Cyber-offenders versus traditional offenders: an empirical comparison

Marianne Junger

Weulen Kranenbarg, M. (2018). Cyber-offenders versus traditional offenders: an empirical comparison (dissertatie Vrije Universiteit Amsterdam

Het doel van Marleen Weulen Kranenbargs promotieonderzoek is om de plegers van cybercriminaliteit te vergelijken met de daders van traditionele criminaliteit.[1] De digitalisering heeft onze wereld in nagenoeg alle opzichten veranderd. Informatie- en communicatietechnologie (ICT) levert vele gemakken en nieuwe mogelijkheden op en creëert tevens nieuwe mogelijkheden voor criminaliteit. Een prangende vraag is: zijn de daders van cybercriminaliteit een nieuw type criminelen of zijn het de 'oude/traditionele' criminelen die zich hebben aangepast? Daaruit vloeit de vraag voort of de traditionele criminologische theorieën nog geldig zijn voor de daders van cybercriminaliteit. Marleen Weulen Kranenbarg bespreekt deze vragen aan de hand van enkele grote thema's in de criminologie: de sociodemografische kenmerken van verdachten, de dader-slachtofferschapoverlap, de invloed van vrienden en de motieven voor het plegen van delicten.

Een belangrijk punt voor onderzoekers op dit terrein is om vooraf te bepalen wat nu precies cybercriminaliteit is. In de beginjaren van de digitalisering ontstond het onderscheid tussen twee typen cybercriminaliteit: de *cyber-dependent* criminaliteit en de *cyber-enabled* criminaliteit. Cyber-enabled misdrijven zijn 'traditionele/oude' misdrijven die worden gefaciliteerd door ICT. Dan gaat het bijvoorbeeld om online fraude, stalken en intimidatie. Bij cyber-dependent criminaliteit gaat het om nieuwe misdrijven, die alleen mogelijk zijn dankzij de ICT-structuur. Hierbij gaat het onder meer om DDoS-aanvallen (Distributed Denial of Service), hacken, *web defacement* (een website aantasten), illegale controle over ICT-systemen en/of malwaregebruik. In haar onderzoek heeft Weulen Kranenbarg de cyber-enabled delicten en daders buiten beschouwing gelaten. Deze beperking heeft belangrijke gevolgen, die later worden besproken.

Weulen Kranenbarg heeft tweemaal twee steekproeven getrokken uit het politiesysteem waarvan de zaak naar het Openbaar Ministerie is gezonden. Ten behoeve van de cyber-dependent misdrijven zijn alle verdachten geselecteerd die in het systeem van de politie bekend waren, dat waren er 870. In het proefschrift worden verschillende steekproeven geanalyseerd. Hoofdstuk 2 is gebaseerd op een vergelijking van alle 870 verdachten van cyber-dependent misdrijven met alle 1.144.740 verdachten van traditionele delicten van 18 jaar en ouder, die bij de

1 De woorden 'criminelen', 'daders' en 'verdachten' worden door elkaar gebruikt, Weulen Kranenbarg spreekt over 'offenders'.

