Nederlandse Vereniging voor Criminologie

DE CRIMINOLOOG

Nieuwsbrief van de Nederlandse Vereniging voor Criminologie

19

jaargang 10 - juni 2018

Voorwoord

Beste criminoloog,

Het maatschappelijke leven verplaatst zich in rap tempo van de offline wereld naar de online wereld. Voor ons privéleven geldt dit al een tijdje. Aankopen doen we steeds meer in internetwinkels, waarbij de pakjes nu nog door bezorgers aan huis worden gebracht maar straks door drones. Alle contacten met banken, verzekeringen en overheden verlopen digitaal. En ook ons sociale leven speelt zich steeds meer via social media af, ook al zullen de organisatiecriminologen onder u het gebruik van Facebook afraden. Omdat we deze verplaatsing als privépersoon doormaken, doen we dat als criminoloog ook. Want de daders en slachtoffers die we bestuderen ontmoeten elkaar ook in de digitale wereld. Daarnaast hebben automatisering en digitalisering de mogelijkheid gebracht voor allerlei nieuwe vormen van criminaliteit die in de offline wereld niet mogelijk zijn, zoals DDOS-aanvallen. Tenslotte verandert digitalisering niet alleen het object van studie van de criminologie, maar ook de wijze waarop we deze bestuderen. Digitalisering biedt nieuwe soorten data en nieuwe methoden voor criminologisch onderzoek. Het Tijdschrift voor Criminologie heeft in 2013 al een themanummer besteed aan “Criminaliteit en criminologie in een gedigitaliseerde wereld”. Deze thematiek is sindsdien niet minder actueel geworden. Omdat dit thema elke criminoloog raakt, heeft het bestuur dit thema gekozen voor het jaarlijks congres van 2018. Daarbij hebben we dankbaar de titel van het tijdschrift geleend.

Traditiegetrouw staat het congresthema centraal in de NVC-nieuwsbrief ’De Criminoloog’ die op het congres uitkomt. De man van het eerste uur van de bestudering van cybercrime in Nederland mag natuurlijk niet ontbreken. In deze nieuwsbrief bespreekt Wouter Stol de geschiedenis van cybercrimeonderzoek en de huidige stand van cybercrimeonderzoek in Nederland. Een andere voorloper, Johan van Wilsem, vertelt ons over het onderzoek naar slachtoffers van cybercrime. Maar de redactie wilde ook een nieuwe generatie cybercriminologen aan u voorstellen, voor zover nog nodig! Marleen Weulen Kranenbarg vertelt over haar promotieonderzoek waarin zij een eerste empirische vergelijking maakte tussen cybercriminelen en traditionele criminelen. Vlak voor het NVC-congres promoveert Wytske van der Wagen en desondanks heeft ze de tijd gevonden om in “From Cybercrime to Cyborg Crime – mijn proefschrift in een notendop” te vertellen over haar resultaten. Veel jonge alumni van opleidingen criminologie komen in het veld van cybercrime en cybersecurity terecht; hoe kan het ook anders. Alumnus Youri Jelsma vertelt over zijn ervaringen met het werken in het cybercrime veld.

Tenslotte nog iets anders. Het bestuur van NVC heeft de statuten nog eens afgestoft en zich daarbij gerealiseerd dat het de hoogste tijd is weer een algemene ledenvergadering te organiseren. Wat is daarvoor een betere gelegenheid van het NVC-congres? Dat stelt zoveel mogelijk leden in de gelegenheid de ALV bij te wonen. In deze digitale tijd wellicht een wat ouderwetse manier (digitale alternatieven via onze website worden verkend), maar toch een goede gelegenheid u in persoon te informeren over ontwikkelingen binnen de vereniging en voor u om daar feedback op te geven.
Ik wens u veel plezier bij het lezen van deze nieuwsbrief en zie u graag op het jaarcongres.

Namens het NVC-bestuur,
Wim Huisman

INHOUDSOPGAVE

1 **Voorwoord**
- Prof. Dr. Wim Huisman (voorzitter NVC)

2 **De criminoloog en cybercrime**
- Prof. Dr. Wouter Stol
(Noordelijke Hogeschool Leeuwarden, Open Universiteit, de Politieacademie)

3 **Over cybercrime en de slachtoffers daarvan**
- Dr. Johan van Wilsem (WODC)

5 **Cybercriminologie: uitdagingen voor criminologisch onderzoek n.a.v. een eerste empirische vergelijking tussen cybercriminelen en traditionele criminelen**
- Dr. Marleen Weulen Kranenbarg
(Vrije Universiteit Amsterdam)

6 **From cybercrime to cyborg crime**
Mijn proefschrift in een notendop
- Dr. Wytske van der Wagen
(Erasmus Universiteit Rotterdam)

7 **Ervaringen uit de praktijk**
- Youri Jelsma, MSc.
(Motiv ICT-security)

8 **Colofon**

De criminoloog en cybercrime

Prof. dr. Wouter Stol
(Noordelijke Hogeschool Leeuwarden,
Open Universiteit, de Politieacademie)

De criminologie reageerde traag op de digitalisering en doet dat vermoedelijk nog steeds. Dit stukje is dan ook mede bedoeld om criminologen aan te moedigen om op zijn minst aan de digitale aspecten van criminaliteit niet voorbij te gaan en er misschien wel een hoofdonderwerp van te maken. Het is niet alleen een actueel, jong en spannend onderwerp, het is ook maatschappelijk gezien nodig dat criminologen zich bezig houden met een terrein dat snel vorm krijgt door systeemontwikkelaars en beta-wetenschappers. Niet tégen hen maar mét hen overigens, als kritische partner. Daar kom ik op terug.

