REDACTIONEEL

Criminaliteit en criminologie in een gedigitaliseerde wereld

Judith van Erp, Wouter Stol & Johan van Wilsem

Wat betekent de komst van het internet voor criminaliteit en de bestrijding ervan? Dit themanummer staat stil bij deze belangrijke ontwikkeling in onze samenleving. In deze redactionele inleiding staan we allereerst stil bij de aan het internet gelieerde criminaliteit: cybercrime. Wat is het precies? Vervolgens richten we ons op de criminologische hoofdvragen die de opkomst van het internet met zich meebrengt. Ontstaat hierdoor meer criminaliteit? Wie zijn de betrokkenen? Wat doen we ertegen? Verder staan we stil bij de mogelijkheden voor het doen van criminologisch onderzoek met onlinemateriaal, zoals onlineobservatie en Big Data. Tot slot geven we een schets van de manier waarop hoogwaardige ICT behulpzaam kan zijn in de opsporing van criminaliteit. Al met al kunnen we spreken van een jong aandachtsveld binnen de criminologie waar tal van interessante onderzoeksthema's vragen om een verdere uitwerking.

Nieuwe perspectieven

Als sociale wetenschappers kunnen wij soms met enige afgunst kijken naar beta's die in hun laboratoria zuivere experimenten opzetten om theorieën te ontwikkelen of aan te scherpen. Maar nu hebben wij criminologen een eigen en uniek sociaal experiment op wereldschaal, en het heet cyberspace. Er is weliswaar geen controlegroep die losstaat van de experimentgroep, want cyberspace en de fysieke wereld zijn innig verweven. Maar we hebben nu wel naast de oude wereld, een nieuwe, nogal andere sociale werkelijkheid waarin we kunnen onderzoeken of bestaande theorieën – ontwikkeld in de oude wereld – standhouden in een gedigitaliseerde omgeving. Een voorbeeld. Terwijl grenzen in cyberspace geen rol zouden spelen, laat onderzoek zien dat in de meeste gevallen waarin iemand in Nederland slachtoffer is van e-fraude, het slachtoffer is opgelicht vanuit Nederland (>80 procent). Dat zien we zowel in analyses van politiedossiers (Leukfeldt e.a., 2010; Junger e.a., 2013) als in slachtofferonderzoek (Domenie e.a., 2013). Kan dit fenomeen worden verklaard op basis van bestaande theorievorming omtrent geografische spreiding van criminaliteit? Kan die theorie overigens ook uit de voeten met internetvarianten van geografische aanduiding, zoals domeinnamen (in plaats van locatie) of connectiesnelheid (in plaats van fysieke afstand)? Doordat zij dingen verandert in de context waarin criminaliteit wordt gepleegd, biedt de digitalisering van de samenleving dus nieuwe perspectieven om criminologische principes beter te leren begrijpen.

Waar hebben we het over?

Cyberspace kunnen we opvatten als sociale structuur die mensen via digitale netwerken (internet) tot stand brengen en onderhouden, innig verweven overigens met de van oudsher bestaande sociale structuur (Stol, 2010). In cyberspace kennen we behalve veel goeds ook cybercrime. Hieronder verstaan we criminaliteit die is gepleegd met behulp van een computer of netwerk. Een nader onderscheid wordt daarbij vaak aangebracht in cybercrime in brede zin (*computer-assisted crimes*) en cybercrime in enge zin (*computer-focused crimes*) (Furnell, 2002). Bij de eerste variant gaat het om traditionele delicten die met computers worden gepleegd. Het kan hierbij gaan om vermogensdelicten, zoals oplichting via internet, om onlinebedreiging, maar ook om cyberspionage of het verspreiden van kinderporno. Bij de tweede variant moeten we denken aan criminaliteit waarbij de computer of software zelf het doelwit is van criminaliteit, zoals bij DDoS-aanvallen of hacken. De gevolgen daarvan hoeven zich echter niet tot cyberspace te beperken. De DDoS-aanvallen op banken in 2012 legden het betalingsverkeer enkele dagen plat en dat had ook effecten buiten cyberspace. Gezien de rol van technologie in de besturing van vitale infrastructuren, kunnen hackers ook daar ernstige fysieke schade veroorzaken en menselijke slachtoffers maken. Denk bijvoorbeeld aan overstromingen, vliegtuig- en treinongelukken via een hack. In beleidskringen heerst dan ook de vrees voor cyberterrorisme, hoewel niet wordt ingeschat dat terroristische netwerken over de technische competenties en menskracht beschikken die nodig zijn om een geavanceerde cyberaanval te plegen (NCTb, 2010).
Hoewel deze twee vormen van cybercrime veel van alle computergerelateerde criminaliteit omvatten, heeft de inzet van hoogwaardige technologie ook tot meer diffuse vormen van criminaliteit geleid, waarbij computers of het internet wel een rol spelen, maar vermengd zijn met traditionele criminele (voorbereidings)handelingen. Een voorbeeld hiervan is drugshandel via internet, waarbij productie en transport van drugs op traditionele manieren kunnen plaatsvinden, maar het bij elkaar brengen van vraag en aanbod en de transactie tussen deze partijen via internet plaatsvinden (Vijlbrief, 2012). Een ander voorbeeld van een mengvorm is *grooming*. Anders dan bijvoorbeeld het verspreiden van kinderporno of handel in drugs is het gebruik van internet een element in de delictsomschrijving en is internet hier dus meer dan enkel een nieuwe manier om een klassiek delict te plegen.

