Misschien is het dié gemeenschap die zich, ondanks de dominante macro- en micropolitieke logica's van staten, deelstaten en/of confederaties, assertief uit te spreken heeft over het soort dienstverlening waartoe zij zich ten aanzien van de asielzoekers gehouden weet. Weze het misschien nog meer om haar eigen waardigheid, dan die van de asielzoeker.

Criminologie en strafrechtstheorie / Criminology and Criminal Law Theory

Slachtofferschap van cybercrime
Twee theorieën en zes problemen waar onderzoekers mee aan de slag moeten

Johan van Wilsem[a]

[a] Universitair Hoofddocent, Afdeling Criminologie, Universiteit Leiden (Corresp.: J.A.van.Wilsem@LAW.leidenuniv.nl).

In de huidige gedigitaliseerde samenleving speelt het Internet een steeds belangrijker rol bij de totstandkoming van criminaliteit (Van Erp, Stol & Van Wilsem, 2013). Allereerst is onder invloed van de technologische ontwikkelingen nieuwe criminaliteit ontstaan in de vorm van aanvallen gericht tegen computers of netwerken, via hacken, malware of botnets. Daarnaast geldt voor diverse bestaande delictsvormen dat zij er een digitale variant bij hebben gekregen, zoals oplichting, bedreiging en identiteitsfraude. Ten slotte zijn er ook hybride vormen van criminaliteit ontstaan waarbij offline en online gedragingen worden gecombineerd voor het nastreven van illegale doeleinden, zoals het gebruik van moderne communicatiemiddelen bij mensensmokkel (Jandl, 2007) of de inzet van online verkoopsites voor de handel in drugs (Vijlbrief, 2012).

Twee theorieën

De afgelopen jaren zijn er met betrekking tot de eerste twee bovenvermelde vormen van cybercrime – de zogenaamde *computer-focused crimes* en *computer-assisted crimes* (Furnell, 2002) – de nodige studies uitgevoerd in de V.S. en Europa, veelal aan de hand van slachtofferenquêtes. Wat zijn de patronen die we daarin tot dusverre waarnemen? Een dergelijke veelomvattende vraag laat zich niet eenvoudig beantwoorden, maar laat zich het beste leiden aan de hand van criminologische theorieën die tot dusverre zijn ingezet ter verklaring van dit fenomeen. Dominant hierin zijn de routine-activiteitentheorie en de zelfcontroletheorie. Beide theorieën hebben een algemeen karakter en lijken vanuit een algemeen principe criminaliteitsverschijnselen te willen verklaren. Voor de zelfcontroletheorie geldt dit zeker. Deze theorie – die van oorsprong door Gottfredson en Hirschi (1990) werd geformuleerd als een dadergeoriënteerde theorie – is sinds ongeveer 15 jaar in opmars als theorie, mede ter verklaring van slachtofferschap (zie voor een overzichtsartikel Pratt *et al.*, 2013). Het uitgangspunt is in principe toepasbaar op alle vormen van criminaliteit – en dus ook op uiteenlopende cybercrimes – en luidt dat impulsief handelen en een focus op korte-termijndoelen en het negeren van lange-termijndoelen leiden tot betrokkenheid in situaties waarin men sneller in de problemen raakt, zoals een ruzie, verkeersongeval, oplichting of ander onheil. Voor slachtofferschap van offline criminaliteit is de theorie inmiddels inderdaad veelvuldig bevestigd en dit geldt in toenemende mate ook voor uiteenlopende *computer-assisted crimes*, zoals online bedreiging en oplichting. Voor slachtofferschap van *computer-focused crimes*, zoals gehackt worden en malware besmetting ontbreekt deze bevestiging van de hypothese veelal, wat tot discussie heeft geleid of de *general theory of crime* wellicht zijn grenzen bereikt bij de verklaring van dit type criminaliteit (Bossler & Holt, 2009; Ngo & Paternoster, 2011). Achterliggende gedachte hierbij is dat *computer-focused crime* gericht is tegen computers en aanvallen mogelijk niet afhankelijk zijn van persoonskenmerken van de gebruiker – het is een delict dat grotendeels buiten de schuld van de gebruiker plaats vindt (Bossler & Holt, 2010). Een zwakheid aan de meeste hypothesetoetsingen hierover tot dusverre is echter dat zij gebaseerd zijn op kleine, selectieve samples onder Amerikaanse studenten. Recent grootschalig Nederlands onderzoek onder de algemene bevolking –waarvoor deze databeperkingen dus in mindere mate golden