politie bekend zijn. Zij worden vergeleken op een aantal sociodemografische kenmerken aan de hand van gegevens van de politie, aangevuld met levensloopgegevens van het CBS. In crosssectionele analyses (hoofdstuk 3 t/m 5) zijn 928 voormalige verdachten van cyber-dependent misdrijven en 875 voormalige verdachten van traditionele misdrijven geselecteerd in de politiesystemen en deze voormalige verdachten ontvingen het verzoek om een online vragenlijst in te vullen. De respons was 29 procent onder de verdachten van cyber-dependent misdrijven en dit leidde tot een uiteindelijke nettosteekproef van N=268; onder verdachten van traditionele misdrijven was de respons 16 procent en uiteindelijk bleven er N=267 verdachten in de nettosteekproef over.
In de eerste studie (hoofdstuk 2) worden verdachten van cyber-dependent misdrijven vergeleken met verdachten van traditionele misdrijven op drie demografische kenmerken, namelijk de samenstelling van het huishouden, opleiding (wel of geen IT) en werkkring. Met een partner en kind samenleven verkleint de kans op een misdrijf sterker bij de verdachten van cyber-dependent misdrijven in vergelijking met de verdachten van traditionele misdrijven (p. 41). Met een kind samenleven vergroot echter de kans op een cyber-dependent misdrijf. Met betrekking tot de opleiding zijn er geen statistisch significante effecten gevonden. Daarnaast vermeldt de auteur ook dat er statistisch significante verschillen zijn gevonden in leeftijd en nationaliteit. De gemiddelde leeftijd van cyber-verdachten is 33,35 en van traditionele verdachten is dat 37,97. Met betrekking tot nationaliteit zijn er ook verschillen: onder cyber-dependent misdrijven is 71 procent van de verdachten Nederlands, en onder traditionele verdachten is dit 66 procent (zie p. 35). Ook andere studies vonden verschillen in leeftijd en nationaliteit (Domenie e.a., 2009; Montoya e.a., 2013). Deze verschillen in leeftijd en nationaliteit worden door Weulen Kranenbarg niet verder besproken. Zij stelt vast dat er een aantal verschillen bestaat tussen de twee categorieën verdachten met betrekking tot de andere sociodemografische variabelen. Maar een dieper inzicht is lastig te verkrijgen op basis van uitsluitend sociodemografische data.
In hoofdstuk 3 onderzoekt Weulen Kranenbarg de overlap tussen verdachten en slachtoffers. In onderzoek naar traditionele criminaliteit zijn sterke verbanden gevonden tussen verdachten en slachtoffers van criminaliteit (Jennings e.a., 2012). Ook in dit proefschrift is er een aanzienlijke overlap gevonden, met een odds ratio (OR)=2,19 voor cyber-dependent criminaliteit en OR=3,27 voor verdachten van traditionele misdrijven.

In verdere analyses maakt de auteur onderscheid tussen 'uitsluitend dader', 'uitsluitend slachtoffer' en de combinatie 'dader-en-slachtoffer'. Dit wil zeggen, zij vergelijkt de categorieën 'uitsluitend dader', 'uitsluitend slachtoffer' en de combinatie 'dader-en-slachtoffer' onder verdachten van cyber-dependent misdrijven met dezelfde categorieën van verdachten van traditionele misdrijven op een aantal risicofactoren. Van de 39 tests zijn er twaalf statistisch significant (daarnaast zijn drie gecombineerde tests ook statistisch significant). De belangrijkste verschillen vat ik als volgt samen:

a Zij vindt geen verschillen in zelfcontrole tussen de verschillende groepen. Dit wil zeggen: de combinatie 'dader-en-slachtoffer' heeft een lagere zelfcontrole

Tijdschrift voor Criminologie 2019 (61) 1
doi: 10.5553/TvC/0165182X2019061001005

dan de categorieën 'uitsluitend dader' en 'uitsluitend slachtoffer', maar dit is het geval onder zowel verdachten van cyber-dependent misdrijven als verdachten van traditionele misdrijven.

b In de 'uitsluitend dader'-categorie blijkt dat de verdachten van cyber-dependent misdrijven en traditionele misdrijven voornamelijk verschillen op één punt: traditionele verdachten programmeren minder. Het andere statistisch significante verschil betreft de gecombineerde cluster van routine activities-variabelen.

c In de gecombineerde 'dader-en-slachtoffer'-categorie verschillen de twee categorieën verdachten van elkaar op drie punten. De 'IT skills' zijn sterker gerelateerd aan de kans op cyber-dependent criminaliteit dan aande kans op het plegen van traditionele misdrijven. Ook leven de daders-en-slachtoffers van cyber-dependent misdrijven vaker bij hun ouders dan de daders-en-slachtoffers van traditionele misdrijven. Het derde punt betreft de gecombineerde cluster van routine activities-variabelen waarop de verschillende groepen van elkaar verschillen.

d De andere zeven verschillen betreffen de vergelijkingen van de verdachten van cyber-dependent misdrijven en de verdachten van traditionele misdrijven in de 'uitsluitend slachtoffer'-categorie. Weulen Kranenbarg stelt vast dat de groep die uitsluitend dader is wat 'technologischer georiënteerd' is dan de andere categorieën die zij analyseert. Daarnaast zijn er duidelijke situationele factoren die verschillend zijn voor daderschap en slachtofferschap.

