From cybercrime to cyborg crime

van der Wagen, Wytske

Nederlandse samenvatting (Dutch Summary)

Achtergrond, vraag- en doelstelling van het proefschrift

De vraag of cybercrime 'oude wijn in nieuwe zakken is' of dat het echt om een fundamenteel nieuw verschijnsel gaat dat om nieuwe theorieën vraagt, heeft tot dusver veel cybercriminologen beziggehouden. Dit proefschrift mengde zich ook in deze discussie door na te gaan of bestaande criminologische theorieën nog voldoende verklaringskracht hebben in het licht van de (a)typische kenmerken van hightech cybercrime, waaronder haar (deels) geautomatiseerde en gedistribueerde karakter. Het proefschrift vertrok vanuit de aanname dat bestaande raamwerken in de (cyber)criminologie (nog) te instrumenteel (substantivistisch), antropocentrisch en dualistisch zijn ingesteld om deze kenmerken te duiden en dat de criminologie daarom haar theoretische grenzen moet verleggen. Het proefschrift beoogde dit te doen door exploratief onderzoek te doen naar het theoretische (cyber)potentieel van de actor-netwerktheorie (ANT). Dit betreft een perspectief (of lens) die de mens-techniek relatie juist niet in uitsluitend instrumentele (of deterministische) termen duidt, die de mens niet als de enige significante actor in de sociale wereld beschouwt en die zich tegen dualistische of binaire denkkaders keert. Het perspectief zou daarmee mogelijk waardevolle handvatten kunnen bieden voor theoretische vernieuwing in de cybercriminologie.

Om de theoretische (meer)waarde van ANT te exploreren, zijn een viertal empirische casestudies uitgevoerd, namelijk een analyse van een botnet, twee kleinschalige etnografische studies naar hackers en een casestudie waarin drie soorten slachtofferschap zijn geanalyseerd (respectievelijk ransomware, botnets en virtuele diefstal). De achterliggende gedachte achter het doen van deze casestudies was dat het theoretische potentieel van ANT beter verkend, getoetst en verfijnd kon worden op basis van empirisch materiaal en dat zo ook de toevoegde waarde ten opzichte van bestaande theorieën beter inzichtelijk zou kunnen worden gemaakt. Het uiteindelijke doel van het onderzoek was om, op basis van deze casestudies een alternatief perspectief te ontwikkelen, wat uiteindelijk het 'cyborg crime' - perspectief is gaan heten.

De vier casestudies en haar bevindingen

Hieronder volgt een samenvatting van de verschillende casestudies die in het proefschrift aan de orde zijn geweest. Wat was het vertrekpunt van de casestudie en wat heeft de studie theoretisch en/of empirisch gezien opgeleverd?

Het botnet als hybride crimineel actor-netwerk (hoofdstuk 2)

De eerste casestudie in het proefschrift betrof de analyse van een botnet, een crimineel fenomeen dat exemplarisch is voor het gerobotiseerde karakter van cybercrime. De studie vertrok vanuit de gedachte dat bestaande criminologische theorieën, inclusief de routine-activiteitentheorie en de rationale keuzetheorie te antropocentrisch

lijken te zijn voor de analyse van vormen van hightech cybercrime die een geautomatiseerd en gedistribueerd karakter hebben zoals botnets. Om deze reden werd een beroep gedaan op de constructivistische lens van ANT en werd het botnet geconceptualiseerd als een hybride crimineel actor-netwerk dat niet uitsluitend wordt aangestuurd door de mens noch door de machine. De vier betekenissen van ANT's concept van technische mediatie ('composition', 'translation', 'delegation' en 'reversible blackboxing') werden gebruikt als conceptueel kader om een botnet-casus te bestuderen. In dit kader zijn politiedossiers geanalyseerd en is een interview met een bij het onderzoek betrokken rechercheur afgenomen.