Hoe kwam ik zelf op dit gebied terecht? Dat was deels toeval en deels fascinatie. Begin jaren tachtig mocht ik als beginnend politie-inspecteur leiding geven aan de automatisering van de meldkamer van de Amsterdamse politie. Ervaring met automatisering was daarvoor geen vereiste. Mateloos interessant vond ik het en ik gebruikte deze casus als onderwerp in mijn studie sociologie. Zo ontstond mijn fascinatie voor mens en technologie. Mijn afstudeeronderwerp was 'automatisering en kwaliteit van de arbeid' – een thema dat tegenwoordig geen issue meer is. Dat laatste zeg ik niet uit spijt maar omdat het leert dat de gevolgen van digitalisering totaal anders kunnen uitpakken dan we in eerste aanleg geneigd zijn te denken. Toen dachten we nog dat de nieuwe technologie vooral op mensen zou inwerken in hun hoedanigheid als arbeider of werknemer. Vandaag zien we dat grote groepen mensen verslaafd zijn aan social media en dat cyber-pesten en sexting mensen er toe kan leiden een einde aan hun leven te maken. Dat is wel wat anders dan 'bewegingsvrijheid op de werkplek' – een item uit mijn afstudeeronderzoek. Het gaat nu eerder om identiteit, kwetsbaarheid, cyberwar, criminaliteit en ondermijning – veel grotere en fundamentelere vragen dus. Weinigen zagen het aankomen. Ik in elk geval niet.

Wel ging eind jaren tachtig mijn aandacht van kantoorautomatisering over op het gebruik van computerdata in politiestraatwerk, met de vraag welke gevolgen dat zou hebben voor het politieoptreden en dus voor de rol van de politie in de samenleving. Daarmee kwamen wel grote vraagstukken in beeld, zoals de balans tussen maatschappelijke vrijheid en overheidscontrole en de balans tussen menselijke waarden en rationaliteit. Dergelijke thema's hebben nog steeds mijn be-langstelling, nu bijvoorbeeld in relatie tot criminaliteit op het darkweb en de vraag wat en hoeveel de overheid daar tegenover kan (of zou moeten) stellen. Maar van een darkweb zoals we dat nu kennen was begin jaren negentig nog geen sprake. Sterker nog: de eerste particuliere aansluitingen op het internet kreeg Nederland pas in 1993. Tijdens het schrijven van mijn proefschrift *Politie-optreden en informatietechnologie: over sociale controle van politiemensen* beloofde ik mezelf een internetaansluiting maar pas ná voltooiing van het laatste hoofdstuk, bang als ik was dat zo'n avontuur het schrijven zou vertragen.

Voorjaar 1996 ging ik online. In 1996 hield de politie ook een digitale conferentie 'Politie op de digitale snelweg?' Let op het vraagteken. De discussie was inderdaad of en zo ja hoe de politie op het internet aanwezig moest zijn. Dat er zoiets bestond als computercriminaliteit of cybercrime werd wel genoemd, maar was geen hoofdlijn in die discussie. Die ging vooral over internet als communicatiekanaal richting publiek. De criminologie speelde in die conferentie geen rol. In 1996 maakte ik de politiewebsite 'The Dutch Police Pages', welke site later is opgegaan in politie.nl. Ik schreef over politie en (de gevolgen van) informatietechnologie. In 1998 mocht ik samen met collega's voor het WODC een onderzoek doen naar criminaliteit op internet, hetgeen uitmondde in het boekje *Criminaliteit in cyberspace* met als hoofdthema's hacken, kinderpornografie en e-fraude, en een artikel in het *Tijdschrift voor criminologie met als titel Criminaliteit met informatie- en communicatietechnologie – politie in een nieuwe sociale context*. Het is één van de eerste Nederlandse criminologische studies naar cybercrime. Maar vroeg was het niet want het moet gezegd dat de juristen zich al veel eerder hadden gebogen over het vraagstuk van cybercrime en dan natuurlijk vanuit de vraag of de wetgeving nog wel was toegesneden op de nieuwe ontwikkelingen. Twee juristen kunnen hier als pioniers te worden genoemd. UL-hoogleraar (em.) dr. mr. Hans Franken was onder meer voorzitter van de Commissie Computercriminaliteit, ingesteld in november 1985 door de Minister van Justitie. Het rapport van de commissie lag aan de basis van de Wet Computercriminaliteit 1993. Ook was hij mede-oprichter van het eLaw, Centrum voor Recht en Digitale Technologie op 1 april 1985, Universiteit Leiden. VU-hoogleraar (em.) dr. mr. Rik Kaspersen mag eveneens worden genoemd als één van de Nederlandse pioniers sinds 1985. Hij verzette onder meer veel werk in de aanloop naar het Cybercrimeverdrag van 2001. Aan de VU was hij actief in het Computer/Law Institute. Tot eind jaren negentig waren op het speelveld dus vooral juristen actief en schiterde de criminologie door afwezigheid. Na de eeuwwisseling ontstond binnen de criminologie langzaamaan meer belangstelling voor het onderwerp.