In hoofdstuk 4 onderzoekt de auteur de samenstelling van het vriendennetwerk van de verdachten. Al heel lang wordt gesteld dat de invloed van criminele vrienden en het 'leren' van criminele waarden belangrijke oorzaken zijn van criminaliteit (Akers, 1990; 1996; Sutherland & Cressey, 1974). Het is daarom interessant om te bekijken wat de impact hiervan is op cyber-dependent misdrijven. Er wordt vaak aangenomen dat de netwerken online aanzienlijk groter zijn. In theorie is het zo dat online, op allerlei manieren, via social media of webfora, gebruikers makkelijk in contact kunnen komen met al dan niet verwante anderen en op die manier hun netwerk sterk kunnen uitbreiden, hetgeen voor het plegen van delicten interessant kan zijn. De auteur stelt terecht dat informatie opzoeken of ontvangen van iemand online niet gelijk betekent dat men een 'netwerk' heeft en dat er 'social learning' plaatsvindt (p. 80).

Om de impact van vrienden te meten wordt gevraagd naar belangrijke significante anderen: respondenten is verzocht 'to name up to five important personal social network members, called alters, with whom they had discussed important things in the preceding twelve months' (p. 84). 8,87 procent van de respondenten heeft online een deviante alter en 4,66 procent heeft een deviante alter in de fysieke wereld. Dat vind ik zelf vrij lage percentages, gegeven dat alle respondenten al voor een misdrijf in het politiesysteem staan geregistreerd en hun zaak sterk genoeg was om naar het Openbaar Ministerie te worden verzonden. Jammer dat deze percentages niet per categorie – cyber-dependent versus traditionele – verdachten worden gegeven.

Interessant is dat de relatie tussen de betrokkenheid bij criminaliteit en alters deviant gedrag veel sterker is onder diegenen die traditionele misdrijven plegen dan onder diegenen die cyber-dependent misdrijven plegen. Ons eigen onderzoek liet eveneens zien dat cybergefaciliteerde fraude vaker alleen wordt gepleegd dan traditionele fraude (Montoya e.a., 2013). Met de hiervoor genoemde lage percentages van deviante 'alters' is het mij niet helder waarom er staat dat de resultaten in lijn zijn met de stelling dat 'older mentors can be important in a social learning process for cyber criminality'.

In hoofdstuk 5 worden de motieven voor cyber-dependent misdrijven en traditionele delicten onderzocht. De auteur vindt dat de financiële motieven van groot belang zijn voor traditionele misdrijven en dat niet-financiële motieven domineren voor cyber-dependent misdrijven. Bij niet-financiële motieven gaat het om verveling of 'fun', de uitdaging aangaan, wraak, boosheid of een boodschap afgeven.

Hierbij wil ik twee opmerkingen plaatsen. Allereerst, hoe valide is het om over 'motivaties' te spreken? De auteur geeft zelf al aan dat vragen naar motivaties naderhand veel lijkt op 'justifications', ofwel rechtvaardigingen (p. 109). Het lijkt verstandig om over doelstellingen te spreken, die beter zichtbaar zijn. Daarnaast denk ik dat het wat gewaagd is om de uitspraken van een onderzoek naar cyber-dependent misdrijven te veralgemeniseren naar de motieven voor cybercriminaliteit meer in het algemeen. De gegevens van, bijvoorbeeld, Verizon Risk Team (2018, 5) leveren een heel ander beeld op. Verizon (2018) analyseerde 53.308 securityincidenten afkomstig van de hele wereld. Hiervan was 76 procent financieel gemotiveerd en 13 procent was spionage, bij elkaar is dat al 89 procent van alle incidenten. Commerciële securitybedrijven zien natuurlijk maar een specifieke selectie van alle online misdrijven en kunnen hun eigen motivatie hebben om cybercrimeverliezen zwaar aan te zetten. Maar ook vele andere bronnen laten zien dat de aantallen economisch gemotiveerde misdrijven enorm zijn (Tcherni-Buzzeo, 2016; Bayoumy, 2018). Ook slachtofferstudies die alleen naar individuen kijken, vinden dat de meeste gerapporteerde delicten een economisch doel hebben (McGuire & Dowling, 2013). De discrepantie tussen de bevindingen van Weulen Kranenbarg en de Verizon-rapportage is apart en doet vermoeden dat in dit proefschrift een bijzondere selectie van verdachten is geanalyseerd. Zoals aangegeven onderzocht zij alleen de 'cyber-dependent' verdachten. Dit is 0,076 procent van alle verdachten.[2] Echter, de meeste cyberdelicten zijn cyber-enabled en zitten verborgen in de politiestatistieken van de traditionele delicten. Montoya e.a. (2013) vonden dat 16 procent van alle bedreigingen ICT-gefaciliteerd is en 41 procent van alle fraude ICT-gefaciliteerd is. Door cyber-enabled criminaliteit niet te onderzoeken heeft Weulen Kranenbarg de veralgemenisering van haar resultaten beperkt.