– bevestigde de zelfcontrolehypothese juist voor gehackt worden: impulsieve mensen bleken beduidend vaker te worden gehackt (Van Wilsem, 2013a). Duidelijk is dat hier aanvullende studies uit verschillende landen en met uiteenlopende samples naar moeten worden blijven verricht om hier meer helderheid in te verschaffen.

Ook de routine-activiteitentheorie vertrekt vanuit een algemeen uitgangspunt: slachtofferschap wordt waarschijnlijker naarmate doelwitten zich meer in de nabijheid bevinden van daders, zich via activiteiten blootstellen aan deze daders, meer (financiële of symbolische) waarde vertegenwoordigen en minder bescherming genieten via derden of via technologische beschermingsmaatregelen (Cohen *et al.*, 1981). De routine-activiteitentheorie is ontwikkeld in het pre-Internettijdperk maar blijkt toepasbaar op cybercrime, ook al zijn de tijd-ruimtedimensies die in de oorspronkelijke theorie werden verondersteld in cyberspace wezenlijk anders. Daarmee is er geen fysieke samenkomst van dader en slachtoffer, maar wel een virtuele samenkomst die in belangrijke mate door gelegenheidsaspecten wordt beïnvloed. Daarmee kunnen de routine-activiteitenbegrippen *proximity, exposure, attractiveness* en *guardianship* vertaald worden naar het Internet. Nabijheid van daders (*proximity*) is bijvoorbeeld aannemelijker indien het doelwit zelf cyberdelicten pleegt of als vrienden dit doen (Bossler & Holt, 2009) – en zo zijn voor de andere drie kernbegrippen ook online operationaliseringen te bedenken. Wel blijkt bij deze exercitie dat het karakter van de routine-activiteitentheorie verandert van algemeen naar specifieker als zij wordt ingevuld voor uiteenlopende Internetdelicten. Zo zijn activiteiten die blootstelling aan daders van online bedreiging verhogen – uiteenlopende vormen van online contact, zoals via Facebook en discussiefora – niet zonder meer risicoverhogend voor gehackt worden. Een systematische analyse van uiteenlopende theoretisch afgeleide risicofactoren vanuit het routine-activiteitenperspectief, zoals blootstelling via sociale media en technische bescherming via computerpreventiemaatregelen, bleken uiteenlopende determinanten op te leveren voor online bedreiging en gehackt worden inderdaad. De overeenkomsten in deze twee vormen van slachtofferschap bleken te liggen in leeftijd en zelfcontrole: voor beide delicten gold dat slachtoffers veelal jong en impulsief zijn (Van Wilsem, 2013a).