‘Internet faciliteert criminaliteit’ … voorlopig

Vaststaat dat de digitalisering een serieus criminaliteitsprobleem met zich mee heeft gebracht en dat politie en justitie nog niet goed weten hoe daarmee om te gaan (gebrek aan kennis en digitale vaardigheden). Misschien is het meest basale probleem nog wel dat mensen in cyberspace niet zo eenvoudig zijn te identificeren en te lokaliseren: niet voor andere burgers, maar ook niet voor de overheid. In zijn kritische maatschappijanalyse wijst de Franse filosoof Michel Foucault

([1975] 1979) op basisprincipes van rechtshandhaving (of in foucaultiaanse termen 'the power of normalisation') in onze moderne samenleving. Volgens Foucault gedragen mensen zich beheerst ('gedisciplineerd') omdat de overheid controlerend op hen inwerkt. In zijn ogen is sprake van een voortdurende disciplineringsmachinerie die mensen murw en gedwee maakt. Identificatie, informatie en voortdurende observatie zijn de belangrijkste elementen van de disciplineringsmachinerie van de overheid. Foucault overleed in 1984 en heeft dus niet kunnen nadenken over gedragsregulering in het digitale tijdperk. In een eerste globale confrontatie tussen Foucaults elementen van overheidscontrole en cyberspace kunnen we constateren dat mensen op internet anoniemer zijn dan offline en dat toezicht houden op internet minder eenvoudig is dan offline. Mensen zijn in cyberspace niet eenvoudig identificeerbaar, hun verblijfplaats is lang niet altijd helder en van systematisch toezicht en informatieverzameling (productie van kennis) door de overheid is hier ook niet echt sprake. Internetsurveillance is in politiekringen een actueel onderwerp, niet omdat zij al van die goede oplossingen biedt, maar omdat politiemensen niet goed weten wat ze ermee aanmoeten. Het systeem van moderne gedragsregulering door de overheid, zoals beschreven door Foucault, is door internet tot op zekere hoogte in verlegenheid gebracht, in ieder geval voorlopig. Foucaults denkmodel leidt tot de conclusie dat politie in cyberspace geen eenvoudige opgave is en dat is ook precies wat we in onderzoek zien. Politie en justitie hebben, zeker in geval van grensoverschrijdende criminaliteit, nogal wat moeite met misdaadbestrijding in cyberspace (vgl. Stol e.a., 2013; Veenstra e.a., 2013). Aan hedendaagse wetenschappers (onder wie criminologen) laat Foucault het over om tegen de achtergrond van zijn werk studies te verrichten naar normafwijkend gedrag in cyberspace en hoe de overheid (al dan niet samen met anderen) daartegen normaliserend optreedt of zou kunnen optreden.
Of er door internet, zoals het voorgaande suggereert, per saldo meer criminaliteit in onze samenleving is, of dat het vooral of misschien zelfs alleen maar gaat om een verschuiving van off- naar onlinecriminaliteit, is een vraag waarop stellige antwoorden ontbreken.

Wat weten we over cybercrime?

Twee hoofdvragen aangaande digitalisering en criminaliteit zijn of de omvang van de criminaliteit verandert en of sprake is van verschuivingen (bijv. criminele jongeren die overgaan van straatroof op e-fraude, of georganiseerde criminaliteit die overgaat van mensenhandel op het aanleggen en uitbaten van botnets). Wordt er door de introductie van het internet meer criminaliteit gepleegd in vergelijking met daarvoor? Komt criminaliteit met een onlinecomponent 'boven op' al bestaande offlinecriminaliteit, of is er sprake van een verschuiving, waarbij computergerelateerde criminaliteit een steeds belangrijker rol inneemt ten koste van traditionele criminaliteit?
Tellingen van politiestatistieken van cybercrime worden niet alleen geplaagd door het welbekende *dark number*-probleem, maar ook door het feit dat er voor veel cyberdelicten geen aparte registratiecodes bestaan. Een inventarisatie van de rol

die computers spelen bij een misdrijf (zoals bij bedreiging, oplichting of identiteitsfraude) kan pas worden vastgesteld door het zaakdossier in te zien (vgl. Junger e.a., 2013). Bovendien was 'cybercrime' tot voor kort niet zichtbaar in de landelijke criminaliteitsstatistieken omdat er in het vaste landelijke slachtofferonderzoek tot aan 2012 eenvoudigweg niet naar werd gevraagd. Het lijkt echter wel plausibel dat het aantal keren dat de wet wordt overtreden, vanwege de digitalisering is toegenomen. Elke illegale download, elke keer dat een kinderpornografische afbeelding wordt verstuurd, elke keer dat een portretrecht wordt geschonden, elke keer dat een computer onrechtmatig wordt gebruikt, en elke keer dat online een belediging of discriminerende opmerking wordt geuit, het zijn vele schendingen van de wet waarvan niet eenvoudig is in te zien hoe daarvoor in de plaats evenveel klassieke delicten verdwijnen. Wat we betreffende de omvang in elk geval weten, is dat cybercrime in onze samenleving flink is doorgedrongen. In 2011 toonde het eerste landelijk slachtofferonderzoek cybercrime een slachtofferpercentage voor hacken van 4,3 procent (Domenie e.a., 2013). In de meting van het Centraal Bureau voor de Statistiek (CBS) van dat jaar kwam alleen fietsendiefstal nog hoger uit met 4,8 procent (CBS, 2012). Het slachtofferpercentage voor e-fraude bij koop of verkoop was in 2011 met 2,7 procent hoger dan het slachtofferpercentage voor zakkenrollerij (1,7 procent). In 2012 heeft het CBS hacken opgenomen in zijn monitor en dat jaar zien we voor hacken een slachtofferpercentage van 5,9 procent. Daarmee komt volgens dit slachtofferonderzoek het delict hacken in Nederland nu vaker voor dan fietsendiefstal (in 2012: 3,7 procent) (CBS, 2012). Ook jongeren zijn geregeld slachtoffer van e-fraude: 5,2 procent van de jongeren van 10 tot 18 jaar is ooit opgelicht bij een onlinekoop of -verkoop. Tegelijk geeft 3,1 procent van de jongeren aan ooit zelf een ander te hebben opgelicht bij een onlinekoop of -verkoop (Jansen, 2012). Kortom, cybercrime is volop aanwezig in onze samenleving. Ook neemt de klassieke criminaliteit af. Maar of er een verband is tussen deze trends is nog niet vast te stellen (Vollaard e.a., 2009).

