Wetenschappelijk Onderzoek- en Documentatiecentrum
Ministerie van Justitie en Veiligheid

Cahier 2018-21a

Tasten in het duister

Een verkenning naar bronnen en methoden om de aard en omvang van de criminaliteit te meten

Deel 1: Hoofdrapport

P.R. Smit (WODC)
R. Ghauharali (WODC)
H.C.J. van der Veen (WODC)
F. Willemsen (WODC)
J. Steur (Dialogic)
R.A. te Velde (Dialogic)
T. van der Vorst (Dialogic)
F. Bongers (Dialogic).

m.m.v:
A. Kabki (Saxion)
D. Zaitch (Universiteit Utrecht)

Cahier
De reeks Cahier omvat de rapporten van onderzoek dat door en in opdracht van het WODC is verricht.
Opname in de reeks betekent niet dat de inhoud van de rapporten het standpunt van de Minister van Justitie en Veiligheid weergeeft.

Voorwoord

Politiestatistieken en slachtofferenquêtes zijn gebruikelijke en beschikbare instrumenten om meer zicht te krijgen op de aard en omvang van criminaliteit. Maar hoe meten we de omvang van een zeer complex en ongrijpbaar fenomeen: verborgen criminaliteit? Deze studie onderzoekt welke andere bronnen en methoden om de aard en omvang van criminaliteit te meten, beschikbaar zijn of ontwikkeld kunnen worden.
Met dit onderzoek geven we geen uitsluitsel over het 'dark number' van de criminaliteit. Het is een complex fenomeen waar we niet met één onderzoek duidelijkheid over kunnen geven. Het is een lang proces, dat we in stappen vorm moeten geven. Met dit onderzoek is zo'n stap gezet. Wat we met deze studie doen, is inzicht bieden in methoden die kunnen helpen om de omvang van verborgen criminaliteit te schatten. Deze inventarisatie kan helpen om delen van criminaliteit die we nu niet goed in kaart hebben, te onderzoeken.
Bijzondere aandacht is besteed aan drie specifieke onderwerpen: horizontale fraude, georganiseerde criminaliteit en cybercriminaliteit.
Dit rapport is het hoofdrapport van deze studie. Meer gedetailleerde bevindingen worden gepubliceerd in een binnenkort te verschijnen technisch rapport. De studie is deels uitgevoerd door WODC onderzoekers en voor wat betreft de bovengenoemde specifieke onderwerpen door het onderzoeksbureau Dialogic.
Tot slot bedanken wij alle respondenten voor het delen van hun kennis en inzichten en de leden van de begeleidingscommissie en de klankbordgroep voor hun constructieve bijdrage gedurende het gehele onderzoek.

Waarnemend directeur WODC
Mw. drs. A.L. Daalder

Inhoud

Afkortingen

BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CBV	Centrum Bestrijding Verzekeringscriminaliteit
CBS	Centraal Bureau voor de Statistiek
CIS	Centraal Informatie Systeem
CJIB	Centraal Justitieel Incassobureau
CMI	het Centraal Meldpunt Identiteitsfraude en -fouten
CPI	ConsumentenPrijsIndex
C&R	(De publicatie) Criminaliteit en Rechtshandhaving
ESM	Enquête Slachtoffers Misdrijven
ERV	Enquête Rechtsbescherming en Veiligheid
FIOD	Fiscale Inlichtingen- en Opsporingsdienst
ICCS	International Classification of Crime for Statistical Purposes
IVM	Integrale VeiligheidsMonitor
JenV	Ministerie van Justitie en Veiligheid
LIS	Letsel Informatie Systeem
LMIO	Landelijk Meldpunt Internet Oplichting
MSVS	Monitor Sociale Veiligheid in Scholen
MZJ	Monitor Zelfrapportage Jeugd
NEA	Nationale Enquête Arbeidsomstandigheden
NVB	Nederlandse Vereniging van Banken
NVI	Nationale VeiligheidsIndex
OM	Openbaar Ministerie
PMB	Politiemonitor Bevolking
POLS	Permanent Onderzoek Leefsituatie
RDS	Respondent Driven Sampling
Sr	Wetboek van Strafrecht
VM	VeiligheidsMonitor
VMR	VeiligheidsMonitor Rijk
WAHV	Wet administratiefrechtelijke handhaving verkeersvoorschriften
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum

Leeswijzer

Dit rapport, zijnde deel 1 van een studie naar het dark number van criminaliteit laat samen met deel 2, het technische rapport (Smit et al., 2018), de resultaten zien van deze studie naar de problematiek van het meten van criminaliteit.
Voor een deel kan dit rapport gezien worden als een uitgebreide samenvatting van het technische rapport, met verwijzingen naar de hoofdstukken en bijlagen van dat rapport waar in meer detail op de materie wordt ingegaan. Ook de meeste literatuurreferenties zullen niet hier maar in het technische rapport te vinden zijn. Daarnaast bevat dit rapport een discussie over de bevindingen en worden aanbevelingen gedaan. Hiermee is dit rapport meer gericht op de praktijk, terwijl het technische rapport meer gericht is op de wetenschap.

Dit rapport is derhalve een volledige, maar niet gedetailleerde weergave van de bevindingen. De lezer die – wellicht op onderdelen – geïnteresseerd is in onderbouwingen en verder uitgewerkte resultaten wordt uitdrukkelijk verwezen naar het technische rapport.

De opbouw van dit rapport is als volgt.
Hoofdstuk 1 beschrijft wat de aanleiding voor deze studie is en wat deze studie beoogt te bereiken. Vervolgens wordt ingegaan op de vraag wat de (conceptuele, statistische en praktische) problemen zijn bij het meten van criminaliteit. Waarom is het (kennelijk) zo lastig criminaliteit te meten? Ten slotte worden in dit hoofdstuk de in de studie gehanteerde begrippen gedefinieerd, wordt er een theoretisch kader geschetst en worden de onderzoekvragen gepresenteerd. In hoofdstuk 2 worden de twee meest gebruikte methoden om criminaliteit te meten, namelijk de politieregistraties en de slachtofferenquête, uitgebreid besproken. Hoofdstuk 3 geeft een overzicht van methoden die gebruikt (kunnen) worden om verborgen (althans niet direct zichtbare) populaties te schatten en of deze methoden gebruikt (kunnen) worden voor het meten van criminaliteit. Waar mogelijk worden hier ook voorbeelden gegeven gerelateerd aan de (verborgen) criminaliteit. Waar in de hoofdstukken 2 en 3 al enigszins ingegaan is op enkele bevindingen ten aanzien van de omvang van criminaliteit, wordt dit in hoofdstuk 4 verder uitgebreid. Per delicttype of verschijningsvorm van criminaliteit worden de eigenschappen en de resultaten van verschillende methoden beschreven. In het bijzonder wordt aandacht besteed aan horizontale fraude, georganiseerde criminaliteit en cybercrime. Hoofdstuk 5 bevat ten slotte een discussie over de gevonden resultaten en geeft enkele aanbevelingen. Tevens wordt hier ingegaan op de in hoofdstuk 1 gepresenteerde onderzoeksvragen.

1 Inleiding

Deze studie gaat over het meten van criminaliteit. Hoe wordt criminaliteit gemeten en wat zijn de resultaten van deze metingen? In het bijzonder wordt aandacht besteed aan wat er *niet* wordt gemeten en wat voor bronnen en welke methoden en technieken bruikbaar zouden kunnen zijn om enig zicht te krijgen op die 'verborgen' criminaliteit.

1.1 Aanleiding en doel

In deze studie worden verschillende methoden beschreven waarmee zicht verkregen kan worden op de aard en de omvang van en de ontwikkelingen in de criminaliteit. Nu is een van oudsher belangrijke criminaliteitsstatistiek (in Nederland vanaf 1948) de Politiestatistiek waarin het aantal door de politie geregistreerde misdrijven wordt bijgehouden. In deze studie wordt dit aangeduid met *geregistreerde* criminaliteit. Ook in andere landen wordt vrijwel altijd wel een Politiestatistiek bijgehouden en meestal is dit de enige regelmatig bijgehouden statistiek die iets zegt over de criminaliteit. In berichtgeving in de media wordt vaak – en niet zelden impliciet – de omvang en ontwikkeling van criminaliteit gerapporteerd op basis van deze geregistreerde criminaliteit.
Het blijkt dat volgens deze Politiestatistiek de geregistreerde criminaliteit in Nederland al geruime tijd continu aan het dalen is: van ruim 9.000 misdrijven (per 100.000 inwoners) in 2002 naar iets minder dan 5.000 in 2016, een daling van bijna 50%. En ook in veel andere Westerse landen is er in deze periode sprake van een daling. Opvallend is dat in de meeste landen, net als in Nederland, de piek in 2002 (of 2003) ligt. Uitzonderingen zijn de VS, waar de daling al in 1991 begon waarbij de geregistreerde criminaliteit in de periode 1991-2016 met ruim 50% gedaald (Friedman et al., 2017) is en Duitsland waar de daling zich vanaf 1995 inzette en de geregistreerde criminaliteit tussen 1995 en 2017 met 29% afnam (BundesKriminalAmt, 2018; Kalidien, 2017). Nog een voorbeeld: in het Verenigd Koninkrijk is de afname in de geregistreerde criminaliteit 34% (tussen 2002 en 2013)[1] (Office for National Statistics, 2018).
Hoewel deze daling ondersteund wordt door de resultaten van een geheel andere methode, namelijk door middel van slachtofferenquêtes, worden er toch vanuit de politiek en in berichtgeving in de media vraagtekens gezet bij deze geconstateerde daling van de criminaliteit. Vanwege het ontstaan van nieuwe, lastig te achterhalen (onder andere vanwege het vaak internationale karakter hiervan) vormen van criminaliteit als cybercrime is het de vraag of de in de politiecijfers *geconstateerde* daling van de criminaliteit in de laatste vijftien jaar wel een *feitelijke* vermindering van de criminaliteit inhoudt. Het onderliggende probleem is dat een deel van de criminaliteit verborgen blijft, het zogenoemde 'dark number'.
Deze dark-numberproblematiek is niet nieuw. En eigenlijk was het ontstaan van statistieken op basis van politieregistraties al een verruiming van het zicht op criminaliteit ten opzichte van de situatie voor het midden van de vorige eeuw waarbij alleen gekeken werd naar rechterlijke vonnissen. Dit zoeken naar methoden om het

[1] Wel lijkt er in de periode na 2013 in Engeland & Wales sprake te zijn van een *toename* in de geregistreerde criminaliteit, vooral van geweldscriminaliteit. Dit is opmerkelijk aangezien de slachtofferenquête in de periode tot 2017 nog wel een afname laat zien (Office for National Statistics, 2018).

dark number zichtbaar te maken – oftewel een zo compleet mogelijk beeld van de criminaliteit te verkrijgen – is blijven doorgaan, met als belangrijkste (maar niet het enige!) resultaat het ontstaan van de hiervoor al genoemde slachtofferenquêtes in de jaren zeventig van de vorige eeuw. Hierbij was Nederland internationaal gezien, samen met de VS en Engeland een voorloper.
Het doel van deze studie is om meer inzicht te krijgen in dit dark number. Enerzijds wordt dit gedaan door een overzicht te geven van *bestaande* bronnen en methoden om criminaliteit te meten, waarbij dus geïnventariseerd wordt welke criminaliteit – ook *buiten* de politieregistraties – wel bekend is en niet tot het dark number behoort. Anderzijds wordt onderzocht welke *nieuwe* – of nog niet vaak gebruikte – (combinaties van) bronnen en methoden beschikbaar en interessant kunnen zijn om meer inzicht te krijgen in de omvang van de criminaliteit. Beide invalshoeken worden uitgewerkt zowel vanuit een wat meer theoretisch en algemeen perspectief, maar ook door in te gaan op een drietal fenomenen waarbij een bepaalde verschijningsvorm van criminaliteit nader bekeken wordt. Het gaat dan om horizontale fraude, georganiseerde criminaliteit en cybercrime.

1.2 De problematiek van het meten van criminaliteit

Het bepalen van de omvang van criminaliteit is een ingewikkeld vraagstuk, onder andere omdat een van de actoren, namelijk de dader, er alle belang bij heeft dat zijn criminele gedrag *niet* bekend raakt. Maar ook andere factoren maken het lastig om methoden te vinden die volledig, eenduidig en accuraat de omvang van de criminaliteit kunnen meten. Deze factoren kunnen grofweg in drie categorieën verdeeld worden. Allereerst is er de *conceptuele* vraag wat er precies gemeten moet worden, oftewel: wat wordt verstaan onder criminaliteit en is een goede en consistente afbakening hiervan wel mogelijk? Ten tweede moeten er – soms arbitraire – *statistische* keuzes gemaakt worden bij het meten van de omvang van criminaliteit. Met name vanwege dit punt zijn internationale vergelijkingen van criminaliteitsstatistieken vaak problematisch. En ten slotte zijn er doorgaans *praktische* beperkingen aan gebruikte methoden. Vaak zijn methoden onvolledig – zoals de statistiek van geregistreerde criminaliteit die alleen de bij de politie bekende criminaliteit in beeld brengt –, indirect en onnauwkeurig.

Voordat op deze drie factoren nader wordt ingegaan, is het allereerst van belang om expliciet als uitgangspunt voor deze studie te noemen dat de omvang van de criminaliteit in principe bepaald wordt door het tellen of schatten van het *aantal* gepleegde *delicten*. Dit impliceert dat bij het gebruik van methoden die *niet* het aantal delicten tellen (bijvoorbeeld het aantal slachtoffers, het aantal daders of geleden schade) er een vertaalslag gemaakt moet worden naar een schatting van het aantal delicten.
Dat criminaliteit gemeten wordt door het tellen van het aantal delicten lijkt vanzelfsprekend maar dat is het niet. In deze studie zal blijken dat het voor sommige delicten zeer lastig (zedendelicten) of eigenlijk onmogelijk (snelheidsovertredingen) is een schatting te maken van het totaal aantal delicten. Ook is er het gegeven dat sommige delicten ernstiger (meer crimineel) zijn dan andere, zoals moord en winkeldiefstal, of 10km/u te hard rijden. En met de opkomst van digitale criminaliteit kunnen de aantallen zeer groot worden: er zijn naar schatting 16 miljoen phishing mails per maand in Nederland. Betekent dit dat er per jaar 192 miljoen delicten 'poging tot diefstal/oplichting/identiteitsfraude' zijn? Dit leidt dan ook tot de fundamentele vraag of 'het aantal delicten' (eventueel gewogen naar ernst of uitgesplitst naar soort delict) wel een goede maat is om datgene te meten wat we zouden willen

weten over de criminaliteit. Of met andere woorden, zelfs al zou 'het aantal delicten' iets zeggen over de omvang van de criminaliteit, wordt met de vraag 'wat is de omvang van de criminaliteit?' wel de juiste vraag gesteld? De vragen 'hoe erg is de criminaliteit?' of 'wat zijn de (maatschappelijke) kosten van criminaliteit?' zijn wellicht relevanter om te bepalen of, hoeveel en welke maatregelen er genomen moeten worden ter bestrijding van de criminaliteit.[2]
Deze fundamentele vraag valt buiten het bereik van deze studie maar geeft wel aanleiding tot de eerste aanbeveling:

> *Aanbeveling 1*: In een vervolgonderzoek expliciet de vraag aan de orde stellen wat een zinvolle en praktisch te implementeren maat voor het meten van criminaliteit kan zijn.

1.2.1 Conceptuele overwegingen

Een eerste constatering is dat wat als criminaliteit beschouwd wordt geen statisch gegeven is, maar onderhevig is aan *veranderingen in de tijd*. Gedragingen die eerst als crimineel gezien worden, kunnen op een gegeven moment gelegaliseerd worden (decriminalisatie), maar ook andersom kunnen legale handelingen op enig moment strafbaar gesteld worden (criminalisatie). Hoewel dit op zich geen probleem hoeft te zijn bij het meten van criminaliteit, maakt dit het interpreteren van ontwikkelingen in de tijd gecompliceerd. Een hieraan gerelateerd punt is het ontstaan van *nieuwe verschijningsvormen* van criminaliteit, momenteel vooral op het gebied van cybercrime en gedigitaliseerde vormen van (soms klassieke) criminaliteit. Deze nieuwe verschijningsvormen vergen vaak ook nieuwe methoden om zicht te krijgen op de omvang.

Daarnaast kan de *houding van de verschillende actoren* (slachtoffers, politie, justitie) ten opzichte van (bepaalde vormen van) criminaliteit veranderen. Denk aan het gedogen van bepaalde vormen van criminaliteit, wijzigende beleidsprioriteiten of mondigere slachtoffers ten aanzien van bijvoorbeeld huiselijk geweld. Er lijkt meer vertrouwen te zijn om misdrijven te benoemen (zie ook de #metoo ontwikkeling). Dit kan resulteren in een verschuiving van bekende naar verborgen criminaliteit (of andersom), zonder dat de criminaliteit daadwerkelijk verandert.

Een ander punt is de bepaling van de *scope* van het begrip 'criminaliteit' en daarmee samenhangend de vraag welke delicten wel en welke niet 'meegeteld' zouden moeten worden. In deze studie is uitgegaan van een formele juridische definitie van criminaliteit (en delicten). Kort gezegd: alles wat volgens de wet niet mag, valt onder criminaliteit. Is het echter wel zinvol om alle delicten mee te nemen bij de maat van de criminaliteit? Wat te doen met overtredingen? Of met misdrijven naar de letter van de wet maar waarvan geen van de betrokkenen (dader, slachtoffer en Justitie)

---

[2] Een mogelijke methode om dit soort vragen te operationaliseren is te werken met een index gemaakt op basis van (het gewogen gemiddelde van) enkele 'producten'. Een product zou kunnen zijn een delict(type). Maar ook 'het percentage jeugdige daders'. Of 'het aantal DDos-aanvallen'. Of 'het aantal slachtoffers van seksueel geweld zoals gemeten in de Veiligheidsmonitor (VM)'. Dit is analoog aan ConsumentenPrijsIndex (CPI) van het Centraal Bureau voor de Statistiek (CBS) of de AEX-index van de effectenbeurs. Het grote voordeel is dat producten gekozen kunnen worden die eenvoudig te meten zijn en dat op natuurlijke wijze verschillende soorten bronnen gecombineerd kunnen worden. Ook is de restrictie van alleen aantallen delicten meten opgeheven. Het nadeel is dat een index geen absolute grootheid is en dat deze – weer naar analogie van de CPI – frequent gekalibreerd moet worden met mogelijke trendbreuken tot gevolg.

van mening is dat het om een misdrijf gaat? Of met een misdrijf dat een slachtoffer kennelijk zo onbelangrijk vindt dat hij/zij geen moeite neemt dat aan te geven?[3] In feite is dit een arbitraire keuze en in de praktijk wordt vaak impliciet de volgende keuze gedaan: vrijwel altijd wordt de criminaliteit afgebakend als zijnde alle *misdrijven*. In deze studie wordt deze beperking evenwel niet gehanteerd, althans niet als uitgangspunt genomen. Wel wordt in de *uitwerking* van dit onderzoek vooral (maar niet uitsluitend) aandacht besteed aan die delicten die bij wet als misdrijf aangeduid worden.