Zes problemen

Daar waar genoemde theorieën al eerder toegepast zijn in empirisch onderzoek naar cybercrime, betekent het nog niet dat deze toepassing probleemloos is. *Ten eerste* is er bij de toetsing van hypothesen uit een theoretisch perspectief de discussie of de operationalisering van theoretische concepten adequaat is – en dat geldt ook voor dit onderzoeksveld. Hoe meet men bijvoorbeeld nu precies blootstelling aan online daders? In het routine-activiteitenperspectief is er in principe een veelheid aan activiteiten te bedenken die daarop van toepassing zouden kunnen zijn (zie voor een offline voorbeeld: Mustaine & Tewksbury, 1998). Wanneer is het goed en afdoende gemeten? Evenzeer geldt dit voor het concept aantrekkelijkheid van het doelwit: de discussie dat dit begrip moeilijk concreet gemaakt kan worden is niet nieuw, maar moet opnieuw gevoerd worden binnen het cyberdomein en daarbinnen voor uiteenlopende Internetdelicten – aantrekkelijkheid van een doelwit betekent voor een Internetfraudeur waarschijnlijk iets anders dan voor een hacker. *Ten tweede*, gesteld dat het theoretisch concept goed is gemeten, wat betekent een eventueel verband met slachtofferschap dan? Heeft de Internetactiviteit dan ook echt bijgedragen aan de totstandkoming van het concrete delict? Onderzoek binnen het offline domein naar de relatie tussen alcoholgebruik en geweldscriminaliteit heeft bijvoorbeeld uitgewezen dat dat niet altijd zo is: jongeren die veel drinken werden weliswaar vaker slachtoffer van geweld, maar bij het incident zelf bleek alcohol vaak geen rol te spelen (Felson *et al.*, 2008). Evenzo kan de frequentie van een Internetactiviteit gerelateerd zijn aan het al dan niet meemaken van slachtofferschap, maar hoeft het niet altijd in causaal verband tot het incident staan. Het uitvragen van incidentkenmerken in een slachtofferenquête kan hier bijvoorbeeld meer duidelijkheid in brengen. *Ten derde* is er discussie mogelijk over het concept zelfcontrole. Een recente meta-analyse

(Pratt *et al.*, 2013) heeft aangetoond dat met name in het cyberdomein er flinke risicoverhogende effecten van lage zelfcontrole op slachtofferschap van cybercrime zijn (zie bv. Van Wilsem, 2013b). Tegelijkertijd is er de vraag of de statische benadering van zelfcontrole, als een min of meer vaststaand persoonskenmerk, niet aanvulling behoeft. Vanuit de psychologie wordt zelfcontrole, naast deze statische benadering, tevens opgevat als een dynamisch concept. Muraven en Baumeister (2000) gebruiken hierbij de vergelijking met een spier: het aanwenden van zelfcontrole in concrete situaties leidt tot een afname in het vermogen om dat bij vervolgacties nogmaals te doen – op een gegeven moment is de 'spier' moe en is men niet meer goed in staat om opnieuw zelfcontrole op te brengen. De toepassing hiervan voor Internetgebruik is niet moeilijk te zien: hier wordt de gebruiker immers geconfronteerd met vele impulsen, waarvan een groot deel van commerciële of anderszins verleidende aard, waartegen de gebruiker zich tot op zekere hoogte zal moeten weren. Een concrete hypothese zou zijn dat naarmate een Internetsessie langer duurt, de gebruiker zijn of haar zelfcontrole heeft opgebruikt en wellicht impulsievere (en daarmee riskante) beslissingen gaat nemen, waarbij het risico op slachtofferschap wordt verhoogd.

Daarmee komen we tegelijk op een *vierde probleem*, namelijk een situationele benadering van cybercrime. Bovenstaand voorbeeld geeft al aan dat slachtoffers in bepaalde *situaties* in de fout gaan; ze worden niet continu opgelicht of bedreigd. Wat zijn kenmerken van die situaties waarin het fout gaat – wat is de site, welke keuzes maakte het doelwit daarbinnen en op basis van welke visuele of tekstuele stimuli? En waarin verschillen ze van situaties waarin het niet misgaat? In onderzoek naar moord en doodslag (Phillips & Cooney, 2005) en jeugdcriminaliteit (Wikstrom *et al.*, 2010) is een dergelijke situationele benadering al toegepast, maar gaat het daarbij om offline criminaliteit. Voor online criminaliteit ontbreken dergelijke studies en weten we dus onvoldoende op basis waarvan doelwitten bepaalde beslissingen op Internet te nemen – en ook hoe dat zich verhoudt tot bepaalde stabiele persoonskenmerken, zoals impulsiviteit. Een dataverzamelingsmethode waarbij doelwitten via een agenda bijhouden *wat ze op welke site op welk moment* doen zou een mogelijkheid in die richting zijn, in navolging van de (offline) PADS-studie in Engeland (Wikstrom *et al.*, 2010). Een andere, minder intensieve manier van bevraging zou zijn doelwitten te laten reflecteren op uiteenlopende sites of online aanbiedingen, eventueel met manipulatie van bonafide en malafide aanbiedingen en – ter toetsing van de bovengenoemde dynamische zelfcontrolehypothese – manipulatie van de mate van blootstelling aan eerdere online impulsen (zie bv. Grazioli, 2004).

