De andere 'anderen'

Een exploratieve studie naar processen van labelling van, door en tussen hackers

Wytske van der Wagen, Martina Althoff & René van Swaaningen

Inleiding

De ontwikkeling van het verschijnsel *hacking* is een schoolvoorbeeld van de sociale constructie van criminaliteit (o.a. Yar, 2005; Steinmetz, 2015). Terwijl de oerhackers in de jaren 1960 en 1970 nog als 'positieve anderen' werden gezien, namelijk als vaardige technologische *whizzkids* die graag de mogelijkheden van technologie willen verkennen en over 'magische krachten' beschikken als het om computers gaat, worden ze tegenwoordig al snel als vandalen of het archetype cybercrimineel beschouwd (Skibell, 2002; Yar, 2005; Steinmetz, 2015). Zo verschijnen er met regelmaat berichten over hackers die ontspoord zijn in de cybercrime en daarbij soms ook aanzienlijke schade aanrichten. We kunnen hierbij denken aan 'de KPN-hack' uit 2012, waarbij een 17-jarige hacker honderden servers van KPN hackte en daarmee in theorie (door het vaste telefonienet te manipuleren) het nummer 112 onbereikbaar had kunnen maken, of aan de recente DDoS-aanval[1] op internetprovider Ziggo, die ervoor zorgde dat miljoenen gebruikers dagenlang geen toegang hadden tot het internet. In beide gevallen had de politie de indruk dat de jongens vooral wilden laten zien dat ze tot 'grote dingen' in staat zijn en hun acties vooral als een 'kwajongensstreek' zagen. De media besteden echter ook steeds meer aandacht aan zogenoemde ethische of 'responsible' hackers, die vooral willen aantonen hoe slecht het gesteld is met de beveiliging van systemen. Een bekend voorbeeld hiervan is de hack op de OV-chipkaart (2011), waarbij de betrokken hacker-journalist drie weken lang op gekraakte OV-chipkaarten reisde en hiermee aantoonde hoe eenvoudig de gegevens op de kaart gemanipuleerd konden worden.[2] Ook de hack op het Groene Hart Ziekenhuis in 2012, waarbij een hacker toegang tot medische gegevens van een half miljoen Nederlanders wist te verkrijgen en daarmee de slechte beveiliging van het ziekenhuis aan de kaak stelde, zou je onder de noemer 'ethisch hacken' kunnen scharen. Echter, in dit geval werd de hacker in kwestie veroordeeld voor computervrede-

1 DDoS staat voor *distributed denial-of-service*. Dergelijke aanvallen dienen om met een 'bombardement' aan aanvragen een bepaalde website ontoegankelijk te maken.

2 Naar aanleiding van dit soort incidenten en diverse debatten in de Tweede Kamer bestaat er sinds 2013 een richtlijn genaamd 'responsible disclosure', die voorschrijft hoe op een verantwoorde manier een eventueel beveiligingslek naar buiten kan worden gebracht, zie: www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsible-disclosure.html. Met dit beleid is Nederland uniek in de wereld.

doi: 10.5553/TCC/221195072016006001003

breuk, omdat hij niet subsidiair zou hebben gehandeld.[3] We lijken dus aan de ene kant te maken te hebben met een negatiever wordend imago van de hacker (als *criminele ander*), maar tegelijkertijd lijkt er ook een zekere toenadering te ontstaan voor 'ethische' of 'helpende' hackers, omdat zij hacken vanuit een groter maatschappelijk belang (zie Van't Hoff, 2015).

Vanuit een cultureel criminologisch oogpunt, waarbij de focus vooral ligt op de wisselwerking tussen maatschappelijke reactie, criminalisering en deviant gedrag en waarbij ook het perspectief van de 'ander' of de 'outsider' wordt belicht, zou het waardevol zijn om na te gaan hoe deze ontwikkelingen door hedendaagse hackers zelf worden beschouwd. Hoe ervaren zij de wijze waarop zij worden afgeschilderd? In hoeverre vinden zij het beeld dat er over ze bestaat reëel? En hoe zien zij zichzelf en andere hackers? Dergelijke inzichten zijn belangrijk voor ons begrip van de vraag in hoeverre hackers het label dat zij krijgen opgeplakt internaliseren of van zich laten afglijden.

Welke rol labelling speelt in het leven van hackers, is echter nog nauwelijks onderzocht in de criminologie. Een van de weinige empirische studies op dit gebied is die van Turgeman-Goldschmidt (2008), welke laat zien dat labelling mogelijk anders uitpakt bij hackers dan bij de klassieke 'buitenstaanders' van Becker (1963). Zij stelt vast dat hackers zich wel verzetten tegen hun stigma als criminele ander, maar niet of nauwelijks negatieve sociaalpsychologische implicaties van labelling ondervinden; of ze zichzelf nu als 'good guys' of 'bad guys' beschouwen. Veeleer zien zij zichzelf als zogenoemde positieve devianten; als getalenteerde mensen die over unieke en bijzondere vaardigheden en eigenschappen beschikken. Hiermee rijst de vraag of de aannames uit de labellingbenadering, waarin vooral de negatieve implicaties van labelling worden benadrukt (een negatief zelfbeeld, secundaire deviantie en sociale uitsluiting), ook opgaan voor hackers. Heeft labelling een minder negatief, of zelfs een positiever effect bij hackers dan bij conventionele of 'pre-digitale' anderen en zo ja, hoe kan dat worden verklaard? Of is er misschien sprake van hele andere processen of effecten? In deze bijdrage proberen wij deze vragen te beantwoorden op basis van de bevindingen uit een tiental interviews met hackers en een vijftal strafdossiers, die wij inzichtelijk proberen te maken met een aan de labellingbenadering ontleend begrippenkader (Becker, 1963; Goffman, 1959, 1963).

Op het eerste gezicht lijkt het misschien niet voor de hand te liggen om bij symbolisch-interactionistische denkers uit het pre-digitale tijdperk te rade te gaan voor de analyse van een groep hedendaagse anderen. De theorie is immers ontwikkeld in een tijd waarin de eigen groep en gemeenschap sterk lokaal waren gedefinieerd en waarin identiteiten nog minder fluïde (Bauman, 2000) en hybride waren (Turkle, 2005). Sterker nog, het uitgangspunt van het onderzoek waarvoor de data werden verzameld, was dat we, om cyberdeviant gedrag te kunnen begrijpen, ons criminologische theoretische raamwerk zouden moeten uitbreiden met een 'cyborgian' dimensie, waarbij ook aan niet-menselijke 'actoren' een rol in

3 In dit geval is de betrokken hacker verder gegaan dan nodig was om het lek aan te tonen, waardoor niet aan de eis van subsidiariteit werd voldaan. Daarnaast werd kinderpornografie op zijn computer aangetroffen (zie Van 't Hof, 2015).