Een aantal zaken viel mij op. Een eerste punt is: hoeveel overlap is er tussen verdachten van cybercriminaliteit en verdachten van traditionele misdrijven?

2 Namelijk: 870 verdachten van cyber-dependent misdrijven gedeeld door alle verdachten (1.144.740 traditionele verdachten + 870 verdachten van cyber-dependent misdrijven).

Zoals hierboven is vermeld, baseert de auteur haar crosssectionele analyses op twee verschillende steekproeven: eerst een steekproef van verdachten van cybercriminaliteit, en ter vergelijking een steekproef van verdachten van traditionele misdrijven. Dan verwacht je als lezer dat steeds de gegevens van deze twee steekproeven worden besproken. Maar het lijkt erop dat beide steekproeven bij elkaar worden gevoegd. Toch wordt er wel onderscheid gemaakt tussen verdachten van cyber-dependent misdrijven en verdachten van traditionele misdrijven, maar dan op basis van zelfrapportage, niet op basis van de gegevens van de politiesteekproeven van de twee categorieën verdachten. Vanuit de opdracht om de twee categorieën verdachten te vergelijken is het samenvoegen een verrassend besluit, dat niet wordt besproken. Dat roept de vraag op waarom dit zo is gedaan. Wellicht waren de twee categorieën daders toch niet zo helder te onderscheiden? Het lijkt mij interessant om te weten hoeveel overlap er is tussen de twee steekproeven in termen van type misdrijven: zijn er veel verdachten van cyber-dependent misdrijven die ook traditionele delicten plegen? Studies, ook in Nederland, laten zien dat er een flinke overlap bestaat (Broek e.a., 2014). Navraag bij de auteur leert dat er inderdaad overlap was tussen de verschillende categorieën. Het was goed geweest om die overlap te presenteren, vooral omdat de gelijkenis dan wel verschillen tussen de twee typen verdachten de hoofdvraag van het proefschrift vormen. Ook is het de vraag hoe er met de overlap is omgegaan: waar zijn de daders die zowel cyber-dependent misdrijven als traditionele delicten plegen ingedeeld?

Het is van belang in herinnering te roepen dat alleen verdachten in het onderzoek zijn betrokken. In hoofdstuk 5 blijkt dat slechts 30 procent van de 504 verdachten tijdens de afgelopen twaalf maanden een delict opgaf (cyber-dependent of traditioneel). Er wordt niet vermeld hoe oud de zaken zijn waarop de verdachten zijn geselecteerd. Dat zou in beginsel van vrij lang geleden kunnen zijn.

Een ander punt is: hoe relevant is het onderscheid cyber-dependent en cyber-enabled? Het onderscheid wordt in het proefschrift naar voren geschoven omdat alleen 'cyber-dependent' verdachten zijn geselecteerd. Maar het onderscheid wordt niet systematisch vastgehouden, want in de zelfrapportage worden delicten als 'guessing passwords', phishing en spam verspreiden ook gemeten en meegenomen in de analyses. Phishing wordt bijvoorbeeld door McGuire omschreven als cyber-dependent en als cyber-enabled (McGuire & Dowling, 2013). Phishing lijkt mij zelf typisch een moderne versie van fraude en dus een cyber-enabled misdrijf.