Een *vijfde probleem* betreft de wijze waarop we het concept 'omgeving' bij cybercrime moeten benaderen. In de offline wereld is de omgeving voor criminaliteit belangrijk omdat de mate van toezicht er varieert en omdat er culturele verschillen kunnen zijn in wat wel en niet mag, maar voor het Internet geldt dat de fysieke omgevingscomponent er niet of nauwelijks is (Yar, 2004). Uiteraard worden omgevingen op Internet nagebootst, bijvoorbeeld in zogenaamde *multiplayer-games* zoals World of Warcraft of Habbo Hotel. Observatiestudies hebben hierbij aangetoond dat hier het nodige plaatsvindt aan intimidatie en diefstal van virtuele goederen (Van Dijk, 2011). Ook kunnen onderzoekers virtuele omgevingen bouwen teneinde respondenten daarin bloot te stellen aan bepaalde situaties en hen te vragen daarop te reflecteren (zie bv. Vanderveen & Koemans (2012) voor een toepassing bij de beoordeling van graffiti). Maar een andere vorm van omgeving binnen het Internet zijn de plekken (sites) waar doelwitten elkaar kunnen vinden en informatie uitwisselen omtrent Internetcriminaliteit en preventietips. Evenzo bestaan er contactsites waarop potentiële daders aan informatie-uitwisseling en uitnodigingen voor criminele samenwerking (Soudijn & Monsma, 2012). Voor slachtofferschap is van belang de positie van dergelijke contactsites in kaart te brengen: zijn bezoekers van dergelijke preventie- en tipomgevingen beter ingelicht en daarmee minder kwetsbaar en minder vaak slachtoffer? Of zijn het juist de slachtoffers die dergelijke sites bezoeken, naar aanleiding van het incident dat ze hebben meegemaakt?

Als laatste en *zesde probleem* geldt dat de toetsing van hypothesen omtrent delicten waar enige computerkennis voor vereist is (hacking, malware) doelwitten die kennis soms ontberen. Dat bemoeilijkt op een aantal manieren de interpretatie van resultaten uit dergelijke studies. Zo is er een flink aantal respondenten dat bij vragen omtrent dergelijke delicten aangeeft niet te weten of hij/zij daar slachtoffer van is geweest. Evenzeer geldt dat bij het vaststellen van de effectiviteit van preventiemaatregelen op de computer: in hoeverre helpt een firewall, een virusscanner en het beveiligen van het draadloze netwerk? Een substantieel aandeel respondenten weet niet in hoeverre deze maatregelen zijn genomen – bijvoorbeeld omdat iemand anders in het huishouden er voor zorgt – en dit bemoeilijkt een antwoord op de effectiviteitsvraag. Ten slotte speelt hierbij ook het niveau van analyse: bij dergelijke *computer-focused crime* wordt aan individuen gevraagd in hoeverre ze dit hebben meegemaakt. Maar de criminaliteit heeft plaats gevonden op een computer en niet zelden bevinden zich er daar meerdere van in het huishouden. Daarmee wordt relevant: welke activiteiten heeft men op welke computer ondernomen? En hoe goed zijn de verschillende computers beveiligd? Tot een dergelijk gedetailleerd niveau dalen de enquêtes echter niet af, gesteld al dat de respondent dit tot in detail zou weten. Dit soort kwesties bemoeilijken de vraag in hoeverre beveiligingsgedrag leidt tot minder slachtofferschap – maar dat betekent niet dat het onmogelijk is. De verschillende foutenbronnen zijn te modelleren: 'weet niet' kan als een aparte categorie expliciet in de analyse worden meegenomen om na te gaan in hoeverre daarbij afwijkende patronen worden gevonden. Ook een onderscheid naar huishoudens met één pc versus meerdere pc's kan duidelijk maken in hoeverre misspecificatie van het niveau van analyse (persoon i.p.v. computer) leidt tot andere (minder sterke) resultaten bij huishoudens met meerdere pc's.