Tijdschrift over Cultuur en Criminaliteit 2016 (6) 1
doi: 10.5553/TCC/221195072016006001003

(delinquente) handelingen wordt toegekend (Van der Wagen & Pieters, 2015). Tijdens de dataverzameling en analyse bleek echter dat labelling zo'n belangrijke rol speelt bij de wijze waarop de hackers betekenis geven aan hun werkelijkheid, dat het materiaal ertoe uitnodigde om bij dit thema nader stil te staan. Het primaire doel van dit artikel is om processen van labelling te exploreren bij een kleine maar diverse groep hackers om daarmee iets beter de wereld van deze groep 'anderen' te begrijpen. Als afgeleide daarvan willen we ook ingaan op de vraag of de labellingbenadering nog wel actueel is in het internettijdperk of dat zij toe is aan vernieuwing, aan een digitale impuls.
Na een beknopt literatuuroverzicht over hacking en labelling wordt het empirisch materiaal besproken en worden de onderzoeksbevindingen uiteengezet. Hierbij wordt op drie aspecten gefocust: a) hoe denken hackers dat zij worden waargenomen door de buitenwereld?; b) (hoe) zien zij zichzelf als 'ander'?; en c) hoe zien zij zichzelf als een 'ander'(e) (groep) binnen de eigen (hackers)gemeenschap en daarbuiten? In de afsluitende discussie wordt nader op de bevindingen gereflecteerd en wordt stilgestaan bij de verklaringskracht van de labellingbenadering voor deze groep 'digitale anderen'.

Hackers: van 'held' naar 'crimineel'

In de jaren 1960 en 1970 werden hackers nog als de 'helden' van cyberspace beschouwd (Levy, 1984), of anders wel als *whizzkids* die de mogelijkheden van computertechnologie wilden exploreren. Vanaf de jaren 1990 werden ze echter in toenemende mate gezien als criminelen, gevaarlijke anarchisten of terroristen (o.a. Halbert, 1997; Nissenbaum, 2004; Skibell, 2002). In de literatuur worden verschillende verklaringen aangedragen voor deze kanteling van het beeld. Een eerste verklaring is dat de betekenis van het begrip 'hacking', dat oorspronkelijk verwees naar het oplossen van obstakels of problemen, in de loop der tijd veranderde (Nissenbaum, 2004). Doordat computertechnologie op grote schaal en voor een breed publiek toegankelijk werd, verscheen er een nieuwe generatie hackers op het toneel voor wie het hacken veeleer uit het breken ('cracken') of saboteren van een computersysteem bestond, hoewel hun professionele ethiek nog sterk leek op die van de vroegere generaties hackers (o.a. Halbert, 1997; Turgeman-Goldschmidt, 2008). Een tweede verklaring hangt samen met de commercialisering van het internet, de strijd tegen cybercrime en de daarmee gepaarde conflictueuze en wantrouwige relatie tussen de 'hacker underground' en de computerindustrie (zie o.a. Skibell, 2002; Taylor, 1999; Yar 2005). Een derde verklaring is de rol van de media en films, die hackers als pathologische, computerverslaafde of gevaarlijke nerds portretteerden (zie o.a. Halbert, 1997; Nissenbaum, 2004; Jordan & Taylor, 1998). Werd de hacker in films als *WarGames* (1983) nog geromantiseerd (Halbert, 1997) of neergezet als degene die de Staat te slim af was, in latere films wordt de hacker steeds meer als een gevaarlijke cybercrimineel afgeschilderd (Wall, 2008).
Hoewel hackers in de loop der tijd een steeds negatiever imago hebben gekregen, zien ze zichzelf niet als 'misfits'. Halbert (1997: 363) beschrijft dat hackers,

ondanks de 'scapegoating' en 'demonisering', zichzelf als positieve anderen zien: '[they] tend to embrace their difference as setting them apart from others'. Turgeman-Goldschmidt (2008), die interviews afnam met 54 Israëlische hackers, komt tot een soortgelijke conclusie. Volgens haar zien hackers zichzelf als *positive deviants*: ze zijn talentvol, superieur en geniaal. De respondenten in haar onderzoek slaagden erin de negatieve consequenties van labelling en secundaire deviantie te vermijden, wisten hun deviante achtergrond om te zetten in sociaal kapitaal en konden een goede plek op de arbeidsmarkt verwerven. Mogelijke verklaringen die worden genoemd, zijn het feit dat hackers vaak uit een hoger geschoold segment van de samenleving komen (en daarom mogelijk beter met het stigma kunnen omgaan) en dat hackers zich ook sneller verzetten tegen sociale conventies of morele grenzen, waardoor ze mogelijk beter opgewassen zijn tegen labelling (idem). Holt (2010) wijst in dit verband op het feit dat hackers eigen (morele) grenzen aanbrengen tussen zichzelf en anderen in de 'scene', wat bijvoorbeeld heeft geleid tot categorieën zoals 'hackers' versus 'crackers' en 'black hat' versus 'white hat hackers'.

Labelling, zelfbeeld en een geschonden identiteit

De labellingbenadering is gericht op de wijze waarop de *reactie van de maatschappij*, zij het formeel door sanctionering of informeel door stigmatisering, (een negatieve) invloed uitoefent op het zelfconcept en de sociale identiteit van de gelabelde (Becker, 1963). Daarbij kunnen verschillende implicaties voor de gelabelde onderscheiden worden, zoals negatief zelfbeeld, uitsluiting uit de gemeenschap en sociale netwerken en het niet kunnen vinden van werk. Wanneer iemand het label dat hem wordt opgeplakt c.q. zijn *stigma* internaliseert, leidt dit volgens Erving Goffman (1963) tot een geschonden identiteit. Dit kan vervolgens resulteren in deviante groepsformatie en verdergaand delinquent gedrag, ook wel *secundaire deviantie* genoemd. Volgens Edwin Lemert (1967: 62-95), die dit begrip heeft geïntroduceerd, begint het proces van secundaire deviantie met een gevoel dat het opgeplakte label onrechtvaardig is, om vervolgens de basis te vormen van iemands 'nieuwe' identiteit; de identiteit van deviant. In die zin lost iemand door secundaire deviantie te vertonen dus ook zijn identiteitsprobleem op. De sterkste variant van een secundair deviante identiteit is die van de gedetineerde: dat is een identiteit waar maatschappelijk nauwelijks aan is te ontsnappen. Maar Lemert ziet ook meer fluïde vormen van secundaire deviantie, waarin bijvoorbeeld leden van een subcultuur 'driften' van een deviante naar de sociaal geaccepteerde identiteit.[4] Met name deze laatste vorm van secundaire deviantie lijkt relevant in het geval van hackers. In de literatuur wordt echter nog maar weinig ingegaan op de invloed van de digitale context bij het al dan niet optreden van secundaire deviantie. In dit artikel willen we deze dimensie ook meenemen door na te gaan of het

4 Het begrip 'drifting' ontleent Lemert aan het beroemde boek van David Matza, *Delinquency and Drift* uit 1964.

Tijdschrift over Cultuur en Criminaliteit 2016 (6) 1
doi: 10.5553/TCC/221195072016006001003

internet het voor hackers eenvoudiger maakt zich te onttrekken aan negatieve labelling of om te 'driften' tussen een deviante en een niet-deviante identiteit.