In december 2010 organiseerde de Nederlandse Vereniging voor Kriminologie (NVK) een studiemiddag cybercrime. De bijeenkomst was in Rotterdam in een klein zaaltje met zo'n 30 belangstellenden, onder wie opvallend weinig wetenschappers maar opvallend veel praktijkmensen met een achtergrond in politiewerk of systeembeheer. Het criminologisch getinte cybercrime-onderzoek speelde zich in Nederland toen af bij: het samenwerkingsverband tussen Noordelijke Hogeschool Leeuwarden (NHL), Open Universiteit (OU) en de Politieacademie (PA) (prof. dr. Wouter Stol), Universiteit Leiden (UL) (dr. Johan van Wilsem), Universiteit Twente (UT) (prof. dr. Marianne Junger) en Onderzoeks- en Adviesbureau Beke (dr. Anton van Wijk). Sprekers die dag waren Wouter Stol (NHL/PA/OU), Marianne Junger (UT), Johan van Wilsem (UL) en Rutger Leukfeldt (NHL). Juridisch onderzoek met criminologische accenten (of andersom) vinden we in die jaren aan de Universiteit van Tilburg (prof. dr. Bert-Jaap Koops).

Voor zover mij bekend komt *Justitiële Verkenningen* de eer toe van het eerste Nederlandse themanummer over het hier besproken onderwerp (2004, 'Cybercrime'). Daarna verschenen in 2012 themanummers van *Tijdschrift voor Veiligheid* ('ICT en Veiligheid') en wederom van *JV* ('Veiligheid in Cyberspace'). In 2013 kwam het Tijdschrift voor Criminologie met haar eerste themanummer op dit terrein ('Criminaliteit en Internet'). De eerste auteurs van de vier artikelen in dat TvC-themanummer zijn Stijn Ruiter (NSCR), Johan van Wilsem (UL), Joyce Kerstens (NHL/OU/PA) en Jurjen Jansen (idem). Het *Tijdschrift voor Veiligheid* heeft een volgend themanummer in de maak (2018).

In de periode 2008-2012 was de NHL/OU/PA samenwerking tamelijk uniek in haar criminologisch cybercrimeonderzoek. Meerdere jaren hing het van deze groep af of er op het jaarlijkse landelijke criminologencongres van de NVK überhaupt aandacht was voor cybercrime. Deze groep bestudeerde in 2009 politiedossiers inzake cybercrime en ontdekte dat cybercrime geen elitair maar een breed voorkomend verschijnsel is (VVC – 'veel voorkomende criminaliteit'). De groep deed in 2011 het eerste Nederlandse bevolkingsonderzoek naar slachtofferschap van cybercrime en vond in het verlengde van de vorige bevinding dat het slachtofferpercentage voor hacken dat van fietsendiefstal toen al bijna had ingehaald. Gaandeweg ontdekten meer criminologen het thema. En kijk nu: cybercrime is het hoofdthema van het NVC-congres in 2018!

Vandaag de dag zijn er in Nederland twee concentraties van criminologische cybercrime-onderzoekers (daarnaast zijn er groepen die cybercrimeonderzoek doen vanuit juridisch, technologisch of governance perspectief). De samenwerking tussen NHL/OU/PA stamt uit 2009, draagt sinds 2016 de naam Cyber Science Center en heeft als onderzoeksprogramma 'Safety, Security and Law Enforcement in Digital Society'. Het Nederlands Studiecentrum voor Criminologie en Rechtshandhaving (NSCR) heeft sinds 2017 een onderzoekscluster Cybercrime, welke is verbonden met de Haagse Hogeschool en onderzoek doet naar de menselijke factor in cybercrime. De trekker van deze NSCR/HHS-combinatie is dr. Rutger Leukfeldt. Binnen de NVC bestaat sinds 2016 de Divisie Cybercrime 'om het onderzoek naar en de uitwisseling van kennis over cybercrime te promoten', aldus de website, met als trekker dr. Johan van Wilsem. Wie via internet zoekt naar "[naam universiteit] cybercrime" vindt overigens vooral veel onderwijsprogramma's. Logisch, want het onderwerp trekt studenten. Natuurlijk zijn er op verschillende plaatsen nog criminologen die zich binnen een 'algemene' afdeling criminologie of strafrecht bezig houden met cybercrimeonderzoek. De nieuwe groep wetenschappers die zijn gepromoveerd op een criminologische cybercrimestudie groeit gestaag, bijvoorbeeld: Litska Strikwerda (UTwente, 2014, *Virtual Cybercrime*), Joyce Kerstens (OU, 2015, *Youth and Cybersafety*), Rutger Leukfeldt (OU, 2016, *Cybercriminal networks*), Bastiaan Leeuw (Unimaas, 2017, *Anti-Piracy Interventions*), Jan-Willem Bullee (Utwente, 2017, *Social Engineering*), Marleen Weulen Kranenbarg (VU, 2018, *Cyber-offenders*), Wytske van der Wagen (RUG, 2018, *Cyborg Crime*). Met excuus aan degenen die ik niet heb genoemd. Ik kom graag in contact!