1.2.2 Statistische keuzes

Allereerst is er het probleem van het kiezen van een teleenheid. Telt een inbraak uitgevoerd door twee daders als een of als twee delicten? Telt een dubbele moord gepleegd door één dader als een of als twee delicten?[4] En hoe worden tien meldingen (van oplettende burgers) van hetzelfde delict geteld? Hoe (en onder welk delict) worden combinaties van misdrijven geteld, zoals bedreiging met een wapen waarvoor geen vergunning is? Wat te doen met een phishing mail naar duizenden mailadressen?[5] Nu is dit probleem redelijk eenvoudig op te lossen door duidelijke keuzes hierin te maken en door eventueel met behulp van goede schattingen de resultaten van methoden aan te passen aan die keuzes. In de statistieken zoals gepresenteerd in het naslagwerk Criminaliteit en Rechtshandhaving (C&R; Kalidien, 2017) zijn deze keuzes ook inderdaad expliciet gemaakt. Wel is het zo dat deze keuzes mogelijk niet constant zijn in de tijd. Hiervoor moet dan gecorrigeerd worden om trends te kunnen bepalen.[6]

Een andere statistische keuze betreft niet de omvang maar de zwaarte van delicten en de mogelijke wens tot weging. Bij het simpel optellen van alle delicten tellen alle delicttypes even zwaar. Dat wil zeggen dat 49 winkeldiefstallen en 1 moord 'evenveel' criminaliteit weergeven als 25 winkeldiefstallen en 25 moorden. Een mogelijke oplossing is het wegen van de diverse vormen van criminaliteit, zoals toegepast is in de Nationale VeiligheidsIndex (NVI) (Cuyper et al., 2015). Ook hier zullen dan keuzes gemaakt moeten worden over de weegfactoren.

1.2.3 Beperkingen van methoden in de praktijk

Methoden zijn niet zelden *onvolledig* met betrekking tot het meten van de criminaliteit. Soms is dat inherent aan de methode, een slachtofferenquête meet nu eenmaal niet de slachtofferloze criminaliteit, maar vaak ligt er een keus aan ten grondslag. Voorbeelden zijn ook hier de huidige slachtofferenquête Veiligheidsmonitor (VM), waarbij alleen natuurlijke personen ouder dan 15 jaar bevraagd worden. Of de Politiestatistiek waarin alleen de formele aangiften geregistreerd worden en niet de meldingen.

---

[3] Voor alle duidelijkheid: dit (het onbelangrijk vinden van een misdrijf) is slechts een van de mogelijke redenen voor een slachtoffer om geen aangifte te doen.

[4] Met als extreem voorbeeld de Breivik-moorden in Noorwegen.

[5] Strafrechtelijk kan bij deze voorbeelden sprake zijn van eendaadse of meerdaadse samenloop. Bij eendaadse samenloop is sprake van één strafbaar feit dat onder meer dan één strafbepaling valt (art. 55 Sr), bij meerdaadse samenloop zijn er meerdere strafbare feiten die 'worden beschouwd als één voortgezette handeling' (art. 56 Sr).

[6] Zie bijvoorbeeld de recente verandering in de definitie van de teleenheid 'verdachte' zoals gepubliceerd door het CBS (Kalidien, 2017).

Daarnaast kan sprake zijn van *onnauwkeurigheid* van de resultaten. Ook dit kan vele oorzaken hebben: de marges in de uitkomsten van een enquête zijn afhankelijk van de grootte van de steekproef, geheugeneffecten kunnen een rol spelen bij respondenten, een politiemedewerker kan fouten maken bij de registratie van een delict, daders kunnen bewust zaken verzwijgen bij een zelfrapportage, slachtoffers kunnen bewust zaken anders weergeven etcetera. Ook bestaat er *onzekerheid ten aanzien van het gebruik van indicatoren*: het aantal gemelde diefstallen bij een verzekeringsmaatschappij kan een indicator zijn voor het delict diefstal. Maar er kan ook iets heel anders aan de hand zijn, namelijk verzekeringsfraude.

Een methode om de omvang van de criminaliteit te bepalen, zal zelden direct het aantal delicten meten. Er zal vrijwel altijd *indirect*, vanuit een bepaald perspectief (politie, dader, slachtoffer, schade, …) gekeken worden. Deels heeft dit te maken met de hierboven aangekaarte (on)volledigheid (slachtoffers 'zien' niet alle delicten, namelijk niet de slachtofferloze delicten; de politie 'ziet' alleen die delicten die gemeld worden of die zij zelf door opsporing ontdekken), maar er is hier ook sprake van het meten van verschillende grootheden. Slachtofferenquêtes rapporteren niet het aantal delicten, maar het aantal slachtoffers.[7] Schattingen naar omvang van verzekeringsfraude meten het schadebedrag en niet het aantal delicten. Enerzijds is dit een probleem omdat bijvoorbeeld de omvang van in beslag genomen drugs niet direct een schatting geeft van het aantal drugs*delicten.* Maar anderzijds is het bestaan van methoden die weliswaar niet direct het aantal delicten maar wel een gerelateerd fenomeen meten ook een verrijking. Met name bij cybercriminaliteit, horizontale fraude en georganiseerde criminaliteit zijn veel methoden gebaseerd op dit soort indirecte metingen.

1.3 Definities en theoretisch kader

1.3.1 Definities

In deze paragraaf worden de kernbegrippen gedefinieerd, die in deze studie gehanteerd worden (zoals criminaliteit en dark number).

Criminaliteit
Criminaliteit bestaat uit een verzameling van uiteenlopende vormen van handelingen die op zichzelf staand erg kunnen verschillen van elkaar (denk bijvoorbeeld aan fietsdiefstal versus mensenhandel), maar die elk wel een aantal gemeenschappelijke noemers kent. Er is namelijk altijd sprake van een 'dader' en van een 'handeling' die bij wet strafbaar is gesteld. Uitgaande van deze twee kenmerken wordt de definitie van criminaliteit voor dit rapport als volgt:

> *Een handeling (of meerdere handelingen die als één voortgezette handeling beschouwd kunnen worden of die anderszins een zekere samenhang vertonen), of pogingen daartoe, door één of meer personen, rechtspersonen of instanties verricht of nagelaten die volgens Nederlandse regelgeving strafbaar gesteld is/zijn.*

[7] De VM probeert overigens wel aantallen delicten te meten door ook aan respondenten te vragen hoe vaak zij slachtoffer waren

Een dergelijke handeling (of samengaan van meer handelingen, denk bijvoorbeeld aan overval met verboden wapenbezit) wordt in dit rapport ook wel aangeduid als 'delict'.
Zoals hiervoor al aangegeven, wordt in deze studie in eerste instantie uitgegaan van een brede definitie. Zowel regelgeving vastgelegd in het Wetboek van Strafrecht (Sr) als regelgeving vastgelegd in overige wetboeken vallen onder deze noemer, waarbij het niet enkel om misdrijven gaat, maar ook om overtredingen.
De hier gepresenteerde definitie van criminaliteit geeft voornamelijk een *afbakening* van wat onder criminaliteit beschouwd wordt en is (nog) niet volledig als *telinstructie* voor het tellen van het aantal delicten. Met name voor het vaststellen van de teleenheid blijven – soms arbitraire -–keuzes een rol spelen (zie paragraaf 1.2.2).

Geregistreerde en ondervonden criminaliteit
De *geregistreerde* en *ondervonden* criminaliteit is die criminaliteit die gemeten wordt in twee bronnen, namelijk de politieregistraties en de slachtofferenquêtes[8]. In dit rapport noemen we de door de politie geregistreerde misdrijven de *geregistreerde* criminaliteit en de schatting van de criminaliteit op basis van de steekproef van de slachtofferenquêtes de *ondervonden* criminaliteit.
Vooral de (definitie van de) geregistreerde criminaliteit kan tot misverstanden leiden. Immers, het gaat hier alleen om *door de politie* geregistreerde *misdrijven.* Er is hiervoor gekozen omdat deze definitie bij criminaliteitsstatistieken gebruikelijk is; ook internationaal. Nu wordt er in deze studie zeker ook gekeken naar door andere instanties geregistreerde delicten (en ook naar delicten die volgens het Wetboek van Strafrecht overtredingen zijn). Deze vallen onder de categorie 'aanvullende bronnen en methoden', zie hierna.

Aanvullende bronnen en methoden
Naast de geregistreerde en ondervonden criminaliteit zijn er nog vele andere al bestaande bronnen en methoden die criminaliteit meten. Registraties van overtredingen, registraties van andere opsporingsdiensten (Fiscale Inlichtingen- en Opsporingsdienst (FIOD)) maar bijvoorbeeld ook de CBS-doodsoorzakenstatistiek waarin onder meer het aantal door moord overleden mensen bijgehouden wordt. Ook bestaan er al andere methoden om (delen van) de criminaliteit te schatten. Zoals (dader)zelfrapportages of vangst-hervangstmethoden om het aantal illegalen te schatten. Deze methoden worden in deze studie *aanvullende bronnen en methoden* genoemd, als aanvulling op de geregistreerde en ondervonden criminaliteit (ofwel de politiestatistieken en slachtofferenquêtes).
Hierbij moet overigens opgemerkt worden dat er vaak een overlap is tussen de verschillende bronnen en methoden, zowel onderling als met de geregistreerde en ondervonden criminaliteit.

Geobserveerde criminaliteit
De geregistreerde en ondervonden criminaliteit en de aanvullende bronnen en methoden *samen* vormen dat deel van de criminaliteit dat bekend is, danwel geschat wordt. Dit wordt hier de *geobserveerde criminaliteit* genoemd.

Dark number
Buiten de geobserveerde criminaliteit blijft er een deel over dat niet gemeten wordt en op dit moment ook niet geschat wordt of kan worden. Dit wordt het dark number van de criminaliteit genoemd. Belangrijk is op te merken dat het dark number niet

[8] Deze twee bronnen worden verder ook aangeduid als de 'traditionele' bronnen, zie hoofdstuk 2.

gelijk is aan de niet-geregistreerde criminaliteit, immers voor een deel wordt de criminaliteit die niet geregistreerd wordt wel gemeten of geschat met andere bronnen of methoden (en is daarmee deel van de geobserveerde criminaliteit).

1.3.2 Theoretisch kader

Zie het technische rapport (Smit et al., 2018, paragraaf 1.6) voor een uitgebreide beschrijving van het theoretisch kader. Hier blijft de beschrijving beperkt tot een korte toelichting.

Een relationeel model
Wanneer een delict gepleegd wordt, is er sprake van een complex aantal verbanden tussen actoren (daders, slachtoffers, ...), wetten, handelingen en gevolgen van het delict. Zo wordt een delict altijd gepleegd door één of meer daders, is er soms sprake van slachtoffer(s), betreft het wellicht meerdere strafbare feiten die ieder gekoppeld zijn aan wetsartikelen, kan er schade zijn als gevolg van het delict, etcetera. Dit kan beschreven worden als relationeel model. Naast de keuze van de teleenheid die met dit model eenvoudig geëxpliciteerd kan worden geeft het model ook een formele basis voor de verschillende gezichtspunten of perspectieven van waaruit de criminaliteit – meestal indirect – waargenomen kan worden.

Classificaties van delicten
Een belangrijke onderverdeling bij het bepalen van de omvang van criminaliteit is naar type delict. Enerzijds vanwege de al eerder genoemde diversiteit in soorten delicten en anderzijds omdat methoden nogal eens betrekking hebben op specifieke vormen van criminaliteit. Nu blijkt dat verschillende instanties (en verschillende bronnen) andere indelingen, classificaties en/of definities hanteren. Voor dit onderzoek is het echter van belang dat er zo veel mogelijk een eenduidige indeling wordt gehanteerd.
Uitgaande van de *International Classification of Crime for Statistical Purposes* (ICCS)[9] is er voor dit onderzoek een eigen indeling naar type delict gemaakt waarvan in dit rapport zo veel mogelijk gebruik wordt gemaakt. Het betreft een hiërarchische indeling, bestaande uit elf hoofdcategorieën en verschillende subcategorieën. De categorieën sluiten elkaar niet helemaal uit. Er is bijvoorbeeld sprake van overlap tussen (horizontale) fraude en cybercrime. Een groot deel van fraude gebeurt via de digitale weg en behoort dus zowel tot de categorie fraude als tot de categorie gedigitaliseerde criminaliteit. Tevens bestaat er overlap tussen georganiseerde misdaad en meerdere vormen van criminaliteit wanneer dit in georganiseerd verband plaatsvindt. Bij het bepalen van de omvang van de totale criminaliteit is het dan ook van belang om zich bewust te zijn van deze overlap. Anders dan bijvoorbeeld het geval is bij de politiestatistieken zijn in deze classificatie niet alleen misdrijven, maar ook – conform de gehanteerde definitie van criminaliteit – overtredingen meegenomen. Zie bijlage 1 in het technische rapport (Smit et al., 2018) voor een overzicht van deze classificatie in typen misdrijf en de relatie met het Wetboek van Strafrecht en de CBS-standaardclassificatie.[10]

[9] DeICCS van de *United Nations Office on Drugs and Crime* is een classificatie van strafbare feiten die gebaseerd is op concepten, definities en principes waarover internationale overeenstemming bestaat (UNODC, 2015).

[10] De CBS-standaardclassificatie wordt gebruikt voor de geregistreerde criminaliteit, zoals gerapporteerd in de Politiestatistiek (Kalidien, 2017).

Schatten van onbekende aantallen
Het schatten van een onbekend aantal (dark number) is een contradictio in terminis: als het aantal eenmaal succesvol is geschat, houdt het op een onbekend aantal te zijn. Criminaliteit is een fenomeen dat zich laat vergelijken met een ijsberg. Slechts een deel is zichtbaar en een ander, niet direct zichtbaar deel waarvan de omvang onbekend is, bevindt zich onder de waterspiegel. De omvang van het deel van de ijsberg onder water is lastig vast te stellen, maar is – met enige moeite – wel tot op zekere hoogte te observeren. In feite zijn er twee benaderingen mogelijk om zicht te krijgen op de omvang van het dark number. De eerste manier, de *bottom-up*-benadering, wordt het meest gebruikt. Hierbij wordt expliciet gezocht naar delen van het dark number die nog niet eerder bekend waren. Het effect is dat er een hogere ondergrens verkregen wordt voor de totale populatie. De tweede manier, de *top-down*-benadering poogt juist elementen in de totale populatie die zeker *niet* tot het dark number behoren uit te sluiten, zodat een lagere bovengrens verkregen wordt. Beide methoden worden in deze studie gebruikt.

1.4 Onderzoeksvragen

De hoofdvraag van dit onderzoek luidt als volgt:

> *Op welke manier kan zowel de geobserveerde criminaliteit als het dark number van criminaliteit zo veel en zo goed mogelijk in kaart gebracht worden?*

De hoofdvraag valt uiteen in drie onderdelen.
Deel A betreft het in kaart brengen van de ontwikkeling van het meten van (de geobserveerde) criminaliteit en de relatie tot het dark number en de stand van zaken van het meten van criminaliteit anno nu.
In deel B van het onderzoek wordt specifiek ingezoomd op drie delicttypen: horizontale fraude, georganiseerde criminaliteit en cybercrime.
In deel C worden de bevindingen uit deel A en deel B bij elkaar gebracht om te komen tot een eerste inventarisatie van de geobserveerde criminaliteit en het dark number en hoe criminaliteit in de toekomst gemeten kan (blijven) worden.
Onderstaand worden per onderdeel de onderzoeksvragen weergegeven.

Onderdeel A
1 Met welke *huidige* instrumenten (bronnen) en schattingsmethodieken wordt momenteel de criminaliteit in Nederland in kaart gebracht (de geobserveerde criminaliteit)? En wat voor extra informatie geeft dit ten opzichte van de geregistreerde criminaliteit?
  Deze inventarisatie is te vinden in bijlage 4 t/m 6 in Smit et al. (2018) en wordt in dit rapport kort weergegeven in hoofdstuk 2 en 4.
2 Welke *nieuwe* initiatieven zijn er op dit moment gaande en kansrijk om inzicht te krijgen in het dark number om daarmee een groter deel van de criminaliteit te observeren? Dit wordt behandeld in hoofdstuk 3 van dit rapport en in hoofdstuk 3 en 4 in (Smit et al., 2018).

Onderdeel B
De uitwerking van de onderzoeksvragen bij B zijn te vinden in paragrafen 4.3.3, 4.5 en 4.9 en zijn tevens onderwerp van de hoofdstukken 6 t/m 8 in Smit et al. (2018).
3 In hoeverre en hoe is op basis van *lopende* inzichten en onderzoeken aan te geven wat omvang, aard en/of trends zijn van horizontale fraude, georganiseerde criminaliteit en cybercriminaliteit?

4 Welke *nieuwe* initiatieven zijn er op dit moment gaande en kansrijk om inzicht te krijgen in het dark number van horizontale fraude, georganiseerde criminaliteit en cybercriminaliteit om daarmee een groter deel van de criminaliteit te observeren?

Onderdeel C

Op de onderzoeksvragen bij C wordt nader ingegaan in hoofdstuk 5: de discussie en aanbevelingen.

5 Wat is er bekend over de trends inzake de omvang van de geobserveerde criminaliteit en hoe verhoudt zich dat tot de politieregistraties en de slachtofferenquêtes?
6 Welke meetinstrumenten/bronnen/technieken zijn het meest geschikt voor het meetbaar maken van welke vormen van niet-geregistreerde criminaliteit?
7 Is het noodzakelijk/wenselijk/mogelijk om op basis van nieuwe inzichten nieuwe meetinstrumenten te ontwikkelen of bestaande meetinstrumenten uit te breiden om criminaliteit te meten?

2 De Politiestatistiek en de slachtofferenquêtes

Een belangrijke plaats bij het meten van de omvang van de criminaliteit wordt ingenomen door de Politiestatistiek en de slachtofferenquêtes. Al enige decennia zijn dit de voornaamste bronnen die door wetenschap, politiek en media gebruikt worden. In deze studie worden ze dan ook aangeduid als de 'traditionele' bronnen, hoewel er wel degelijk ook andere bronnen en methoden zijn die (bepaalde vormen van) criminaliteit meten. Die komen in hoofdstuk 4 van dit rapport aan bod. Dit hoofdstuk gaat in op de vraag wat de twee traditionele bronnen meten (en wat niet), toont enkele resultaten van beide bronnen en tracht uitspraken te doen over de kwaliteit van de twee bronnen door de bevindingen te analyseren bij het koppelen van beide bronnen. Een meer uitgebreide beschrijving van deze beide bronnen en hun eigenschappen is te vinden in hoofdstuk 2 van Smit et al. (2018) en in Kalidien (2017).

2.1 De Politiestatistiek en de slachtofferenquêtes in de afgelopen decennia

2.1.1 De Politiestatistiek van het CBS

Sinds 1948 maakt het CBS jaarlijks de Politiestatistiek. In eerste instantie alleen de registraties van misdrijven door de politie, maar al snel bevatte de Politiestatistiek ook gegevens over verdachten. In de Politiestatistiek worden enkel misdrijven opgenomen. Andere volgens de Nederlandse regelgeving strafbare handelingen, zoals overtredingen, worden hier niet meegenomen. Alle misdrijven die door de Nationale Politie (momenteel de tien regionale eenheden en de landelijke eenheid) en door de Koninklijke Marechaussee geregistreerd zijn, worden opgenomen. Het gaat hier om misdrijven volgens het Wetboek van Strafrecht en een aantal andere specifieke wetten (onder andere Opiumwet, Wapenwet, Wegenverkeerswet).
Om verschillende redenen is de Politiestatistiek niet uniform over de jaren heen, zeker aangezien het gaat om een periode van zeventig jaar. Zo worden de registratiesystemen van de politie – waarop de statistieken gebaseerd zijn – soms aangepast. Alleen al de overgang van handmatige naar geautomatiseerde systemen kan een effect hebben gehad op het registreren van misdrijven. Maar ook de overwegingen om bij een melding inderdaad over te gaan tot een registratie zullen niet constant in de tijd zijn. Vervolgens zijn er ook statistische keuzes – zoals hoe om te gaan met verschillende misdrijven binnen één incident – die in de loop van de tijd anders kunnen uitvallen. Voor het interpreteren van trends op basis van de Politiestatistiek moet dus enige voorzichtigheid betracht worden.