Aangezien het empirische materiaal dat is gebruikt voor deze studie voornamelijk inzage geeft in het zelfbeeld van hackers en in mindere mate aspecten als uitsluiting, baankansen en secundaire deviantie belicht, hebben we 'het deviante zelf' (als 'ander') uit het symbolisch-interactionisme (o.a. Mead, 1934; Goffman, 1959; Goffman, 1963) als uitgangspunt voor deze studie genomen, om zodoende het zelfbeeld van hackers nader te kunnen analyseren. We onderscheiden hierbij drie met elkaar samenhangende dimensies van het deviante zelfconcept. Ten eerste is er de dimensie van hoe hackers (als 'anderen') denken te worden waargenomen door de buitenwereld en welke houding 'normale mensen' ten aanzien van hen hebben (Goffman, 1963). De tweede dimensie is hoe de hackers zichzelf zien en hoe zij hun eigen handelen beoordelen. Hierbij kan het gaan om aspecten als competenties, eigenwaarde, identiteit of moraliteit. De wisselwerking tussen deze twee dimensies is een belangrijk thema in het werk van Erving Goffman (1959; 1963), omdat iemand zich altijd bewust is c.q. inbeeldt hoe anderen ('het publiek') hem of haar observeren of classificeren en dit beïnvloedt op haar beurt ook weer het zelfconcept of de sociale identiteit. Goffman (1963) spreekt over een proces waarbij iemand 'leert' dat hij gestigmatiseerd is en zich bewust wordt van de daarmee gepaarde consequenties. In het werk van Becker (1963) komt er ook een 'technische' dimensie bij: je moet bijvoorbeeld eerst *leren* hoe je een joint moet roken, voordat je je de identiteit van een marihuanagebruiker kunt aanmeten. Als derde dimensie is er de vraag hoe hackers, als 'buitenstaanders', zichzelf zien in relatie tot de brave burger en tot andere (groepen) buitenstaanders (Goffman, 1963: 130-131). David Matza wijst er bijvoorbeeld op dat anderen vaak zelf categorisaties aanbrengen in de groep waartoe zij worden gerekend. 'From the outside, deviant persons (…) tend to look alike. From the inside, there is bound to be assortment and variety, observable, known, and usually designated by those who inhabit that world' (Matza, 1969: 28). Ook kan er sprake zijn van een vergelijking ten opzichte van andere ('externe') groepen, een dimensie die mogelijk juist voor hackers een belangrijke rol zou kunnen spelen. Bruno Latour (2005: 32) stelt in dit verband: 'It is always by comparison with other competing ties that any tie is emphasized. So for every group to be defined, a list of anti-groups is set up as well.'

Empirisch onderzoek naar hackers

Voor dit artikel is datamateriaal geanalyseerd dat in de context van het promotieonderzoek van de eerste auteur is verzameld. In dat onderzoek wordt de actor-netwerktheorie (ANT) van Bruno Latour als centrale benadering gebruikt, om nadere duiding te krijgen van het hackersfenomeen. Binnen de ANT-benadering wordt uitgegaan van een onderzoeksmethodologie die vrij nauw aansluit bij de 'verstehende' benadering van de culturele criminologie (Ferrell, 1997). In zijn actor-netwerktheorie bepleit Latour dat het perspectief van de onderzoeksobjec-

ten zelf zo veel mogelijk op de voorgrond zou moeten komen te staan als we fenomenen willen begrijpen. Zij zijn volgens Latour (2005) niet alleen goed in staat om hun eigen sociale werkelijkheid te construeren en te definiëren, maar ook kom je met een 'agnostische' onderzoekshouding meer te weten over hun belevingswereld dan met een vooropgezet frame (Latour, 2005). Op dit punt plaatst Latour zich dus in de traditie van het symbolisch-interactionisme, waar ook de labellingbenadering uit is voortgekomen. Voor het onderzoek is gekozen voor semigestructureerde interviews, waarin diverse (algemene) thema's met de respondenten werden besproken, zoals beweegredenen, leerprocessen, zelfbeeld, morele perceptie en de beleving van de hack. Het theoretische element dat in dit artikel centraal staat, labelling, drong zich als het ware op uit de interviews, maar was niet *a priori* het centrale onderwerp van de interviews of van het promotieonderzoek zelf.

Van de tien interviews zijn er acht face-to-face afgenomen, één via skype en één via e-mail. De eerste vijf interviews zijn afgenomen in de periode mei 2013 tot en met mei 2015 door de eerste auteur.[5] De tweede vijf zijn afgenomen in april en mei 2013 door een groepje studenten die de eerste auteur begeleidde in het kader van het vak Cybercrime aan de Rijksuniversiteit Groningen. Hoewel de interviews door verschillende personen en in andere contexten zijn afgenomen, zijn de thema's die aan de orde kwamen in de interviews voor een groot deel overlappend geweest. De respondenten zijn gezocht via 'hackerspaces',[6] via (student)contacten en door middel van de sneeuwbalmethode. De zoektocht naar hackers die bereid waren om mee te werken aan een interview verliep moeizaam. Dit lijkt ten eerste te worden veroorzaakt door de vele interviewverzoeken die hackers krijgen en de daarmee gepaarde media- en onderzoeksmoeheid. Via hackerspaces kregen we bijvoorbeeld te horen dat ze dagelijks verzoeken krijgen van journalisten of onderzoekers. Ten tweede speelde het gevoel 'daar heb je weer zo'n onderzoeker die niks van onze wereld begrijpt' een belangrijke rol in de geringe bereidheid om mee te werken, zoals we van personen te horen kregen die aangaven hackers te kennen. Ten derde leek de vrees te bestaan om met cybercrime te worden geassocieerd. Zo kregen we van een van de hackerspaces het antwoord: 'Om duidelijkheid te scheppen vooraf, welke betekenis van het woord "hacken" houden jullie aan? Een groot deel van de buitenwacht bedoelt er verschillende vormen van online en computer-georiënteerde misdaad mee. Afhankelijk van de soort hacker waar u naar op zoek bent zullen wij uw bericht en antwoord graag verder verspreiden onder onze deelnemers.' Kortom, negatieve toeschrijvingen en labelling bleken dus ook een negatief effect te hebben op de dataverzameling en heeft mogelijk ook invloed gehad op de samenstelling van de groep. Uiteindelijk is één respondent afkomstig uit een hackerspace, zijn er drie respondenten geworven via de sneeuwbalmethode en is de rest van de respondenten via (studenten)contacten gevonden.