Goed, wij criminologen zijn traag op gang gekomen. Erg traag. In Nederland is begin jaren tachtig een groepje hackers actief ('techno-anarchisten'). Juristen buigen zich in de jaren tachtig over aanpassingen in de wetgeving. De politie start ongeveer tegelijk haar eerste team Computer-criminaliteit. De pers schrijft in die jaren over het onderwerp. Het eerste criminologische onderzoek naar cybercrime komt tien jaar later op gang en pas nog eens twintig jaar later is cybercrime het hoofdthema op het jaarlijkse criminologencongres. Inmiddels heeft Nederland (inclusief de politie) een schrijnende achterstand in kennis over cybercrime en hoe dat te bestrijden. We mogen dus wel een tandje bijzetten! Graag geef ik daarover nog de volgende suggestie mee.

Naast disciplinaire studies is vooral behoefte aan multidisciplinair onderzoek, niet alleen tussen juristen of psychologen en criminologen maar vooral tussen computerwetenschappers en criminologen. Complexe maatschappelijk problemen lossen we niet op met monodisciplinaire antwoorden. Dat vraagt dat we ons durven bewegen in een technologische wereld, dat we in debat durven gaan met systeemontwikkelaars, securityspecialisten en computerwetenschappers. Dat is niet altijd eenvoudig maar het is noodzaak. Digitalisering betekent nu eenmaal dat onze samenleving technologischer wordt. Er is geen weg terug dus wen er maar aan. Wat voor een criminologisch onderwerp je ook kiest, er is een digitale dimensie. Onderzoek naar cybercrime en vooral het bestrijden daarvan vergt dan ook dat verschillende disciplines hun krachten bundelen.

Over cybercrime en de slachtoffers daarvan

Dr. Johan van Wilsem (WODC)

Cybercrime is here to stay. Dat kunnen we, pak 'm beet 15 jaar nadat het verschijnsel echt vaste voet aan de grond kreeg, inmiddels gerust stellen. Cybercriminologie is inmiddels ook een blijvertje. Het NVC congres 2018 met als thema **Criminaliteit en criminologie in een gedigitaliseerde wereld** is daar een mooie weerslag van. Van origine gaat er -terecht- veel aandacht uit naar de rol van de dader. Maar wat weten we over de andere actor, het *slachtoffer*, binnen de cybercriminologie?

'What we know' en 'need to know'

Inzichten over cybercrime leunen vooralsnog sterk op kennis die vanuit de 'oude' -offline- criminologie is ontwikkeld. Niet onlogisch: goede ideeën moet je toetsen op hun bruikbaarheid in een nieuwe werkelijkheid. Maar een eerste -en heel basale- vraag in de cybercriminologie die hierbij gesteld moet worden is: over wie of wat hebben we het? Kort gezegd: kijken we naar mensen –zoals we in de criminologie gewend zijn- of naar computers en

andere gegevensdragers? En vergt de keuze daarover dat we door kunnen met oude inzichten uit de offline criminologie of zijn er voor een 'machine-georiënteerde' insteek nieuwe inzichten nodig? – zie het werk van Wytske van der Wagen hierover.

Voor de toepassing van oude theorieën op cybercrime-verschijnselen -op slachtoffers en daders- kunnen we vaststellen dat die zoektocht bepaald niet voltooid is. Binnen die oude benadering is daarnaast een open vraag of voor het toetsen van theorieën voor de afhankelijke variabele niet deels andere vormen van dataverzameling vereist is - of aanpassing van vertrouwde manieren van dataverzameling. Daarmee hebben we het gelijk over een basisprobleem: hoe meten we cyberslachtofferschap?

Want: aan de traditionele metingen en vraagstellingen van slachtofferschap (via enquêtes of via aangiftes) kleven bij cybercrime wel wat nadelen. Bij aangiftes is het bijvoorbeeld nogal moeilijk om de cybercrime er uit te filteren - tenzij geselecteerd wordt op wetsartikelen, maar de consequentie is dan dat je je als onderzoeker beperkt tot 'computervredebreuk'. Uiteraard doen mensen ook aangifte van andere vormen van cybercrime, zoals online identiteitsfraude, oplichting, bedreiging, stalking – maar die staan niet apart geregistreerd en staan dus tussen aangiftes van offline varianten van diezelfde delicten. Via textmining van politiedossiers kunnen de relevante zaken eruit gevist worden – een ingewikkeld proces, wat de komende tijd in veel varianten zal moeten worden uitgeprobeerd om te kijken hoe stabiel de omvangschattingen daarover zijn. Het WODC heeft op dit moment een interessant project op dit terrein lopen.

Los daarvan is er natuurlijk het bekende probleem dat aangiftes van cybercrime selectief zijn, want lang niet iedereen doet aangifte. De slachtofferenquête, het traditionele instrument om het dark number van criminaliteit mee vast te stellen, wordt ook voor cybercrime ingezet. Dat levert naast inzichten ook problemen op. Want: wat weet een doelwit over zijn of haar slachtofferervaringen? Is die in staat om vast te stellen of diens computer met malware is besmet? Of slachtoffer van identiteitsfraude is geworden? Of, aan de preventiekant: welke maatregelen iemand heeft genomen op zijn of haar computer(s) of telefoon?
Maar laten we niet pessimistisch worden, er zijn daarnaast cyberdelicten die slachtoffers vrij goed kunnen vaststellen (of ze opgelicht of bedreigd zijn bijvoorbeeld). En: er zijn enkele interessante studies waarin aan de hand van alternatieve vraagstellingen een vollediger zicht wordt verkregen van wie wel of niet slachtoffer wordt van technologisch geavanceerde delicten. Visualisering van riskante online situaties in een enquête werd hiervoor gebruikt - en alternatieve vraagstellingen die niet zozeer gericht zijn op slachtofferschap maar op problemen die iemands PC vertoont - en die duiden op malwarebesmetting.