2.1.2 De slachtofferenquêtes

De eerste slachtofferenquête onder de bevolking in Nederland werd in 1973 gehouden. In de periode 1973-1979 werd deze jaarlijks door het WODC uitgevoerd. Sinds 1980 heeft het CBS – tot 1985 in overleg met het WODC – dergelijke enquêtes regelmatig gehouden: in de periode 1981-1985 gebeurde dit jaarlijks, na 1985 telkens in de oneven jaren. Dit was de Enquête Slachtoffers Misdrijven (ESM). Met ingang van 1992 was de Enquête Rechtsbescherming en Veiligheid (ERV) de opvolger van de ESM. Deze continue enquête is in 1997 als module Recht opgenomen in het Permanent Onderzoek Leefsituatie (POLS), een continu CBS-onderzoek naar verschillende aspecten van de leefsituatie van de Nederlandse bevolking. Vanaf 2005

is deze module Recht binnen POLS vervallen. Sinds 1993 is parallel aan de CBS-enquêtes in opdracht van de toenmalige ministeries van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties (BZK) de Politiemonitor Bevolking (PMB) uitgevoerd. Tot en met 2001 was de PMB een tweejaarlijks onderzoek. Van 2002 tot en met 2005 is de PMB jaarlijks uitgevoerd.

De belangrijkste onderwerpen van de CBS-enquêtes en de PMB zijn door het ministerie van Justitie en Veiligheid[11] vanaf 2005 geïntegreerd in een nieuwe slachtofferenquête, de VeiligheidsMonitor Rijk (VMR), in 2008 opgevolgd door de vergelijkbare Integrale VeiligheidsMonitor (IVM) en vanaf 2012 door de VeiligheidsMonitor (VM). De uitvoering van deze enquêtes werd uitbesteed aan verschillende partijen, momenteel verzorgt het CBS de uitvoering.[12]

De uitkomsten van persoonsenquêtes zoals slachtofferenquêtes zijn sterk afhankelijk van de opzet: welke vragen worden gesteld en in welke volgorde, hoe worden respondenten benaderd, hoe wordt omgegaan met beperkte respons van bepaalde groepen respondenten etcetera. Nu is de opzet van de enquêtes in de afgelopen veertig jaar wel eens gewijzigd, hetgeen telkens een trendbreuk veroorzaakte.[13] Ook hier geldt derhalve, net als bij de Politiestatistiek, dat ontwikkelingen in de tijd zoals slachtofferenquêtes die laten zien met enige voorzichtigheid bekeken moeten worden.

2.1.3 Resultaten in de periode 1950-2017

Figuur 2.1 laat de resultaten zien van de Politiestatistiek en de verschillende slachtofferenquêtes. De Politiestatistiek begint hier in 1950. In de periode 1950-2017 is er vier keer sprake geweest van een trendbreuk vanwege een andere opzet van de statistiek. Met name de laatste wijziging (in 2005) had een forse invloed op de resultaten (in de orde van 7%). In de gepresenteerde reeks is zo goed mogelijk voor deze trendbreuken gecorrigeerd.
Wegens te grote verschillen in opzet met latere enquêtes konden de resultaten van de WODC slachtofferenquêtes (1973-1979) hier niet gebruikt worden. De slachtofferschappen in figuur 2.1 beginnen dan ook in 1980. Ook hier is sprake van trendbreuken waarvoor gecorrigeerd is. Voor de periode 1980-2003 zijn de CBS-enquêtes gebruikt (ESM, ERV en POLS), vanaf 2004 zijn de enquêtes van het ministerie van Justitie en Veiligheid gebruikt (VMR, IVM en VM). De resultaten van de PMB zijn niet gebruikt.

Zoals uit de figuur blijkt is het aantal slachtofferschappen zoals gemeten door de slachtofferenquêtes veel hoger (met een factor 6 tot 7) dan de geregistreerde criminaliteit.[14] Wat desalniettemin opvalt zijn de overeenkomsten: in de periode 1980-2002 is er geen duidelijke richting, maar zijn er wel grote schommelingen, na 2002 is er sprake van een forse continue daling. Daarnaast valt de sterke toename van de geregistreerde criminaliteit in de periode 1969-1982 op. De jaarlijkse groeipercentages waren in deze periode meestal boven de 10%. Het is niet duidelijk wat deze toename veroorzaakt heeft.

---

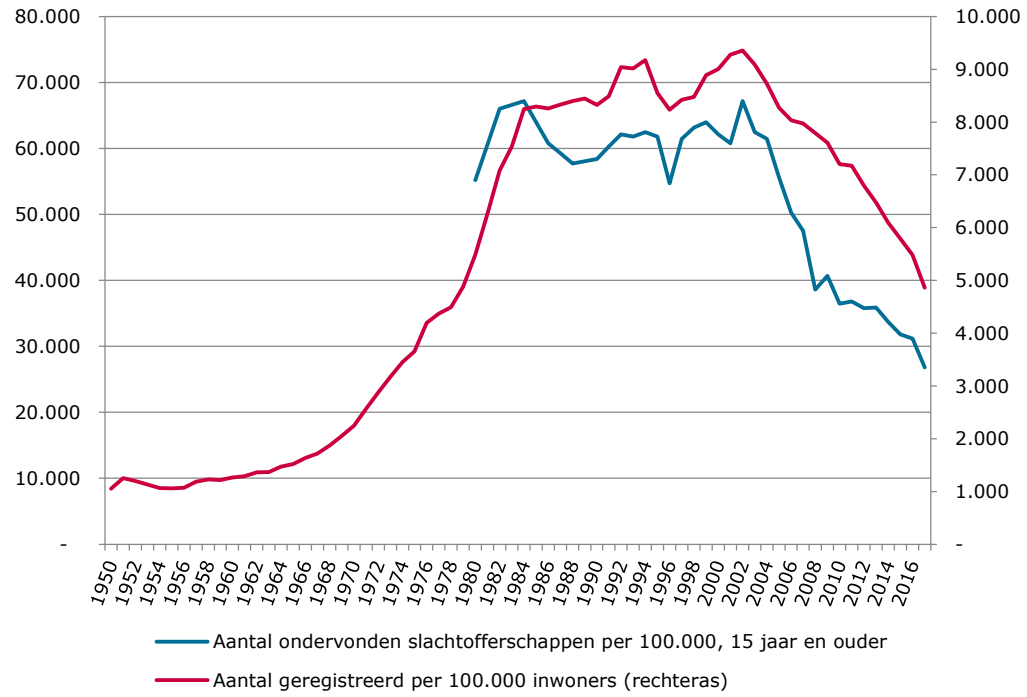
[11] In eerste instantie waren dat het toenmalige ministerie van Justitie en het ministerie van BZK.

[12] Sinds 2012 in samenwerking met I&O Research.

[13] Bij de introductie van de VM in 2012 is door parallel uitvoeren van de verschillende instrumenten zo veel mogelijk gecorrigeerd voor trendbreuken. Zie de onderzoeksverantwoording in de VM (Veiligheidsmonitor, 2017).

[14] Let op de verschillende schalen: slachtofferschappen staan op de linkeras, registraties op de rechteras.

Figuur 2.1 Geregistreerde criminaliteit en slachtofferschappen (aantallen per 100.000 inwoners), 1950-2017



Bron: CBS, JenV; bewerking WODC

2.2 De reikwijdte van beide bronnen

De Politiestatistiek en de slachtofferenquêtes kijken beide vanuit een verschillend perspectief naar de criminaliteit (de delicten). De slachtofferenquêtes meten criminaliteit vanuit het perspectief slachtofferschap, de Politiestatistiek vanuit het perspectief geregistreerd strafbaar feit. De directe implicatie is dat er in ieder geval een vertaalslag plaats moet vinden om een telling van aantal *delicten* te verkrijgen. Dit gebeurt ook inderdaad. Zo wordt bijvoorbeeld in de Politiestatistiek bij een incident bestaande uit een combinatie van strafbare handelingen alleen de handeling met de zwaarste strafdreiging geteld. En in de slachtofferenquête wordt niet alleen naar slachtofferschap gevraagd, maar ook naar het *aantal* ondervonden slachtofferschappen. Verder is inherent aan de methode dat de slachtofferenquêtes beperkt zijn tot die delicten die een *slachtoffer* kennen en dat de Politiestatistiek beperkt is tot die delicten die *geregistreerd* worden door de politie.

Daarnaast zijn er nog andere beperkingen bij beide methoden waardoor deze niet de totale criminaliteit meten. Bij de Politiestatistiek gaat het alleen om *misdrijven* die *door de politie* geregistreerd worden. Overtredingen maken hier geen deel van uit,[15] evenmin als misdrijven die elders geregistreerd worden.[16] Verder is hier een onderscheid tussen 'breng'- en 'haal'-delicten. Bij brengdelicten moet iemand het

[15] Wat overigens niet wil zeggen dat er geen andere bronnen voor geregistreerde overtredingen zouden zijn; zie hoofdstuk 4.

[16] Met als voorbeeld belastingfraude. In veel gevallen wordt dit door de Belastingdienst zelf afgehandeld.

misdrijf *gemeld* hebben en vervolgens moet deze melding ook daadwerkelijk resulteren in een *aangifte* en een *registratie*. De hoeveelheid haaldelicten, delicten die zelf door de politie opgespoord worden (bijvoorbeeld drugs of rijden onder invloed) wordt beperkt door de inspanning/capaciteit van de politie om deze misdrijven te achterhalen.
De beperking bij de slachtofferenquête is dat niet alle soorten slachtoffers worden bevraagd. Zo vallen bijvoorbeeld bedrijven en personen onder de 15 jaar buiten het steekproefkader. Belangrijk is bovendien dat een slachtoffer een delict ook daadwerkelijk als misdrijf herkend moet hebben. Dit laatste kan zowel tot onder- als overrapportage leiden: een slachtoffer heeft niet door dat hij opgelicht wordt of is zelf van mening dat een gebeurtenis niet telt als misdrijf. Of andersom: iemand interpreteert een bepaalde gebeurtenis als misdrijf, terwijl het ofwel een overtreding of zelfs helemaal geen strafbaar feit is.

2.3 Een vergelijking tussen de Politiestatistiek en de VM

De Politiestatistiek en de slachtofferenquêtes zijn verschillende bronnen die verschillende uitkomsten laten zien. Een voor de hand liggende oorzaak voor het grote verschil in niveau is dat niet elk door een slachtoffer ondervonden delict gemeld wordt bij de politie. Toch zou er ook een duidelijke overeenkomst moeten zijn. Immers, in de slachtofferenquêtes wordt ook gevraagd of een slachtoffer het ondervonden delict heeft aangegeven bij de politie. En dat deel (de aangegeven delicten) zou dus overeen moeten komen met de in de Politiestatistiek geregistreerde brengdelicten met personen als slachtoffer. Dit blijkt echter niet helemaal het geval te zijn. In enkele analyses – onder andere een analyse waarbij op individueel niveau de Politiestatistiek (het slachtoffer) gekoppeld is aan de VM (de respondent) voor de periode 2012-2016 (zie bijv. Reep, 2014) – is nagegaan of:

- mensen die slachtoffer geweest zijn meer of juist minder geneigd zijn een slachtofferenquête in te vullen (selectieve respons);
- mensen die in de politieregistratie bekend zijn als slachtoffer en die gerespondeerd hebben in de VM, ook daadwerkelijk in de VM verklaard hebben slachtoffer te zijn geweest en dit aangegeven te hebben bij de politie (reverse record check);
- mensen die in de VM verklaard hebben slachtoffer te zijn geweest en dit aangegeven te hebben bij de politie, ook in de politieregistratie terug te vinden zijn (forward record check).

Uit verschillende onderzoeken blijkt dat de selectiviteit in respons over alle delicten niet zo groot is. Wel lijken er per delictsoort verschillen te zijn: over het algemeen (met enkele uitzonderingen) zijn slachtoffers van vermogensdelicten wat meer geneigd te responderen dan respondenten die geen slachtoffer waren, terwijl slachtoffers van geweldsdelicten juist minder responderen dan respondenten die geen slachtoffer waren.
Als bij de *reverse record check* blijkt dat een geregistreerd delict niet genoemd is in de VM is er sprake van een *onderrapportage* in de VM. Over alle delicten melden de verschillende onderzoeken onderrapportages uiteenlopend van 8% tot 48%. Het meest complete onderzoek (Reep, 2014) vindt een onderrapportage van 37%, met wel grote verschillen tussen de delictscategorieën. Bij de *forward record check*, waarbij een aangifte zoals gemeld in de VM niet als registratie bij de politie teruggevonden kan worden, is de situatie wat complexer: het kan hier gaan om een overrapportage in de VM, maar ook om een onderrapportage bij de politie (een slachtoffer is daadwerkelijk naar de politie geweest om aangifte te doen, maar dit heeft niet geresulteerd in een registratie). De percentages niet-gevonden registraties

liggen hier in het algemeen wat hoger dan bij de reverse record check. (Reep, 2014) vindt hier ongeveer 50%, maar dit is ook zeer afhankelijk van het type delict.
Er zijn verschillende redenen waarom er kennelijk een discrepantie zit tussen de misdrijven waarvan in de VM verklaard is aangifte gedaan te hebben en de registraties bij de politie. Zo kan de respondent in de VM het voorval verkeerd in de tijd geplaatst hebben (telescoping) of gerubriceerd hebben onder een ander delict. Ook kan het zijn dat niet de respondent, maar iemand anders aangifte heeft gedaan (bijvoorbeeld een huisgenoot).

2.4 Conclusie

Overtredingen, delicten die elders geregistreerd worden, haaldelicten die vanwege een gebrek aan capaciteit niet ontdekt worden en misdrijven met een slachtoffer waarvan geen aangifte gedaan wordt, zijn geen onderdeel van de Politiestatistiek. Deels kan dit ondervangen worden door aanvulling met andere methoden, veel van deze komen in hoofdstuk 3 en 4 aan bod.
Een belangrijke aanvulling op de Politiestatistiek is de slachtofferenquête. In feite wordt met dit instrument voor een specifiek deel van de criminaliteit – namelijk delicten met *personen* als *slachtoffer* – de dark-numberproblematiek voor een groot aantal delicten opgelost. De vraag blijft of respondenten volledig en naar waarheid de vragen in de enquête beantwoorden. Met name bij cybercrime en fraude, maar mogelijk ook bij andere delictsoorten, kan het voorkomen dat de respondent het delict niet als zodanig herkent (of gewoon vergeten is), waardoor de slachtofferenquête niet *volledig* zal zijn. Andere methoden, die niet vanuit het perspectief van het *slachtoffer* maar bijvoorbeeld vanuit het perspectief van *handelingen* of *impact/schade* het aantal delicten benaderen kunnen hier een aanvulling zijn (zie hoofdstuk 3 en 4). Daarnaast kunnen de antwoorden *onjuist* zijn (verkeerd in de tijd geplaatst, verkeerd delict, …). Hiervoor zou mogelijk gecorrigeerd kunnen worden op basis van (verder) onderzoek waarbij de resultaten uit de slachtofferenquêtes vergeleken worden met andere methoden, zoals de Politiestatistiek.

3 Een overzicht van methoden voor het meten van criminaliteit

Naast de in het vorige hoofdstuk behandelde twee 'traditionele' bronnen zijn er nog vele andere bronnen en methoden die gebruikt worden – of mogelijk gebruikt kunnen gaan worden – om criminaliteit of bepaalde verschijningsvormen van criminaliteit te meten. Dit hoofdstuk geeft een overzicht van methoden en beschrijft op hoofdlijnen de werking en de mogelijke toepasbaarheid voor het meten van criminaliteit. De resultaten – waar aanwezig – van het toepassen van methoden komen in hoofdstuk 4 aan bod. Wel zullen in dit hoofdstuk enkele voorbeelden gegeven worden, die overigens niet noodzakelijkerwijs betrekking hoeven te hebben op het meten van criminaliteit. Voor een uitgebreide beschrijving wordt verwezen naar hoofdstuk 3, 4 en 5 van Smit et al. (2018) .

Paragraaf 3.1 is in feite een uitbreiding op hoofdstuk 2. Hier worden bronnen beschreven waarbij direct[17] een deel van de criminaliteit gemeten of geschat wordt door middel van registraties of enquêtes. Waar het hier nog gaat om het meten van een *zichtbaar deel* van de criminaliteit (de geobserveerde criminaliteit) worden in paragraaf 3.2 methoden beschreven die expliciet tot doel hebben ook het *onzichtbare deel* (het dark number) te schatten. Paragraaf 3.3 is een introductie in het gebruik van geheel andersoortige bronnen waarbij met 'big data'-technieken gewerkt wordt, onder meer toegepast op social media. In paragraaf 3.4 wordt ingegaan op triangulatie: het gebruiken van combinaties van methoden om hetzelfde fenomeen te meten.

3.1 Registraties en enquêtes

In deze studie is een inventarisatie gemaakt van aanvullende databronnen (buiten de twee traditionele bronnen) over criminaliteit. Op basis van literatuur- en webresearch is een overzicht gemaakt van mogelijke bronnen die informatie bevatten over één of meerdere vormen van criminaliteit. Daarnaast zijn verschillende instanties en (branche-)organisaties benaderd om na te gaan of zij relevante data in huis hebben. Op basis van een aantal criteria is tot een selectie gekomen van bronnen. Eenmalige dataverzamelingen, bronnen zonder landelijke dekking en van de politiestatistiek afgeleide bronnen zijn bijvoorbeeld niet meegenomen.

Er wordt een onderscheid gemaakt tussen *registraties*, die vaak betrekking hebben op een specifiek delict, en *enquêtes*. De meeste bronnen zijn publiek, dat wil zeggen verzameld door of in opdracht van overheidsinstanties. Maar er zijn ook enkele databronnen die door private partijen gevuld en onderhouden worden.

3.1.1 Registraties

Er zijn negen registraties, vijf publieke en vier private, waarin (onder meer) vormen van criminaliteit geregistreerd worden. De vijf publieke registraties zijn de registra-

[17] Directe methoden zijn methoden die gebruikmaken van data die betrekking hebben op criminaliteit. Indirecte methoden meten of schatten niet de criminaliteit zelf, maar gebruiken andere fenomenen die een indicator kunnen zijn van criminaliteit.

tie Discriminatie.nl, het centraal meldpunt identiteitsfraude en -fouten (CMI), het landelijk meldpunt internetoplichting van de politie (LMIO), de CBS-doodsoorzakenstatistiek en de data van de stichting Coördinatie Mensenhandel. De vier private registraties zijn het Letselinformatiesysteem (LIS), de CIS-databank van verzekeraars, de Fraudehelpdesk en data van de Nederlandse Vereniging van banken (NVB).

Veel van deze registraties geven informatie over fraude en oplichting.