5 Twee hiervan zijn afgenomen met een studente criminologie van de Universiteit Leiden die voor haar scriptie nog enkele eigen vragen heeft gesteld.

6 Wellicht anders dan de naam suggereert, zijn dit offline ontmoetingsplaatsen voor hackers waar gewerkt wordt met computers en elektronica.

doi: 10.5553/TCC/221195072016006001003

Alle respondenten zijn (jonge) volwassen mannen, ze hebben (op één Australiër na) de Nederlandse nationaliteit en ze hebben allemaal een ICT-gerelateerd, gemiddeld tot hoog opleidingsniveau. De groep is echter zeer divers als het gaat om hun ervaring en motieven. Vijf van de tien respondenten beschouwen zichzelf vooral als *ethische* of *white hat* hacker. Zij zijn zelf of namens een bedrijf (al dan niet in opdracht) op zoek naar kwetsbaarheden in systemen, maken hier melding van en brengen het in sommige gevallen ook in de publiciteit. De andere helft van de groep is in mindere of meerdere mate in het *black hat* circuit actief geweest. Twee respondenten hebben meerdere hele grote bedrijven of organisaties gehackt en hebben hier ook voor gevangen gezeten. Thans beschouwen zij zichzelf als (*ex-)black hat* of *grey hat* hacker: zij geven aan nog af en toe de grenzen op te zoeken en zich niet met de 'white hat scene' te associëren. Twee andere respondenten zijn actief geweest als black hat hacker en gaven aan nu niet meer illegaal te hacken. Een laatste respondent, die zichzelf niet als 'prototype hacker' beschouwt, was vier jaar lang betrokken bij virtuele diefstal, waarbij hij accounts van medespelers hackte en leeghaalde. Hij is de enige respondent die aangeeft (ook) een financieel motief te hebben gehad.

Naast deze interviews is een aanvullende analyse gedaan van vijf strafdossiers waarin computervredebreuk de centrale aanklacht was.[7] Dit onderzoek heeft in een later stadium plaatsgevonden, namelijk in de periode juli en augustus 2015 bij het Openbaar Ministerie in Rotterdam.[8] Het gaat hierbij om de analyse van vier zaken waar een individuele hacker één of meerdere grotere bedrijven of organisaties hackte en om één zaak waarbij de hacks door een hacktivistische groepering werden gepleegd. De dossiers bevatten onder meer politieverhoren of gesprekken met de verdachten (bijvoorbeeld met de reclasseringsambtenaar) en soms ook uitgebreide chatconversaties tussen hackers onderling. Omdat in ieder dossier naar voren komt hoe de hackers tegen hun gepleegde delict aankijken en naar zichzelf als hacker kijken, kon dit aspect worden meegenomen voor de onderhavige studie. Natuurlijk wordt rekening gehouden met het feit dat verhoren en dergelijke in de context van een strafrechtelijk onderzoek zijn afgenomen en mogelijk niet de betekenisgeving van de verdachten weergeven. In de bevindingen wordt het dan ook expliciet vermeld als iets uit de dossiers komt.

De beschrijving van het empirisch materiaal (interviews en strafdossiers) maakt duidelijk dat hier sprake is van een kleine en tevens zeer diverse groep respondenten, wier enige gemeenschappelijke kenmerk is dat zij zichzelf als hacker zien. Verder lopen hun ethiek, hun normatieve positie ten aanzien van hacking en hun strafrechtelijke antecedenten behoorlijk uiteen. Generaliserende uitspraken over 'de hackersgemeenschap' kunnen we in het kader van dit onderzoek niet doen. Wel beogen wij inzicht te geven in de belevingswereld van hackers. De geconstateerde grote diversiteit aan belevingen dient ook het theoretische doel van dit onderzoek naar de meerwaarde van de labellingbenadering voor de analyse van

7 Zaken waarin bijvoorbeeld sprake was van criminele netwerken die zich bezighielden met de grootschalige verspreiding van (banking) malware zijn voor deze studie buiten beschouwing gelaten.

8 Dit waren vanzelfsprekend niet de dossiers waar de geïnterviewden bij betrokken waren.

hacking, doordat hierdoor ook de wederzijdse etikettering transparant kan worden gemaakt. In de hiernavolgende analyse wordt, aan de hand van uitspraken van de geïnterviewde hackers, de wijze waarop zij hun werkelijkheid construeren gepresenteerd. De bevindingen zijn geclusterd in drie secties. Ten eerste wordt ingegaan op de wijze waarop hackers menen door de buitenwereld te worden gezien en tot 'de ander' worden bestempeld. Vervolgens wordt uiteengezet hoe hackers zichzelf zien als 'de ander'. En daarna gaan we in op de wijze waarop hackers aankijken tegen andere hackers c.q. hoe ze elkaar als 'de ander' bestempelen. Om de anonimiteit te waarborgen hebben wij fictieve namen aan de geïnterviewde hackers gegeven en waar nodig delictgerelateerde informatie weggelaten.