Op microniveau dienen zich ook de nodige interessante vragen aan. Wie pleegt cybercrime en wie is slachtoffer? Zijn het 'nieuwe' daders en slachtoffers of mensen die ook bij traditionele criminaliteit betrokken waren? Indien dat laatste het geval is, stappen ze dan over op cybercrime of doen ze het 'ernaast'? Wat zijn, in bredere zin, de risicofactoren van verschillende vormen van cybercrime? Sommige bevindingen duiden erop dat cybercrime samenhangt met factoren die ook worden teruggevonden bij traditionele criminaliteit. Slachtofferstudies laten bijvoorbeeld zien dat risico's voor onlinebedreiging en -oplichting geconcentreerd zijn bij jongeren en bij personen met een lage zelfcontrole (Domenie e.a., 2013; Van Wilsem, 2011; 2013). Anderzijds zijn er ook aanwijzingen voor de assumptie dat bestaande theorieën niet opgaan voor cybercrime – en het (deels) nieuwe verklaringen behoeft. Bossler en Buruss (2011) laten voor het plegen van hacken bijvoorbeeld zien dat lage zelfcontrole geen risicofactor is; sterker nog, voor dit delict lijken er eerder indicaties voor het tegenovergestelde, omdat er vaak kennis, toewijding en volharding nodig is om de techniek te doorgronden. Daarmee is de verwachting ook dat een eventuele verschuiving van 'offlinedaders' slechts

beperkt plaats zal vinden richting deze zogenoemde *computer-focused crimes*. Al in het pre-internettijdperk gaven Cornish en Clarke (1987) aan dat de specifieke expertise en vaardigheden die verschillende vormen van criminaliteit met zich meebrengen een beletsel kunnen zijn voor verplaatsing van criminaliteit door daders naar andere delicttypen. Het zou goed kunnen dat dit ook hier geldt, maar dit behoeft uiteraard empirische toetsing.

Het artikel van **Ruiter en Bernaards** omtrent plegers van computervredebreuk (crackers) voorziet in deze behoefte – en dat is voor Nederlands onderzoek nieuw: ze onderzoeken persoonskenmerken van aangehouden verdachten van *cracking* en gaan daarbij ook na in hoeverre deze verdachten overeenstemmen met overige criminelen, ten aanzien van hun sociaal-demografische kenmerken en het verloop van hun criminele carrières. Anders dan wel wordt verondersteld (Vollaard e.a., 2009), vertonen verdachten van computervredebreuk zowel wat betreft hun sociaal-demografische kenmerken als hun leeftijdscriminaliteitsverloop sterke gelijkenissen met overige criminelen.

Vanuit een ander licht biedt de bijdrage van **Van Wilsem, Van der Meulen en Kunst** ook zicht op vragen over omvang en schade voor een vorm van criminaliteit die met de opkomst van het internet bezig is aan een snelle opmars: identiteitsfraude. In hun bijdrage staan ze stil bij de prevalentie en schade onder slachtoffers van dit delict en de mate waarin persoonskenmerken van slachtoffers gerelateerd zijn aan vergoeding van de ondervonden schade. De omvangsvraag omtrent cybercrime wordt daarmee breder getrokken door ook naar schade te kijken en naar de mogelijke sociale ongelijkheid hierin.

Criminologische theorie en cybercrime

Behalve aantonen dat criminaliteit toeneemt of verschuift, wil de criminologie de bewegingen in de criminaliteit ook verklaren. Daarvoor beschikt zij over theorie. Die is ontwikkeld voor de offlinewereld; waarmee de vraag ontstaat in hoeverre deze 'oude theorie' behulpzaam kan zijn bij het begrijpen van criminaliteit in cyberspace. Kunnen we die theorieën nu wel afschrijven of krijgen ze juist nieuwe perspectieven? Verschillende auteurs hebben zich die vraag gesteld en hebben de bruikbaarheid van oude theorieën in een digitale wereld beproefd (bijv. Grabosky, 2001; Yar, 2005). Naast directe toepasbaarheid van theorieën of de bevinding dat zij juist niet bruikbaar lijken, wordt ook nog een derde variant aangetroffen: de theorie blijkt bruikbaar, maar in voor de context van het internet aangepaste vorm. De routineactiviteitentheorie is hiervan een voorbeeld. Deze wordt voor cybercrime toegepast, maar de vertrouwde concepten van dadernabijheid, blootstelling aan daders, aantrekkelijkheid en bescherming tegen daders (Cohen e.a., 1981) worden in de operationalisering in daartoe relevante begrippen gegoten, zoals de hoeveelheid tijd die aan specifieke internetactiviteiten wordt besteed, computerkennis van de gebruiker, gebruik van beschermingssoftware en beschikbaarheid van persoonlijke informatie op sociaalnetwerksites (Holt & Bossler, 2009; Reyns, 2013; Van Wilsem e.a., 2010; Domenie e.a., 2013). Ook zien we dat

bestaande risicofactoren nieuw leven wordt ingeblazen in de veronderstelling dat computergebruik er invloed op kan hebben. Een belangrijk voorbeeld hiervan is disinhibitie – het wegvallen van remmingen in specifieke situaties – waarbij wordt aangenomen dat dit aangewakkerd wordt door het internet, waarbij in sociale interacties vaak sprake is van anonimiteit en fysieke onzichtbaarheid (Suler, 2004; Kerstens & Stol, 2012).

De bijdragen aan dit themanummer van respectievelijk **Kerstens en Veenstra** en **Jansen, Leukfeldt, Van Wilsem en Stol** hanteren vorenstaande invalshoek. Kerstens' en Veenstra's bijdrage behandelt het zogenoemde cyberpesten door scholieren en vergelijkt dit met offline pesten. Hierin wordt niet alleen gekeken naar de rol van bindingen met anderen op beide vormen van pesten, maar onder andere ook specifiek naar de rol van onlinedisinhibitie bij deze gedragingen. De bijdrage van Jansen e.a. past de routineactiviteitentheorie toe op slachtofferschap van uiteenlopende delicten, door een ruime verscheidenheid aan computeractiviteiten te relateren aan de kans om gehackt, online gestalkt of bedreigd te worden.