- De fraudehelpdesk richt zich op horizontale fraude (fraude gepleegd door burgers en bedrijven en waarvan burgers en bedrijven het slachtoffer zijn) en onderscheidt 62 verschillende vormen van horizontale fraude onderverdeeld in ongeveer 25 hoofdcategorieën. 80% à 90% van de meldingen betreft fraude via internet.
- Het CMI heeft als doel om slachtoffers van identiteitsfraude (en fouten wanneer het registratiefouten betreft) die in de knel komen te zitten met verschillende instanties te begeleiden bij het herstellen van de problemen. Dit bestand geeft dus informatie over identiteitsfraude waarbij gebruik is gemaakt van identiteitsdocumenten of kopieën daarvan (paspoort, rijbewijs, etcetera), van openbare gegevens (NAW uit bijvoorbeeld telefoonboek), persoonlijke gegevens (zoals DigiD, BSN), etc.
- Het LMIO houdt zich sinds 2010 bezig met aan- en verkoopfraude via internet en geeft dus informatie over internetoplichting waarbij sprake is van een online handelsplaats.
- De CIS-databank wordt beheerd door de stichting Centraal Informatie Systeem (CIS, een organisatie van en voor verzekeraars) en omvat gegevens die van belang zijn voor verzekeraars. In het CIS wordt informatie over verzekeringsfraude bijgehouden. Maar op basis van de claimmeldingen kan ook informatie verschaft worden over andere delicten als woninginbraken, autodiefstal, overige diefstal, brandstichting en verkeersmisdrijven.
- De NVB publiceert cijfers over diverse onderwerpen die van belang zijn voor de bankensector, zoals betalingsverkeer, sparen, beleggingen, maar ook met betrekking tot veiligheid. De delicten waarvan informatie wordt verkregen zijn naast fraude met internetbankieren ook skimming, bankovervallen en aanvallen op geldautomaten, witwassen en financieren van terrorisme.

Een tweetal registraties richten zich op geweldscriminaliteit.

- In het LIS wordt geregistreerd met wat voor soort letsel een patiënt bij de spoedeisende hulp van een ziekenhuis terecht komt. Ondervonden letsel bij slachtoffers als gevolg van geweld wordt vastgelegd. Omdat er ook gevraagd wordt naar relatie dader-slachtofferschap en locatie (indien bekend) kunnen verschillende vormen van geweld worden onderscheiden, zoals huiselijk geweld of geweld in horecagelegenheden.
- De doodsoorzakenstatistiek van het CBS bestaat uit een registratie van alle doodsoorzaken van overleden inwoners van Nederland (ingeschreven in de Basisregistratie Personen). Hieruit kan het aantal slachtoffers van moord en doodslag (het onderscheid tussen deze twee wordt niet gemaakt) bepaald worden.

Ten slotte nog twee registraties die betrekking hebben op specifieke delicten.

- De registratie discriminatie.nl is een verzameling van meldingen van discriminatie die binnenkomen bij de gemeentelijke antidiscriminatievoorzieningen. Meldingen en klachten over discriminatie op diverse gronden, zoals ras, leeftijd, geslacht,

godsdienst, etcetera, worden bijgehouden alsook de aard en maatschappelijk terrein waar het incident heeft plaatsgevonden.
- De stichting Coördinatie Mensenhandel zet zich in voor slachtoffers van mensenhandel. Eén van de kerntaken van CoMensha is het in beeld brengen van en rapporteren over (mogelijke) slachtoffers van mensenhandel in Nederland. Mensenhandel wordt hier uitgesplitst naar seksuele uitbuiting en overige uitbuiting.

3.1.2 Enquêtes

Er zijn acht enquêtes, alle publiek, die informatie geven over vormen van criminaliteit, hoewel dat in de meeste gevallen niet het primaire doel is van deze enquêtes.

De GezondheidsMonitor en de Monitor Seksuele gezondheid in Nederland hebben tot doel een beeld te krijgen van de (seksuele) gezondheid van de Nederlandse bevolking. In de GezondheidsMonitor worden vragen gesteld over drugsgebruik (hoewel de relatie met criminaliteit hier indirect is) en huiselijk geweld en in de Monitor Seksuele gezondheid wordt gevraagd naar seksueel grensoverschrijdend gedrag zoals seksueel geweld en agressie.

De Monitor Sociale Veiligheid in en om Scholen (MSVS) en de Monitor Zelfgerapporteerde Jeugdcriminaliteit (MZJ) richten zich beide (voornamelijk) op jeugdigen. Het doel van de MSVS is om het sociale veiligheidsbeleid, de veiligheidsmaatregelen en ervaren sociale (on)veiligheid in het voortgezet en primair (speciaal) onderwijs in kaart te brengen. Het onderzoek wordt uitgevoerd onder leerlingen, leraren, ouders en leidinggevenden. De volgende vormen van criminaliteit (direct of indirect) worden onderscheiden: discriminatie, wapenbezit, extremisme (religieus of anders), seksuele uitbuiting, pesten, geweld en drugsgebruik. In de MZJ wordt gevraagd naar daderschap van jeugdigen van een groot aantal delicten.

De Nationale Enquête Arbeidsomstandigheden (NEA) is een grootschalig onderzoek onder Nederlandse werknemers. De NEA verschaft informatie voor overheid, werkgevers, vakbonden, brancheverenigingen, etcetera, over een veelheid aan onderwerpen met betrekking tot arbeid, zoals arbeidsomstandigheden, -inhoud, -voorwaarden, dienstverband, gezondheid en arbeidsongevallen. De NEA levert informatie op over pesten, lichamelijk geweld, intimidatie, ongewenste seksuele aandacht en discriminatie van werknemers.
Een specifiek onderzoek naar werkomstandigheden in het Openbaar Vervoer is de Personeelsmonitor OV. Dit is een grootschalig onderzoek onder rijdend en controlerend personeel van openbaar vervoer (stads- en streekvervoer, minus de NS) naar subjectieve en objectieve veiligheid en veiligheidsbeleid van de werkgever. Vandalisme en slachtofferschap van mishandeling, bedreiging, diefstal, lastigvallen, treiteren/pesten van medewerkers in het openbaar vervoer zijn onderwerpen die aan bod komen.
Een andere enquête in het openbaar vervoer is de OV-klantenbarometer. Dit is een klanttevredenheidsonderzoek onder reizigers van alle openbaar vervoerders. Reizigers ontvangen gedurende hun rit een schriftelijke enquête waarin verschillende aspecten met betrekking tot het gebruik van openbaar vervoer bevraagd worden en verschaft onder meer informatie over bedreiging, diefstal en mishandeling/geweld in het openbaar vervoer.

Voor het specifieke delict rijden onder invloed is er het onderzoek Rijden onder Invloed met als doel het alcoholgebruik van bestuurders van motorvoertuigen in weekendnachten vast te stellen.

3.2 Dark number schattingsmethoden

In deze paragraaf worden drie schattingsmethoden beschreven: de multiplier-methode, vangst-hervangstmethoden en sociale-netwerkmethoden.

3.2.1 De multipliermethode

Een veel gebruikte methode om verborgen populaties te schatten (zoals van misdrijven, daders of slachtoffers) is de multipliermethode.[18] Uitgangspunt is een bron waar slechts een deel van een fenomeen gemeten wordt, zoals de door de politie geregistreerde criminaliteit waarvan bekend is dat dit een bepaald deel (*x*%) van de totale criminaliteit in beeld brengt. Het idee achter de multipliermethode is dat er vervolgens een *onafhankelijke* tweede bron wordt gebruikt die een schatting kan geven van de grootte van de onbekende *x*. Zo kan bijvoorbeeld op basis van de politiecijfers een schatting gemaakt worden van de ondervonden criminaliteit door gebruik te maken van het percentage respondenten dat na een slachtofferschap ook zegt aangifte gedaan te hebben. Dit percentage is dan een schatter voor *x*. Eventueel kan dit nog verfijnd worden door het percentage niet voor het totaal maar per delictcategorie te bepalen.[19]
Wel moet aan enkele voorwaarden voldaan worden bij deze methode. Zo moeten bijvoorbeeld beide bronnen onafhankelijk van elkaar zijn en moeten de definities overeenkomen.[20]

3.2.2 Vangst-hervangstmethoden

Vangst-hervangstmethoden zijn vooral bekend uit de biologie voor het schatten van de omvang van dierpopulaties. Een bekend voorbeeld is hoe het aantal vissen in een vijver geteld wordt. Eerst worden er 100 vissen gevangen. Deze worden gemarkeerd en weer teruggezet in de vijver. Na enige tijd worden er weer 100 vissen gevangen. Stel nu dat van deze tweede vangst er 5 gemarkeerd blijken te zijn, dan is de logische veronderstelling dat kennelijk 5% van de vissen gemarkeerd is. En er waren er 100 gemarkeerd, dus de totale populatie vissen in de vijver wordt dan geschat op 100 / (5/100) = 2.000.

Waarschijnlijk het meest toegepast is de vangst-hervangst schattingsmethode die gebruikmaakt van informatie over de overlap van twee (of meer) bestanden die aan elkaar gekoppeld zijn. De verhoudingen tussen de deelpopulaties die in beide bestanden voorkomen en die alleen in het eerste en alleen in het tweede bestand voorkomen kunnen resulteren in een schatting van de deelpopulatie die in geen van beide bestanden voorkomt.

Maar de vangst-hervangstmethode kan ook goed uitgevoerd worden op één bestand, waarin bij een steekproef leden van de populatie één, twee of meer keer kunnen voorkomen. De verborgen populatie bestaat dan uit de leden van de popu-

---

[18] Wiskundig gezien is de multipliermethode niets anders dan een bijzonder geval van vangst-hervangst. In de praktijk, en ook in dit rapport, worden de twee methoden vaak gescheiden gepresenteerd.

[19] Soms is de multiplier zo vanzelfsprekend dat deze impliciet gebruikt wordt. Zo wordt het percentage slachtofferschappen uit de slachtofferenquête (hier als primaire bron) vermenigvuldigd met de bevolkingsaantallen uit de bevolkingsstatistiek (onafhankelijke tweede bron) om tot een totaalaantal slachtofferschappen te komen.

[20] In de praktijk wordt – door gebrek aan volkomen onafhankelijke bronnen – niet altijd (geheel) voldaan aan de voorwaarden.

latie die *niet* in de steekproef voorkomen. Een veelgebruikt model is hier het afgeknotte Poisson regressiemodel. Op basis van de gemeten frequenties van leden van de populatie die één, twee, drie, … keer voorkomen wordt de verborgen populatie geschat, onder de veronderstelling dat de geobserveerde frequenties een Poisson kansverdeling volgen. Zo is deze methode bijvoorbeeld gebruikt bij het schatten van het aantal dronken rijders, waarbij mensen één keer of vaker gepakt worden.

Ook bij vangst-hervangsmethoden moet aan een aantal voorwaarden voldaan worden om betrouwbare resultaten te verkrijgen. Zo is een belangrijke voorwaarde (die waarschijnlijk het vaakst wordt geschonden) bij de methode met twee of meer bestanden dat de bestanden onafhankelijk zijn, zodat de kans om in het eerste bestand te worden geregistreerd onafhankelijk is van de kans om te worden geregistreerd in het andere bestand. Dit wordt ondervangen in het afgeknotte Poisson model, omdat daar sprake is van slechts één bestand. Wel speelt hier de aanname van onafhankelijkheid van observaties: de kans op het observeren van een lid van de populatie mag niet veranderen als gevolg van het optreden van een eerdere observatie. Dit is in de praktijk lastig. Zo is het niet ondenkbaar dat het gedrag van dronken rijders wijzigt na een (of meer) keer 'gepakt' te zijn. Om tegemoet te komen aan aannameschendingen worden dan ook met enige regelmaat nieuwe varianten van het afgeknotte Poisson regressiemodel ontwikkeld.

3.2.3 Sociale-netwerkmethoden

Sociale-netwerkmethoden zijn methoden die gebruikmaken van de sociale context van (initiële) respondenten. Het idee is dat aan respondenten gevraagd wordt nieuwe respondenten te zoeken uit hun eigen kennissenkring of vragen te beantwoorden over het gedrag van personen uit hun kennissenkring.

Bij *Respondent Driven Sampling* (RDS) is de doelstelling om een representatieve steekproef te verkrijgen, van waaruit mogelijk schattingen voor verborgen populaties gemaakt kunnen worden. Uitgaande van een kleine (waarschijnlijk selctieve) steekproef van initiële respondenten wordt aan deze respondenten gevraagd andere mogelijke respondenten uit hun kennissenkring aan te leveren. Deze nieuwe respondenten worden vervolgens weer gevraagd andere respondenten aan te dragen etcetera. Het idee is – ook hier afhankelijk van een aantal aannames – dat na een aantal stappen een representatieve steekproef verkregen wordt. Deze methode is bijvoorbeeld gebruikt om schattingen te verkrijgen van het aantal drugsgebruikers en het aantal HIV-geïnfecteerden.

Een verwante methode is *network scale-up*. De doelstelling van deze methode is expliciet om omvangsschattingen te krijgen van verborgen populaties. Zo is deze methode voor het eerst gebruikt voor de schatting van het aantal dodelijke slachtoffers van de aardbeving in Mexico in 1985. De schatting baseerde zich op een survey waarin de respondenten is gevraagd het aantal personen uit hun familie-, vrienden- en kennissenkring weer te geven dat is overleden ten gevolge van de aardbeving. Kenmerkend aan de methode is dat de respondenten in een surveyonderzoek niet om hun *eigen* gedrag wordt gevraagd maar om het gedrag van de mensen in hun sociale netwerk. Deze methode kwam naar voren als kansrijk bij een vooronderzoek naar jeugdige cybercriminelen.

Waar het voordeel van deze netwerkmethoden ligt in het op deze manier beter kunnen bereiken van groepen die anders lastig te bereiken zijn, zijn er ook enkele mogelijke nadelen. Aangezien de respondenten de steekproef bepalen ontstaat

mogelijk een selecte steekproef. Alleen als de methode optimaal zijn werk kan doen dan ontstaat er een steekproef met kenmerken die vergelijkbaar zijn van die van een aselecte steekproef. Wel moet worden gezegd dat het bereiken van een steekproef met deze optimale kenmerken een arbeidsintensieve en dus kostbare aangelegenheid betreft.Dit maakt het generaliseren van sociale-netwerkdata, bijvoorbeeld bij omvangschattingen, problematisch. Er kunnen vertekeningen en clustereffecten optreden. Vertekening treedt op wanneer geen rekening wordt gehouden met verschillen in de omvang van de persoonlijke netwerken van de respondenten. Personen met grotere netwerken hebben grotere kans om in de steekproef te vallen dan personen met kleinere sociale netwerken. Clustereffecten kunnen optreden als de respondenten niet onafhankelijk van elkaar geselecteerd worden. Als de aangebrachte personen weinig verschillen vertonen met de initiële respondenten, bijvoorbeeld omdat ze in dezelfde omstandigheden leven of dezelfde denkbeelden hebben, leveren de nieuw geworven personen minder nieuwe informatie op dan de initiële respondenten.

3.3 'Big data' en sociale media

De tot nu toe in paragraaf 3.1. en 3.2 beschreven methoden, hoewel soms gebruikmakend van nieuwe technieken, zijn gebaseerd op het gebruik van meer reguliere dataverzamelingen voor schatting van criminaliteitscijfers, zoals registers en enquêtes. In deze paragraaf onderzoeken we de bruikbaarheid van geheel andersoortige dataverzameling en methoden. Er worden twee bronnen gepresenteerd die in potentie zouden kunnen bijdragen aan het beantwoorden van dark-numbervraagstukken, te weten sociale-mediadata en Google data.

3.3.1 Sociale-mediadata

Sociale media is een verzamelnaam voor alle internettoepassingen waarmee informatie tussen mensen wordt gedeeld op een gebruiksvriendelijke en persoonlijke of meer zakelijke wijze. Het betreft informatie in de vorm van tekst (zoals nieuws), geluid (denk aan podcasts) en beeld (fotografie, video), die wordt gedeeld via social media platforms. Bij sociale media draait het vooral om *user generated content,* die door de website-bezoekers online wordt gezet. De essentie van sociale media is dat er een online platform is waar de gebruikers de inhoud verzorgen, zonder of met minimale tussenkomst van een professionele redactie.

Doordat sociale media door zo veel mensen vaak intensief worden gebruikt,[21] worden er dagelijks enorme hoeveelheden data gegenereerd. Derhalve is de verwachting dat het steeds beter mogelijk moet zijn om op basis van deze data uitspraken te doen over deelpopulaties of over de samenleving in zijn geheel. Sociale-mediadata is bijvoorbeeld beschikbaar van Coosto, een Eindhovens techbedrijf dat dagelijks 400.000 online bronnen bezoekt en de data opslaat en rubriceert. Coosto beheert inmiddels een database waarin miljarden documenten, posts en (nieuws)berichten zijn opgeslagen vanaf 2009.
Fluctuaties in berichtgeving over (bepaalde vormen van) criminaliteit zouden dan mogelijk iets kunnen zeggen over de prevalentie van fenomenen of over mediahypes. Er zijn echter nog geen voorbeelden bekend van het gebruik van sociale

[21] Zo heeft in Nederland 97% van de bevolking van 12 jaar en ouder toegang tot internet en is het gebruik van social media hoog en stijgend.

media voor het meten van criminaliteit. Als illustratie van de mogelijkheden dient wel het voorbeeld waarbij een sentimentsindex werd bepaald door het aantal negatieve berichten in de Coosto-database af te trekken van het aantal positieve berichten. Dit bleek een sterk verband te hebben met de consumentenindex zoals die door het CBS middels een enquête gemeten wordt.

3.3.2 Google data

De zoekmachine van Google heeft in Nederland een marktaandeel van 93%. Het is dus niet gek om te veronderstellen dat (fluctuaties in) zoekgedrag van burgers ons iets kan vertellen over fenomenen die zich voordoen in de 'echte wereld'. Fluctuaties in het gebruik van zoektermen kunnen via Google Trends worden opgevraagd. Google Trends laat zien hoe vaak een bepaalde zoekterm is ingevoerd en relateert dit aan het totale zoekvolume in een land of een regio. Google Trends levert dus relatieve getallen (0-100) op, maar wel met terugwerkende kracht vanaf het jaar 2004. Een andere tool is Google Correlate. Deze tool verwacht een willekeurige tijdreeks als input (per maand een bepaalde waarde).
Google Correlate laat vervolgens een algoritme los op miljoenen kandidaat-zoektermen en presenteert de zoektermen die de hoogste correlatie hebben met de ingevoerde tijdreeks.
Als voorbeeld is de (CBS-)tijdreeks 'aantal faillissementen per maand' aangeboden aan Google Correlate. Deze blijkt een hoge correlatie te hebben met zoektermen als 'WW', 'Doorstart', en 'Credios'.[22]

3.3.3 Mogelijkheden voor het meten van dark number van criminaliteit

Met de voorbeelden in de vorige twee paragrafen wordt aannemelijk gemaakt dat het (soms) mogelijk is om direct waargenomen of klassiek gemeten fenomenen te beschrijven met behulp van alternatieve databronnen. De voorbeelden gaan echter niet over het dark number van criminaliteit. Er is hier immers een grote beperking: bij het dark number zijn er per definitie geen tijdreeksen waar social mediadata en Google data aan gerelateerd kunnen worden. Wel kan gekeken worden met welke frequentie wordt gesproken over of gezocht op fenomenen die te maken hebben met (bepaalde vormen van) criminaliteit. De achterliggende idee is dat wanneer (nieuwe) fenomenen zich (vaker) voordoen, en het slachtofferschap toeneemt, mensen (vaker) gaan zoeken naar het betreffende fenomeen op Google of hier melding van maken via social media. In feite wordt criminaliteit hier bezien vanuit het perspectief '' handeling' (zie figuur 1.1 in Smit et al., 2018). Als voorbeeld is voor het fenomeen 'ransomware' gebruikgemaakt van sociale data, Google Trends en Google Correlate. De resultaten komen in hoge mate overeen en in het voorjaar 2017 is duidelijk de verspreiding van de 'wannacry' malware te zien. Hoewel er wel trends te onderscheiden zijn blijft het een probleem om absolute omvangsschattingen te maken.