Een uitdaging voor de toekomst is om aan de hand van online materiaal schattingen over cyberslachtofferschap te kunnen doen: hoe vaak wordt in een bepaalde taal een online bedreiging geuit op sociale media, hoe veel creditcardgegevens worden in diverse online fora te koop aangeboden, hoeveel malwaremeldingen krijgen softwareproducenten binnen, etc.?

Over wie hebben we het?
Met name op basis van slachtofferenquêtes zijn we het nodige te weten gekomen over wie er slachtoffer wordt van cybercrime. In ieder geval kunnen we op basis daarvan vaststellen dat -voor een aantal cyberdelicten- er wel parallellen zijn met patronen in de offline wereld. Kort gezegd: online en offline slachtoffers hebben gemeenschappelijk dat ze vaak jong en bovengemiddeld impulsief zijn. Dat blijkt althans uit verschillende studies, ook uit Nederland, voor verschillende typen delicten zoals online bedreiging, oplichting en gehackt worden. Ook presenteren we (Tom Holt, Steve van de Weijer, Rutger Leukfeldt en ondergetekende) tijdens dit NVC-congres een paper waaruit blijkt dat dit patroon ook gevonden wordt voor indicaties van malware-besmetting - de al eerder gememoreerde computerproblemen die we aan respondenten vroegen.

Grote uitzondering tot dusver vormt identiteitsfraude - waarvoor noch bovenstaande noch andere duidelijke risicofactoren konden worden onderscheiden voor slachtofferschap. Met de metingen die we voorhanden hadden kwam er voor dit delict een patroon van behoorlijke willekeur naar voren in de doelwitkeuze. Mogelijk is het risico op identiteitsfraude vooral bepaald door het beveiligingsniveau van de organisaties waar identiteitsgegevens zijn opgeslagen – en minder terug te voeren op eigen gedrag.

Of: spelen er ook aspecten van het slachtoffer zelf mee waar we tot nu toe onvoldoende zicht op hebben met het huidige onderzoek? Voor veel cybercrime geldt namelijk dat slachtofferschap de uitkomst is van een proces waarbij de reactie van het slachtoffer kan hebben bijgedragen aan het eigen slachtofferschap. Een statement dat zou kunnen worden opgevat als victim blaming, maar zo is het niet bedoeld. Veel van deze interacties zijn er bijvoorbeeld vanuit het perspectief van de dader op uit om het doelwit op het verkeerde been te zetten - een tactiek die bij phishing en aanverwante technieken een belangrijk onderdeel van de modus operandi vormt. Een vraag die hieruit voortkomt is: hoe reageren online doelwitten en waar hangt hun reactie dan van af? Naast (vaste) persoonskenmerken, zoals leeftijd en impulsiviteit, spelen mogelijk componenten van de inhoud (tekstueel, visueel) een rol evenals situationele invloeden (bijv. vermoeid of afgeleid zijn). Een verdere zoektocht naar deze vragen kan een completer beeld schetsen wie slachtoffer wordt. Want hoewel voor veel delicten een patroon van 'jong en wild' geldt, zijn er voldoende uitzonderingen op dat patroon – de r kwadraat kan nog een stuk beter! Respondenten aan de hand van concrete online situaties of tijdens online sessies blootstellen aan boodschappen en monitoren hoe ze daarop reageren, is een vorm van onderzoek die over cyberslachtofferschap veel kan opleveren.

Tot slot. Cybercrime is niet alleen 'here to stay', het heeft ook een aantal elementen in zich die het doen verschillen van offline criminaliteit, zoals de mogelijkheid om te interacteren met iemand die in wezen een volstrekt ander iemand is dan hij/zij zich voordoet (bijv. een groep cybercriminelen in plaats van een potentiele liefdespartner, zoals bij romance scams gebeurt), cyberaanvallen die zonder aanziens des persoons massaal worden uitgevoerd met voor slachtoffers onduidelijke mogelijkheden om zich daar tegen te wapenen, mogelijkheden om iemand zeer vaak of massaal lastig te vallen en de mogelijkheid dat kwalijke uitingen permanent geregistreerd blijven op Internet. Onderzoek naar de prevalentie van dit soort kwalitatieve aspecten van cybercrime delicten – en de effecten die dit heeft op het welzijn, online gedrag en beveiligingsgedrag van slachtoffers vormen een belangrijk onderdeel van toekomstig cyberonderzoek op dit thema.

Cybercriminologie: uitdagingen voor criminologisch onderzoek

Dr. Marleen Weulen Kranenbarg
(Vrije Universiteit Amsterdam)

Cybercriminologie: uitdagingen voor criminologisch onderzoek n.a.v. een eerste empirische vergelijking tussen cybercriminelen en traditionele criminelen

Het is nu bijna 5 jaar geleden dat ik aan mijn promotieonderzoek bij het NSCR begon. In die tijd was cybercrime iets waar voornamelijk techneuten zich mee bezig hielden. Op een enkele uitzondering na, was het voor criminologen nog onontgonnen terrein. Nu, 5 jaar later, is het hét onderwerp van ons jaarlijkse congres.