Uit het onderzoek kwam ten eerste naar voren dat diverse menselijke en niet-menselijke actoren (groot en klein) een rol spelen in de opzet van de infrastructuur van het botnet, de besmetting van de computers, het gebruik en het beheer van het botnet en bij de ontmanteling van het botnet. Hoewel de rol van de botherder belangrijk was, zou het te beperkt zijn om het botnet slechts als een door de mens (botherder) aangestuurd netwerk te beschouwen. De studie liet namelijk zien dat er verschillende actoren direct of indirect (actief) betrokken waren bij het 'succes' van dit botnet. Deze actoren waren ofwel gecreëerd, bestonden al of moesten misleid worden om in het handelingsprogramma van de botherder te worden opgenomen. De studie liet ten tweede zien dat de rol van de betrokken technische entiteiten niet slechts functioneel en passief was. Ze konden bijvoorbeeld een bepaald gebruik of nieuwe (criminele) handelingen uitlokken (zowel bij de botherder of zijn

klanten) en brachten ook onverwachte situaties teweeg voor de botherder. Zo kon de explosieve groei van het botnet niet op voorhand voorspeld worden en moest de botherder aanpassingen maken in de infrastructuur. Ten derde kwam uit het onderzoek naar voren dat de continuering of 'overleving' van het botnet ook afhankelijk was van een complexe vermenging tussen zowel menselijke als niet-menselijke componenten. Zo kon het botnet pas ontmanteld worden zodra de botherder, de infrastructuur en de individuele infecties werden gestopt. Als slechts een of twee element uit het netwerk werden gehaald, kon het botnet blijven voortbestaan.

De studie concludeerde dat ANT in drie opzichten toegevoegde waarde had ten opzichte van bestaande perspectieven zoals de routine-activiteitentheorie (RAT) en de rationele keuze theorie (RC). Allereerst maakte ANT het mogelijk om een grotere en diversere groep actoren in kaart te brengen die een rol spelen bij het ontstaan en de ontwikkeling van een botnet. Het kon zo inzichtelijk maken dat de betrokken entiteiten (inclusief de botherder) pas kracht en betekenis krijgen in relatie tot andere entiteiten in het netwerk. Daarnaast kon de ANT lens ook goed laten zien hoe daderschap, slachtofferschap en preventie/toezicht met elkaar verweven kunnen zijn. Waar de RAT dit min of meer als drie aparte en vooraf bestaande statische elementen beschouwt, ziet ANT deze elementen als dynamisch en beschouwt hen als met elkaar vervlochten of gedeeltelijk overlappende netwerken. Tot slot werd gesteld dat ANT's visie van actorschap beter inzichtelijk kan maken hoe technologie actief het criminele proces en het resultaat daarvan kan

vormgeven, omdat zij de mens niet als de (enige) centrale kracht ziet achter (de uitvoering van) criminele activiteiten. De algehele conclusie van deze studie was dat ANT en haar hybride en 'genetwerkte' duiding van actorschap bepaalde (complexe) elementen en dynamieken van het criminele proces beter in kaart kan brengen dan een traditionele criminologische benadering. De eerste contouren van het 'cyborg crime' - perspectief waren getekend in deze studie.

Waar deze eerste casestudie zich vooral focuste op de aard van hightech cybercrime, het geautomatiseerde of gerobotiseerde karakter in het bijzonder, trachtten de opvolgende casestudies licht te werpen op de (a)typische cyberdader: de hacker. De eerste studie (hoofdstuk 3) benaderde het fenomeen vooral vanuit een meer conventionele criminologische lens (de labellingbenadering) en de tweede studie (hoofdstuk 4) maakte gebruik van de ANT lens. Zo kon de toegevoegde waarde ANT beter inzichtelijk worden gemaakt.

De andere 'anderen' (hoofdstuk 3)

Deze studie ving aan met de constatering dat hacking een schoolvoorbeeld is van de notie dat criminaliteit een sociale constructie is. Waar hackers in de jaren zestig nog beschouwd werden als helden of whizzkids; sinds de jaren negentig worden ze vooral geportretteerd als stereotypische cybercriminelen. Tegenwoordig, althans in Nederland, lijkt er echter tegelijkertijd sprake te zijn van enige toenadering tot zogenaamde 'ethische' hackers, hackers die zich vooral richten op het

vinden van beveiligingslekken en deze gedicht willen krijgen. Deze studie had als doel om te onderzoeken hoe hackers zelf tegen deze ontwikkelingen aankijken en om te exploreren of zij het label dat zij opgeplakt krijgen van zich afwerpen en/of internaliseren. Meer specifiek, wilde de studie achterhalen hoe hackers denken dat de buitenwereld hen ziet, hoe zij zichzelf zien en hoe zij zichzelf beschouwen ten opzichte van anderen. Voorts, in het verlengde hiervan, beoogde de studie de verklaringskracht van de labellingbenadering te exploreren voor hackers als 'digitale anderen,' om zo na te gaan of de theorie een digitale impuls nodig heeft. Naast interviewmateriaal werd ook nog een vijftal strafdossiers geanalyseerd waarbij hacking de centrale aanklacht was.