3.4 Combinaties van methoden

Bij dark-numberschattingen wordt de omvang van een deels verborgen populatie geschat. Inherent aan een verborgen populatie is dat deze niet volledig waargenomen kan worden en dat een (eenvoudige) directe check op de juistheid van de

[22] Credios is een incassobureau.

schatting derhalve niet mogelijk is. Door het combineren van verschillende methoden in het bestuderen van hetzelfde fenomeen (triangulatie) kan dit enigszins ondervangen worden. Het idee achter triangulatie is dat men meer vertrouwen kan hebben in een onderzoeksresultaat, bijvoorbeeld een dark-numberomvangschatting, als het resultaat van de schatting gevalideerd is door – bij voorkeur onafhankelijk – onderzoek met een andere dataset, onderzoeker, theoretisch kader of methode. Triangulatie wordt met enige regelmaat toegepast bij onderzoek naar verborgen populaties, zoals bij onderzoek naar slachtoffers en daders van huiselijk geweld waarbij een onderzoek op basis van vangst-hervangst getrianguleerd is met een survey onder slachtoffers van huiselijk geweld.

3.4.1 Een voorbeeld van triangulatie

Box 3.1 geeft een voorbeeld van triangulatie. Voor het bepalen van de omvang van het delict 'diefstal met geweld' zijn er drie bronnen voorhanden: de politieregistratie, de VM en de MZJ. Alle drie deze bronnen hebben in meer of mindere mate te kampen met onvolledigheid en onnauwkeurigheid en geen van de drie meet direct het aantal delicten. Voor elk van de drie methoden wordt nu een schatting gemaakt van het aantal delicten 'diefstal met geweld', waarbij – onder zekere aannames – de resultaten van de methoden onderling en van enkele elders gevonden resultaten gebruikt worden. Hierbij wordt ook veelvuldig gebruikgemaakt van de multiplier-methode, bijvoorbeeld om de resultaten van de MZJ te 'vertalen' naar de volledige populatie daders. Overigens wordt ook in dit voorbeeld niet geheel aan de voorwaarde van onafhankelijkheid van bronnen en/of methoden voldaan. Zo wordt de multiplier van 47% (straatroof ten opzichte van totaal diefstal met geweld) bij twee van de drie methoden gebruikt.

Bij triangulatie zullen er altijd verschillen in de uitkomsten zijn. In het voorbeeld zijn er drie uitkomsten: respectievelijk 24, 31 en 43 duizend delicten diefstal met geweld. De vraag is dan hoe deze verschillende uitkomsten te interpreteren. Als de uitkomsten van dezelfde orde van grootte zijn dan voldoet wellicht een gemiddelde van de uitkomsten als acceptabele schatting.[23] Zijn de uitkomsten sterk verschillend dan kan dit aanleiding geven tot nadere analyse van de berekeningen. Zijn bijvoorbeeld de juiste multipliers toegepast en zijn die voldoende betrouwbaar? Of is er bijvoorbeeld een onderrapportage waarvoor (nog) niet gecorrigeerd is? Dit laatste zou in het voorbeeld de lage uitkomst van de MZJ kunnen verklaren waarbij het vermoeden bestaat dat respondenten nogal eens hun gepleegde delicten verzwijgen.

[23] Waarbij het begrip 'dezelfde orde van grootte' natuurlijk subjectief is: de een zal een verschil van een factor 2 tussen de laagste en de hoogste waarde acceptabel vinden, terwijl een ander een verschil van 10% al te veel vindt.

Box 3.1 Triangulatie bij bepaling aantal delicten 'diefstal met geweld'

Allereerst de relevante karakteristieken en resultaten[a] van elke methode afzonderlijk.

Politieregistratie
- Is niet volledig en indirect, omdat alleen geregistreerde delicten geteld worden. Bij vergelijk met de VM blijkt de registratie – althans in combinatie met de VM – onnauwkeurig te zijn. Zie hoofdstuk 2.
- Het aantal geregistreerde delicten 'diefstal met geweld' is 9.040, waarvan 4.250 'straatroof'.
- Het totale aantal verdachten van 'diefstal met geweld' is 4.660 (4.090 uniek). Dat wil zeggen een verdachte pleegt per jaar gemiddeld 4.660 / 4.090 = 1,14 delicten.
- Het aantal *jeugdige* verdachten (12-17) van 'diefstal met geweld'is 1.290 (1.010 uniek).

VM
- Is (onder andere) niet volledig, omdat alleen gevraagd wordt naar slachtofferschap van straatroof.
- Voor de onnauwkeurigheid zie de opmerking bij de Politieregistratie.
- Aantal delicten overeenkomend met straatroof: 27.800
- Percentage dat zegt aangifte te doen: 29,1%

MZJ
- Is niet volledig, omdat alleen naar straatroof gevraagd wordt en het alleen gaat om delicten waar een jeugdige dader bij betrokken was.
- Is indirect omdat daders en geen delicten geteld worden.
- Aantal jeugdige (12-17 jaar) daders van delict overeenkomend met straatroof: 2.431

Daarnaast worden de volgende resultaten uit andere onderzoeken gebruikt:
NVI synthesestudie (Cuyper et al., 2015)
- Voor geweldsdelicten moet een factor 0,82 toegepast worden op de resultaten van de VM om eenzelfde onder/overrapportage te hebben als het meest voorkomende delict diefstal.

Overige bevindingen:
- Uit (Van Dijk, 1992) is bekend dat er bij 12% van de respondenten in slachtofferenquêtes sprake is van forward telescoping. Dit resulteert in een correctiefactor van 0,88.

Ten slotte zullen de berekeningen gebaseerd zijn op de volgende aannames: (Aannames 1-3 zijn in feite multipliers).
- *Aanname 1:* Het percentage geregistreerde straatroven ten opzichte van totaal diefstal met geweld (4.250 / 9.040 = 47,0%) is algemeen toepasbaar (dus ook op slachtofferschappen en daderschappen).
- *Aanname 2:* Het aangiftepercentage voor straatroof (29,1%) geldt ook voor diefstal met geweld totaal.
- *Aanname 3:* De verhouding unieke jeugdige verdachten ten opzichte van totaal unieke verdachten voor diefstal met geweld totaal bij de politie (1.010 / 4.090 = 24,7%) geldt ook voor straatroof.
- *Aanname 4:* De bij de NVI gevonden correctiefactor 0,82 voor geweldsdelicten ten opzichte van diefstal is een aanvaardbare benadering van de benodigde correctiefactor diefstal met geweld ten opzichte van misdrijven totaal.
- *Aanname 5:* De algemene correctiefactor 0,88 voor forward telescoping geldt ook voor diefstal met geweld

Voor elk van de drie methoden kunnen we nu, gebruikmakend van resultaten uit de andere bronnen, een schatting maken van het aantal delicten.
- Aantal delicten uitgaande van Politieregistratie (perspectief geregistreerd feit) is onder aanname 2:
  9.040 / (29,1/100) = *31.065*
- Aantal delicten uitgaande van VM (perspectief slachtofferschap) is onder aannames 1, 4 en 5:
  (27.800 / (47,0/100)) * 0,82 *0,88 = *42.700*
- Aantal delicten uitgaande van MZJ (perspectief daderschap) is onder aannames 1 en 3:
  ((2.431 / (47,0/100)) / (24,7/100)) * 1,14 = *23.860*

[a] Bij de Politieregistratie en de VM betreft het 2016, bij de MZJ 2015.

3.5 Conclusie

In dit hoofdstuk is gekeken naar bronnen en methoden – buiten de twee 'traditionele' bronnen (politieregistraties en slachtofferenquêtes) die in hoofdstuk 2 aan bod kwamen – die gebruikt (kunnen) worden voor het meten van criminaliteit en daarmee ofwel bijdragen aan de kennis over de geobserveerde criminaliteit, ofwel gebruikt kunnen worden om meer inzicht te krijgen in het dark number.
Allereerst valt op dat er eigenlijk al veel bronnen en methoden zijn die buiten de twee traditionele bronnen informatie geven over de omvang van de criminaliteit. Met andere woorden, de geobserveerde criminaliteit is duidelijk groter dan de geregistreerde en ondervonden criminaliteit. Kenmerkend is dat deze methoden doorgaans slechts een deel van de criminaliteit in kaart pogen te brengen (bijvoorbeeld alleen overtredingen of alleen slachtoffers van moord of doodslag) en dat vaak vanuit een specifiek perspectief, zoals dader of impact/schade. Ook komt het nogal eens voor dat deze methoden onregelmatig of slechts eenmalig gebruikt zijn of zelfs gestopt zijn.

Hoewel er dus uit verschillende bronnen redelijk wat bekend is over de criminaliteit, blijft er nog wel een verborgen deel over, het dark number. Met name de vangst-hervangstmethoden en de netwerkmethoden alsook de social media en big-data-technieken, zijn interessant om dit dark number verder te onderzoeken. Wat opvalt, is dat het hier vaak gaat om methoden en technieken die al veelvuldig in andere disciplines gebruikt worden (biologie en medische wetenschappen), maar – met uitzondering van de vangst-hervangstmethoden – (nog) niet voor criminaliteit.

4 Bevindingen naar delictcategorie of verschijningsvorm

Met als indeling de delictclassificatie zoals gepresenteerd in paragraaf 1.3.2 worden hier de huidige bronnen en methoden per delicttype of verschijningsvorm gepresenteerd. Kort wordt ingegaan op de bronnen die gebruikt zijn, de gevonden aantallen en de implicaties – voor zover bekend – voor het dark number. Vanwege het inventariserend karakter van deze studie is in het algemeen geen gedetailleerd onderzoek gedaan naar de cijfermatige verschillen tussen de verschillende bronnen. Op hoofdlijnen wordt wel aangegeven waar deze verschillen naar de mening van de auteurs plausibel zijn of substantieel zijn. In het bijzonder wordt ingegaan op de vraag of andere bronnen meerwaarde (kunnen) hebben ten opzichte van de Politiestatistiek en de VM. Gepresenteerde aantallen uit de Politiestatistiek en de VM hebben betrekking op het jaar 2017.

Voor meer details wordt verwezen naar hoofdstuk 3, 6, 7 en 8 in Smit et al. (2018) en voor een cijfermatig overzicht naar bijlage 6 van Smit et al. (2018). In het bijzonder wordt in dit hoofdstuk veel aandacht besteed aan de delicten mensenhandel, horizontale fraude, georganiseerde criminaliteit en cybercrime. In feite zijn dit uitgebreide samenvattingen van de hoofdstukken 6, 7 en 8 in Smit et al. (2018) en hier wordt ook ingegaan op de bronnen en methoden die specifiek voor deze delicten gebruikt (kunnen) worden.

4.1 Levensdelicten

Voor levensdelicten zijn drie bronnen beschikbaar: de CBS-Politiestatistiek, de CBS-Doodsoorzakenstatistiek en de jaarlijkse lijst met moorden zoals gepubliceerd door Elsevier. De Politiestatistiek is breder dan de andere twee (hier worden ook pogingen en andere levensdelicten dan moord en doodslag meegeteld) en meet vanuit het perspectief van het aantal geregistreerde feiten en daderschap . De andere twee bronnen gaan uit van slachtofferschap en meten alleen de voltooide moorden en doodslagen. Het is dan ook niet verwonderlijk dat de Politiestatistiek een groter aantal levensdelicten telt (3.000 per jaar) dan de andere twee bronnen (beiden ruim 100 per jaar).
Hoewel niet uit te sluiten valt dat een aantal *voltooide* moorden/doodslagen onopgemerkt blijft (vermissingen, een schouwarts die ten onrechte een natuurlijke dood vaststelt) zal het dark number hier mogelijk niet al te groot zijn. Bij de *andere* levensdelicten is de situatie minder duidelijk. Vanwege de ernst van de delicten zal er eerder een aangifte komen dan bij minder ernstige misdrijven. Verder is het niet onmogelijk dat deze delicten ook onderdeel zijn van (geteld worden bij) de VM, zij het onder een andere noemer (mishandeling of bedreiging).

4.2 Geweldsdelicten

4.2.1 Vermogensdelicten met geweld

Onder vermogensdelicten met geweld vallen een aantal soorten delicten (hoewel alles valt onder één artikel Sr, namelijk artikel 312: diefstal met geweld). Naast de CBS-Politiestatistiek die vanuit het perspectief van geregistreerde feiten en dader-

schap alles van artikel 312 Sr telt, zijn andere bronnen de VM (perspectief slachtofferschap) en de MZJ (vanuit perspectief daderschap). Deze laatste twee meten echter slechts een deel van diefstal met geweld namelijk alleen 'straatroof'. In box 3.1. is op basis van de uitkomsten van alle drie de bronnen een schatting gemaakt van de geobserveerde omvang van vermogensdelicten met geweld. De resultaten lopen uiteen van 24.000 tot 43.000 per jaar.
Net als bij levensdelicten is de verwachting dat voor dit delict het dark number niet al te groot zal zijn. Immers, met name in de VM zal een respondent vanwege de ernst van het delict over het algemeen aangeven slachtoffer te zijn geweest (los van de vraag of het delict ook aangegeven wordt).[24] Dit is ook aannemelijk omdat de schatting op basis van de VM de hoogste van de drie schattingen is.

4.2.2 Seksuele delicten

Naast de Politiestatistiek en de VM zijn er diverse andere bronnen die informatie kunnen geven over seksuele delicten: de Monitor Seksuele gezondheid, de Nationale Enquête Arbeidsomstandigheden (NEA) vanuit het slachtofferperspectief, de MZJ (daderperspectief) en de MSVS (zowel daders als slachtoffers). Mede omdat de verschillende bronnen zeer uiteenlopende definities en doelgroepen kennen zijn de resultaten in hoge mate verschillend. Zo loopt het aantal slachtoffers uiteen van 15.000 (VM) tot 460.000 (NEA). Wel zijn de resultaten van de Politiestatistiek en de VM – bij het tellen van het aantal delicten – redelijk met elkaar in overeenstemming: 8.000 (Politiestatistiek) en 22.000 (VM), zeker omdat uit de VM blijkt dat ruwweg een op de drie slachtoffers aangifte doet.[25] Immers, bij gebruik van dit aangiftepercentage als multiplier voor de Politiestatistiek zou het aantal delicten op 24.000 komen.
Bij seksuele delicten spelen twee zaken een rol die het moeilijk maken – wellicht onmogelijk – een goed beeld te krijgen van het dark number. Ten eerste is er de schaamte en het taboe die om dit soort delicten hangen, waardoor ze verborgen blijven. Ten tweede zijn er – zowel voor de dader als het slachtoffer – diffuse grenzen tussen wat gewenst is, wat ongewenst is en wat strafbaar is. Het gaat bij dit laatste niet zozeer om onduidelijkheden in de wet, maar veel meer om de interpretatie van dader en slachtoffer van een specifieke gebeurtenis.

4.2.3 Mishandeling

De bronnen voor mishandeling zijn deels dezelfde als bij seksuele delicten. Dit betreft de Politiestatistiek, de VM, de NEA, de MZJ en de MSVS. Daarnaast is er ook het LIS, waarbij slachtoffers van geweld geregistreerd worden die bij de spoedeisende hulp komen. Ook zijn er twee bronnen specifiek gericht op het Openbaar Vervoer: de Personeelsmonitor Vervoer die slachtofferschap onder personeel meet en de OV-Klantenbarometer die slachtofferschap onder reizigers meet. Vanwege verschillende vraagstelling en doelgroepen lopen ook hier de resultaten ver uiteen. Zo zit er een groot verschil tussen LIS (18.000 slachtoffers), de VM (98.000 slachtoffers) en NEA (505.000). Dat het LIS een lager aantal slachtoffers laat zien dan de VM is begrijpelijk: het gaat hier alleen om slachtoffers die op de spoedeisende hulp terechtkomen. Het verschil met de NEA is lastiger te duiden, mogelijk dat de vraag-

[24] Tevens blijkt uit de analyse van respons (zie tabel 2.1 in Smit et al., 2018) – dat slachtoffers van diefstal met geweld iets meer dan gemiddeld geneigd zijn te responderen.

[25] Dit is een zeer grof gemiddelde over de afgelopen jaren. Het aangiftepercentage in de VM voor seksuele delicten laat van jaar op jaar zeer grote mutaties zien.

stelling hier debet aan is. Ook hier is het aantal delicten zoals geteld door Politiestatistiek (45.000) en VM (138.000) redelijk vergelijkbaar aangezien 34% van de slachtoffers zegt aangifte te doen. Bij het gebruik van de 34% als multiplier voor de Politiestatistiek zou het aantal delicten op 132.000 komen.
De reserves ten aanzien van het dark number zoals hiervoor genoemd bij seksuele delicten gelden hier niet of in mindere mate. Nadere analyses op de diverse bronnen en het gebruikmaken van multipliers in combinatie met triangulatie kan mogelijk inzicht opleveren in de omvang van het dark number.

4.2.4 Bedreiging/bedreiging met geweld

De beschikbare bronnen voor het delict bedreiging zijn dezelfde als bij mishandeling. Ook hier lopen de resultaten fors uiteen: van 271.000 slachtoffers (VM) tot 1.613.000 (NEA). Wat hier met name lijkt te spelen is het verschil tussen door respondenten gepercipieerde bedreiging en gedrag dat daadwerkelijk strafbaar is. En anders dan bij seksuele delicten en mishandeling is hier nu een duidelijk verschil tussen het aantal delicten in de Politiestatistiek (24.000) en de VM (463.000). Dit verschil kan slechts deels verklaard worden door het aangiftepercentage (ongeveer 15%). Bij het gebruik van dit percentage als multiplier voor de Politiestatistiek zou het aantal delicten op 160.000 komen.
Vergelijkbaar met seksuele delicten is het probleem van het bepalen van het dark number voor bedreiging niet zozeer een gebrek aan bronnen maar meer het afstemmen van de juridische definitie in het wetboek van Strafrecht enerzijds op de vraagstelling richting respondent anderzijds.

4.2.5 Stalken

Alleen de Politiestatistiek en de VM geven informatie over stalken. Er is wel een groot verschil: de VM heeft het uitsluitend over 'on-line'-stalken als onderdeel van slachtofferschap van cybercrime. Aangezien het aangiftepercentage bij cybercrime zeer laag is (13% terwijl het aangiftepercentage voor delicten totaal 34% is), is het dan ook te verwachten dat de tellingen/schattingen van het aantal delicten fors verschilt: van 3.000 in de Politiestatistiek tot 64.000 in de VM.
De omvang van het dark number van het 'normale' stalken is lastig te bepalen aangezien de Politiestatistiek de enige bron is. Voor het 'on-line'-stalken zie paragraaf 4.5 over cybercriminaliteit.