Daarnaast kunnen verschillende typen cybercrime het best worden beschreven als 'crime scripts', die bestaan uit een aantal stappen. Dit staat ook op pagina 113 beschreven: 'for hacking and related crimes, you first have to hack into a system to steal data from it' en 'before you intercept communication you need to take control over an IT-system'. Deze misdrijven zijn als aparte misdrijven gecodeerd door de auteur, maar behoren vaak tot dezelfde 'crime scripts'. Daarom is tegenwoordig de vraag eerder: welke rol heeft ICT gespeeld, ergens in het crime script? De rol van cyber in criminaliteit kan dan als een dimensie worden opgevat, van 'geen rol' naar 'maximaal' met vele gradaties ertussen. Deze dimensionale aanpak

staat dichter bij de realiteit van wat verdachten in de praktijk allemaal uitvoeren (Jardine, 2015; Montoya e.a., 2013).
Weulen Kranenbarg heeft een belangwekkende studie uitgevoerd naar een nieuw onderwerp. De hoofdconclusie – een geluk voor onze discipline – is dat veel (doch niet alle) van de bevindingen en modellen voor de traditionele criminaliteit ook gelden voor de cyber-dependent criminaliteit. Vanzelfsprekend zijn sommige routine activities verschillend, maar dat toont aan dat deze benadering flexibel is en de veranderingen die zich voordoen, zijn geïncorporeerd in haar principes.

Literatuur

Akers, R.L. (1990). Rational choice, deterrence, and social learning theory in criminology: the path not taken. *The Journal of Criminal Law and Criminology, 81*(3), 653-676.

Akers, R.L. (1996). Is differential association/social learning cultural deviance theory? *Criminology, 34*, 229-248.

Bayoumy, Y. (2018). *Cybercrime Economy-A Netnographic Study on the Dark Net Ecosystem for Ransomware*. Norwegian University of Science and Technology, Department of Computer Science,

Broek, T.C. van den, Weijters, G. & Laan, A.M. van der (2014). *Antisociaal gedrag van jongeren online* (Fact sheets 2014-01). Den Haag: WODC. Gevonden op www.wodc.nl/onderzoeksdatabase/2189a-antisociaal-gedrag-van-jongeren-online.aspx.

Domenie, M.M.L., Leukfeldt, E.R., Toutenhoofd-Visser, M.H. & Stol, W.P. (2009). *Werkaanbod cybercriminaliteit bij de politie. Een verkennend onderzoek naar de omvang van het geregistreerde werkaanbod cyber criminaliteit* .

Jardine, E. (2015). A continuum of internet-based crime: how the effectiveness of cybersecurity policies varies across cybercriminality types. In: F.X. Olleros & M. Zhegu (eds.). *Research handbook on digital transformations*. Northampton, MA: Edward Elgar.

Jennings, W.G., Piquero, A.R. & Reingle, J.M. (2012). On the overlap between victimization and offending: a review of the literature. *Aggression and Violent Behavior, 17*(1), 16-26. doi:http://dx.doi.org/10.1016/j.avb.2011.09.003.

McGuire, M. & Dowling, S. (2013). *Cyber crime: a review of the evidence*. Retrieved from www.gov.uk/government/publications/crime-against-businesses-headline-findings-from-the-2012-commercial-victimisation-survey--2/crime-against-businesses-headline-findings-from-the-2012-commercial-victimisation-survey.

Montoya, L., Junger, M. & Hartel, P. (2013). How 'digital' is traditional crime? *European Intelligence and Security Informatics Conference (EISIC) 2013* , 31-37. Retrieved from http://ieeexplore.ieee.org/search/searchresult.jsp?newsearch=true&queryText=how+digital+is+traditional+crime%2C+montoya&x=-1280&y=-331.

Sutherland, E.H. & Cressey, D.R. (1974). *Criminology*. Philadelphia: J.B. Lippincott Company.

Tcherni-Buzzeo, M., Davis, A., Lopes, G., & Lizotte, A. (2016). The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave? *Justice Quarterly, 33*(5), 890-911. doi:10.1080/07418825.2014.994658

Verizon Risk Team. (2018). *2018 data breach investigations report. 11th edition*. Retrieved from www.verizonenterprise.com/DBIR/2013/.