Onlineonderzoek en onderzoek naar onlineverschijnselen

Ook voor het doen van criminologisch onderzoek vormt de komst van computertechnologie een uitbreiding van de mogelijkheden. Allereerst zijn er traditionele dataverzamelingsmethoden die nu online kunnen worden ingezet, zoals bijvoorbeeld dader- en slachtofferenquêtes. Los van het feit dat hiermee tegen lagere kosten en inspanning *(convenience) samples* kunnen worden getrokken, is het ook interessant om te kijken naar de effecten die online enquêteren heeft. Hierover is verrassend weinig criminologisch onderzoek verricht. Enkele studies duiden erop dat onlinesurveys gepaard gaan met een hogere respons, maar vooral onder studenten (Shih & Fan, 2008) en dat antwoordpatronen anders zijn. In algemene zin kan worden verwacht dat het beantwoorden van gevoelige vragen eerlijker wordt naarmate de setting anoniemer is; een onlinesurvey, waarbij er geen sprake is van een interviewer die de antwoorden noteert, is een enquêtevorm die dergelijke anonimiteit in hogere mate met zich meebrengt. Inderdaad worden met dergelijke surveys hogere percentages gevonden voor zaken als drugsgebruik en deviant seksueel gedrag (Tourangeau & Yan, 2007). Voor crimineel gedrag zal onderzoek naar dergelijke *mode effects* nog verder in kaart moeten worden gebracht.
Ten tweede zijn er door de digitalisering nieuwe gegevensbronnen waar criminologisch relevant materiaal te vinden is. Een belangrijke ontwikkeling hierin vormt de opkomst van Big Data: gegevens van mensen (of objecten) die geautomatiseerd worden opgeslagen en op onderliggende patronen kunnen worden geanalyseerd. Een voorbeeld vormen registraties van Twitterboodschappen (Procter e.a., 2013) of van transacties bij creditcardmaatschappijen. Big Data afkomstig van sociale media kunnen bijvoorbeeld worden gebruikt om meningsvorming over een bepaald onderwerp vast te stellen. Big Data van klantendatabases kunnen worden aangewend om te zoeken naar afwijkingen van gangbare patronen, die kunnen duiden op fraude (Bolton & Hand, 2002). Een ander mooi voorbeeld verscheen

onlangs in het *Tijdschrift voor Criminologie*: Soudijn en Monsma (2012) analyseerden de activiteiten binnen een onlineforum waarin samenwerking voor creditcardfraude werd gefaciliteerd door de uitwisseling van tips en het contact leggen voor samenwerkingsverbanden. Van dit forum was door het Team High Tech Crime een digitale kopie gemaakt waarmee communicatiepatronen uit ruim 200.000 berichten konden worden bekeken. Andere nieuwe mogelijkheden voor het verzamelen van data die het internet biedt, zijn participerende observatie, bijvoorbeeld in *multiplayer games*. Het onderzoek van Van Dijk (2011) laat bijvoorbeeld op deze manier zien dat in Habbo Hotel, een onlinegame voor kinderen, het nodige aan deviant gedrag voorkomt, zoals schelden en stelen van virtuele goederen. Ook inhoudsanalyse van onlinecontent is een groeiende tak van criminologische wetenschap. De online-uitingen van deviante groeperingen (Gerstenfeld e.a., 2003), of de faciliterende rol van internet voor georganiseerde misdaad, kunnen op deze wijze worden bestudeerd. Complicerend hierbij is dat het altijd de vraag is in hoeverre onlinebeweringen ook daadwerkelijk offline worden waargemaakt. Ook worden deviante of verboden uitingen op afgeschermde omgevingen geplaatst, zoals het zogenoemde Dark Web (zie bijv. Chen e.a., 2008). In een verkennend onderzoek laat Fung (2013) zien dat dit Dark Web technisch relatief eenvoudig te betreden valt, maar dat het bestaan van de daar aangeboden criminele waar nauwelijks valt te verifiëren doordat andere bezoekers nauwelijks informatie over zichzelf prijsgeven. Ook riskeert de onderzoeker zelf betrokken te raken bij criminaliteit, bijvoorbeeld door het ongewild downloaden van kinderporno. Het is de vraag of justitie, maar ook de onderzoeksinstelling als werkgever, ruimte zal willen geven aan dergelijk wetenschappelijk onderzoek.

Ten derde kan computertechnologie gebruikt worden als een aanvullend hulpmiddel voor onderzoek waarmee de respondent aan virtuele situaties kan worden blootgesteld en daarover worden bevraagd. Een voorbeeld daarvan is het onderzoek van Vanderveen en Koemans (2012), waarin respondenten door een virtuele wijk 'wandelden' om hun mening over de (door de onderzoekers gemanipuleerde) lokale graffiti te geven. Een ander voorbeeld betreft het experimentele onderzoek van Van Gelder e.a. (2013), waarbij respondenten werden geconfronteerd met een avatar die henzelf uitbeeldde. In de experimentele conditie beeldde de avatar de respondent uit in een beduidend oudere versie van zichzelf – wat via digitale *facial morphing* van het gezicht tot stand kwam – terwijl in de controleconditie de avatar hun huidige (niet-verouderde) zelf betrof. Degenen in de experimentele conditie maakten zich in een vervolgtest minder vaak schuldig aan oplichting dan in de controleconditie. Mogelijk zorgen beelden van hoe mensen er in de toekomst uitzien voor een verminderde oriëntatie op het hier en nu – en een focus op de lange termijn – en daarmee op een verminderde kans op delinquentie.

Preventie van cybercrime

De oogst is op het gebied van de preventie van computergerelateerde criminaliteit tot dusverre niet rijk. Als eerste presenteren Leeuw en Leeuw (2012) een *systematic review* van evaluatieonderzoek naar maatregelen tegen illegaal downloaden van

onlinecontent. Zij vonden veertien studies op dit gebied. De meerderheid hiervan betrof echter plannen voor evaluatie, terwijl de resterende empirische studies niet of nauwelijks voldeden aan de interne validiteitsvereisten, zoals randomisering van condities of überhaupt het werken met een controlegroep. Leeuw en Leeuw (2012) merken hier terecht over op dat er sprake is van 'room for improvement' (p. 122). Ten tweede biedt het Campbell Collaboration-rapport van Mishna e.a. (2009) ook een *systematic review*, maar dan van andere problematiek, namelijk zogenoemde *cyber abuse* onder kinderen. Dit is een paraplubegrip waaronder uiteenlopende activiteiten vallen, zoals 'cyber bullying, cyber stalking, cyber sexual solicitation [vgl. *grooming*; JvE, WS & JvW], and cyber pornography' (p. 5). Binnen de inclusiecriteria van de Campbell Collaboration (pre- en posttest en een controlegroep naast de experimentele groep) bleven er maar weinig studies over die expliciet gericht waren op kinderen (of hun ouders): drie. Uit een daarvan bleek dat het risicobewustzijn van kinderen door een voorlichtingscampagne was toegenomen, maar hun concrete internetgedrag niet was veranderd. Ook op dit gebied is er gezien de beperkte hoeveelheid studies sprake van veel onontgonnen terrein.