4.2.6 Mensenhandel

Verschillende organisaties en onderzoekers proberen het aantal slachtoffers van mensenhandel in kaart te brengen. In Nederland is dat vooral de Nationaal Rapporteur Mensenhandel die de registraties van de stichting Coördinatie Mensenhandel analyseert en in 2017 ook een schatting heeft gegeven van het aantal slachtoffers. Internationaal zijn de *International Labour Organisation en de Global Slavery Index* van de *Walk Free Foundation* de meeste bekende metingen.
De meest gebruikte methode voor data-analyse bij het schatten van de omvang van slachtoffers van mensenhandel is de vangst-hervangstmethode, of de variant daarop: *multiple systems estimation* (MSE-methode). Door het toevoegen van covariaten en meer beschikbare data lijkt het meest recente MSE-model voor het eerst stabiel over tijd en passend bij de Nederlandse verwachtingen (cf. slachtoffermonitor mensenhandel 2012-2016 van de nationaal rapporteur mensenhandel). Er is inmiddels een redelijke betrouwbare schatting beschikbaar voor vijf groepen slachtoffers die in Nederland het vaakst voorkomen binnen de registraties. Wel zou meer

informatie het model nog betrouwbaarder en stabieler kunnen maken. Dat zal mettertijd gebeuren, omdat er steeds meer jaren aan worden toegevoegd. Een andere mogelijkheid is het toevoegen van extra databronnen, zoals medische informatie of verdachte advertenties op internet over seksuele diensten. Ook hierbij geldt dat het belangrijk is dat de koppeling van databronnen mogelijk is.
Kenmerkend is dat al deze bronnen en methoden uitgaan van het slachtofferschap. Alleen de Politiestatistiek telt delicten en daders. De schatting van het aantal slachtoffers is hoger dan de registratie in de Politiestatistiek (690 delicten). De meeste schattingen uitgaande van de registraties van de stichting Coördinatie Mensenhandel komen op in de orde van 7.000 slachtoffers.
Het is onbekend in welke mate deze geobserveerde criminaliteit (7.000 slachtoffers) verschilt van het daadwerkelijke aantal. Andere methoden (zoals bijvoorbeeld *respondent driven sampling*) kunnen hier mogelijk uitsluitsel over geven.

4.3 Vermogensdelicten

4.3.1 Diefstal

Met als mogelijke uitzondering online-criminaliteit en/of cybercrime, is diefstal het delict dat het meeste voorkomt in de statistieken. Naast de Politiestatistiek en de VM rapporteren ook de al eerder genoemde MZJ, Personeelsmonitor OV en de OV-klantenbarometer over diefstallen. Daarnaast is een interessante bron de CIS Databank van verzekerings-maatschappijen), deze is echter niet openbaar en ook niet onafhankelijk van de Politiestatistiek. Immers, over het algemeen is een aangifte bij de Politie vereist om een diefstal te kunnen claimen. Onder andere vanwege een vrij laag aangiftepercentage (in de orde van grootte van 1 op 4) is er een groot verschil tussen het aantal delicten in de Politiestatistiek (285.000) en de VM (1.736.000). Met als perspectief de dader (hier de jeugdige dader van 10-22 jaar) komt de MZJ op 447.000 daders. Als dit cijfer gecorrigeerd wordt voor daders algemeen en rekening houdend met het feit dat één dader meerdere diefstallen kan plegen, lijkt het aantal gevonden in de VM plausibel (en wellicht in verband met het telescoping effect eerder aan de hoge kant) en zal er mogelijk geen substantieel dark number zijn.

4.3.2 Inbraak

Voor inbraak in totaal (zowel woninginbraak als andersoortige inbraak) zijn naast de Politiestatistiek, die 177.000 delicten telt, geen andere bronnen beschikbaar. Wel zijn er enkele databronnen beschikbaar die specifiek over woninginbraken rapporteren. Het gaat hier vooral om de VM, de MZJ en de CIS Databank waarin het Verbond van Verzekeraars jaarlijks rapporteert over het aantal schadeclaims in verband met woninginbraken. Waar de aantallen van de Politiestatistiek (49.000 delicten), CIS (64.000 schadeclaims) en de MZJ (10.000 jeugdige daders) redelijk met elkaar overeen komen, is het aantal delicten geschat door de VM hoog met 232.000 delicten. Dit kan verklaard worden doordat hier ook de pogingen tot inbraak meegenomen zijn, die echter niet of minder tot een aangifte of schadeclaim zullen leiden. Voor (voltooide) inbraken lijken de aantallen in de Politiestatistiek en CIS een redelijke benadering te geven van de werkelijke aantallen, zeker omdat er doorgaans sprake is van verzekerde schade.

4.3.3 Fraude/bedrog

Het delict fraude kent veel verschijningsvormen en de meeste databronnen rapporteren over één of enkele subtypen van dit delict. Zo zijn er bijvoorbeeld naast de Politiestatistiek en de VM: de MZJ, het Centraal Meldpunt Identiteitsfraude, de CIS-Databank, het Landelijk Meldpunt Internet Oplichting (LMIO) en de Fraudehelpdesk. De enige bronnen die in het algemeen iets zeggen over fraude (en bedrog en oplichting) is de Politiestatistiek en de Fraudemonitor van het OM.

Horizontale fraude algemeen

Horizontale fraude[26] heeft betrekking op gevallen van bedrog waar burgers of organisaties slachtoffer van zijn geworden. Fraude verhult zich altijd als een bonafide handeling of transactie. Dit maakt het vaak moeilijk om frauduleuze handelingen van bonafide handelingen te onderscheiden. Strafrechtelijk moet er sprake zijn van een element van valse voorwendselen. In de perceptie van de benadeelde is dit element echter van ondergeschikt belang: men *ervaart* simpelweg dat men is opgelicht, of dat nu strafrechtelijk zo is of niet.

Het feit dat fraude een malafide handeling binnen het reguliere economische verkeer betreft, zou wel eens een zegen kunnen zijn. Dit economische verkeer wordt steeds beter en steeds gedetailleerder bijgehouden in allerhande registratiesystemen die voor dat specifieke verkeer zijn ingericht. Door binnen een register grote aantallen records onderling en door te tijd te vergelijken, kunnen er afwijkende patronen worden gedetecteerd die een aanwijzing zijn dat er van frauduleuze handelingen sprake is. De mogelijkheden tot detectie worden nog veel krachtiger als er meerdere informatiesystemen uit meerdere domeinen worden gekoppeld en afzonderlijke gevallen in een bepaalde context worden geplaatst (bijvoorbeeld in netwerken) en als er combinaties van beslisregels in de analyse worden gebruikt. De crux is om op groepsniveau patronen te herkennen in de denk- en handelswijze van fraudeurs die het mogelijk maken om op het niveau van individuele cases voorspellingen te doen. In de private sector worden dit type geavanceerde big-data-analyses reeds op grote schaal toegepast (verzekeringsfraude, zakelijke informatie en kredietchecks).

In het Wetboek van Strafrecht worden hoofzakelijk algemene vormen van fraude onderscheiden. Deze algemene vormen zeggen niet veel over het type fraude waarvan in een bepaalde situatie sprake is. Het zijn veeleer terugkerende elementen in fraudegevallen. Ten behoeve van de kwalificatie van fraudedelicten worden er daarom zogenoemde *maatschappelijke classificaties* toegekend.

Ten opzichte van 2015 is er sprake van een significante *stijging* van het aantal aangemelde fraudezaken. Horizontale fraude is daarmee een van de weinige typen criminaliteit waarbij er sprake is van een toename van het aantal bekende zaken. Het aandeel zaken dat wordt geclassificeerd stijgt sneller dan het totale aantal zaken. Meer dan de helft van de zaken wordt echter nog aan de restcategorie 'overig' toegewezen.

Op basis van alternatieve bronnen kunnen we afleiden dat in de restcategorie 'fraude overig' vooral sprake zal zijn van niet-geclassificeerde gevallen van *online handelsfraude*, *faillissementsfraude*, en *verzekeringsfraude*.

[26] Is louter de overheid het slachtoffer (bijvoorbeeld bij uitkeringsfraude) dan wordt er gesproken van *verticale* fraude. Bij de mengvorm waarbij zowel burgers of bedrijven en de overheid zijn benadeeld, wordt er gesproken van *diagonale* fraude.

Mede vanwege de verwachtte grote omvang van deze drie specifieke soorten fraude wordt in het vervolg van dit hoofdstuk de omvang van niet-geregistreerde criminaliteit voor deze soorten fraude verder beschreven.

Faillissementsfraude

Van faillissementsfraude is sprake als schuldeisers op wederrechtelijke wijze opzettelijk worden benadeeld in hun verhaalsmogelijkheden door gedragingen die vóór of tijdens een faillissement plaats kunnen vinden.

Het CBS meet sinds 2004 de omvang en oorzaken van faillissementen op basis van de openbare dossiers faillissementsverslagen. Het CBS classificeert de faillissementen volgens de indeling (i) geen, (ii) zekere en (iii) waarschijnlijke strafbare en of onrechtmatige benadeling.

De ontwikkeling van het aantal frauduleuze faillissementen hangt samen met de ontwikkeling van het totale aantal faillissementen. Het totale aantal faillissementen hangt op zijn beurt uiteraard weer sterk samen met de ontwikkeling van de economie. Vanaf 2012 is er weer sprake van een economisch herstel, en dus van een afname. De ontwikkeling in het relatieve aandeel van faillissementsfraude in het totaal aantal faillissementen laat echter een constante stijging zien over de gehele periode 2004-2015. Daarbinnen is het aandeel van 'zeker frauduleuze gevallen' relatief sterk gestegen. (+9%). Vanuit het perspectief impact/schade is de totale *omvang* van onbetaald gebleven schulden van zekere frauduleuze faillissementen exponentieel toegenomen: van 0,2 miljard euro in 2004 tot 1.1 miljard euro in 2015.

In 2015 zijn er volgens het CBS bijna 2.000 frauduleuze gevallen, waarvan ruim 1.100 zeker. Het merendeel van deze zaken zal niet aan het OM zijn aangeleverd. De huidige schatting van CBS kan worden beschouwd als de minimale omvang van faillissementsfraude. Het totale aantal zaken kan om ten minste drie redenen naar boven worden bijgesteld.

1 Zaken waarvan de administratie ontbreekt worden door het CBS buiten beschouwing gelaten. Het doen verdwijnen van de administratie maakt echter onderdeel uit van de modus operandi van fraudeurs en is sinds 2016 ook formeel strafbaar gesteld (art. 340 Sr).
2 Curatoren krijgen alleen – en dan nog maar deels – betaald voor het doen van aangifte als de melding ook daadwerkelijk door het OM wordt opgepakt. De aangiftebereidheid onder curatoren is mede daardoor laag. Het is niet onredelijk om te veronderstellen dat een groot aantal van de 'waarschijnlijke' gevallen in feite 'zekere' gevallen zijn die de curator niet verder heeft doorgezet.
3 Niet alle schuldeisers dienen daadwerkelijk een vordering in. Dat gebeurt vooral bij kleinere schulden omdat de kosten van het vorderen in de perceptie van de benadeelde partij niet opwegen tegen de baten. Omdat ze niet in de rapportages van de curatoren voorkomen, worden ze ook niet in het totaal van de niet-betaalde schulden meegeteld. Hoewel het hier gemiddeld om lage schuldbedragen gaat, kan het totaal vanwege de grote aantallen toch aanzienlijk zijn, en zou er dus sprake kunnen zijn van een forse onderschatting.

Online handelsfraude

Online handelsfraude is koop- of verkoopfraude waarbij het internet als medium wordt gebruikt. Het gaat met andere woorden om de klassieke vormen van het niet nakomen van leverings- en/of betalingsverplichtingen. Hierin schuilt het element van fraude (misleiding). Het merendeel van de aangiften heeft betrekking op aankoopfraude. Om te voorkomen dat de wederpartij verhaal kan halen, wordt vaak de identiteit en verblijfsplaats verhuld. Online zijn er ook varianten van verkoop- en

aankoopfraude mogelijk die voorheen praktisch gezien niet mogelijk waren (zoals het exploiteren van fictieve webshops).
Het gebruik van het internet als medium maakt het mogelijk om aan- en verkoopfraude op een veel grotere schaal te plegen dan voorheen. Vanwege het schaaleffect wordt de strafbaarheidsstelling van online handelsfraude uitgebreid: partijen die er *een gewoonte van maken* om goederen of diensten online te verkopen maar niet te leveren kunnen nu ook strafrechtelijk worden vervolgd.
Het online mes snijdt aan twee kanten. Het maakt steeds geavanceerdere vormen van identiteitsfraude en aankoop- en verkoopfraude op grote schaal mogelijk. Tegelijkertijd kunnen in de opsporing steeds beter digitale sporen worden gevolgd. Ook waarschuwingen kunnen makkelijker op grote schaal worden afgegeven en meldingen en aangiften kunnen makkelijker worden gedaan.
Online handelsfraude is, in tegenstelling tot andere soorten criminaliteit, ook relatief goed zichtbaar. Zo zegt 93% van de respondenten van de VM die heeft aangegeven het slachtoffer te zijn geweest van koop- of verkoopfraude, ook aangifte gedaan te hebben van de oplichting. Dit is een uitzonderlijk hoog percentage dat door de jaren heen alleen maar verder is gestegen. Dit kan erop duiden dat het dark number voor online handelsfraude relatief laag is – het is een veelvoorkomend fenomeen maar er zijn geen grote groepen slachtoffers die buiten de bekende cijfers blijven.
Volgens de VM van het CBS zijn er in 2015 meer dan 580.000 mensen in Nederlandse huishoudens *slachtoffer* geworden van fraude met online handel (697.000 delicten). Het aantal *aangiften* bij het LMIO, dat landelijk de centrale ingang is voor meldingen van online handelsfraude, ligt al jaren rond de 45.000. In 2017 lijkt er echter sprake van een trendbreuk naar beneden.
LMIO heeft in 2016 voor een aantal aangiften de bankrekeningnummers onderzocht waarop de betalingen van de gedupeerden zijn gestort. Dit zijn de *zwaardere* gevallen waarbij minstens vijfmaal hetzelfde tegenrekeningnummer is gebruikt. In de helft van de gevallen konden de betalingen op deze rekeningnummers worden teruggeleid tot personen die ook aangifte hadden gedaan bij LMIO. Dat betekent dat de andere helft geen aangifte heeft gedaan. Voor de berekening van het dark number is dit laatste percentage F een belangrijk gegeven omdat op basis van dit percentage het totale aantal slachtoffers kan worden geschat (=1/F). Gaan we uit van de pessimistische aanname dat in alle gevallen waarbij geen aangifte is gedaan, sprake was van fraude (kortom dat alle potentiële slachtoffers daadwerkelijk slachtoffer zijn), dan komen we uit op een ophoogfactor van 2,0. Na correctie voor ingetrokken meldingen komt dit neer op ruim 70.000 slachtoffers van online handelsfraude in 2015. Dit aantal ligt een factor 8 lager dan de 580.000 beleefde slachtofferschappen uit de VM.

Zowel op de cijfers van de VM als op die van LMIO moeten verschillende correcties worden uitgevoerd. Om de vergelijking tussen de twee bronnen mogelijk te maken is het ten eerste nodig om dezelfde definities te gebruiken. De cijfers van VM hebben betrekking op *slachtoffers*, die van LMIO op *aangiften*. De conversie van aantal LMIO aangiften naar aantal slachtoffers loopt via de ophoogfactor 1/F. Voor de lichtere gevallen zijn geen getallen beschikbaar. Voor deze categorie kan wel redelijkerwijs worden aangenomen dat de aangiftebereidheid F' lager zal zijn dan bij de zwaardere gevallen. Omdat het leeuwendeel van de gevallen (92% van het totaal) tot de 'lichtere' categorie behoort zal een klein verschil tussen F en F' al leiden tot een relatief grote toename van de ophoogfactor. Bij een behoudende schatting gaat de ophoogfactor voor *alle* gevallen omhoog van 2,0 naar 3,0.
De cijfers van VM hebben betrekking op *beleefd* slachtofferschap. Burgers voelen zich al snel opgelicht, ook als dat strafrechtelijk niet zo zal zijn (wanprestatie). Een behoudende aanname is dat er in 20% van het beleefde slachtofferschap de jure

geen sprake zal zijn geweest van online handelsfraude. Uit de LMIO-cijfers is verder bekend dat ruim 30% van de aangiftes onterecht is gedaan omdat het product later alsnog wordt geleverd of het aankoopbedrag wordt geretourneerd. Van de 582.000 beleefde slachtofferschappen uit 2015 heeft minimaal de helft dus geen betrekking op online handelsfraude.
Voor de andere helft geldt weliswaar dat het om feitelijke slachtoffers van online handelsfraude gaat maar dat een groot deel van de delicten meer dan een jaar geleden hebben plaatsgevonden, dus buiten de meetperiode vallen. Volgens de eigen berekeningen van CBS bedraagt de correctiefactor voor dit *telescoping effect* 1.96 in 2015. Dat komt neer op een verlaging van 48%.
Het nettoresultaat van deze correcties is dat het (vermeende) feitelijke aantal slachtoffers van online handelsfraude op basis van de bijgestelde VM-cijfers (~150.000) en de bijgestelde LMIO-cijfers (~110.000) veel dichter bij elkaar komen te liggen.

Verzekeringsfraude
Verzekeringsfraude is het met opzet misleiden van een verzekeraar bij de totstandkoming en/of uitvoering van een verzekeringsovereenkomst met de bedoeling om onrechtmatig verzekeringsdekking, -uitkering, -prestatie of dienstverlening te krijgen. Of er sprake is van opzet of niet is in de praktijk niet makkelijk vast te stellen. Van verzekeringsfraude (dit geldt overigens voor alle vormen van fraude) is alleen sprake als de feiten *ondubbelzinnig* en *onomstotelijk* op verzekeringsfraude wijzen. De bewijslast ligt hier bij de verzekeraar.
Er zijn nauwelijks publieke schattingen van de totale omvang van verzekeringsfraude beschikbaar. Zeldzame uitzonderingen zijn de gedateerde studies (2005 en 2007), met als perspectief de geleden *schade*, waar nog steeds veelvuldig naar wordt verwezen. De studies komen uit op een totale omvang van verzekeringsfraude van circa 500 miljoen euro, waarvan ruim 60% (320 miljoen euro) voor het particuliere verzekeringsdeel. Na correctie voor inflatie zou de totale omvang in 2016 zijn toegenomen tot 600 miljoen. In de periode 2004-2016 is de totale schadelast echter constant gedaald. Deze twee tegengestelde effecten heffen elkaar op. Dat betekent dat de totale omvang in 2016 nog steeds 500 miljoen zou bedragen.
Het Centrum Bestrijding Verzekeringscriminaliteit (CBV) van het Verbond van Verzekeraars (VvV) publiceert jaarlijks het aantal onderzoeken naar mogelijke gevallen van verzekeringsfraude, evenals de uitkomsten daarvan. In 2016 werden door 80 van de leden van het VvV ruim 27.000 onderzoeken gemeld bij het CBV. Hierbij blijkt in 37% van de onderzochte gevallen daadwerkelijk sprake te zijn van fraude. In totaal wordt er voor ruim 80 miljoen euro aan fraude gedetecteerd. Dit ligt een factor 6 lager dan de schatting die hierboven staat genoemd. De vraag is nu of de verzekeraars daadwerkelijk meer dan 80% van de fraude niet zouden detecteren.
Verzekeringsfraude onderscheidt zich van alle andere typen fraude omdat de groep van directe slachtoffers beperkt is tot een honderdtal bedrijven: de verzekeraars in Nederland. Deze bedrijven bevinden zich in een andere positie dan de 'handhavers' bij andere soorten van fraude – ze kunnen de schade doorberekenen aan hun klanten. De markt voor verzekeringen is echter bijzonder concurrerend en individuele verzekeraars hebben er daarom zelf ook alle baat bij om fraude te bestrijden. Doen ze dit niet dan zullen ze immers veel geld moeten doorrekenen aan hun klanten, zullen hun premies daardoor relatief hoog zijn, en zullen de klanten overstappen naar concurrenten waar minder geld weglekt door fraude.
Verzekeraars die in staat zijn om een hoger percentage van fraudegevallen te detecteren – en dus te voorkomen – hebben daardoor een belangrijk concurrentievoor-

deel. Alle (grotere) verzekeraars hebben daarom '*special investigation units*' om fraude op te sporen. Daarnaast bestaan er tal van specialistische bedrijven die zich met screening van verzekeringsnemers bezighouden (*underwriting*) en/of met de detectie van fraude. Dat laatste is een typisch kenmerk van markten voor producten of diensten waar sprake is van een grote mate van informatie-asymmetrie. Dit soort tussenpersonen voorziet in twee belangrijke functies: ze verzamelen informatie over individuele 'verkopers' (hier: verzekeringsnemers) en ze verspreiden informatie over kwaliteit (hier: het delen van informatie over malafide verzekeringsnemers). Verzekeraars winnen steeds meer informatie in over verzekeringsnemers en delen ook steeds meer informatie. Door de inzet van geavanceerde big-datatechnieken zijn deze grote hoeveelheden informatie ook steeds beter te koppelen en te analyseren. Er zijn specialistische data analytics bedrijven die in staat zijn om op groepsniveau patronen te herkennen in de handelswijze van fraudeurs die het mogelijk maken om op het niveau van individuele cases voorspellingen te doen. Deze technieken kunnen door het gehele verzekeringsproces worden toegepast, dus niet alleen in nader onderzoek (na uitbetaling van de claims) maar in toenemende mate reeds bij de aanmelding. Een duidelijke aanwijzing dat het verzamelen, delen en analyseren van informatie de opsporing van verzekeringsfraude sterk hebben verbeterd is de verschuiving in fraudedetectie van de claim naar de aanmeldfase. Hoe eerder in het verzekeringsproces fraude kan worden opgespoord, hoe geringer de schade voor de verzekeringsorganisatie.