Dit laatste probleem toont aan dat er met de huidige gegevens omtrent Internetgedrag en slachtofferschap van cybercrime moet worden nagedacht over slimme toepassingen om de toetsingen van de huidige dominante theorieën in het cyberdomein – de zelfcontroletheorie en routine-activiteitentheorie – recht te doen, op het gebied van data, metingen van centrale concepten maar ook verdere specificatie van de bestaande theorie binnen het cyberdomein.

Referenties

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.

Bossler, A.M. & Holt, T.J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice, 38*, 227-236.

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.

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.

Erp, J. van, Stol, W. & Wilsem, J. van (2013). Criminaliteit en criminologie in een gedigitaliseerde wereld. *Tijdschrift voor Criminologie, 55*, 327-341.

Felson, R., Savolainen, J., Aaltonen, M. & Moustgaard, H. (1998). Is the association between alcohol use and delinquency causal or spurious? *Criminology, 46*, 785-808.

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

Gottfredson, M. & Hirschi, T. (1990). *A general theory of crime*. Stanford: Stanford University Press.

Grazioli, S. (2004). Where Did They Go Wrong? An Analysis of the Failure of Knowledgeable Internet Consumers to Detect Deception Over the Internet. *Group Decision and Negotiation, 13*, 149-172.

Jandl, M. (2007). Irregular Migration, Human Smuggling, and the Eastern Enlargement of the European Union. *International Migration Review, 41*, 291-315.

Muraven, M. & Baumeister, R.F. (2000). Self-regulation and depletion of limited resources: Does self-control resemble a muscle? *Psychological Bulletin, 126*, 247-259.

Mustaine, E.E. & Tewksbury, R. (1998). Predicting risks of larceny theft victimization: A routine ac-

tivity analysis using refined lifestyle measures. *Criminology, 36*, 829-857.
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.
Phillips, S. & Cooney, M. (2005). Aiding Peace, Abetting Violence: Third Parties and the Management of Conflict. *American Sociological Review, 70*, 334-354.
Pratt, T.C., Turanovic, J.J., Fox, K.A. & Wright, K.A. (2013). Self-control and victimization: A meta-analysis. *Criminology*, DOI: 10.1111/1745-9125.12030.
Soudijn, M. & Monsma, E. (2012). Virtuele ontmoetingsruimtes voor cybercriminelen. *Tijdschrift voor Criminologie, 54*, 349-360.
Vanderveen, G. & Koemans, M. (2012). Omgevingscriminologie 2.0. Criminologisch onderzoek in een virtuele omgeving. *Tijdschrift voor Criminologie, 54*, 373-387.
Vijlbrief, M. (2012). *Synthetische drugs en precursoren. Criminaliteitsbeeldanalyse 2012*. Woerden: KLPD.
Wikström, P.O., Ceccato, V., Hardie, B. & Treiber, K. (2010). Activity Fields and the Dynamics of Crime. Advancing Knowledge About the Role of the Environment in Crime Causation. *Journal of Quantitative Criminology, 26*, 55-87.
Wilsem, J. van (2013a). Hacking and harassment – Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice, 29*, 437-453.
Wilsem, J. van (2013b). 'Bought it, but never got it.' Assessing risk factors for online consumer fraud victimization. *European Sociological Review, 29*, 168-178.
Yar, M. (2005). The novelty of 'cybercrime': an assessment in light of routine activity theory. *European Journal of Criminology, 2*, 407-427.