De onderzoeksbevindingen lieten zien dat hackers het gevoel hebben dat de buitenwereld hen ziet als mysterieuze, 'nerderige' en gevaarlijke anderen, maar bovenal als criminele anderen, een label die ze volledig afwijzen. In plaats daarvan definiëren de hackers hun 'anders zijn' vooral in niet-criminele termen. Ze typeren zichzelf als hobbyisten met een specifieke belangstelling voor technologie en beschouwen hacking in termen van creativiteit en kunst, 'out of the box' denken en een bepaalde 'state of mind.' Tevens zien respondenten (ook de black hat hackers) zichzelf veeleer als helpers dan als criminelen. Ook al doen ze een hack die illegaal is, ze stellen dat ze het slachtoffer - het bedrijf dat de beveiliging niet op orde heeft - juist helpen, onderwijzen en confronteren. De geïnterviewden positioneren zichzelf ook sterk ten opzichte van andere 'anderen'. Ze distantiëren zich van de 'echte'

cybercriminelen met betrekking tot hun intentie, modus operandi en verantwoordelijkheid en ten opzichte van andere hackers in termen van intentie en karakter. Hackers slagen er in ieder geval in om het opgeplakte label succesvol van zich af te werpen. De studie brengt tevens naar voren, in lijn met de bevindingen van Turgeman-Goldschmidt (2008), dat hackers in staat zijn om het label ook niet te internaliseren. In plaats van een negatief zelfbeeld, zien zij zichzelf vooral als positieve anderen. Zij hebben geen tekortkomingen, maar iets extra's waar zij trots op zijn.

Deze laatste bevinding rijmt dan ook niet met de assumpties van de labellingtheorie. Deze benadering gaat er namelijk van uit dat labelling leidt tot een negatiever zelfbeeld of zelfs tot een geschonden identiteit. De verklaring voor het feit dat dit bij hackers minder of niet speelt, werd vooral gezocht in de kenmerken van het hackerfenomeen zelf. Hacking vraagt om een specifieke skillset en ook hebben hackers een sterk eigen moraal waarin zij hun handelingen betekenis geven. Niet de buitenwereld, maar vooral andere hackers (de exclusieve groep waarmee ze zich associëren) zijn belangrijk bij de vorming van hun zelfbeeld. Ook de rol van de digitale wereld is mogelijk van belang. Het feit dat hackers kunnen driften tussen de online en offline wereld, zou er voor kunnen zorgen dat ze twee identiteiten tegelijkertijd kunnen managen. Dit laatste reduceert mogelijk niet alleen de negatieve implicaties van labelling, maar het neutraliseert ook hun betrokkenheid bij eventueel schadelijke activiteiten. Naast het toevoegen van een digitale dimensie aan de labelling benadering, werd gesteld dat de

theorie verrijkt zou kunnen worden door meer aandacht te besteden aan labelling binnen groepen. In deze context, leek Latours (2005) concept van de 'anti-groep' relevant. 'Anders zijn' is namelijk niet alleen een kwestie van associatie met soortgelijke anderen, maar juist ook een proces van zich distantiëren van andere binnen of buiten de eigen groep.

De cyborg-deviant (hoofdstuk 4)

Het startpunt van deze studie was dat hackers, of ze nu betrokken zijn bij legale of illegale hackerpraktijken, een benadering behoeven die de relatie tussen mens en technologie centraler stelt in de analyse. Hoewel bestaande studies ook wel naar deze relatie kijken, wordt hier op een vrij antropocentrische, dualistische en hiërarchische manier naar gekeken. Gesteld werd dat ANT, een perspectief die een meer 'post-menselijke' of 'cyborg' kijk hanteert ten aanzien van actorschap, in staat zou kunnen zijn om een genuanceerder begrip te kunnen krijgen van deze relatie. Op basis van tien interviews met zowel hackers, die betrokken waren legale als illegale hacks, verkende deze studie hoe hackers betekenis geven aan zichzelf en hun acties en hoe dit mede werd gevormd door hun (deviante) relatie met technologie.

