1 Inleiding

Wytske van der Wagen, Jan-Jaap Oerlemans & Marleen Weulen Kranenbarg*

1.1 Cybercriminaliteit als nieuw terrein voor de criminologie

Criminaliteitsstatistieken laten een steeds completer beeld zien van cybercriminaliteit in Nederland. Uit diverse rapporten die in dit boek naar voren komen van onder andere het Centraal Bureau voor de Statistiek (CBS), het Wetenschappelijk Onderzoek- en Datacentrum (WODC) van het ministerie van Justitie en Veiligheid en het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR), blijkt dat cybercriminaliteit inmiddels relatief vaak voorkomt.

Dit boek geeft een overzicht van criminologisch onderzoek en relevante juridische aspecten van cybercriminaliteit ten behoeve van wetenschappelijk onderwijs en de professionele praktijk. Daarbij is het van belang om zich te realiseren dat criminologisch onderzoek naar cybercriminaliteit pas de laatste jaren echt goed op stoom komt en nog sterk in ontwikkeling is. Hoewel er al publicaties zijn uit de jaren negentig, zien we de laatste jaren een sterke toename van kwalitatief en kwantitatief onderzoek op dit gebied. Er is niet alleen sprake van een toename in de hoeveelheid onderzoek, maar ook in de kwaliteit ervan. Steeds meer onderzoeken maken gebruik van statistisch sterke onderzoeksmethoden, grotere en relevantere onderzoekspopulaties, vernieuwende (online) onderzoeksmethoden, diepgaander kwalitatief onderzoek en data- of methodentriangulatie. Ook op theoretisch gebied zien we dat nieuwe concepten worden geïntroduceerd en toegepast. Daarnaast zien we dat de verwevenheid tussen het online en offline leven ervoor zorgt dat er steeds meer gebieden zijn binnen de criminologie waar digitalisering een rol gaat spelen, ook buiten het onderzoek specifiek naar cybercriminaliteit.

* Dr. W. van der Wagen is als criminoloog gespecialiseerd in cybercriminaliteit. Prof. mr. dr. J.J. Oerlemans is werkzaam als universitair docent Strafrecht bij het Instituut voor Strafrecht & Criminologie van de Universiteit Leiden. Daarnaast is hij bijzonder hoogleraar Inlichtingen en Recht bij de Universiteit Utrecht. Dr. M. Weulen Kranenbarg is werkzaam als universitair docent Criminologie bij de afdeling Criminologie van de Vrije Universiteit (VU) Amsterdam.

Cybercriminaliteit als criminaliteitsdomein ontwikkelt zich snel en daarom is het uitdagend en fascinerend om hier onderzoek naar te doen. Ook is enige kennis van en inzicht in ICT vereist om de materie te doorgronden. Dit boek geeft op een heldere wijze – en aan de hand van concrete voorbeelden – deze technische kennis mee in de beschrijving van de ontwikkeling van het internet en cybercriminaliteit in hoofdstuk 2, bij de uitleg van de verschijningsvormen van cybercriminaliteit en gedigitaliseerde criminaliteit in hoofdstuk 3 en 4 en bij de bespreking van de uitdagingen in opsporingsonderzoeken naar cybercriminaliteit in hoofdstuk 9.

In het nu volgende worden allereerst de aangehouden definitie en nadere categorisering van cybercriminaliteit toegelicht in paragraaf 1.2. Paragraaf 1.3 geeft vervolgens de doelstellingen van het studieboek weer en paragraaf 1.4 biedt een korte weergave van de opbouw van het boek.

1.2 Wat is cybercriminaliteit?

1.2.1 Terminologie

Hoewel 'cybercriminaliteit' (ofwel *cybercrime*) tegenwoordig de meest gebruikte term is als we het hebben over digitale of online vormen van criminaliteit, zijn er door de tijd heen ook diverse andere termen de revue gepasseerd. Gedacht kan worden aan *netcrime* (Mann & Sutton, 1998), *Internet crime* (Burden & Palmer, 2003; Jewkes & Yar, 2010; Jaishankar, 2011), *hypercrime* (McGuire, 2008), *virtual criminality* (Capeller, 2001; Grabosky, 2001), *high-tech crime* (Van der Hulst & Neve, 2008), *computer crime* (Casey, 2011) en *technocrime* (Steinmetz, 2015a; Steinmetz & Nobles, 2017). In Nederland zien we dat ook steeds vaker de overkoepelende term 'online criminaliteit' wordt gebruikt, bijvoorbeeld door organisaties als het CBS en het WODC en soms ook door wetenschappers. In dit boek hanteren wij de term 'cybercriminaliteit' – als Nederlandse benaming van cybercrime – omdat deze het meest gangbaar is. We hanteren het als overkoepelende term waar alle cyber-gerelateerde vormen van criminaliteit onder vallen.