Tot slot is er vanuit slachtofferstudies het een en ander bekend geworden over de effectiviteit van technische beschermingsmaatregelen (firewall, virusscanner, enz.) op het ervaren van computergerelateerde delicten als hacken en *malware*-infectie (Bossler & Holt, 2009; Ngo & Paternoster, 2011). Uit deze onderzoeken bleek geen relatie tussen mate van bescherming en slachtofferrisico. Wel dienen daar twee kanttekeningen bij te worden geplaatst. Ten eerste betreft het hier crosssectionele studies, waarbij de timing van het beveiligingsgedrag en het incident niet nauwkeurig is vastgelegd. Dat brengt het risico met zich mee dat het beveiligingsgedrag in sommige gevallen heeft plaatsgevonden na de slachtoffer-ervaring. Ten tweede is het vaststellen van risicofactoren van slachtofferschap van dit soort delicten in zijn algemeen – en dus ook met betrekking tot beschermingsmaatregelen – moeilijk omdat niet elk doelwit weet heeft van zijn of haar slachtofferervaring. Het vereist enige computerervaring en -inzicht om te weten of er sprake is geweest van bijvoorbeeld *malware* op de computer. In die zin zijn dadergeoriënteerde studies vereist waarin wordt nagegaan op welke factoren men let bij het 'kiezen' van bepaalde slachtoffers voor dit type criminaliteit.

Internet als wapen tegen criminaliteit

Internet is niet alleen een platform voor criminaliteit, maar kan ook worden ingezet *tegen* criminaliteit, ten behoeve van toezicht en handhaving. Dit onderwerp is in dit themanummer nog onderbelicht. Voor toezichthoudende instanties vormen internet en sociale media een manier om in contact met de burger te treden, enerzijds om hen te informeren over het toezicht, en anderzijds om tips en meldingen te ontvangen. De politie bijvoorbeeld maakt gebruik van Twitter, van websites (depolitiezoekt.nl), YouTube, apps, Burgernet en Amber Alert. Het doel van dergelijke communicatie is in de eerste plaats het beter zichtbaar maken van het politiewerk – men verwacht dat onlinecommunicatie een bijdrage kan leveren aan

het imago van de politie als een moderne, professionele en open organisatie, en daarmee aan het vertrouwen in de politie (Cornelissens & Ferwerda, 2010; Bekkers & Meijer, 2010, 113 e.v.). De brede doelstelling maakt het echter moeilijk de opbrengsten van deze initiatieven te meten. In de ervaring van politieagenten kan Twitter een waardevolle rol spelen in *community policing* in wijken; op dat niveau ontvangt de politie ook actief reacties van burgers. 'Een beter netwerk' vertaalt zich wellicht indirect in betere resultaten, maar of door het twitteren van wijkagenten uiteindelijk de criminaliteit beter wordt bestreden, is een vraag die nog op een empirisch onderbouwd antwoord wacht (Meijer e.a., 2013).

Internet wordt ook gebruikt voor het verspreiden van opsporingsberichten, in aanvulling op het klassieke medium televisie. Effectiviteitsonderzoek naar opsporingsberichtgeving via het televisieprogramma Opsporing Verzocht (Van Erp e.a., 2012) wees uit dat het aantal kijkers bepalend is voor het succes van een opsporingsbericht. Ook in het tijdperk van social media is televisie daarom nog altijd het belangrijkste kanaal voor opsporingsberichtgeving – wekelijks kijkt ruim een miljoen Nederlanders naar Opsporing Verzocht. Uitzending via Opsporing Verzocht doet de kans op oplossing stijgen met 15 procentpunt ten opzichte van niet-uitgezonden zaken; en het oplossingspercentage daalt als er minder mensen kijken. Opsporingsberichtgeving via internet kent in de verste verte niet de massale kijkersaantallen als Opsporing Verzocht. Alleen berichten met een hoge maatschappelijke urgentie worden actief op internet verspreid. Digitale media kunnen wel ondersteunend werken om een gerichte doelgroep te bereiken.

Aan het inschakelen van burgers in de opsporing wordt wel het predicaat 'burgerrechercheur' verbonden. Het is de vraag of dit helemaal terecht is: het gebruik van nieuwe media door de politie is vooral nog een nieuwe manier om hetzelfde te doen – face-to-facecontact wordt vervangen door online zenden van en vragen om informatie, zonder dat sprake is van daadwerkelijke interactiviteit (Meijer e.a., 2013). Enkele keren worden ook innovatievere manieren ontwikkeld om het internet te benutten, zoals onlinegames om op nieuwe manieren informatie te ontvangen of scenario's te exploreren (Bos & Broer, 2011). Over het algemeen is de politie redelijk traditioneel en terughoudend in het gebruik van internet en sociale media. Dat heeft deels te maken met gebrekkige kennis en ICT-faciliteiten en deels met juridische kaders: de publicatie van opsporingsberichten dient gepaard te gaan met een zorgvuldige afweging van belangen, niet alleen van de privacy van verdachten, maar ook van getuigen, slachtoffers en andere betrokkenen. Maar het is ook een kwestie van controle: veel politiemensen vrezen dat verdergaande digitale interactie leidt tot informatiestromen die niet te beheersen zijn.

Maar het is de vraag in hoeverre het politiemonopolie op de publicatie van opsporingsberichten nog brede publieke en politieke steun heeft. In Nederland is de minister van Veiligheid en Justitie voornemens de mogelijkheden voor burgers te verruimen om camerabeelden die betrekking hebben op strafbare feiten zelf te publiceren. Het hiertoe strekkende wetsvoorstel is inmiddels ingetrokken.[1]

1 https://zoek.officielebekendmakingen.nl/dossier/33662/kst-33662-4?resultIndex=6&sorttype=1&sortorder=4.

Mogelijk speelde hierbij een rol dat de Raad van State het wetsvoorstel onvoldoende onderbouwd vond, mede in het licht van de vergaande inbreuk op de privacy van slachtoffers, getuigen en onterecht verdachte personen. Het publiceren van gegevens over verdachten op internet blijft voor burgers voorlopig dus nog verboden, hoewel de praktijk uitwijst dat men zich van dit verbod over het algemeen weinig aantrekt. Websites als geenstijl.nl, boevenvangen.nl en opgelichtopinternet.nl verspreiden opsporingsberichten en andere politie-informatie, soms met een commercieel oogmerk, soms met een preventief doel door informatie uit te wisselen over onbetrouwbare internethandelaren. Het interessantst is de berichtgeving op geenstijl.nl, die veel meer dan opsporing is gericht op *shaming* van overtreders: informele bestraffing door de dader op internet bekend te maken en te veroordelen. Het bekendste recente voorbeeld is de uitzending van de beelden van een mishandeling in Eindhoven door Opsporing Verzocht, die uitmondde in een 'manhunt' op GeenStijl, waarbij de verdachten op internet en in de echte wereld zodanig werden bedreigd dat ze zelf beveiliging nodig hadden. Dit is een voorbeeld van 'out of control' internet-*shaming*, die de Amerikaanse privacyjurist Daniel Solove (2007, 102) typeert als buitenproportioneel en losgezongen van de context: 'Shaming becomes uncivil, moblike, and potentially subversive of the very social order it tries to protect.'