Hoe hackers denken dat zij worden waargenomen door de buitenwereld

Op de vraag hoe ze denken dat de buitenwereld de hacker ziet, wijzen de respondenten in eerste instantie op het onbegrip. Ze geven aan dat buitenstaanders 'hun wereld' niet begrijpen en wellicht ook niet goed *kunnen* begrijpen. Dit onbegrip of onvermogen wordt door sommige respondenten verklaard door de kloof in digitale kennis die er bestaat tussen hackers en de doorsnee-burger, die volgens de respondenten op zijn beurt kan leiden tot verschillende reacties. Eric (een ex-black hat hacker) heeft de indruk dat er veel maatschappelijke angst is en dat veel mensen het een groot 'mysterie' vinden. Anderen wijzen op vooroordelen en dat veel mensen denken dat hackers hun skills per definitie voor kwaadaardige doeleinden inzetten door overal maar in te breken. Daarnaast wordt door sommige respondenten aangegeven dat er door dit onbegrip allerlei stereotyperingen ontstaan, variërend van hackers als nerds tot hackers als gevaarlijke mensen; en die stereotypen worden door media bevestigd of versterkt. Volgens Paul (een ex-black hat hacker) worden hackers geportretteerd als: 'Nerdachtige types die op kleine zolderkamers zitten, in het donker, hele dag achter de pc dingen kapot maken. Er zijn media die het echt zo opschrijven ook. Ik denk dat de media en de meeste mensen dat wel van hackers denken; dat zijn nerds met slechte bedoelingen, antisociaal, die de hele dag alleen dat doen. Alhoewel, dat beeld begint te veranderen, doordat het meer in de openbaarheid komt, bijvoorbeeld doordat hackers meer in de publiciteit treden.' Jack (de hacker uit de hackerspace) wijst hierbij nog op de negatieve beeldvorming in de media en in films. Desalniettemin geven de geïnterviewde hackers soms ook aan dat het lastig is voor buitenstaanders om 'hun wereld' te begrijpen. Daarmee zeggen ze dus dat het onbegrip en de angst die er bestaat ten aanzien van hackers ook een reële basis heeft. De respondenten beschrijven de hackerscene als een aparte gemeenschap en ze typeren deze soms ook als 'geheimzinnig', 'underground' of 'lastig toegankelijk'. Als hackers meer naar buiten zouden treden, zou er, zoals Paul al opmerkte, verandering kunnen komen in de stereotypen die er bestaan en zou de wereld van de hacker minder mysterieus en beangstigend zijn.

Naast het gevoel als een soort mysterieuze of gevaarlijke ander te worden beschouwd, ervaren de hackers, eigenlijk nog veel meer, als *criminele* ander te worden gezien. De gedachte dat hackers als criminelen of als criminele organisa-

Tijdschrift over Cultuur en Criminaliteit 2016 (6) 1
doi: 10.5553/TCC/221195072016006001003

ties worden gezien, is een centraal thema dat door de respondenten unaniem naar voren wordt gebracht. Een belangrijke factor die zij als mogelijke verklaring voor dit negatieve beeld noemen, is de toename van cybercrime. David (een white hat hacker die bij een beveiligingsbedrijf werkt) stelt bijvoorbeeld dat er de laatste jaren veel nieuwe actoren en criminele organisaties zijn opgekomen die zich met hacking bezig zijn gaan houden, waardoor alle hackers een slechte naam krijgen. Daarnaast geven enkele respondenten aan dat de media door hun selectieve berichtgeving – dat hackers criminelen zouden zijn – dit beeld nog extra versterken. Paul stelt: 'Je leest niet "hacker vindt gat in elke versie van Windows"; vind je niet in de media. In de media vind je "hacker hackt bedrijf X en steelt 3 miljoen creditcardgegevens"; dat vind je. Ja, tuurlijk schept dat een negatief beeld, dat begrijp ik ook wel: die klootzakken die mijn rekening leegplunderen.'
De respondenten geven voorts aan dat ze niet alleen als criminelen worden *gezien*, maar ook zo worden behandeld. Volgens Jan (een ethische hacker) worden hackers, ook als ze goede bedoelingen hebben, altijd met argwaan benaderd. 'In plaats van het voordeel van de twijfel, gaat het Openbaar Ministerie altijd uit van het nadeel van de twijfel.' Jan geeft hierbij ook aan het gevoel te hebben dat hier een verdraaiing plaatsvindt. Eigenlijk zijn de bedrijven die gehackt worden veel 'crimineler' bezig, doordat zij onzorgvuldig met hun data omgaan, hetgeen juist door hackers zichtbaar wordt gemaakt. De hackers zijn echter degene die 'serieuze strafvervolging riskeren'. Volgens Jan kunnen ethische hackers zich behoorlijk opwinden over de slechte beveiliging van systemen en voelen ze zich vaak niet serieus genomen. Dit kan er zelfs toe leiden dat hackers die goede intenties hadden te ver gaan. Als voorbeeld haalt hij een hacker aan die ontdekt dat hij gratis dingen kan bestellen bij een webshop. Als hier vervolgens, na het te melden, niets mee wordt gedaan, kan die hacker bijvoorbeeld (als een soort ludieke actie) een bankstel (gratis) gaan bestellen en het vervolgens bij het kantoor van het desbetreffende bedrijf laten bezorgen.

Hoe hackers zichzelf zien als 'de ander'

Veel hackers beschouwen hun scene, zoals gezegd, als een aparte gemeenschap. Ook geven zij aan zichzelf als anders (dan anderen) te beschouwen; iets wat soms van jongs af aan al speelde. Zo brengt Jan naar voren: 'Als kind wilde ik al op allerlei knopjes drukken om te zien wat er vervolgens gebeurde. Ik denk voor een gedeelte dat het omgaan met technologie, daar zit wel iets van een aangeboren iets in, dat jij gewoon iets met het verschijnsel technologie hebt.' Hiermee verbonden is de neiging om elkaar op te zoeken, zij het online of in de fysieke wereld. De eerste reden hiervoor is dat je 'mensen zoals jij' opzoekt of mensen met een soortgelijke interesse, omdat je daar een sterkere binding mee voelt. Daarnaast geven de geïnterviewden aan dat het heel belangrijk voor ze is om kennis te delen en te kunnen praten met mensen die begrijpen waar zij het over hebben of zoals Paul zegt: 'die je niet schaapachtig aan zitten te kijken van: waar heeft hij het over?' Meerdere geïnterviewden geven tevens aan hun online vrienden en hun online wereld te scheiden van de offline vrienden en wereld, of ze in ieder geval als twee

aparte categorieën te beschouwen. Met offline vrienden gaan ze uit, naar de kroeg of gamen, maar ze praten niet of nauwelijks met hen over computergerelateerde onderwerpen.

Naast het gevoel 'anders' te zijn en deel uit te maken van een groep 'anderen' zien de geïnterviewde hackers zichzelf als 'positieve anderen'. Zo geeft een aantal respondenten aan dat je hacken vooral in termen van creativiteit, fantasie, 'out of the box denken', kunst of genialiteit kunt beschouwen. Zo is een hacker volgens Jack iemand 'die slimme dingen doet, op een speelse manier'. Jan definieert hacking als een 'state of mind', als het denken buiten de geëigende paden en signalen oppikken die 'normale mensen' niet zien, wat op zijn beurt een kloof tussen de hackers en de samenleving creëert. 'Het niet gehoord worden, dat dingen niet worden opgelost, dat er lacherig over wordt gedaan, maar ook het zich niet begrepen voelen. Waarom zie jij nou niet dat de hele wereld groen is? Waarom zie ik dat nou wel, waarom zie jij dat nou niet?' Voor sommige (ex-)black of grey hat hackers zijn dergelijke definities eigenlijk weer veel te breed. Zij definiëren hacking veeleer in termen van 'het verkrijgen van controle over andermans systeem' of 'het overnemen van een server'. Het idee dat bijvoorbeeld een 'biertap maken' onder hacking zou kunnen vallen, wordt door Eric (een ex-black hat hacker) dan ook belachelijk gemaakt.