Het feit dat het percentage geconstateerde fraudegevallen al een aantal jaren zeer hoog ligt (rond de 40%) – in vergelijking met andere typen fraudes – kan twee dingen betekenen:

1 verzekeringsfraude is wijdverspreid en de eerdere schattingen uit 2005/2007 (ca 10% van alle schadeclaims zijn malafide) zijn realistisch;
2 verzekeraars zijn zeer goed in staat om fraude op te sporen, met andere woorden het 'oplossingspercentage' ligt in vergelijking tot andere typen criminaliteit zeer hoog. In het tweede geval ligt de feitelijk geconstateerde omvang van verzekeringsfraude dicht bij de ondergrens en is het dark number dus klein.

Gegeven de sterke concurrentie op de markt voor verzekeringen ligt het eerste scenario niet voor de hand. Dat zou namelijk betekenen dat de verzekeraars *collectief* een factor 6 van de fraudegevallen over het hoofd zien. In het tweede scenario is het in theorie nog steeds mogelijk dat er veel fraudegevallen onbekend blijven, namelijk vooral in de gevallen die niet worden onderzocht. Statistisch gezien is het echter niet aannemelijk dat verzekeraars wél goed zijn in het voorselecteren van verdachte inschrijvingen en/of claims – meer dan een derde van de onderzochte gevallen blijkt inderdaad frauduleus te zijn – en tegelijkertijd veel andere cases geheel zouden missen.

Op basis van deze redenatie is het realistischer om te veronderstellen dat de werkelijke jaarlijkse omvang van de financiële schade door verzekeringsfraude dicht bij de feitelijk geconstateerde fraude zal liggen (circa 80 miljoen euro). Met andere woorden, het dark number is voor dit type criminaliteit klein. De (geëxtrapoleerde) schattingen uit 2005 en 2007 (ruim 320 miljoen voor het particuliere verzekeringsdeel) lijken sterk overdreven.

4.3.4 Chantage

Voor dit specifieke delict zijn geen aanvullende bestaande bronnen gevonden buiten de politiestatistiek en de VM. Deze zijn echter niet vergelijkbaar, vooral omdat de VM vraagt naar internetchantage waarbij slechts een klein deel aangegeven wordt. Zo rapporteert de Politiestatistiek 1.500 delicten en de VM 236.000 delicten. Met name bij dit delict speelt de verschuiving naar internet, gepaard gaande met grote aantallen, een rol.

4.4 Vandalisme/vernieling

Voor vandalisme zijn naast de beide traditionele bronnen, twee andere bestaande bronnen beschikbaar die over dit delict rapporteren, de MZJ en de MSVS. Er is een groot verschil in de aantallen delicten in de Politiestatistiek (82.000) en de VM (1.183.000). Dit wordt deels verklaard door het lage aangiftepercentage (1 op 7). Dat het aantal gemeten door de VM redelijk plausibel is wordt ondersteund door de MZJ: 313.000 jongeren (10-22) jaar zeggen zich wel eens schuldig te hebben gemaakt aan vandalisme.
Het percentage slachtofferschap in de MSVS is van dezelfde orde van grootte als bij de VM.

4.5 Cybercriminaliteit

Het onderscheiden van cybercriminaliteit van 'traditionele' criminaliteit is niet eenvoudig. Dit is één van de redenen waarom cybercriminaliteit niet of niet eenduidig wordt geregistreerd. Onder cybercriminaliteit vallen misdrijven die ICT als middel gebruiken (*cyber-enabled crime*) en criminaliteit die bestaat bij de gratie van ICT (*cyber-dependent crime*'). Onder *cyber-enabled* criminaliteit worden vormen van criminaliteit bedoeld die computersystemen gebruiken om een traditioneel misdrijf op een grotere schaal te plegen. Onder *cyber-dependent* criminaliteit vallen vormen van criminaliteit die zonder computersystemen niet mogelijk zouden zijn, en zich expliciet richten op computernetwerken en -systemen.

Bestaande inschattingen en haar methodologie
Een duidelijke definitie is om enkel misdrijven die ICT systemen als doel hebben te beschouwen als 'echte' cybercriminaliteit. Cyber-*enabled* crimes zouden bij de traditionele vormen van criminaliteit moeten worden meegerekend omdat het conceptueel gezien vreemd is om een instrument (ICT) leidend te laten zijn in de classificatie.
In de praktijk lopen loopt het gebruik van cyber-dependent en cyber-enabled crime vaak door elkaar. De Nederlandse politie gebruikt daarom een brede definitie en beschouwt beide soorten als cybercriminaliteit.
Schattingen over omvang en economische impact van cybercriminaliteit lopen sterk uiteen. Dit komt omdat de schattingen van de omvang moeten worden vermenigvuldigd met een factor (schade) die grotendeels onbekend is. Onduidelijk is bijvoorbeeld in hoeverre indirecte schade (bijvoorbeeld imagoschade vanwege security incidents) kunnen en moeten worden meegeteld. Naast het feit dat de verschillende frequentie en impactinschattingen sterk uiteen lopen is de methode die is gehanteerd vaak ook onbekend, niet robuust, of dekt deze niet de volledige problematiek. Er is een prikkel voor veel van de publicerende partijen om niet transparant te zijn over de gehanteerde methoden, en cijfers over de omvang en impact van cyber-

crime te overdrijven. Ook zijn algemene schattingen vaak gebaseerd op incomplete data, die daarnaast niet representatief zijn voor een gehele samenleving of economie. Ten derde is er het probleem van 'under-reporting': in veel gevallen zijn individuen en bedrijven niet geneigd een melding te maken van een cybercriminele activiteit, omdat ze niet bekend willen maken dat ze slachtoffer zijn geweest. Ten slotte is het zo dat slachtoffers, met name als ze weinig cyberexpertise hebben, soms niet eens weten dat ze slachtoffer zijn geweest.
Over cyber-dependent crime houdt de Politiestatistiek alleen apart het delict 'computervredebreuk' apart bij. In 2015 zijn er 2.175 aangiften van computervredebreuk gedaan. De VM gebruikt een ruime definitie ('hacken') en rapporteert een veel hoger aantal delicten, namelijk meer dan 1.000.000. De MZJ gebruikt weer andere definitie en rapporteert dat 450.000 jongeren (tussen de 12 en 22 jaar) in 2015 online een delict hebben gepleegd. Dit kunnen dus zowel cyber-dependent als cyber-enabled delicten zijn.
Cyber-enabled delicten worden in de Politiestatistiek wel bijgehouden maar ze zijn niet te onderscheiden van 'traditionele' (offline) delicten. In de VM worden delicten zoals cybercrimedelicten, identiteitsfraude, koop en verkoopfraude en cyberpesten wel in hun gedigitaliseerde vorm onderscheiden. In totaal zou het daarbij gaan om 1.600.000 delicten op jaarbasis.

Nieuwe manieren om te meten
Een verschijningsvorm van cybercrime kan worden uitgewerkt aan de hand van de interacties die over de tijd heen en op (verschillende lagen van) een online platform (e-mail, Facebook, Tor, online marktplaatsen, Bitcoin, etcetera) tussen relevante actoren plaatsvinden. In feite wordt hier vanuit het perspectief voorbereidings/uitvoeringshandeling gekeken. We beschouwen hierbij de kernactoren die terugkomen in alle verschijningsvormen: *slachtoffer*, *dader*, (onbewust) *medeplichtige*, *beveiliger* en *justitiële actoren* (politie/Openbaar Ministerie (OM)). In bijlagen 7 t/m 10 van Smit et al. (2018) zijn deze schema's in meer detail uitgewerkt voor DDoS, phishing, pharming en ransomware. Op basis van deze uitwerking kan systematisch worden gezocht naar geschikte meetpunten en meetmethoden. Iedere interactie die plaatsvindt in een digitaal systeem is in principe ergens meetbaar. We onderscheiden daarbij drie varianten: (1) *victim centric* (op het computersysteem of netwerk van een slachtoffer), (2) *perpetrator centric* (bij de dader) en (3) *network centric* (op een tussenliggend platform).
Interessant is hierbij dat een aantal interacties terugkomen bij meerdere verschijningsvormen. Deze zijn bij uitstek geschikt om te meten. Zo kan bij zowel phishing als ransomware sprake zijn van een betaling, en zou in beide gevallen Bitcoin kunnen worden gebruikt. De interacties zijn door ons als volgt gegroepeerd:
- acquisitie malware/tools;
- verspreiding/plaatsing van aanval;
- bescherming en beveiligingsacties;
- betalingen;
- aangifte.

Conclusie
Het is niet mogelijk om de omvang van cybercriminaliteit op een betrouwbare wijze vast te stellen. Uit interviews en literatuuronderzoek komt duidelijk naar voren dat het niet mogelijk is om te voorspellen welke nieuwe typen cybercriminaliteit zullen ontstaan, en waar aanvallen met name zullen plaatsvinden. Detectiemethoden lopen per definitie achter de feiten aan, en zullen altijd maar een deel van de incidenten kunnen meten (De Cuyper & Weijters, 2017). Dit geldt voor opsporing in het alge-

meen maar in een zeer dynamisch domein zoals cybercrime vormt dit met name een probleem.
Daarnaast doet zich een aantal ontwikkelingen voor die het steeds moeilijker maken om de cybercriminele activiteiten op dit moment nog wél bekend zijn, goed te kunnen blijven monitoren:

- steeds meer data wordt opgeslagen 'in de cloud';
- steeds meer data wordt versleuteld (in zowel opslag als transmissie);
- steeds meer data wordt over de grens opgeslagen (ook vanwege de tendens richting cloud);
- de algehele hoeveelheid data en de kanalen waarover deze worden gedeeld nemen toe, en daarmee ook de complexiteit van analyse ervan;
- steeds meer cybercriminelen gebruiken de techniek van *'blending in'* (het er zo normaal mogelijk uit laten zien van verdachte activiteiten om detectie te ontlopen);
- de complexiteit van software neemt toe aan de slachtofferkant, waardoor verdediging lastiger wordt;
- aan de aanvallende zijde worden aanvalstechnieken steeds geavanceerder; de capaciteit van opsporing, detectie en onderzoek volgen niet altijd de snelheid van deze ontwikkelingen.

Deze wedloop valt niet te winnen maar de achterstand ten opzichte van de cybercriminelen kan weldegelijk beperkt worden gehouden of zelfs nog worden verkleind. De afgelopen jaren is de bestrijding van cybercrime verder gerprofessionaliseerd en beter georganiseerd. In toenemende mate nemen de verschillende partijen in de security keten (zoals ISP's en banken) hun verantwoordelijkheid en wordt er ook beter samengewerkt (ISP's voorbeeld in het NaWas-verband).

In de volgende twee paragrafen wordt aangegeven welke bronnen iets zeggen over cybercrime.

*4.5.1 Cyberdelicten(*cyber-dependent crime*)*

De Politiestatistiek houdt alleen apart het delict computervredebreuk bij. Het gaat hier om 2.300 delicten. De VM rapporteert 1.050.000 delicten, het gaat hier dan om 'hacken'. Ook de MZJ rapporteert specifiek over cyberdelicten. Het aantal daders onder jongeren van 10 tot 22 jaar bedraagt in totaal 453.000.

*4.5.2 Gedigitaliseerde criminaliteit (*cyber-enabled crime*)*

In de Politiestatistiek worden deze delicten wel bijgehouden, maar de gedigitaliseerde delicten zijn niet te onderscheiden van de 'gewone' delicten. Alleen in de VM zijn delicten als identiteitsfraude, koop- en verkoopfraude en cyberpesten wel in hun gedigitaliseerde vorm te onderscheiden. Het gaat hier dan om 1.559.000 delicten.

4.6 Wapendelicten

Omdat het hier gaat om slachtofferloze delicten geeft de VM hier geen informatie over. Er zijn twee bronnen die iets zeggen over vuurwapendelicten. De Politiestatistiek telt hier 4.700 delicten, het LIS telt 300 mensen die met een opzettelijk toegebracht letsel door een schot van een vuurwapen bij de spoedeisende hulp terechtkomen.

Twee andere bronnen, de MZJ en de MSVS, rapporteren over wapenbezit en wapenincidenten in het algemeen, dus niet beperkt tot vuurwapens. Zo geven in de MZJ 67.000 jongeren aan in het bezit te zijn van een wapen voor zelfverdediging. Dit is een delict waarbij het dark number onbekend is en waarschijnlijk hoog zal zijn. Immers, over het algemeen wordt (verboden) wapenbezit pas ontdekt bij het plegen van een ander delict. En bij zelfrapportages is het onduidelijk of het gerapporteerde wapen ook daadwerkelijk een verboden wapen is, waardoor er hier sprake kan zijn van overrapportage.

4.7 Verkeersdelicten

Op enkele uitzonderingen na (verlaten plaats ongeval, joyriding) zijn verkeersdelicten slachtofferloze delicten oftewel 'haal'delicten. De belangrijkste bron voor verkeers*misdrijven* is dan ook de Politiestatistiek, deze telt 111.000 misdrijven. Voor *overtredingen* van de Wet administratiefrechtelijke handhaving verkeersvoorschriften (WAHV) wordt het aantal opgelegde boetes door het Centraal Justitieel Incassobureau (CJIB) bijgehouden, dit zijn er 9.223.000.
Voor een specifiek verkeersdelict, namelijk rijden onder invloed, zijn meer bronnen beschikbaar. Zo wordt ook in de MZJ gevraagd naar rijden onder invloed, hieruit blijkt dat 145.000 jongeren zich hieraan schuldig maken. Ter vergelijking: van de 111.000 verkeersdelicten in de Politiestatistiek zijn er 25.000 voor rijden onder invloed. Ook vanuit het periodieke onderzoek Rijden onder invloed blijkt dat de aantallen gevonden in de Politiestatistiek een lage ondergrens is van dit delict.

4.8 Drugsdelicten

Voor drugsdelicten is een andere bestaande bron naast de Politiestatistiek onder andere de MZJ, waarin gevraagd wordt naar daderschap van het verkopen van drugs (softdrugs, xtc/amfetemine/paddo's, harddrugs). 110.666 jongeren (17-22 jaar) geven aan zich hieraan schuldig te hebben gemaakt. Dit aantal jongere daders is veel meer dan het totaal aantal verdachten (ongeacht leeftijd) geregistreerd in de Politiestatistiek, namelijk 17.000.
In de volgende paragraaf zijn in het kader van het fenomeen georganiseerde misdaad de mogelijkheden voor het in kaart brengen van het drugsdelict 'wietteelt' nader onderzocht.

4.9 Georganiseerde criminaliteit

In Nederland wordt doorgaans de volgende definitie van georganiseerde criminaliteit aangehouden: '*Groepen van personen die primair gericht zijn op illegaal gewin door systematisch misdaden te plegen met ernstige gevolgen voor de samenleving, en die in staat zijn deze misdaden op betrekkelijk effectieve wijze af te schermen, in het bijzonder door de bereidheid te tonen fysiek geweld te gebruiken of personen door middel van corruptie uit te schakelen.'* De term georganiseerde criminaliteit slaat dus niet zozeer op het soort misdrijf, maar meer op de manier waarop misdrijven uitgevoerd worden, namelijk in georganiseerd verband. Criminaliteit wordt dus vanuit het perspectief (lidmaatschap van) criminele organisatie benaderd.
Ook is er een doublure met de misdrijftypen die in paragraaf 4.1 t/m 4.8 beschreven zijn.

Huidige werkwijzen voor het meten van georganiseerde criminaliteit
In de huidige aanpak in meten en rapporteren over georganiseerde criminaliteit in Europese landen zijn de officiële misdaadstatistieken (verzameld door politie) en politiedata nog steeds de belangrijkste bronnen van informatie. Het valt echter te betwisten of zulke data ooit een valide beeld gaan geven van dit type misdaad. Deze cijfers geven vermoedelijk eerder de prestaties van de politie aan dan de ware mate van criminele activiteit. Waar gestandaardiseerde slachtofferenquêtes een beeld geven van 'gewone' misdaad en een aanvulling zijn op politiedata worden huishoudens doorgaans echter niet direct slachtoffer van georganiseerde criminaliteit. Er is dus behoefte aan een betere manier om de omvang van georganiseerde criminaliteit in kaart te brengen.
In dit verkennende onderzoek wordt gekeken naar twee invalshoeken en drie cases: illegale markten (case 1: wietteelt; en case 2: mensenhandel) en de netwerkbenadering (case 3). Bij deze laatste invalshoek nemen we criminele netwerken als uitgangspunt voor het schatten van de totale omvang van georganiseerde criminaliteit.

Wietteelt (case 1)
Voor wietteelt geldt bij uitstek dat er bronnen beschikbaar zijn die kunnen bijdragen aan het schatten van de omvang van georganiseerde wietteelt. Denk aan onder andere inbeslagnames, enquêtes onder telers, interviews onder politiemedewerkers, omzet van coffeeshops zoals geregistreerd door de Belastingdienst en cijfers omtrent energiediefstal. Op basis van deze bronnen zijn diverse rekenmodellen opgesteld (doorgaans gebaseerd op inbeslagname en pakkans). Het verschil tussen de schattingen is echter nog erg groot, mede vanwege de verschillen in de geschatte omvang van de export uit Nederland. De introductie van nieuwe databronnen is beperkt gebleven tot energiediefstal en energieverlies, wat overigens een veelbelovende variabele is. Meer databronnen zou er echter toe kunnen leiden dat de bandbreedte in de verschillende modellen verkleind kan worden. Mogelijke databronnen zijn de belastingdienst, BAG, websites van growshops, watertoevoer en -kwaliteit en overlastmeldpunten. Veel bronnen bevatten in potentie waardevolle informatie om de omvangschattingen van wietteelt te verbeteren. De grootste uitdaging is om deze kennis toe te passen in dit domein, zowel wat betreft het vinden van databronnen als het koppelen van deze bronnen en er de juiste analyses op toe te passen.