De resultaten lieten zien dat hackers zichzelf zien als actoren met een hele specifieke 'skillset' en 'mindset', welke hen onderscheidt van 'normale' mensen en criminelen. Ten eerste zien ze zichzelf als getalenteerde en creatieve personen die een aangeboren fascinatie en affiniteit hebben met objecten en technologie. Ze typeren zichzelf zowel

als ‘reversible blackboxers’ als ‘out of the box denkers’. De respondenten zien zichzelf ook als helden of moraalridders die hun eigen specifieke ideeën hebben over goed en kwaad. (Bestaande) grenzen zijn onnatuurlijk voor hen. Ze willen deze (door)breken, verleggen of juist eigen grenzen stellen. Ze geloven ook over bepaalde zintuigelijke vaardigheden of krachten te beschikken waarmee ze bepaalde dingen kunnen zien, opmerken of doorgronden waar normale mensen blind voor zijn. In dat opzicht zien ze zichzelf ook in zeker zin als supermensen of cyborgs, want hun lichaam en geest heeft een extensie. Hoewel we hackers als een atypische of unieke deviante groep kunnen beschouwen vond de studie ook gelijkenissen met andere deviante en niet-deviante groepen, waaronder bankrovers, graffitispuiters, sporters en gamers.

Een tweede bevinding was dat de geïnterviewde hackers hun relatie met technologie niet slechts als instrumenteel of functioneel beschouwden. Zij beschreven deze relatie onder meer als coöperatief, competitief, intiem en exploratief. Zo zien de respondenten hacking bijvoorbeeld niet slechts als een menselijke solo-operatie, omdat ze ook een beroep moeten doen op bestaande technologische tools c.q. ‘wapenarsenaal’. Ze passen deze aan naar hun eigen voorkeur of handelingsprogramma. Hier zien we dan ook duidelijk Latours ‘wapen-mens hybride’ in terug, welke illustratief is voor de notie dat (de functionaliteit van) technologie menselijke capaciteiten, vaardigheden en intenties kan medevormgeven.

In theoretisch opzicht werd geconcludeerd dat ANT’s cyborg-perspectief een nieuwe dimensie toevoegt aan bestaande concepten (bijvoorbeeld

'meesterschap', 'spanning zoeken', 'plezier') die gebruikt worden om het hackerfenomeen te duiden, omdat het zich specifieker richt op hoe de interactie met technologie deviante handelingen, percepties en intenties mede vormgeeft. Hiermee bouwde de studie dus voort op het 'cyborg crime' concept zoals deze was geformuleerd in de eerdere botnetstudie. Het voegde echter een subjectieve dimensie hieraan toe, welke ook alleen te exploreren en te achterhalen was door middel van diepte-interviews. In het kader van de toegevoegde waarde van ANT ten opzichte van bestaande concepten, concludeerde de studie dat ANT bepaalde aspecten beter kon duiden omdat het naar de verschillende hybride hoedanigheden kijkt waarin een hacker handelt en beweegt en daarmee hun betekenisgeving niet loskoppelt van de tools en technologie waarmee zij in verbinding staan. In het kader van dit laatste werd dan ook de toegevoegde waarde zichtbaar van het cyborg-perspectief ten opzichte van de labellingbenadering, toegepast in het voorafgaande hoofdstuk.

Een andere belangrijke conclusie was dat de ANT lens, net als de bredere notie van Haraway's (1987) cyborg, het mogelijk maakt om het hackerfenomeen op een minder dualistische manier te benaderen. Zo was het mogelijk om te (laten) zien dat hacking als een praktijk en vorm van deviant gedrag, een complex samenspel is van zowel grenzen doorbreken als grenzen bepalen en verleggen, zowel technisch als moreel. De algehele conclusie was dat ANT's post-menselijke benadering zeker theoretisch potentieel heeft voor de studie van hacking en andere vorm van hightech cybercrime of deviant gedrag.