Een andere 'hoedanigheid' waarin hackers zichzelf zien is die van 'helper'. Bij ethische hackers ligt dat voor de hand. Zij geven aan met hun hacks bedrijven te helpen de kwetsbaarheden te dichten of, in Jans woorden, 'misstanden aan te tonen in de samenleving' en ook de maatschappij te waarschuwen of te beschermen tegen dergelijke misstanden. Het idee van de hacker als helper speelt echter ook een rol bij de wijze waarop de black of grey hat hackers soms betekenis geven aan hun acties. Dylan, die lange tijd actief was in de black hat hacker scene, stelt bijvoorbeeld dat hij de bedrijven die hij hackt eigenlijk helpt: 'Als wij, de meer mid- of low-level hackers er niet zouden zijn om bedrijven te onderwijzen over hun veiligheid, zouden ze levend worden opgegeten.' Het bedrijf waarbij is ingebroken, wordt hierbij niet als slachtoffer gezien, maar als degene die de beveiliging niet op orde heeft en daardoor de hack over zichzelf afroept. Dit is overigens een aspect dat ook in alle vijf strafdossiers door de verdachten naar voren wordt gebracht. Zo merkt een verdachte in één van de strafdossiers hierover op: 'Het is belachelijk dat mensen hun gegevens invullen en vervolgens kunnen mensen zoals ik met gemak deze gegevens achterhalen. Het releasen is het online zetten van data om mensen te shockeren en ze ervan bewust te maken wat er met je gegevens kan gebeuren. Het doel is vooral om het bedrijf voor lul te laten staan. Er wordt veel geld uitgegeven aan mooie plaatjes, maar de veiligheid is blijkbaar niet belangrijk.' Paul relateert het feit dat de effecten van hacking ook positief voor de samenleving kunnen zijn aan de proportionaliteit van de (aan hem) opgelegde straf. 'De veroordeling is niet onterecht. Wel te zwaar denk ik. Vooral ook omdat ik die systemen niet kapot maakte. Ik maakte ze eigenlijk alleen maar beter zelfs, zo voelde ik dat toen hè; ik hielp die mensen dus eigenlijk.'

Tijdschrift over Cultuur en Criminaliteit 2016 (6) 1
doi: 10.5553/TCC/221195072016006001003

Hoe hackers zichzelf zien ten opzichte van 'de anderen'

Niet iedereen kan zich volgens de respondenten zo maar een hacker noemen. Het *kan* wel ('het is geen beschermde titel'), maar er is ook sprake van een zekere exclusiviteit. Een hacker moet in staat zijn iets geniaals of creatiefs te doen. 'Iets briljants doen' heeft echter niet per se te maken met de vraag of iets legaal of illegaal is. Volgens Jan kunnen sommige criminele acties ook wel redelijk briljant zijn, ook al zijn ze illegaal. Daniël (een white hat hacker) refereert in dit kader aan het verschil tussen iemand die de kluis bij een bank weet te kraken en een inbreker die simpelweg de sleutel onder de deurmat vindt. Volgens de respondenten wordt in de hackersscene negatief aangekeken tegen zogenoemde 'scriptkiddies', omdat ze bestaande tools gebruiken c.q. de sleutel onder de deurmat vonden en dus niet echt weten hoe ze echt werken. In die zin lijkt er door de respondenten een onderscheid te worden gemaakt tussen de 'echte' hacker en de amateur of *wannabe* hacker. Eric geeft echter aan het 'fucking bullshit' te vinden dat 'scriptkiddies' door hackers zo negatief worden bekeken, omdat iedereen zo begint. Vincent, de respondent die betrokken was bij virtuele diefstal, distantieert zich juist weer van hackers die alles van systemen willen afweten. 'Die hebben niks beters te doen, die vind ik nerderig. Ik vind het ook tijdverspilling.' Hij geeft aan meer geïnteresseerd te zijn in wat je met het programma kunt doen en daarbij in het bijzonder hoe je de computer van andere mensen onder jouw controle kunt krijgen. Zo kwam hij bij zogenoemde 'Remote Access Tools' terecht, waarmee hij de computer en webcam van andere gebruikers kon overnemen.

Skills spelen op hun beurt een belangrijke rol in de hackersscene en bij de toegang daartoe. Naast de open forums waarop je actief bent, breng je volgens de geïnterviewden veel meer tijd door op privéchatkanalen en daar kom je niet zomaar binnen. Volgens Kevin gaat het dan om een select vriendengroepje waar je skills en 'exploits'[9] mee uitwisselt. Buitenstaanders, ook wel 'het publiek' genoemd, worden hierbij buiten de deur gehouden. Voor veel kanalen moet je volgens de respondenten specifiek worden uitgenodigd. Kevin (een ex-black hat hacker) geeft aan dat de lastige toegang en de daarmee gepaard gaande 'geheimzinnigheid' hem extra aantrok: 'Ze laten niet zomaar iedereen toe en leren zeker de nieuwelingen niet hoe het moet. Dat maakte het voor mij spannender en interessanter om het zelf te doen.' Paul merkt op dat de criteria om toegelaten te worden nu wel anders zijn dan in de tijd dat hij actief was in de black hat scene: 'Iemand stelt een vraag, maakt niet uit wat voor een vraag en jij kan die beantwoorden. Dan laat je zien van goh, hij weet dat! Hij weet er wat van af. Het was niet opscheppen van: nou ik heb vandaag vierhonderd websites gehackt, ik hoor bij de groep.' Met andere woorden, hackers lijken tevens te ervaren een soort 'exclusieve' ander te zijn of deel uit te maken van een exclusieve groep.