In die 5 jaar werkte ik aan mijn promotieonderzoek, waarin ik cybercriminelen heb vergeleken met traditionele criminelen op 4 onderzoeksgebieden die traditioneel gezien belangrijk zijn in criminologisch onderzoek: 1. daderschap gedurende de levensloop, 2. persoonlijke en situationele risicofactoren voor daderschap en slachtofferschap, 3. overeenkomst in crimineel gedrag van een persoon en diens sociale omgeving en 4. motieven voor het plegen van verschillende delicten. Gezien de digitale context waarin cybercrime plaatsvindt, was het de vraag in hoeverre bestaande criminologische kennis nog steeds van toepassing was. Op elk van deze vier gebieden bleken zowel belangrijke overeenkomsten als verschillen te ontdekken.

Ten eerste bleek voor de levensloop dat voor cybercrime het samenwonen met een gezin zelfs in sterkere mate samenhing met een lagere kans op daderschap dan voor traditionele criminaliteit. Ondanks dat direct toezicht op online gedrag lastig is, lijkt de indirecte sociale controle van een gezin dus wel degelijk een belangrijke beschermende factor. In de levensloop was echter ook een belangrijk verschil te vinden: het hebben van werk heeft geen verminderend effect op cyber-daderschap. Sterker nog, in deze populatie van cyber-verdachten bleek dat een persoon een hogere kans heeft op cyber-daderschap in jaren waarin die persoon in de IT-sector werkt of een opleiding volgt dan in jaren waarin die persoon geen werk heeft of geen opleiding volgt. Hieruit blijkt dat de gelegenheid voor cybercrime zich in andere situaties voordoet dan de gelegenheid voor traditionele criminaliteit.

Dat verschil in gelegenheid was ook terug te zien in het tweede deelonderzoek, waarin bleek dat cybercriminelen vooral verschillen van traditionele criminelen in situationele risicofactoren zoals dagelijkse (online) activiteiten. Daarnaast bleek dat er ook bij cybercrime sprake is van een overlap tussen daderschap en slachtofferschap en dat personen die zowel dader als slachtoffer zijn de meeste risicofactoren hebben, zoals een lage zelfcontrole, enige IT-kennis en dagelijkse online activiteiten die zowel gelegenheid bieden voor daderschap als risico's voor slachtofferschap. Personen die enkel dader waren pleegden de meer technische cybercrimes, wat ook terug te zien was in factoren als hogere zelfcontrole, meer IT-kennis en meer gerichte online activiteiten waarin die kennis kon worden opgedaan, zoals gebruik van fora.

De sociale omgeving van cybercriminelen bleek wat betreft cybercrimineel gedrag en attitudes een minder sterke overeenkomst te vertonen dan de sociale omgeving van traditionele criminelen. Hier bleek mijn empirische vergelijking een belangrijke toegevoegde waarde, aangezien er wel degelijk een overeenkomst in cyber-crimineel gedrag is in het sociale netwerk, maar deze veel minder sterk is. Dit kan verschillende dingen betekenen, zo zouden cybercriminelen hun deviante contacten wellicht meer in losse contacten op het internet kunnen zoeken en daarnaast kan dit betekenen dat voor cybercriminaliteit alles wat je nodig hebt aan informatie online te vinden is, waardoor directe criminele contacten overbodig zijn geworden.

Als laatste heb ik nog exploratief gekeken naar de motieven voor cybercriminaliteit. Deze bleken sterk af te wijken traditionele motieven. Cybercrime wordt voornamelijk gepleegd vanuit intrinsieke motieven, zoals nieuwsgierigheid, uitdaging en zien hoe ver je kunt komen. Financiële motieven ontbraken vrijwel volledig en andere extrinsieke motieven zoals indruk maken op anderen waren veel minder belangrijk.

Hoewel de criminologie inmiddels een stuk verder is op het gebied van cybercrime, volgen er ook uit mijn onderzoek weer veel nieuwe criminologische onderzoeksvragen. Zo is diepgaand longitudinaal onderzoek naar daderschap over de levensloop een must. Hoe vergaren cybercriminelen hun kennis en op welke manier doen gelegenheden zich voor tijdens dagelijkse bezigheden? Is er een causale relatie tussen daderschap en slachtofferschap? In hoeverre is er sprake van selectie van of beïnvloeding door de sociale omgeving? Is er ook selectie en beïnvloeding van online sociale contacten? Ik hoop dat de criminologie ook de komende jaren dit onderzoeksgebied verder gaat ontwikkelen en zich onder andere gaat richten op deze vragen.

Mijn volledige proefschrift en de Nederlandse samenvatting, inclusief een meer uitgebreide omschrijving van implicaties voor toekomstig onderzoek, zijn te downloaden via: http://dare.ubvu.vu.nl/handle/1871/55530

From Cybercrime to Cyborg Crime – mijn proefschrift in een notendop

Dr. Wytske van der Wagen
(Erasmus Universiteit Rotterdam)

Universiteiten die worden gehackt, computersystemen die worden gegijzeld of tot 'zombies' gemaakt, servers van internetproviders die worden gebombardeerd, we worden bijna dagelijks wel geconfronteerd met cybercrime en haar gevolgen. Deze meer technische vormen van cybercrime wijken op verschillende fronten af van traditionele criminaliteit, waaronder hun deels geautomatiseerde en gedistribueerde karakter, het feit dat ze niet of nauwelijks gehinderd worden door barrières van tijd en plaats en ook een enigszins andere dynamiek hebben in termen van oorzaak en gevolg. Al langere tijd is er in de criminologie dan ook veel discussie over de vraag of bestaande criminologische theorieën nog voldoende verklaringskracht hebben in de digitale wereld. Een van de heikele punten hierbij is de relatie tussen de online en de offline wereld. Moet cyberspace beschouwd worden als een aparte wereld of is het veeleer een verlengstuk van de fysieke wereld?