1.2.2 Definiëring

Het feit dat er een breed scala aan delicten onder cybercriminaliteit valt, maakt het een lastig te definiëren fenomeen. Veel definities zijn dan ook vrij breed en benadrukken vooral de rol van ICT bij het plegen van deze delicten.

Yar (2013) geeft bijvoorbeeld de volgende definitie: 'A range of illicit activities whose "common denominator" is the central role played by networks of ICT in their commission' (p. 9). Gordon en Ford (2006) spreken van: 'Any crime that is facilitated or committed using a computer, network, or hardware device' (p. 14). De definitie van Thomas en Loader (2000) lijkt hier sterk op, maar daarbij worden ook niet gecriminaliseerde activiteiten onder de definitie geschaard: 'Computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks' (p. 3). In dit boek focussen we ons voornamelijk op *strafbaar* gesteld gedrag en willen we de rol van ICT bij deze delicten benadrukken. Daarom hanteren wij in dit boek de volgende definitie, die gebaseerd is op bovenstaande definitie van Yar (2013):

> 'Cybercriminaliteit omvat alle strafbare gedragingen waarbij ICT-systemen van wezenlijk belang zijn in de uitvoering van het delict.'

1.2.3 Classificering

Binnen de definities worden vaak weer classificaties gehanteerd waarbij verschillende delicten worden ingedeeld in categorieën (Van der Wagen, 2018a). Een veelgebruikte classificatie van cybercriminaliteit is het onderscheid tussen cybercriminaliteit in *enge zin* en cybercriminaliteit in *ruime zin*. Eerstgenoemde verwijst naar nieuwe delicten die in het verleden nog niet bestonden en waarbij ICT zowel het doelwit als het middel is (denk aan hacken, ddos-aanvallen en het verspreiden van een computervirus). Laatstgenoemde verwijst naar traditionele delicten die door middel van ICT worden gepleegd en waarbij ICT van wezenlijk belang is in de uitvoering van het delict (denk aan cyberstalking, *grooming* en internetoplichting). Tegenwoordig wordt (ook door organisaties zoals de politie) in plaats van *ruime zin* vaak gesproken van *gedigitaliseerde criminaliteit*. In dit boek spreken wij ook van 'gedigitaliseerde criminaliteit'. Gezien de steeds sterkere verwevenheid van de online en offline wereld is het van belang om te benadrukken dat technologie bij heel veel delicten een rol speelt, onder andere in de communicatie tussen daders. Vandaar dat als eis om te spreken over 'gedigitaliseerde criminaliteit' het gebruik van ICT van wezenlijk belang moet zijn. Dit betekent dat het delict er echt wezenlijk anders uit zou zien als er geen ICT-systeem gebruikt zou worden. In paragraaf 2.3 bespreken we een aantal verschillende manieren waarop ICT-systemen criminaliteit wezenlijk hebben veranderd.

De tweedeling tussen enge en ruime zin wordt ook vaak in buitenlandse studies gehanteerd. Daarin spreekt men dan van *computer-focused* versus *computer-enabled* crime (Furnell, 2002) of *cyber-focused* (of *cyber-dependent*) versus *cyber-enabled* crime (McGuire & Dowling, 2013a; 2013b). De tweedeling is, zoals zichtbaar, vooral gebaseerd op het doelwit (wel of niet ICT). De tweedeling kan echter ook worden beschouwd als een continuüm van criminaliteit die heel technisch van aard is aan de ene kant, en criminaliteit die in de basis nog heel mens-gerelateerd is aan de andere kant (Gordon & Ford, 2006). Daarnaast kan een dader ook een combinatie van cyberdelicten in enge zin en gedigitaliseerde delicten plegen (ook wel een 'keten van delicten' genoemd), bijvoorbeeld wanneer naaktfoto's worden gestolen door middel van hacking om deze vervolgens te gebruiken bij digitale afpersing.