Een minstens zo belangrijke manier waarop hackers zichzelf als groep definiëren, wat al eerder naar voren is gekomen, is door zich te distantiëren van cybercriminelen (als antigroep). Ze leggen dan ook, om zich te verzetten of verdedigen tegen dat label, nadrukkelijk uit wat de verschillen zijn tussen hackers en cybercrimine-

9 Exploits zijn zogenaamde fouten of beveiligingslekken in besturingssystemen.

len (c.q. 'de klootzakken die je rekening leegplunderen'). Een eerste scheidslijn die wordt getrokken, hangt samen met de intenties van de hacker. Volgens Paul zijn 'hackers gewoon mensen met een hobby, die alles van het systeem af willen weten, die willen weten hoe het werkt, hoe je het kapot kan maken, wat het doet als ik dit doe'. Soms loopt de hobby dan wel uit de hand - zoals dat bij hemzelf ook het geval is geweest - maar dan kun je een hacker nog niet vergelijken met een crimineel die dingen verkoopt of steelt. Door Paul en ook door andere respondenten wordt de scheidslijn tussen crimineel en niet-crimineel dus voornamelijk bij financieel gewin gelegd. Hiermee komen we op een tweede scheidslijn die door meerdere 'gepakte' hackers naar voren wordt gebracht, namelijk de gedachte dat hackers zich überhaupt niet willens en wetens schuldig maken aan strafbare feiten en ook geen 'calculerende' criminelen zijn. In een van de dossiers wordt door een verdachte opgemerkt: 'Je bent een beetje keet aan het trappen met een paar man, maar het is geen georganiseerde misdaad! In mijn optiek zouden we met zijn allen van te voren plannen moeten maken en bedenken hoe je zaken gaat doen en wat je met de gegevens gaat doen. Dit doen we niet, dit is meer het leuk iets doen met wat je aantreft maar er zit geen plan achter.' Door sommige respondenten, ook door een van de verdachten in een van de dossiers, wordt tevens gewezen op de rol van groepsinvloed en dat grenzen in een (black hat) groep gemakkelijk vervagen. Eric brengt naar voren: 'Er is niemand die tegen jou zegt van hé, is misschien wel strafbaar dit', waardoor 'veel jongens erin verdrinken'. Volgens Simon zijn hackers vaak getalenteerde jongens die 'nog zoekende zijn' en niet weten hoe ze hun talent moeten inzetten. Echter, uiteindelijk zal een black hat hacker, zo geven de respondenten aan, aan de 'goede kant' stranden. Ze wijzen er bijvoorbeeld op dat de lol en uitdaging er op een gegeven moment afgaat, maar ook dat je op een gegeven moment een normaal inkomen wil. Sterker nog, veel van de (ex black hat) respondenten wijzen erop dat hun black hat verleden juist een positieve bijdrage heeft geleverd aan hun carrière. Ze kwamen na hun gevangenisstraf vrijwel gelijk aan een baan en kunnen hun skills ook goed gebruiken in hun werk. Een derde scheidslijn die wordt gemaakt, is de modus operandi, die volgens de respondenten voor een hacker heel anders is dan voor een crimineel. Eric zegt bijvoorbeeld dat beschermingsmaatregelen door hackers vaak maar 'half-half' worden doorgevoerd en dat ze vaak onvoorzichtig zijn: 'Iemand die er financieel gewin uit probeert te halen, die zorgt vanaf het begin dat er nergens sporen zijn te vinden en die gaat niet overal zijn naam op kalken, omdat die er geen belang bij heeft om bekend te worden. Terwijl jongens die de technische mogelijkheden aan het verkennen zijn, die maken hele stomme foutjes. Die zetten ergens hun naam gewoon bij en maar ondertussen zitten ze allemaal mensen te besmetten.' Hackers willen in tegenstelling tot cybercriminelen ook graag opscheppen op chatkanalen, waardoor ze volgens Vincent sneller worden gepakt. Paul spreekt van 'mediageile typjes' die zo stom zijn dat ze hun huisadres er gewoon bijzetten. Hij denkt overigens dat dit wel specifiek iets is voor de hackers van deze tijd. Volgens hem is de 'schreeuwbaarheid' de laatste jaren enorm toegenomen en bestaan er groepen die alleen maar hacken om 'erover op te scheppen'.

Tijdschrift over Cultuur en Criminaliteit 2016 (6) 1
doi: 10.5553/TCC/221195072016006001003

Naast processen van 'othering' aangaande wie of wat zich een hacker kan noemen, zijn er ook processen van labelling tussen hackergroepen onderling. Het duidelijkste voorbeeld hiervan is de wijze waarop black hat en white hat hackers elkaar bekijken. De meerderheid van de respondenten geeft aan dat er een duidelijk onderscheid kan worden aangebracht tussen deze twee groepen. Er wordt in dit kader vooral gesproken in termen van goede en kwade intenties of in termen van legaliteit en illegaliteit. Paul legt uit: 'Een white hat is echt iemand die het goed wil doen, niks fouts wil doen, niks illegaals; we hebben een bug gevonden en we rapporteren het bij de persoon die de bug heeft; en een black hat wil er misbruik van maken, die zou zeggen van nou, eens even binnen kijken. We rapporteren helemaal niks.' Kevin stelt in dit kader dan ook dat hij de term 'grey hat hacker' onzin vindt. 'Een persoon kan niet en goed zijn en slecht zijn. Iemand hackt ofwel voor geld, houdt het voor zichzelf, verkoopt het op de zwarte markt of veroorzaakt schade (black hat). Of hij is een "good guy" en hackt professioneel.' Dit betekent volgens Jan echter niet dat een black hat geen goede dingen kan doen (of vice versa). Hij verwijst hierbij naar een maffiabaas die geld geeft aan een goed doel.

Eric stelt dat er sprake is van een voortdurende strijd tussen black en white hat hackers, dat is verbonden aan het eerder besproken slechte imago van de hacker: 'Op twitter of dat soort dingen zitten ze elkaar allemaal zwart te maken. En alle black hats hebben een hekel aan de white hats en alle white hats hebben een hekel aan de black hats, omdat die allemaal criminele dingen doen en dat is niet goed voor het aanzien van de hacker.' Als we vervolgens kijken naar hoe de ethische hackers in de interviews de black hat hackers beschrijven, zien we dat vooral in termen van goed en kwaad, moraliteit of schade wordt gesproken. Black hat hackers worden bestempeld als 'mensen die hacken om anderen te irriteren', 'schade veroorzaken', 'bad guys', 'inbrekers', 'hackers met andere morele standaarden' en 'kwaadaardig'. Andersom wordt niet alleen gerefereerd aan 'goed en kwaad', maar ook gewezen op karakterverschillen en verschillende emoties. Eric beschrijft white hat hackers als 'brave lulletjes', 'die zich aan de regels houden,' 'hele nette beschaafde jongens', die 'white zijn geboren', 'overdreven braaf', 'die gillen bij elk lekje dat ze zien' en 'die een duidelijke grens zien tussen wat wel en wat niet mag', terwijl hij black hats als de 'stoutste jongens van de groep' beschouwt die op zoek zijn naar spanning.