Mijn proefschrift tracht ook een bijdrage te leveren aan het 'nieuwheidsdebat' door kritisch te kijken naar de houdbaarheidsdatum van bestaande criminologische theorieën. Het focust zich echter op een vraagstuk dat relatief nog weinig aandacht heeft gekregen, namelijk hoe we de rol van technologie moeten duiden in cybercriminaliteit. Het onderzoek richt zich niet zozeer op de grens tussen online en offline, maar op die tussen mens en machine. Kunnen we criminele verschijnselen zoals botnets of gijzelsoftware wel begrijpen vanuit een traditionele (antropocentrische) bril? Is daderschap of slachtofferschap in cyberspace nog wel iets exclusief menselijks? Kunnen we in het licht van hedendaagse technologische ontwikkelingen nog wel een strikte scheiding aanbrengen tussen mens (doel) en technologie (middel)?

In mijn proefschrift stel ik dat we in de criminologie (uitzonderingen daargelaten) nog op een (te) instrumentele (substantivistische), antropocentrische en dualistische manier naar de relatie tussen mens en technologie kijken en dat hier verandering in moet komen. In deze context heb ik een beroep gedaan op de actor-netwerktheorie (ANT) van Bruno Latour (e.a.), een anti-dualistisch perspectief c.q. lens die specifiek oog heeft voor de verweving van mens en technologie en die ook actorschap aan technologie toekent. De (toegevoegde) waarde van dit perspectief heb ik in verschillende empirische casestudies verkend.

De eerste casestudie betrof een ANT-analyse van een grootschalig botnet (op basis van politiedossiers), waarbij is gekeken naar welke actoren een rol spelen bij het ontstaan, de ontwikkeling en het uiteenvallen van een botnet. Hieruit kwam naar voren dat een botnet niet slechts als een door de mens (botherder) aangestuurd netwerk kan worden beschouwd, maar juist gevormd en in stand gehouden wordt door een hybride netwerk van menselijke en niet-menselijke entiteiten. Ook heb ik ANT toegepast op het hackerfenomeen, waarbij interviews met hackers zijn afgenomen. Deze casestudie heeft laten zien dat we een genuanceerder beeld kunnen verkrijgen van de wereld van de hacker, hun zelfbeeld, motieven en morele percepties, als we explicieter aandacht besteden aan hoe zij betekenis geven aan hun (deviante) relatie en interactie met technologie. In de laatste casestudie van het proefschrift worden drie soorten high tech slachtofferschap onder de loep genomen, namelijk botnets, ransomware en virtuele diefstal. Hierbij wordt (eveneens) het standpunt ingenomen dat bestaande dualismen zoals menselijk versus niet-menselijk, echt versus fictioneel, dader versus slachtoffer niet langer productief zijn bij de duiding van het cyberslachtoffer(schap). Geconcludeerd wordt dat het conceptuele raamwerk van ANT waardevolle aanknopingspunten kan bieden voor de analyse van slachtofferschap.

Mijn proefschrift heeft uiteindelijk geresulteerd in een alternatief en/of additioneel perspectief op high tech cybercrime, wat ik aanduid als het 'cyborg crime' - perspectief. De belangrijkste uitgangspunten van dit perspectief zijn dat 1) dader- en slachtofferschap van high tech cybercrime moeten geanalyseerd worden als hybride producten van menselijke, technische en/of virtuele (inter)acties en 2) dat de rol van technologie meer aandacht moet krijgen in de analyse van fenomenen en niet slechts in instrumentele of functionele termen moet worden geduid. Uiteraard ga ik in mijn proefschrift uitgebreid in op de mogelijkheden, beperkingen en implicaties van een dergelijk perspectief.

Al met al hoop ik met mijn onderzoek een bijdrage te hebben geleverd aan theoretische vernieuwing in de cybercriminologie en ook nieuwe discussies aan te wakkeren over de rol van technologie in criminaliteit, nu en in de toekomst. Hoewel computers nog niet slimmer zijn dan de mens, moeten we als criminologen zeker al vast stilstaan bij dat scenario.

Ervaringen uit de praktijk

Youri Jelsma, MSc.
(Motiv ICT-security)

Bij criminaliteit heb je vaak een bepaald beeld. Meestal denken mensen dan aan vormen van 'offline' criminaliteit. De traditionele vormen van criminaliteit zijn veelal meer tastbaar en spreken meer tot onze verbeelding. Cybercrime daarentegen is voor velen nog een ongrijpbaar begrip.

Ook binnen de criminologie is pas sinds enkele jaren een groeiende aandacht voor cybercrime. Gedurende de master criminologie aan de Erasmus Universiteit kwam ik, na enkele colleges van Wytske van der Wagen, in aanraking met het thema cybercrime. Cybercrime bleek een thema te zijn dat mij intrigeerde, waarop ik dan ook besloot mijn afstudeerscriptie te schrijven over dé stereotype cybercrimineel, namelijk hackers. Deze stereotypering generaliseert een zeer heterogene en diverse gemeenschap. De hackergemeenschap en de wijze waarop hackers onderling differentiatie aanbrengen naar aanleiding van dergelijke stereotyperingen waren dan ook onderwerp van onderzoek.

