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 Documentatiecentrum (WODC) van het ministerie van Justitie en Veiligheid en het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR), blijkt dat cybercriminaliteit in opkomst is en 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 sinds een aantal jaren echt volop 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 meer relevante onderzoekspopulaties, vernieuwende onderzoeksmethoden en data- of methodentriangulatie. Ook op theoretisch gebied zien we dat nieuwe concepten worden geïntroduceerd en toegepast.

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

* Dr. W. van der Wagen is werkzaam als universitair docent bij de sectie Criminologie van de Erasmus Universiteit Rotterdam (Erasmus School of Law). Prof. mr. dr. J.J. Oerlemans is bijzonder hoogleraar Inlichtingen en Recht bij de Universiteit Utrecht. Hij is verbonden aan het Willem Pompe Instituut voor Strafrechtswetenschappen en het Montaigne Centrum voor Rechtsstaat en Rechtspleging. Dr. M. Weulen Kranenbarg is werkzaam als universitair docent Criminologie bij de afdeling Criminologie van de Vrije Universiteit Amsterdam.

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 in hoofdstuk 3, en bij de bespreking van de uitdagingen in opsporingsonderzoeken naar cybercriminaliteit in hoofdstuk 7.

Voordat de opbouw van de rest van het boek wordt besproken, worden de aangehouden definitie en nadere categorisering van cybercriminaliteit toegelicht in paragraaf 1.2. Paragraaf 1.3 geeft 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]

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 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.

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

1 Deze paragraaf is deels gebaseerd op hoofdstuk 1 van het proefschrift van de eerste auteur (Van der Wagen, 2018a).

geschaard. Deze definitie luidt: 'Computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks' (p. 3). Deze definities zijn allemaal vrij breed en algemeen. 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.

Classificering

Binnen de definities worden vaak weer classificaties gehanteerd waarbij verschillende delicten worden ingedeeld. 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'.

De tweedeling tussen enge en ruime zin wordt ook vaak in buitenlandse studies gehanteerd. Daar 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, 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 vaak gebruikte classificaties te bespreken waarin

drie of meer groepen delicten worden onderscheiden. Koops en Kaspersen (2019) hanteren 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 (2007). 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 nu een globaler of mondialer karakter hebben. 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 en makkelijke schaal waarop kinderpornografie kan worden verspreid over de hele wereld. In deze misdaden fungeert technologie als een *force multiplier*, wat verwijst naar het principe dat één persoon op grote schaal een misdaad kan plegen (Wall, 2007; Yar, 2005a, zie ook paragraaf 2.3.2). De derde generatie wijst op de zogenaamde '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 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 (2007) 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).

1.3 Doelstelling van het boek

De kennis over cybercriminaliteit in Nederland is de laatste jaren enorm toegenomen, maar is nog wel gefragmenteerd. In de afgelopen vijf jaar zijn enkele promotieonderzoeken over cybercriminaliteit verschenen, zijn de eerste 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 geïntensiveerd en financiert ook steeds meer wetenschappelijk onderzoek op dit gebied, bijvoorbeeld via het programma Politie en Wetenschap. Ook in het buitenland startte het onderzoek naar cybercriminaliteit op. 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 cybercriminaliteit. Dat is zichtbaar in de hoeveelheid presentaties en sessies die georganiseerd wordt. Daaruit zijn ook diverse internationale netwerken van onderzoekers voortgekomen zoals de 'Annual Conference on the Human Factor in Cybercrime',[2] die gestart is in 2018 (met jaarlijks ook een conferentie), het 'International Interdisciplinary Research Consortium on Cybercrime'[3] en de 'Working Group on Cybercrime' van de 'European Society of Criminology'.[4] Tot slot is er een niet-aflatende stroom aan nieuwsberichten en rapporten van cybersecuritybedrijven die ons voortdurend herinneren aan de impact die cybercriminaliteit op onze maatschappij heeft.

Bij de Erasmus Universiteit Rotterdam, de Vrije Universiteit Amsterdam en de Universiteit Leiden worden sinds een aantal jaren diverse colleges verzorgd over cybercriminaliteit bij bestaande vakken en/of aparte vakken verzorgd over cybercriminaliteit. Wij stelden vast dat we in dit onderwijs gebruikmaakten van deels dezelfde Nederlandstalige en Engelstalige artikelen en rapporten, maar dat een overzicht van dit materiaal in de Nederlandse taal ontbrak. Om deze reden hebben wij onze krachten gebundeld en is dit studie-

2 Zie www.rechten.vu.nl/conferencecybercrime.
3 Zie https://cj.msu.edu/iircc/iircc.html.
4 Zie www.cybercrimeworkingroup.com.

boek tot stand gekomen, waarin de bestaande kennis over cybercriminaliteit op een overzichtelijke wijze wordt samengebracht.