Het hybride slachtoffer (hoofdstuk 5)

De laatste casestudie in het proefschrift nam drie soorten hightech slachtofferschap onder de loep. Deze studie was relatief theoretischer dan de vorige studies en had ook een andere opbouw. Het hanteerde een probleemgestuurde benadering door drie empirische casussen van cyber-slachtofferschap (ransomware, botnets and high-tech virtuele diefstal) als startpunt te nemen. Door (a)typische kenmerken uit de casussen te abstraheren, beoogde de studie de beperkingen en blinde vlekken van bestaande benaderingen, die gebruikt worden om slachtofferschap te verklaren, bloot te leggen. Het liet zien dat benaderingen zoals de levensstijlbenadering en de routine-activiteitentheorie (RAT) te antropocentrisch, reductionistisch en dualistisch zijn voor de analyse van de casussen. Ze conceptualiseren kwetsbaarheid bijvoorbeeld vooral als een kenmerk dat toegeëigend kan worden aan een enkele entiteit (mens of object). De casussen laten echter zien dat kwetsbaarheid wordt gegenereerd door verschillende entiteiten samen. Zo worden computergebruikers vaak bereikt via de kwetsbaarheid van andere actoren waar ze mee in verbinding staan (bijvoorbeeld kwetsbare websites) en/of moeten ze eerst op een technische manier getarget worden voordat er een 'menselijke' kwetsbaarheid ter sprake komt. Met andere woorden: de menselijke kwetsbaarheid kan ook niet losgezien worden van de technische kwetsbaarheid. De casussen laten tevens (en wederom) zien dat het handhaven van bestaande dualismen zoals menselijk versus niet-menselijk, echt versus fictioneel, dader versus slachtoffer niet langer

productief is bij de duiding van het cyberslachtoffer(schap) als entiteit en als proces. Op basis van deze analyse, heeft de studie het theoretische potentieel van ANT onderzocht in relatie tot deze casussen en gekeken of ANT een alternatief zou kunnen bieden voor de conceptuele beperkingen van de eerder besproken theorieën.

Het onderzoek resulteerde uiteindelijk in drie alternatieve op ANT-gebaseerde concepten, aangeduid als de 'hybride slachtoffertheorie.' Het concept 'victim composition' weerspiegelt de notie dat het (kwetsbare) slachtoffer beschouwd moet worden als een hybride en gedistribueerd netwerk dat bestaat uit verschillende menselijke, technische en/of virtuele entiteiten die moeten worden 'getarget' door de dader. Vanuit dit perspectief wordt kwetsbaarheid geconceptualiseerd op een meer gedistribueerde en emergente manier en wordt het niet beschouwd als een kenmerk dat toegekend kan worden aan een enkele entiteit – of het nu een technisch systeem of een persoon betreft. Het concept 'victim delegation' vestigt de aandacht op hoe de taken en rollen verdeeld zijn in de totstandkoming van slachtofferschap over tijd. Het concept 'victim translation' stelt in staat om slachtofferschap als een meer veranderlijk, interactioneel en fluïde proces te analyseren in plaats van als een afgebakende concrete gebeurtenis ('event'). Het beschouwt slachtofferschap derhalve als het resultaat van een complexe interactie tussen verschillende handelingsprogramma's en anti-programma's. Alle drie concepten benadrukken dat de grenzen tussen dader en slachtoffer, mens en machine, instrument en doelwit en fictie en werkelijkheid vervagen of wegvallen. De studie concludeert dat de geformuleerde

concepten nieuwe aanknopingspunten kunnen bieden voor de analyse van hightech slachtofferschap, maar ook dat deze concepten er toe uitnodigen om anders (meer hybride) te denken over belangrijke facetten van slachtofferschap, waaronder wie/wat slachtoffers kwetsbaar en weerbaar maakt en hoe preventiemaatregelen vormgegeven zouden kunnen worden.

De vier dimensies van het 'cyborg crime' perspectief

Op basis van de casestudies zijn vervolgens vier dimensies van het 'cyborg crime' - perspectief onderscheiden die waardevol zouden kunnen zijn bij de analyse van hightech cybercrime. Ze staan niet los van elkaar, maar liggen in elkaars verlengde. Het betreft de volgende dimensies:

1. Technologieën moeten beschouwd worden als actieve entiteiten, bemiddelaars of participanten in hightech cybercrime;
2. De relatie tussen daders van hightech cybercrime daders en technologie is meer dan slechts functioneel;
3. Daders van hightech cybercrime interacteren met technologieën waar ze mogelijk niet de volledige controle over hebben;
4. Dader- en slachtoffers van hightech cybercrime zijn hybride producten van menselijke, technische en/of virtuele (inter)acties;

Gesteld werd dat deze dimensies vooral als een aanvulling en niet als vervanging dienen voor het bestaande theoretische repertoire van de

criminologie. Ze leggen vooral de nadruk op de wijze waarop technologie criminele handelingen, processen en intenties en de resultaten daarvan kan medevormen, dimensies die nog (te) onderbelicht zijn in de criminologie.