Uit mijn afstudeeronderzoek 'Still Hacking Anyway' komt naar voren dat hackers deel uitmaken van een subcultuur die wordt gekenmerkt door een sterke verbondenheid met technologie, humor en een sterk eigen moraal. (Offline) hackerspaces en hackerconferenties nemen een belangrijke plaats in binnen de hackergemeenschap. Daarnaast blijkt dat de categorisering die binnen de hackergemeenschap plaatsvindt, lijkt te zijn ontstaan uit een tegenreactie op de negatieve connotaties die aan het begrip hacken kleven. De noodzaak tot categorisering lijkt echter af te nemen nu de negatieve beeldvorming rondom hackers stukje bij beetje wordt afgebroken. Een goed voorbeeld hiervan is de leidraad Responsible Disclosure aan de hand waarvan een organisatie een Responsible Disclosure beleid kan opstellen. Hiermee kunnen op voorhand spelregels worden opgesteld waar welwillende hackers zich aan dienen te houden, zoals het opstellen van een goed en duidelijk rapport, het geven van een redelijke termijn aan de organisatie om het lek te dichten en het betrachten van proportionaliteit bij het aantonen van het lek. De leidraad erkent dat de hulp van welwillende hackers, mits het voldoet aan bepaalde voorwaarden, in de huidige maatschappij geaccepteerd en zelfs aangemoedigd wordt. Daarnaast bied het de hacker bescherming tegen vervolging wanneer deze de voorwaarden van Responsible Disclosure in acht heeft genomen. Initiatieven zoals de leidraad Responsible Disclosure toont aan dat er een groeiende bewustwording voor de helpende hacker is en lijkt de kloof tussen hackers, de overheid en het bedrijfsleven langzaam maar zeker te dichten.

In de huidige maatschappij zijn bedrijven, overheidsinstanties en burgers steeds meer afhankelijk geworden van informatica, waarbij vaak gevoelige data wordt gedeeld en opgeslagen. De afgelopen decennia is dan ook een grote toename in cybercriminaliteit waar te nemen, terwijl de algemene tendens is dat de criminaliteitscijfers van de traditionele criminaliteit dalen. Van state-sponsored cyberwarfare tot aan script-kiddies, van het plat leggen van kritieke infrastructuur tot het stelen van naaktfoto's uit de iCloud. De impact die cybercrime kan hebben op onze samenleving en bedrijven is enorm. Ransomware aanvallen, zoals met 'WannaCry' en 'NotPetya', hebben dit vorig jaar nog maar eens bewezen. Voor mij als criminoloog was het dan ook snel duidelijk dat ik mezelf verder wilde ontwikkelen binnen de cybersecurity en hiermee een bijdrage wilde leveren aan het veiliger maken van onze maatschappij.

Ondanks het feit dat de meeste criminologen geen ICT-achtergrond hebben, is de criminologische kennis die je op doet en de kritische en analytische denkwijze die je aanneemt gedurende de opleiding van toegevoegde waarde. Daarnaast wordt gedurende de opleiding tot criminoloog ook veel aandacht besteed aan beleid en beleidsonderzoek, waarbij je vaardigheden en kennis opdoet die je ook binnen de ICT-security kan gebruiken. Het duurde dan ook niet lang voordat ik na het afstuderen aan de slag kon op het Security Operations Center (SOC) bij Motiv ICT-security.

Motiv ICT-security is, de naam verraadt het al, een bedrijf dat zich volledig heeft gespecialiseerd in ICT-security en diensten aanbiedt ter voorkoming van cybercriminaliteit, datadiefstal en datalekken. Een belangrijk onderdeel van de dienstverlening die ICT-security bedrijven leveren, is het monitoren van de netwerken van klanten door middel van een SIEM (Security Information & Event Management) oplossing. Het verkeer dat via de SIEM oplossing wordt gemonitord, komt binnen bij het SOC. Op het SOC bestaan mijn werkzaamheden uit het analyseren van events die binnen onze monitoring worden gedetecteerd. Hierbij komt mijn analytisch vermogen en kritische houding zeer goed van pas. Daarnaast is het van belang om op de hoogte te blijven van de laatste beveiligingsdreigingen, waarbij threat-intelligence en open source intelligence (OSINT) een grote rol spelen. Het trianguleren van verschillende bronnen om vanuit je analyse tot een degelijke conclusie te komen, is iets wat ik heb geleerd tijdens mijn opleiding en nog altijd dagelijks gebruik in mijn analyses. Verder heeft de Motiv-Academy mij de kans geboden om in een traject van acht maanden verder te worden opgeleid tot securityspecialist op het gebied van netwerken, cryptografie en malware forensics. Waarbij ik vaardigheden op doe op het gebied van scripting en hacking. Als criminoloog heb je een goede basis en als je bereid bent om jezelf wat extra technisch te verdiepen, dan zijn er kansen genoeg om binnen de ICT-security een bijdrage te leveren aan een veiligere maatschappij.

COLOFON

Redactie:
Tamar Fischer
Steve van de Weijer

vormgeving:
Joost van Ommen

Correspondentieadres:
De Criminoloog
Postbus 71304
1008 BH Amsterdam

info@criminologie.nl
www.criminologie.nl