Hoewel bovenstaande classificatie centraal staat in dit boek, is het belangrijk om ook een aantal andere veel gebruikte classificaties te bespreken waarin drie of meer groepen delicten worden onderscheiden. Koops en Kaspersen (2019) hanteren bijvoorbeeld een driedeling waarin de computer wordt beschouwd als object, instrument of omgeving voor criminaliteit, een indeling die terug te voeren is naar het werk van Parker (1973). Bij de computer als *object* richt de dader zich op het beïnvloeden of aantasten van de opgeslagen gegevens in computers, waaronder programma's. Bij de computer als *instrument* zet de dader een computersysteem naar zijn hand om een (traditioneel) feit te kunnen plegen. Bij de computer als *omgeving* van de strafbare gedraging is het computersysteem onderdeel van een bredere omgeving waarbinnen het strafbare feit wordt gepleegd en heeft het mogelijk een rol in de bewijsvoering.

Een andere classificatie die vooral in het verleden veel gebruikt is in de criminologie, is die van Wall (2007a). Hij beschrijft drie opeenvolgende generaties van cybercriminaliteit, gebaseerd op de mate waarin het delict nieuw of afwijkend is ten opzichte van traditionele criminaliteit. De eerste generatie betreft misdaden waarbij de computer wordt gebruikt om traditionele misdaden te plegen. Deze misdaden zijn in feite 'oud', maar vinden plaats met nieuwe technologieën (zoals cyberstalking, haatmisdrijven en (kleinschalige) cyberfraude). De tweede generatie omvat traditionele vormen van criminaliteit, die door digitalisering een globaler of mondialer karakter hebben gekregen. Ze zijn oud als het gaat om het basisdelict zelf, maar nieuw wat betreft de gebruikte instrumenten en hun reikwijdte. Voorbeelden zijn grootschalige fraude of oplichting waarbij meerdere slachtoffers tegelijkertijd het doelwit zijn, of de grote schaal waarop materiaal van seksueel kindermisbruik kan

worden verspreid over de hele wereld. In deze misdaden fungeert technologie als een *force multiplier*, een begrip dat verwijst naar het principe dat één persoon op grote schaal een misdaad kan plegen (Wall, 2007a; Yar, 2005a, zie ook paragraaf 2.3.2). De derde generatie wijst op de zogenoemde 'echte' cybercriminaliteit, misdaden die volledig worden gegenereerd door netwerktechnologie. Ze hebben een gedistribueerd en geautomatiseerd karakter, zijn niet beperkt door tijd en ruimte en zouden volledig verdwijnen als het internet ophoudt te bestaan. Bij deze misdaden is technologie niet alleen een force multiplier, maar ook het doelwit van de misdaden net als bij cybercriminaliteit in enge zin zoals hierboven besproken. Wall includeert ook misdaden in deze generatie die volledig plaatsvinden in virtuele werelden, zoals cyberverkrachting of cyberdiefstal (zie verder paragraaf 2.2.6). De classificatie van Wall (2007a) legt dus meer de nadruk op hoe technologische ontwikkelingen invloed hebben gehad op de verschillende verschijningsvormen van cybercriminaliteit (zie hoofdstuk 2 voor een overzicht van hoe technologie en cybercriminaliteit zich globaal door de tijd heen hebben ontwikkeld).

Voor een gedetailleerde inventarisatie van alle definities, typologieën en taxonomieën die in de literatuur worden gebruikt verwijzen we naar het onderzoek van Phillips et al. (2022).

1.3 Doelstelling van het boek

De kennis over cybercriminaliteit in Nederland is de laatste jaren enorm toegenomen. In de afgelopen tien jaar zijn verscheidene promotieonderzoeken over cybercriminaliteit verschenen, zijn enkele monitors voor cybercriminaliteit opgestart door het CBS en het WODC en is het ministerie van Justitie en Veiligheid zich intensiever gaan bezighouden met de bestrijding van cybercriminaliteit. Ook de politie heeft de bestrijding van cybercriminaliteit (inclusief verstoring en preventie) geïntensiveerd en financiert ook steeds meer wetenschappelijk onderzoek op dit gebied, bijvoorbeeld via het programma Politie en Wetenschap. Hoewel Nederland, samen met een aantal andere landen, een belangrijke positie inneemt in het veld van cybercriminologisch onderzoek, is er inmiddels ook in het buitenland veel onderzoek naar cybercriminaliteit gedaan. Al deze activiteiten resulteerden in talloze wetenschappelijke artikelen, boeken en andere publicaties over cybercriminaliteit. Ook is er op zowel Nederlandse conferenties zoals het Nederlandse Vereniging voor Criminologie Congres (NVC) als op buitenlandse conferenties zoals de European Society of Criminology Conference (ESC) steeds meer aandacht voor