Zo creëert het internet nieuwe vormen van punitiviteit die buitenproportioneel kunnen uitpakken. Internet-*shaming* is tot dusver voornamelijk onderzocht door privacyjuristen en mediasociologen. Maar de vraag in welke mate het stigma van 'bestraffing' op internet doorwerkt in de offlinewereld, is ook een belangrijke penologische vraag. Internetsites kunnen een permanent, openbaar toegankelijk strafblad creëren (Solove, 2007). In de Verenigde Staten worden strafbladen, vanouds al openbaar, nu nog toegankelijker gemaakt door ze in onlineregisters te plaatsen. Ook namen, woonplaatsen en foto's van zedendelinquenten zijn openbaar toegankelijk via Megan's Law-websites,[2] met bijbehorende app die een alarm geeft als je in de buurt van een verblijfslocatie van een zedendelinquent komt.[3] Jacobs en Larrauri (2012) plaatsen het in de Verenigde Staten geldende recht op informatie over antecedenten in de context van het grondrecht op zelfbescherming, zoals het recht op wapenbezit. Informatie over antecedenten geldt in de Verenigde Staten daarmee als een publiek goed. In Europese landen geldt vanouds de opvatting dat het verspreiden van informatie over veroordelingen een straf is die buitenproportioneel en stigmatiserend is. Deze informatie behoort in de Europese politieke traditie niet in het publieke domein, maar in handen van overheidsorganisaties. Het is de vraag hoe lang dit onderscheid tussen de Europese en Amerikaanse traditie nog blijft bestaan, nu ook in Europese landen stigmatisering, ter bescherming van het publiek of met punitief oogmerk, een hernieuwde populariteit kent. Het internet zou deze ontwikkelingen kunnen versterken – het is een van de 'dingen' die techniekfilosoof Peter-Paul Verbeek in zijn boek *De daadkracht der dingen* (2000) als morele entiteiten benoemt die mede vormgeven aan de vraag 'hoe te leven'. Als informatie over daders via internet steeds gemak-

2 Voor een voorbeeld zie www.meganslaw.ca.gov/.

3 https://play.google.com/store/apps/details?id=com.fsp.android.h&hl=nl.

kelijker openbaar en vindbaar wordt, komt ook de vraag op of de onlinecommunity manieren vindt om informatie 'ongedaan te maken' om daders de mogelijkheid te geven terug te keren in de maatschappij. In zijn boek *Delete* stelt Mayer-Schonberger (2009) daarom dat het internet onze maatschappij verandert van een maatschappij waarin we moeite moeten doen om informatie te bewaren, naar een samenleving waarin we moeite moeten doen om zaken te vergeten.
Maar internet biedt niet alleen bestraffing, internet biedt ook bescherming. Door Amber Alert of Burgernet kunnen omstanders worden geactiveerd om misdrijven te voorkomen. Via Twitter en Facebook kunnen slachtoffers om hulp vragen – na de terroristische aanslag van Breivik op het Noorse eiland Utoya werden mensen die zich in de omgeving op het water bevonden, op deze manier geïnformeerd en konden zij eerste hulp bieden (Van Duijn, 2011). Mensenrechtenactivisten dragen een armband, vergelijkbaar met een elektronische enkelband, die een tweet uitstuurt op het moment dat het zegel wordt verbroken, om de buitenwereld te informeren als zij worden gearresteerd. Internet en sociale media kunnen totalitaire, repressieve regimes ondermijnen, zoals tijdens de Arabische Lente, en de internationale gemeenschap alarmeren over misdrijven van regimes die geen journalisten toelaten – onze informatie over Syrië komt voor een groot deel via blogs en Facebookberichten. En ook in westerse landen speelt de website WikiLeaks een rol bij het onthullen van staatsmisdrijven of *state-corporate crimes*. Kortom, internet verandert de verhouding tussen vrijheid en controle op nieuwe en onvoorziene manieren (Solove, 2007, 205). Criminologen die zich bezighouden met sociale controle mogen dit niet laten liggen.

Opsporing in cyberspace

Hoewel cybercrimebestrijding de inzet vraagt van veel partijen (bijv. producenten, gebruikers, aanbieders van webdiensten, internet service providers, overheid) hebben politie en justitie een speciale positie. Zij beschikken immers over opsporingsbevoegdheden, ook speciaal voor opsporing in een digitale omgeving (bijv. art. 125i t/m 125o Sv). Een van de dringende kwesties op dit gebied is hoe ver de bevoegdheden van de politie in cyberspace reiken en hoe effectief ze zijn. De politie mag bijvoorbeeld, net als ieder ander, rondkijken op internet en informatie verzamelen (*'internetsurveillance'*). Maar het 'systematisch verzamelen' van informatie is een bijzondere opsporingsbevoegdheid (art. 126j Sv) die pas mag worden uitgeoefend indien aan twee voorwaarden is voldaan: er moet sprake zijn van een verdachte en van een bevel van de officier van justitie om over die verdachte systematisch informatie te verzamelen. Internet maakt het zeer eenvoudig om systematisch informatie over iemand te verzamelen. De politie staat nu voor de vraag waar het altijd toegelaten 'rondkijken' overgaat in het aan voorwaarden gebonden 'systematisch informatie verzamelen', en voor de vraag hoe effectief die methode is. Een ander voorbeeld is de kwestie die kinderhulporganisatie Terre des Hommes in november 2013 via diverse media op de publieke agenda plaatste door met een 10-jarig virtueel Filipijns meisje (een computeranimatie) in tien weken tijd ruim duizend mannen te lokken die in chatrooms uit waren op (web-

cam)seks met kinderen en van hen persoonsgegevens te achterhalen. Terre des Hommes adviseert de politie deze methode over te nemen. Of de methode juridisch gezien toelaatbaar moet worden geacht is primair een vraag voor juristen; voor criminologen is vooral de vraag wat deze en andere nieuwe methoden betekenen in termen van effectiviteit. Sinds de Parlementaire Enquêtecommissie Opsporingsmethoden (1996) was de onduidelijkheid omtrent het gebruik van politiebevoegdheden niet zo groot als vandaag de dag in cyberspace.

