

Over het centraliseren van de aanpak van cybercrime noemen respondenten twee best practices. In onderstaande tekstbox worden deze bestaande praktische oplossingen beknopt beschreven

Best practices: de gecentraliseerde aanpak van cybercrime

Gecentraliseerde aanpak kinderporno
Vanaf volgend jaar wordt de aanpak van kinderporno gecentraliseerd. Alle aangiften van kinderporno worden verzameld door IPOL. De Dienst IPOL is een (inter) nationaal informatieknooppunt van de Nederlandse politie.[38] Daar worden aangiften gebundeld en wordt vooronderzoek naar verdachten gedaan (wie hoort er bij dit IP adres). IPOL stuurt de gebundelde en voorbereide zaken vervolgens naar de regiokorpsen. Dat voorkomt dat korpsen langs elkaar heen werken en zonder dat zij dit van elkaar weten opsporingsonderzoek verrichten naar dezelfde daders.

Gecentraliseerde aanpak internetgerelateerde fraude
Internetgerelateerde fraude is de meest voorkomende vorm van cybercrime. Door de relatief geringe omvang van de afzonderlijke fraudes, de gefragmenteerde registratie en de veelal schaarse expertise krijgt dit soort zaken vaak een lage prioriteit. Daardoor blijven veel zaken 'op de plank' liggen terwijl het aantal gedupeerden toeneemt. Om die reden is het Meldpunt Internet Gerelateerde Fraude ingesteld. Het meldpunt verzorgt een landelijk gecoördineerde aanpak van dit type criminaliteit.

We willen op deze plaats benadrukken dat hoewel respondenten op het oog veelbelovende verbetersuggesties en best practices aandragen, we aan de gedane suggesties geen waardeoordeel kunnen geven. Daarvoor is het van belang om op basis van de genoemde verbetersuggesties initiatieven te ontplooien en deze te evalueren en/of om evaluatieonderzoek uit te voeren naar reeds bestaande projecten waarin conform dergelijke uitgangspunten wordt gewerkt.

[38] http://www.politie.nl/KLPD/organisatieonderdelen/dienst_ipol - laatst geraadpleegd op 03-05-2012