Discussie

In dit artikel zijn we ingegaan op de vraag in hoeverre hackers als 'digitale anderen' negatieve gevolgen van hun labelling als 'outsiders' ondervinden en of de klassieke labellingbenadering ook verklaringskracht heeft in het digitale tijdperk. We hebben hiervoor drie dimensies van het zelfconcept van een kleine, maar diverse groep hackers onder de loep genomen. In lijn met de bevindingen van Turgeman-Goldschmidt (2008) ervaren de geïnterviewden negatieve labelling, maar zien ze zichzelf vooral als positieve anderen. Ze hebben naar eigen zeggen niet zozeer tekortkomingen, maar juist iets *extra's* ten opzichte van andere men-

sen: skills, intelligentie en een state of mind waarmee ze dingen kunnen signaleren, doorgronden en briljante dingen kunnen doen. Op basis van onze analyse van het empirische materiaal kunnen we dus niet zeggen dat hackers een geschonden identiteit hebben.

Dat labellingprocessen bij hackers minder stigmatiserende effecten lijken te hebben dan bij de 'traditionele' devianten, waar het in de labellingbenadering meestal om gaat, lijkt voor een groot deel te maken te hebben met kenmerken van het fenomeen hacking zelf. Het verschijnsel hacking, dat verbonden is met de eigen skills, mindset en moraal, is het domein van een exclusieve groep 'ingewijden', die als online groep op het *world wide web* actief is. Je moet niet alleen de skills leren om deze 'exclusieve andere' te worden, je moet jezelf ook nog eens bewijzen. Zonder interactie met en bevestiging van de anderen (je publiek) in de scene ben je feitelijk verloren in cyberspace. Als je erin slaagt om briljante hacks te doen, dan kun je mogelijk een heldenstatus verwerven. Hoe daar dan door de 'echte wereld' door minder significante anderen over wordt gedacht, is dan wellicht minder belangrijk. Met andere woorden: het positieve zelfbeeld dat hackers van zichzelf hebben, de (online) gemeenschap waartoe zij zich rekenen en het duidelijke morele kader waarbinnen zij hun handelingen betekenis geven, kunnen mogelijk verklaren dat zij zich als het ware boven de negatieve oordelen van de (offline) buitenwereld kunnen plaatsen die de hackerwereld niet kan begrijpen. Onze bevindingen suggereren bovendien dat sommige hackers een scheiding aanbrengen tussen online en offline identiteit, waarmee ze mogelijk twee identiteiten naast elkaar kunnen managen en/of kunnen 'driften' tussen een deviante en niet-deviante identiteit. Voor sommige (black hat) hackers lijkt hacking dan ook veeleer 'criminal role play' te zijn dan het willens en wetens plegen van criminaliteit. Uiteindelijk doen ze iets goeds voor de samenleving door de slechte beveiliging van bedrijven en organisaties bloot te leggen, die in hun ogen eigenlijk veel fouter bezig zijn.

Hoewel de morele grenzen tussen de black en white hat hackers verschillen, zijn ze het erover eens dat je hackers niet met de echte cybercriminelen kunt vergelijken die voor het grote geld gaan. Dit brengt ons ook bij het punt dat het anders *zijn* niet alleen een kwestie is van een associatie met 'gelijkgestemde anderen', maar ook nadrukkelijk een dissociatie ten opzichte van andere groepen. In die zin lijkt Latours begrip 'anti-group' wel toepasselijk om de verhouding tussen hackers en criminelen te beschrijven, maar ook tussen black en white hackers. Het feit dat labellingprocessen dus ook binnen de groep 'anderen' plaatsvinden, neutraliseert waarschijnlijk de negatieve beeldvorming. Kortom, naast een digitale dimensie zou dergelijke (anti)groepsdimensie de labellingbenadering mogelijk ook kunnen verrijken. Daarmee concluderen we niet zozeer dat de labellingbenadering 'outdated' is, maar wel een 'update' kan gebruiken om ook in de toekomst een rol van betekenis te kunnen spelen in (cyber)criminologisch onderzoek.

Literatuur

Bauman, Z. (2000), *Liquid Modernity*. Cambridge: Polity.

doi: 10.5553/TCC/221195072016006001003

Becker, H.S. (1963), *Outsiders. Studies in the Sociology of Deviance*. New York: The Free Press.
Ferrell, J. (1997), Criminological Verstehen: Inside the immediacy of crime. *Justice Quarterly*, 14(1), 3-23.
Goffman, E. (1959), *The Presentation of Self in Everyday Life*. London: Penguin Books.
Goffman, E. (1963), *Stigma. Notes on the Management of Spoiled Identity*. Englewood Cliffs: Prentice-Hall.
Halbert, D. (1997), Discourses of danger and the computer hacker. *The Information Society*, 13(4), 361-374.
Hof, C. van 't (2015), *Helpende Hackers. Verantwoorde onthullingen in het digitale polderlandschap*. Creative Commons 2015 Tek ToK Uitgeverij.
Holt, T.J. (2010), Examining the role of technology in the formation of deviant subcultures. *Social Science Computer review*, 28(4), 466-481.
Jordan, T. & P. Taylor (1998), A sociology of hackers. *The Sociological Review*, 46(4), 757-780.
Latour, B. (2005), *Reassembling the Social. An Introduction to Actor-Network-Theory*. New York: Oxford University Press.
Lemert, E. (1967), *Human Deviance, Social Problems and Social Control*. Englewood Cliffs: Prentice Hall.
Levy, S. (1984), *Hackers Heroes of the Information Age*. New York: Doubleday.
Matza, D. (1964), *Delinquency and Drift*. New York: John Wiley.
Matza, D. (1969), *Becoming Deviant*. Englewood Cliffs: Prentice Hall.
Mead, G.H. (1934), *Mind, Self and Society: From the Standpoint of a Social Behaviorist*. Chicago: Chicago University Press.
Nissenbaum, H. (2004), Hackers and the contested ontology of cyberspace. *New Media Society*, 6(2), 195-217.
Skibell, R. (2002), The myth of the computer hacker. *Information, Communication and Society*, 5, 336-356.
Steinmetz, K.F. (2015), Craft(y)ness. An ethnographic study of hacking. *British Journal of Criminology*, 55, 125-145.
Taylor, P.A. (1999), *Hackers. Crime in the Digital Sublime*. London/New York: Routledge.
Turgeman-Goldschmidt, O. (2008), Meanings that hackers assign to their being a hacker. *International Journal of Cyber Criminology*, 2(2), 382-396.
Turkle, S. (2005), *The Second Self: Computers and the Human Spirit*. Cambridge: MIT press.
Wagen, W. van der & W. Pieters (2015), From cybercrime to cyborg crime: botnets as hybrid criminal actor-networks. *British Journal of Criminology*, 55(3), 578-595.
Wall, D. (2008), Cybercrime and the culture of fear. Social science fiction(s) and the production of knowledge about cybercrime. *Information, Communication & Society*, 11(6), 861-884.
Yar, M. (2005), Computer hacking: just another case of juvenile delinquency?. *The Howard Journal*, 44(4), 387-399.