Het toekennen van actorschap aan technologie roept uiteraard ook diverse vragen op, waaronder de vraag hoe technologisch actorschap in relatie staat tot het actorschap van de mens. Het 'cyborg crime' - perspectief volgt ANT in zoverre dat het in de analyse (in eerste instantie) evenveel aandacht wil besteden aan hoe menselijke en niet-menselijke entiteiten een rol spelen in handelingen en benadrukt eveneens dat beide in essentie niet hetzelfde zijn. Het 'cyborg crime' - perspectief zou echter wel iets meer ruimte willen toelaten voor een gedifferentieerde opvatting van menselijk en technisch actorschap door nader te specificeren op welke verschillende manieren technologie als actor kan fungeren. Het stelt derhalve dat een hybride opvatting van actorschap hand in hand kan gaan met (iets meer) herkenning van de eigenheid van mens en machine. Tot slot werd nog op mogelijke juridische en praktische implicaties van (het) 'cyborg crime' (-perspectief) ingegaan. Het cyborg crime perspectief betekent niet dat (een deel van de) verantwoordelijkheid moet worden afgeschoven op technologie in plaats van de mens, maar stipt wel aan dat bepaalde aspecten (bijvoorbeeld waar het gaat om het vaststellen van causaliteit) lastiger zouden kunnen zijn bij cybercrime dan bij traditionele criminaliteit. In het kader van de bestrijding van hightech cybercrime, veronderstelt het 'cyborg crime' - perspectief dat de aanpak gericht moet

worden op zowel menselijke als niet-menselijke actoren (infrastructuur, malware, tools, marktplaatsen, etc) en ook dat dat er een netwerk van actoren nodig is om deze vormen van criminaliteit te bestrijden.

ANT en cybercriminologie: mogelijkheden en beperkingen

Hoewel de ideeën van ANT aanvankelijk vergezocht leken, kwam naar voren dat het perspectief interessante aanknopingspunten biedt voor de studie van cybercrime, vooral als het gaat om de duiding van de relatie tussen mens en technologie. Ook biedt ANT de mogelijkheid om cybercriminele fenomenen met een minder dualistische bril te bestuderen. Een enigszins provocatief perspectief zoals ANT is tegelijkertijd geschikt in het kader van theoretische vernieuwing. Het stelt minder voor de hand liggende vragen en stelt ook in staat om kritisch naar bestaande concepten te kijken. Zoals het proefschrift heeft laten zien, heeft het ANT het 'nieuwheidsdebat' in de cybercriminologie zeker een nieuwe impuls geven. Toch zijn er ook beperkingen te signaleren waar het gaat om de toepassing of het gebruik van ANT. Zo heeft ANT weinig te melden over hoe mensen (los van de dingen) tot morele keuzes komen en ook is het maar de vraag of het realistisch en wenselijk is om als onderzoeker, zoals Latour dat voorschrijft, weg te blijven van interpretatie en alleen te beschrijven. Desalniettemin lijkt ANT, althans daar ben ik zelf van overtuigd geraakt, een zeer passend perspectief te zijn voor de studie van cybercrime. Ik verwacht en hoop dan ook dat cybercriminologen vaker een beroep zullen gaan doen op ANT of andere perspectieven binnen de filosofie van de techniek.

Toekomstig onderzoek zou aanvullende of nieuwe casestudies kunnen doen op het gebied van dader- en slachtofferschap en/of het 'cyborg crime' - perspectief op een grotere dataset kunnen loslaten om bevindingen uit dit onderzoek nader te valideren. Tevens zou het perspectief op andere cyber-gerelateerde thema's kunnen worden toepast, zoals cyberverkrachting en de rol van bots en botnets in de manipulatie van de publieke opinie.