Onze verwachting is dat met het bestuderen van dit boek de noodzakelijke basiskennis over cybercriminaliteit wordt verschaft. Wij zijn ons ervan bewust dat niet álle verschijningsvormen, strafbaarstellingen en beschikbare studies over cybercriminaliteit worden genoemd. Als auteurs en redacteuren hebben wij daarin keuzes gemaakt in wat ons betreft het meest belangrijk is, op basis van de jarenlange ervaring die wij hebben bij het onderzoek doen naar cybercriminaliteit. Door het noemen van enkele discussievragen bij de afsluiting van de hoofdstukken geven wij aan wat geschikte onderwerpen zijn om met elkaar over van gedachten te wisselen en welke onderwerpen mogelijk interessant zijn voor nader onderzoek. Ook wordt aan het einde van elk hoofdstuk een overzicht gegeven van de belangrijkste kernbegrippen die aan bod zijn gekomen. Het is de bedoeling dat docenten zelf materiaal meegeven voor een eventuele verdieping op onderdelen uit het boek. Door de snelle ontwikkelingen op het gebied van cybercriminaliteit is het van belang dat docenten alert zijn op verouderde feiten, nieuwe studies en nieuwe strafbare feiten of normering van digitale opsporingsmethoden. Ook studenten kunnen hierin een actieve rol spelen, door zich bij ieder hoofdstuk af te vragen hoe de besproken stof is toe te passen op recente technologische ontwikkelingen.

Ten slotte bespreken wij relatief uitvoerig de voor- en nadelen van verschillende methoden (hoofdstuk 2) bij het doen van onderzoek naar cybercriminaliteit, zodat studenten en toekomstige onderzoekers hier rekening mee kunnen houden bij het uitvoeren van wetenschappelijk onderzoek en bij het interpreteren van de resultaten in cybercriminologisch onderzoek. Wij zijn ervan overtuigd dat de onophoudelijke digitalisering van de maatschappij en van criminaliteit nu en in de toekomst vraagt om nog veel meer onderzoek naar cybercriminaliteit en een continue ontwikkeling van de daarbij gebruikte methoden en theorieën. Wij hopen de lezer van dit boek te laten zien hoe fascinerend cybercriminaliteit is en de benodigde basiskennis bij te brengen die criminologen anno 2020 nodig hebben over dit fenomeen.

1.4 Opbouw van het boek

Dit studieboek is als volgt opgebouwd. Hoofdstuk 2 biedt een overzicht van de historische ontwikkelingen van cybercriminaliteit, ontwikkelingen binnen de cybercriminologie en een theoretisch en methodologisch perspectief op cyber-

criminaliteit. Hoofdstuk 3 biedt een overzicht van de verschillende verschijningsvormen en de belangrijkste strafbaarstellingen bij cybercriminaliteit. In hoofdstuk 4 worden ontwikkelingen, kenmerken en factoren besproken die een rol spelen bij daderschap. Hoofdstuk 5 gaat in op de ontwikkeling van slachtofferschap en de factoren die daarmee samenhangen. Hoofdstuk 6 gaat in op de mate waarin bestaande criminologische theorieën kunnen worden toegepast op cybercriminaliteit en bespreekt nieuwe (cyber)criminologische concepten. Het is daarmee ook het theoretisch criminologisch perspectief dat nodig is om de informatie uit hoofdstuk 4 en 5 te verklaren en ook in de toekomst te kunnen toepassen op nieuwe ontwikkelingen. Hoofdstuk 7 gaat over het opsporingsproces in cyberzaken, waarbij veel aandacht is voor de normering van de gebruikte opsporingsmethoden. Het boek sluit in hoofdstuk 8 af met een bespreking van interventies gericht op daders van cybercriminaliteit.

Bij het lezen van het boek is het tot slot belangrijk om rekening te houden met het feit dat de meeste hoofdstukken zich zowel richten op cybercriminaliteit in enge zin als op gedigitaliseerde criminaliteit (hoofdstuk 2, 3, 5, 6 en 7), maar dat ook enkele hoofdstukken vooral toegespitst zijn op cybercriminaliteit in enge zin (hoofdstuk 4 en 8).