Nog veel te doen

Er is, zo maakt het vorenstaande duidelijk, nog veel te doen als het gaat om cybercrime. Dit themanummer levert daaraan een wetenschappelijke bijdrage, maar tegelijk valt op dat de huidige bijdragen zich inhoudelijk vooral concentreren op determinanten van uiteenlopende vormen van daderschap en slachtofferschap van cybercrime. Andere thematiek die we in deze introductie hebben behandeld – zoals preventie van cybercrime in brede zin, het gebruik van ICT-middelen door politie en justitie, het gebruik van Big Data en van virtuele omgevingen voor de beantwoording van onderzoeksvragen – is echter niet vertegenwoordigd in dit themanummer. Op allerlei terreinen binnen het cybercrimeveld is er voor wetenschappers veel te ontginnen.
Voor het bevoegde gezag geldt dat het zijn weg moet vinden in een digitale wereld en nieuwe vraagstukken omtrent criminaliteit en opsporing moet zien op te lossen. Ook de criminologie moet haar weg vinden, maar dan met het in kaart brengen en vooral helpen begrijpen van de nieuwe fenomenen en ontwikkelingen. Daarvoor is vermoedelijk nog wel even de tijd, want het is niet te verwachten dat de criminaliteitsproblemen waarvoor de digitalisering onze samenleving stelt snel tot het verleden zullen behoren. Dat kunnen we althans concluderen uit hoeveel tijd het nam voordat onze samenleving de negatieve gevolgen van een andere massaal ingevoerde nieuwe technologie heeft weten terug te dringen: het aantal dodelijke slachtoffers als gevolg van de toegenomen verkeersmobiliteit vanaf de jaren vijftig in de vorige eeuw. In 1950 vielen er in Nederland 1.082 verkeersdoden. Dat aantal steeg tot een recordaantal dodelijke slachtoffers van 3.460 in 1972. Daarna zette de daling eindelijk in om in 2001 – dus na 50 jaar werken aan de verkeersveiligheid – weer uit te komen op dezelfde hoogte als in 1950 (Goldenbeld e.a., 2002; SWOV, 2007). Het succes is te danken aan een veelheid elkaar versterkende maatregelen (bijv. technische verbeteringen, gedragsbeïnvloeding) met inbreng van diverse partijen (bijv. fabrikanten, overheid, wetenschap). In 2012 vielen er niet meer dan 650 doden in het verkeer (CBS). Natuurlijk gaat de vergelijking in vele opzichten mank, maar de casus van de verkeersproblematiek leert ons in elk geval dat wanneer een massaal in gebruik genomen nieuwe technologie leidt tot ongewenste neveneffecten, het mogelijk is om die effecten met succes tegen te gaan – en dat daarvoor tijd nodig is. We zijn met internet nu nog geen twintig jaar onderweg en het kan dus nog wel even duren voordat we grip krijgen op de negatieve neveneffecten: cybercrime in dit geval. Het verkeersvoorbeeld leert ook dat de wetenschappen, zowel de technische als de maatschappijweten-

schappen, een belangrijke rol daarbij spelen. Het *Tijdschrift voor Criminologie* hoopt met dit themanummer een bijdrage in die richting te leveren.

Literatuur

Bekkers, V. & Meijer, A. (2010). *Cocreatie in de publieke sector. Een verkennend onderzoek naar nieuwe, digitale verbindingen tussen overheid en burger*. Den Haag: Boom juridische uitgevers.

Bolton, R.J. & Hand, D.J. (2002). Statistical fraud detection: a review. *Statistical Science, 17*, 235-255.

Bos, E. & Broer, W. (2011). Innovatie in de opsporing: social gaming als methode. In: L.G. Moor, F. Hutsebaut, P. van Os & D. van Ryckeghem (red.). *Burgerparticipatie. Cahiers Politiestudies 19*. Antwerpen/Apeldoorn: Maklu, 89-106.

Bossler, A.M. & Buruss, G.W. (2011). The general theory of crime and computer hacking: low self-control hackers? In: T.J. Holt & B.H. Schell (eds.). *Corporate hacking and technology-driven crime: social dynamics and implications*. Hershey, PA: Information Science Reference, 38-67.

Bossler, A.M. & Holt, T.J. (2009). On-line activities, guardianship, and malware infection: an examination of routine activities theory. *International Journal of Cyber Criminology, 3*, 400-420.

Centraal Bureau voor de Statistiek (CBS) (2012). *Veiligheidsmonitor 2012*. Den Haag: CBS.

Chen, H., Chung, W., Reid, E., Sageman, M. & Weimann, G. (2008). Uncovering the Dark Web: a case study of jihad on the web. *Journal of the American Society for Information Science and Technology, 59*, 1347-1359.

Cohen, L.E, Kluegel, J.R., & Land, K.C. (1981). Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *American Sociological Review, 46*, 505-524.

Cornelissens, A. & Ferwerda, H. (2010). *Burgerparticipatie in de opsporing. Een onderzoek naar de aard, werkwijze en opbrengsten*. Reed Business: Amsterdam.

Cornish, D.B. & Clarke, R.V. (1987). Understanding crime displacement: an application of rational choice theory. *Criminology, 25*, 933-947.

Dijk, T. van (2011). *Kommer en kwel in het hotel? De veiligheidsrisico's voor en veroorzaakt door jongeren in Habbo Hotel* (afstudeerscriptie NHL Hogeschool). Leeuwarden.

Domenie, M.M.L., Leukfeldt, E.R., Wilsem, J.A. van, Jansen, J. & Stol, W.Ph. (2013). *Slachtofferschap in een gedigitaliseerde samenleving*. Den Haag: Boom Lemma uitgevers.

Duijn, M. van (2011). Sociale media en crisisbeheersing. In: P. Tops & G. Snel (red.). *Een wereld te winnen. Sociale media en politie, een eerste verkenning*. Apeldoorn: Politieacademie.