Mensenhandel (case 2)
Deze case is eerder aan de orde gesteld bij de bespreking van geweldsdelicten, zie paragraaf 4.2.6

Netwerkbenadering (case 3)
Het netwerkperspectief houdt in dat de meeste criminele organisaties 'loosely knit' zijn met regelmatig veranderende leden in plaats van de piramidaal opgebouwde misdaadorganisaties. Om een netwerk in kaart te kunnen brengen is het dus van belang om actoren te kennen, hun verbindingen met elkaar (sociale relaties) en de posities van de actoren binnen het netwerk. Hoe meer informatie er voorhanden is, hoe beter er iets over het gehele netwerk gezegd kan worden. Verschillende typen netwerken hebben verschillende karakteristieken waarop de grootte van het dark number kan variëren (bijv. gebruik van geweld en de grootte en dichtheid). Voor het schatten van de omvang is het belangrijk om het type netwerk te kennen. Het dark number verschilt namelijk per type netwerk.
De netwerkbenadering kan zeker nuttig zijn voor het bepalen van de omvang van georganiseerde criminaliteit in Nederland. Zo kan het antwoord geven op vragen

als: hoe groot is het regionale netwerk, hoeveel criminele organisatoren zijn er en wat is het aantal internationale actoren.

Conclusie
Voor de uitgewerkte cases geldt dat er al veel (in potentie waardevolle) informatie beschikbaar is, maar dat dit nog te gefragmenteerd is om direct te kunnen gebruiken. Het lijkt dan ook onnodig om verder in te zetten op primaire dataverzameling. Deze weg kan wel ingezet worden als 'tweede' stap om initiële schattingen op basis van secundaire bronnen bij te schaven. Voor nu is de aanbeveling een volgende slag te maken over de aanvullende bronnen en modellen.

5 Discussie en aanbevelingen

Een belangrijke constatering in deze studie is dat er naast de bekendste en meest gebruikte twee bronnen, namelijk de Politiestatistiek en de VM – veel andere bronnen zijn die een indicatie geven over de omvang van criminaliteit.
Met name gegevens die marktpartijen (verzekeringsmaatschappijen, gezondheidszorg, ...) tot hun beschikking hebben kunnen interessant zijn. Nadere samenwerking verdient dan ook aanbeveling, waarbij sprake kan zijn van het delen van informatie (wederkerigheid).
Hoewel er dus uit verschillende bronnen redelijk wat bekend is over de criminaliteit blijft er nog wel een verborgen deel over, het dark number. Het deel van de criminaliteit dat verborgen blijft is sterk afhankelijk van de verschijningsvorm of van het type delict. Over het algemeen (met enkele uitzonderingen, zie paragraaf 5.1.1) kan voor delicten *met* een slachtoffer die *niet* cyber-enabled of cyber-dependent zijn (hier vallen in ieder geval alle geweldsdelicten onder) gezegd worden dat de geobserveerde criminaliteit vanuit de Politiestatistiek en de VM, al dan niet opgehoogd met multipliers en gebruikmakend van andere bronnen, vermoedelijk redelijk in de buurt komt van de daadwerkelijke criminaliteit. Het is dan ook plausibel dat voor *deze* delicten de *geconstateerde* daling sinds het begin van deze eeuw ook een *feitelijke* daling inhoudt.

Voor *andersoortige* delicten (zonder slachtoffer of met slachtoffer maar cyber-enabled/-dependent) is de situatie veel minder duidelijk. Hier zouden vangst-her-vangstmethoden en netwerkmethoden als ook de social media en big-datatechnieken interessant kunnen zijn om dit dark number verder te onderzoeken. Ook een gerichte en intensievere opsporing zou hier zinvol kunnen zijn. Wat opvalt is dat het hier vaak gaat om methoden en technieken die al veelvuldig in andere disciplines gebruikt worden (biologie en medische wetenschappen), maar (nog) niet vaak voor criminaliteit.

Een andere constatering is dat triangulatie, het gebruikmaken van verschillende bronnen of methoden (of theorieën of onderzoekers) om eenzelfde fenomeen te meten, zeer nuttig en vaak noodzakelijk is. Triangulatie geeft echter – haast per definitie – verschillende uitkomsten. Of liever gezegd, na triangulatie moet nog bepaald worden hoe om te gaan met de verschillende uitkomsten. Dat is immers het hele idee achter triangulatie waarbij door analyse van verschillende bronnen, methoden en resultaten inzicht verkregen wordt in de 'werkelijke'omvang. Daarom lijkt het op het eerste gezicht in tegenspraak met het vaak gewenste idee van 'eenduidigheid in cijfers'. Deze eenduidigheid kan echter alleen verkregen worden als datgene wat gemeten wordt direct gemeten *kan* worden en precies en ondubbelzinnig gedefinieerd is. Aan deze voorwaarden voldoet de criminaliteit niet: er blijft een deel onzichtbaar, dat indirect gemeten of geschat moet worden. En ook bij de definitie van het begrip criminaliteit zijn er keuzes te maken over de afbakening en de manier van tellen.

Een volgende constatering heeft te maken met de eerdere opmerking dat het aantal delicten over het algemeen indirect bepaald wordt. Vaak ligt het meer voor de hand vanuit een andere perspectief (zoals dader of slachtoffer) te kijken. Ook kan het bij een aantal delicten (denk aan verschillende soorten fraude) eenvoudiger zijn de schade te bepalen in plaats van het aantal delicten. Dit bekijken van criminaliteit vanuit andere perspectieven (dan delict) komt ook terug bij het fenomeen georgani-

seerde criminaliteit. In feite is dit niet een onderscheiden delictgroep, maar het perspectief criminele organisatie (zie figuur 1.1 in Smit et al., 2018) van waaruit een onderliggend delict (zoals wietteelt) bekeken wordt.

5.1 Drie onderscheiden categorieën

De mogelijkheden om zicht te krijgen op de omvang van de criminaliteit en het dark number worden sterk bepaald door het type delict. Elk type delict of verschijningsvorm van criminaliteit kent zijn eigen bronnen of methoden, soms specifiek voor een enkel delict (verzekeringsfraude), soms voor een aantal delicten (de MZJ voor een aantal delicten waar jeugdige daders geteld worden). Om de discussie over de bevindingen van deze studie te structureren wordt uitgegaan van een grove indeling van criminaliteit in drie soorten delicten: allereerst is er een onderscheid tussen delicten met en zonder slachtoffer (oftewel breng- en haaldelicten). De delicten met een slachtoffer worden vervolgens nog onderscheiden in *niet*-cybergerelateerde en cybergerelateerde delicten.

5.1.1 Delicten met slachtoffer, niet-cybergerelateerd

Van veel delicten *met* een slachtoffer die *niet* cybergerelateerd zijn kunnen redelijk goed de aantallen delicten geteld of geschat worden met behulp van de Politiestatistiek en de VM. Wel is de Politiestatistiek alleen niet voldoende. In ieder geval dienen de in de VM gevonden aangiftepercentages als multiplier gebruikt te worden om de bevindingen van de Politiestatistiek op te hogen. Daarnaast zijn er in de VM een aantal zaken, zoals het telescoping effect[27] en selectiviteit in respons, waar (meer) rekening mee gehouden moet worden om betrouwbaarder schattingen te krijgen over het aantal delicten.

> *Aanbeveling 2*: Vanwege het belang van Politiestatistiek en VM voor het meten van een groot deel van de criminaliteit is een diepgaand en periodiek uitgevoerd onderzoek naar de eigenschappen van deze twee instrumenten nodig om goed de resultaten te kunnen corrigeren en ophogen teneinde betrouwbaarder schattingen te krijgen over het aantal delicten. Het recente onderzoek waarbij de twee instrumenten op microniveau gekoppeld werden kan hier als voorbeeld dienen (Reep,2014).

Een aantal delictsoorten blijkt echter niet goed bepaald te kunnen worden met alleen de Politiestatistiek of VM. Het gaat hier bijvoorbeeld om zedendelicten, stalken, bedreiging, mensenhandel, vandalisme, maar ook vermogensdelicten waar bedrijven slachtoffer van zijn. Nu zijn voor de meeste van deze delicten ook andere bronnen beschikbaar die iets zeggen over de omvang, soms vanuit een specifieke en mogelijk beperkte invalshoek. Een voorbeeld is de MSVS voor het delict vandalisme/vernielingen, waarbij de beperking is dat het hier uitsluitend gaat om vandalisme/vernielingen in het onderwijs. Er blijven wel enige lacunes over. Met name delicten met bedrijven als slachtoffer blijven onderbelicht. Ook ontbreekt een goed periodiek overzicht van al deze bronnen en hun resultaten. Statistische publicaties over de omvang van criminaliteit zoals de jaarlijkse Criminaliteit en Rechtshandhaving beperken zich meestal tot de Politiestatistiek en de VM.

[27] Het door een respondent verkeerd plaatsen in de tijd van een gebeurtenis zoals slachtofferschap.

Aanbeveling 3: Vanwege het beperkte inzicht in slachtofferschap van bedrijven dient het aanbeveling hier meer op in te zetten. Te denken valt aan een nauwere samenwerking met verzekeringsmaatschappijen. En/of een instrument ter vervanging van de Monitor Criminaliteit Bedrijfsleven zoals die een aantal jaren geleden uitgevoerd werd.

Aanbeveling 4: Een periodiek overzicht van de bevindingen van alle bronnen (niet alleen Politiestatistiek en VM) die rapporteren over de omvang – of althans trends binnen een bepaalde bandbreedte – van (delen van) criminaliteit zou wenselijk zijn. Hiertoe zou een uitbreiding van C&R kunnen dienen, maar ook publicatie op de website 'Criminaliteit in Beeld' zou een mogelijkheid kunnen zijn.

Bij enkele delicten, in het bijzonder zedendelicten, speelt nog een ander aspect een rol. De grenzen tussen wat gewenst is, wat ongewenst is en wat strafbaar is zijn hier zeer diffuus. Het gaat hier niet zozeer om onduidelijkheden in de wet, maar veel meer om de interpretatie van (de dader en) het slachtoffer van een specifieke gebeurtenis. Dit maakt het zeer lastig de omvang te bepalen van die gebeurtenissen die daadwerkelijk strafbaar zijn. Ook de lastige bewijsbaarheid speelt hier een rol.

Aanbeveling 5: Een specifiek onderzoek naar de omvang van ongewenst en/of strafbaar seksueel gedrag zou wellicht inzicht kunnen geven in de manier waarop het strafbare gedrag gemeten zou kunnen worden.

5.1.2 Delicten met slachtoffer, cyber-enabled of -dependent

Het gaat hier deels om 'klassieke' vormen van criminaliteit die met behulp van een computer uitgevoerd worden (cyber-enabled, denk aan online fraude of online bedreiging en deels om delicten die naar hun aard alleen in het digitale domein voorkomen (cyber-dependent, denk aan DDos-aanvallen of ransomware).
De Politiestatistiek geeft maar een beperkt beeld van de omvang van deze categorie delicten. Voor een deel (voor de cyber-enabled delicten) worden ze wel geteld in de Politiestatistiek, maar zijn ze niet te onderscheiden van de niet-cybergerelateerde delicten. Maar ook worden er kennelijk maar weinig van deze delicten aangegeven of anderszins opgespoord door de Politie.
Dat het hier om grote aantallen delicten gaat, blijkt uit de VM. Sinds enige jaren vraagt die naar slachtofferschap van onder andere online bedreiging, phishing en koop- en verkoopfraude vraagt, maar ook uit de MZJ die jeugdig daderschap meet. Met deze twee (en enkele andere) bronnen wordt redelijk goed zichtbaar dat er kennelijk zowel een verschuiving als een toename plaatsvindt van offline naar cyber-enabled delicten. Naast de aanbevelingen 2, 3 en 4, die ook voor deze delicten gelden, en de algemene opmerking dat bij deze cyber-enabled delicten het ook van belang is te kijken naar bronnen en methoden die iets zeggen over impact en schade zijn er geen specifieke aanbevelingen.

Een kenmerk van cyber-dependent delicten is dat ze een – mogelijk verborgen – digitaal spoor achterlaten. Dit geeft in principe mogelijkheden om – vanuit het perspectief van voorbereidings- of uitvoeringshandeling – zicht te krijgen op dit soort delicten. Dit wordt echter nog maar sporadisch toegepast.

5.1.3 Delicten zonder slachtoffer, niet-cybergerelateerd

Het gaat hier om een groot deel van de verkeersdelicten, maar ook drugshandel en verboden wapenbezit. Uiteraard geeft de VM hier geen informatie over, de belangrijkste bronnen zijn de Politiestatistiek (voor misdrijven) en het CJIB (voor verkeersovertredingen in het kader van de WAHV, feitgecodeerde verkeersovertredingen (niet-WAHV) en rijden onder invloed tot een bepaald promillage). De aantallen hier gevonden zullen een (lage) ondergrens zijn van het daadwerkelijk aantal delicten en zijn eigenlijk meer een maat van de opsporingsinspanningen.
Op enkele uitzonderingen na zijn er ook geen andere bronnen voorhanden. Zo geeft de MZJ informatie over rijden onder invloed en drugsdelicten gepleegd door jongeren. En ook is er enige informatie over de impact of de schade van een aantal van deze delicten (drugs: productie, handel en consumptie). Een voorbeeld is de vangst-hervangstmethode die gebruikt is bij een schatting van het aantal dronken rijders. Met name voor deze categorie is het interessant om dit soort geavanceerde methoden toe te passen. Hierbij moet dan niet zozeer gekeken worden naar het aantal delicten, maar ook naar andere invalshoeken zoals schade, voorbereidings- en uitvoeringshandelingen, criminele organisaties etcetera.
Naast aanbeveling 4, die ook voor deze categorie geldt, kan het volgende aanbevolen worden.

> *Aanbeveling 6*: Apart nagaan in deze categorie van delicten zonder slachtoffer en niet cyber gerelateerd (1) welke delicten relevant zijn, (2) in hoeverre vangst-hervangstmethoden bruikbaar kunnen zijn, ook voor andere delicten dan rijden onder invloed

> *Aanbeveling 7*: Onderzoek of en hoe de resultaten uit de MZJ geëxtrapoleeerd kunnen worden naar de totale daderpopulatie. Overwogen kan worden ook een zelfrapportage onder volwassenen uitte voeren.

5.2 Tot slot

De aanleiding voor dit onderzoek was de twijfel over de realiteit van de bevindingen van de twee instrumenten die al enkele decennia de omvang van de criminaliteit meten, namelijk de politiestatistiek en de slachtofferenquête. Deze lieten een daling van de criminaliteit in de laatste twee decennia zien. Hierdoor rees de vraag of deze twee instrumenten wel voldoende zicht geven op *alle* vormen van criminaliteit. Het antwoord op deze vraag is niet eenduidig. Enerzijds valt niet te ontkennen dat er inderdaad sprake is van een daling van de 'traditionele' criminaliteit maar anderzijds zijn er nieuwe verschijningsvormen van criminaliteit, met name cybergerelateerde criminaliteit, waar minder over bekend is. Dit rapport laat zien wat wél bekend is en geeft suggesties met wat voor methoden en technieken mogelijk meer zicht op criminaliteit verkregen kan worden. Wel moet opgemerkt worden dat 'het aantal delicten' – in ieder geval voor cybergerelateerde criminaliteit – wellicht geen goede of in de praktijk goed hanteerbare maatstaf is voor de omvang van het fenomeen.

Literatuur

BundesKriminalAmt (2018). *Police Crime Statistics 2017* Geraadpleegd op <mei 2018>: https://www.bka.de/EN/CurrentInformation/PoliceCrimeStatistics/2017/pcs2017.html;jsessionid=FC71D7A30B66EA186951349F174F558D.live0612?nn=39580

Cuyper, R.H. de, Weijters, G., Jennissen, R.P.W. (2015).*Resultaten van de Nationale Veiligheidsindices 2014*. Den Haag: WODC. Fact sheet 2015-4.

Dijk, J.J.M. van (1992) Als de dag van gisteren: Over de betrouwbaarheid van het slachtofferverhaal. *Justitiële verkenningen 18*, 47-65.

Friedman, Matthew, Ames C. Grawert, James Cullen (2017). *Crime trends: 1990-2016.* New York: Brennan Centre for Justice.

Kalidien, S.N. (2017). *Criminaliteit en Rechtshandhaving 2016*. Den Haag: WODC. Cahier 2017-12.

Office for National Statistics (2018). *Crime in England and Wales: Year ending december 2017*. Statistical Bulletin, 26 april 2018.

Reep, C. (2014). *Slachtoffer geweest? Antwoorden uit de VeiligheidsMonitor vergeleken met politieregister.* Z.pl.: CBS. CBS methodologie paper 2014/01.

Smit, P.R., Ghauharali, R., Veen, H.C.J. van der, Willemsen, F., Steur, J., Velde, R.A. te, Vorst, T.van der, & Bongers, F. (2018). *Tasten in het duister: Een verkenning naar bronnen en methoden om de aard en omvang van de criminaliteit te meten*. *Deel 2: Technisch rapport*. Den Haag: WODC. Cahier 2018-21b.

UNODC (2015). *International Classification of Crime for Statistical Purposes, Version 1.0*. Vienna, 2015

Veiligheidsmonitor (2017). *Veiligheidsmonitor 2016.* Den Haag/Heerlen/Bonaire: CBS/Ministerie van Veiligheid en Justitie.

Bijlage 1 Samenstelling begeleidingscommissie en klankbordgroep

Begeleidingscommissie

Voorzitter

prof. mr. dr. C.C.J.H. Bijleveld	Nederlands Studiecentrum Criminaliteit & Rechtshandhaving

Leden

dr. C.J. Albers	Rijksuniversiteit Groningen
drs. R.R.R. Ghauharali	Ministerie van Justitie en Veiligheid, Wetenschappelijk Onderzoek- en Documentatiecentrum
drs. H. Kroes	Ministerie van Justitie en Veiligheid, DG Rechtspleging en Rechtshandhaving
drs. T.L. van Mullekom	Ministerie van Justitie en Veiligheid, Wetenschappelijk Onderzoek- en Documentatiecentrum

Klankbordgroep

Voorzitter

prof. mr. dr. C.C.J.H. Bijleveld	Nederlands Studiecentrum Criminaliteit & Rechtshandhaving

Leden

drs. R.R.R. Ghauharali	Ministerie van Justitie en Veiligheid, Wetenschappelijk Onderzoek- en Documentatiecentrum
R.P. Lucas	Nationale Politie
drs. T.L. van Mullekom	Ministerie van Justitie en Veiligheid, Wetenschappelijk Onderzoek- en Documentatiecentrum
G. Paulides	Raad voor de Rechtspraak
drs. J.P. Raeven	Ministerie van Justitie en Veiligheid, DG Rechtspleging en Rechtshandhaving
drs. J. de Ridder	Openbaar Ministerie, Parket Generaal
drs. M.J. Schep	Ministerie van Justitie en Veiligheid, DG Straffen en Beschermen
mr. R. van den Sigtenhorst	Ministerie van Justitie en Veiligheid, DG Veiligheid en Bestuur
W.J.C. Speller-Boone	Ministerie van Justitie en Veiligheid, DG Rechtspleging en Rechtshandhaving
A.S. Toornstra	Ministerie van Justitie en Veiligheid, DG Politie
C.J. van Vliet	Ministerie van Justitie en Veiligheid, Programma Politiële Taken
mr. drs. P.J.J. van Voorst	Ministerie van Justitie en Veiligheid, DG Rechtspleging en Rechtshandhaving