Erp, J. van, Gastel, F. van & Webbink, D. (2012). *Opsporing Verzocht. Een quasi-experimentele studie naar de bijdrage van het programma Opsporing Verzocht aan de oplossing van delicten* (Politiewetenschap nr. 61). Amsterdam: Reed Business.

Foucault, M. ([1975] 1979). *Discipline and punish*. New York: Vintage Books.

Fung, K. (2013). *Het deep web: waar Big Brother je niet ziet* (masterscriptie Erasmus Universiteit). Rotterdam.

Furnell, S. (2002). *Cybercrime: vandalizing the information society*. Boston: Addison-Wesley.

Gelder, J.L. van, Hershfield, H.E. & Nordgren, L.F. (2013). Vividness of the future self predicts delinquency. *Psychological Science*. DOI: 10.1177/0956797612465197.

Gerstenfeld, P.B., Grant, D.R. & Chiang, C. (2003). Hate online: a content analysis of extremist internet sites. *Analyses of Social Issues and Public Policy, 3*, 29-44.

Goldenbeld, C., Bax, C. & Schagen, I. van (2002). Verkeersveiligheid in Nederland. *Tijdschrift voor Veiligheid en Veiligheidszorg, 1*(1), 5-17.

Grabosky, P. (2001). Virtual criminality: old wine in new bottles? *Social & Legal Studies, 10*, 243-249.

Holt, T. & Bossler, A. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*, 1-25.

Jacobs, J. & Larrauri, E. (2012). Are criminal convictions a public matter? The U.S. and Spain. *Punishment & Society, 14*, 3-28.

Jansen, J. (2012). Online financieel-economische criminaliteit. In: J. Kerstens & W. Stol (red.). *Jeugd en cybersafety*. Den Haag: Boom Lemma uitgevers, 105-134.

Junger, M., Montoya, L. & Hartel, P. (2013). *Modus operandi onderzoek naar door informatie en communicatie technologie (ICT) gefaciliteerde criminaliteit*. Enschede: Universiteit Twente.

Leeuw, F. & Leeuw, B. (2012). Cyber society and digital policies: challenges to evaluation? *Evaluation, 18*, 111-127.

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

Mayer-Schönberger, V. (2009). Delete: the virtue of forgetting in the digital age. Princeton: Princeton University Press.

Meijer, A.J., Grimmelikhuijsen, S.G., Fictorie, D., Thaens, M. & Siep, P.A. (2013). *Politie & sociale media. Van hype naar onderbouwde keuzen* (Politiewetenschap nr. 64). Amsterdam: Reed Business.

Mishna, F., Cook, C., Saini, M., Wu, M. & MacFadden, R. (2009). *Interventions for children, youth, and parents to prevent and reduce cyber abuse: a meta-analytic review*. Campbell Collaboration. DOI: 10.4073/csr.2009.2.

Nationaal Coördinator Terrorismebestrijding (NCTb) (2010). *Jihadisten en internet. Update 2009*. Den Haag: NCTb.

Ngo, F.T. & Paternoster, R. (2011). Cyber crime victimization: an examination of individual and situational level factors. *International Journal of Cyber Criminology, 5*, 773-793.

Parlementaire Enquêtecommissie Opsporingsmethoden (1996). *Inzake opsporing*. Den Haag: Sdu.

Procter, R., Vis, F. & Voss, A. (2013). Reading the riots on Twitter: methodological innovation for the analysis of big data. *International Journal of Social Research Methodology, 16*, 197-214.

Reyns, B.W. (2013). Online routines and identity theft victimization. Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50*, 216-238.

Shih, T. & Fan, X. (2008). Comparing response rates from web and mail surveys: a meta-analysis. *Field Methods, 20*, 249-271.

Solove, D. (2007). *The future of reputation: gossip, rumor, and privacy on the internet*. New Haven, CT: Yale University Press.

Soudijn, M. & Monsma, E. (2012). Virtuele ontmoetingsruimtes voor cybercriminelen. Tijdschrift voor criminelen. *Tijdschrift voor Criminologie, 54*, 349-360.

Stichting Wetenschappelijk Onderzoek Verkeersveiligheid (SWOV) (2007). *De top bedwongen. Balans van de verkeersonveiligheid in Nederland 1950-2005*. Leidschendam: SWOV.

Stol, W. (2010). *Cybersafety overwogen. Een introductie in twee lezingen*. Den Haag: Boom Juridische uitgevers.

Stol, W., Leukfeldt, R. & Klap, H. (2013). Policing a digitized society. The state of affairs in the Netherlands in 2013. In: W.Ph. Stol & J. Jansen (eds.). *Cybercrime and the police*. The Hague: Eleven International Publishers, 61-74.

Suler, J.R. (2004). The online disinhibition effect. *CyberPsychology and Behavior, 7*, 321-326.

Tourangeau, R. & Yan, T. (2007). Sensitive questions in surveys. *Psychological Bulletin, 133*, 859-883.

Vanderveen, G. & Koemans, M. (2012). Omgevingscriminologie 2.0. Criminologisch onderzoek in een virtuele omgeving. *Tijdschrift voor Criminologie, 54*, 373-387.

Veenstra, S., Leukfeldt, R. & Boes, S. (2013). Fighting crime in a digitized society. The criminal justice system and public-private partnerships in the Netherlands. In: W.Ph. Stol & J. Jansen (eds.). *Cybercrime and the police*. The Hague: Eleven International Publishers, 75-87.

Verbeek, P. (2000). *De daadkracht der dingen*. Amsterdam: Boom.

Vijlbrief, M. (2012). *Synthetische drugs en precursoren. Criminaliteitsbeeldanalyse 2012*. Woerden: KLPD.

Vollaard, B., Versteegh, P. & Brakel, J. van den (2009). *Veelbelovende verklaringen voor de daling van de criminaliteit na 2002*. www.politieenwetenschap.nl.

Wilsem, J. van (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology, 8*, 115-127.

Wilsem, J. van (2013). 'Bought it, but never got it.' Assessing risk factors for online consumer fraud victimization. *European Sociological Review, 29*, 168-178.

Wilsem, J. van e.a. (2010). Is online zichtbaarheid riskant? Onterechte bankafschrijvingen en persoonlijke informatie op sociale netwerksites. *Proces, 89*, 344-354.

Yar, M. (2005). The novelty of 'cybercrime': an assessment in light of routine activity theory. *European Journal of Criminology, 2*, 407-427.