DD 2019/28

Criminologie

Datum 18-04-2019

Datum
18-04-2019

Folio weergave
Download gedrukte versie (PDF)

JCDI
JCDI:ADS48487:1

Vakgebied(en)
Strafrecht algemeen (V)

Cybercrime: een complex en uitdagend fenomeen

Vijf jaar geleden wijdden Huisman, Weerman en De Keijser deze rubriek aan het thema ‘Criminaliteit in cyberspace’. Zij constateerden dat de criminologische aandacht voor cybercrime eerder was achtergebleven, maar in 2014 goed op stoom begon te komen. De afgelopen vijf jaar is de aandacht voor cybercrime verder gegroeid. In deze rubriek zullen we ingaan op de huidige stand van zaken op het gebied van criminologisch onderzoek naar cybercrime. We zullen daarbij ingaan op wat er op dit moment bekend is over de aard en omvang van cybercrime in Nederland, daders van cybercrime en de aanpak van cybercrime.

Aard en omvang van cybercrime

Hoewel een eenduidige definitie van cybercrime ontbreekt, wordt met cybercrime in het algemeen gedoeld op de criminele activiteiten waarbij een centrale rol wordt gespeeld door (netwerken van) informatie- en communicatietechnologie (ICT) (o.a. Yar & Steinmetz 2019, p. 35). In de literatuur wordt gebruikelijk een indeling gemaakt op basis van welke rol ICT speelt bij deze vorm van criminaliteit (o.a. Yar & Steinmetz 2019, p. 36 e.v.; Clough 2015, p. 9 e.v.; Wall, 2005/15). Drie categorieën kunnen worden onderscheiden. De eerste categorie, waarbij ICT slechts een hulpmiddel is bij de (voorbereiding op de) criminele handeling, is *‘cyber-assisted’* (Wall, 2005/15) of *‘computer-supported’* criminaliteit (Clough, 2015). De vormen van criminaliteit die in te delen zijn in deze categorie zouden (waarschijnlijk) nog steeds bestaan (in de offlinewereld) zonder ICT (als hulpmiddel). Wall noemt dit de ‘transformatietest’. Bij de tweede categorie, ‘*cyber-enabled*’ criminaliteit, geldt ook dat als de ICT wegvalt, de vorm van criminaliteit nog steeds blijft bestaan, maar dan op minder grote schaal. Hierbij kan onder andere gedacht worden aan oplichting via het internet of het verspreiden van kinderporno. Ten slotte zou de derde categorie cybercrime, cyberafhankelijke (of ‘*computer-focused*’ (Yar & Steinmetz 2019)), niet hebben bestaan zonder ICT of internet. Het gaat dan bijvoorbeeld om *spamming*, *phishing* en *hacking*. Deze laatste categorie wordt gezien als de ‘echte cybercriminaliteit’.
Cybercrime kan worden gezien als een vorm van veelvoorkomende criminaliteit. Zo gaven meer mensen in de Veiligheidsmonitor in 2017 aan slachtoffer te zijn van hacken (4,9 procent) dan van fietsendiefstal (3,3 procent) (CBS, 2017). In 2012, toen voor het eerst in de Veiligheidsmonitor werd gevraagd naar slachtofferschap van cybercrime, gaf volgens deze monitor 12 procent van de Nederlandse bevolking aan het afgelopen jaar slachtoffer te zijn geweest van cybercrime. In 2017, toen de meest recente monitor verscheen, was dit 11 procent (CBS, 2017). In die veiligheidsmonitor wordt onderscheid gemaakt tussen identiteitsfraude (0,4 procent), koop- en verkoopfraude (3,9 procent), hacken (4,9 procent) en cyberpesten (3,1 procent). Deze cijfers laten zien dat, ten opzichte van 2012, koop- en verkoopfraude significant zijn gestegen, terwijl slachtofferschap van identiteitsfraude en hacken zijn gedaald.
Doordat in de Veiligheidsmonitor sinds 2012 aandacht wordt besteed aan slachtofferschap van cybercrime ontstaat iets meer zicht op de omvang van cybercrime. Echter, het daadwerkelijk vaststellen daarvan blijft ontzettend lastig. Het probleem van het *dark number* lijkt nog groter te zijn dan bij andere typen criminaliteit. De bestaande registratiegegevens van politie en justitie geven onvoldoende beeld van de omvang van cybercrime. Dit wordt nog eens versterkt door een lage aangiftebereidheid ten aanzien van cybercrime. Wat hierbij ook een rol lijkt te spelen, is dat burgers vaak niet weten dat ze slachtoffer zijn. Daar komt bij dat daderschap op basis van zelfrapportageonderzoek wijst op een veel grotere omvang van cybercrime dan schattingen op basis van politieregistraties (Leukfeldt & Weulen Kranenbarg, 2017). De voorgaande omstandigheden maken dat een groot deel van de cybercrime onbekend blijft en een goed beeld van de aard en omvang van cybercrime ontbreekt.

Georganiseerde cybercrime

De afgelopen jaren is er in toenemende mate wetenschappelijke aandacht voor meer georganiseerde vormen van cybercrime. Een van de vragen die daarbij centraal staat is in hoeverre deze vormen van cybercrime aangemerkt kunnen worden als georganiseerde criminaliteit (Leukfeldt, Lavorgna & Kleemans 2017, p. 288-289). De analyse van Leukfeldt e.a. (2017), op basis van een analyse van 40 opsporingsonderzoeken uit Nederland, Duitsland, het Verenigd Koninkrijk en de Verenigde Staten over criminele netwerken die zich bezighielden met financiële cybercrimes gericht op de bancaire sector – waaronder phishing en aanvallen met zogenaamde 'malware' (malicious software) – geeft hier geen eenduidig antwoord op. Dit is in eerste instantie vooral te wijten aan het feit dat georganiseerde criminaliteit een zogenaamd paraplubegrip is waar verschillende (wetenschappelijke) invullingen aan worden gegeven.
Als gekeken wordt naar de structuur en samenstelling van de door Leukfeldt e.a. (2017) bestudeerde cybercriminele netwerken, dan voldoen ze aan de gangbare, maar doorgaans bredere criminologische definities van georganiseerde criminaliteit. Over de mate van ernst van de criminele activiteiten, een tweede definitie van georganiseerde criminaliteit en af te leiden uit de minimum strafmaat voor cybercrimes, bestaat in de landen waar de door Leukfeldt e.a. (2017) bestudeerde onderzoeken hebben gedraaid, geen overeenstemming. Ook de laatste invulling van georganiseerde criminaliteit, waarin werd gekeken of er in het geval van cybercrime wel gesproken kan worden over het uitoefenen van controle over bepaalde lokaliteiten en sectoren, levert geen eenduidig beeld op. In sommige gevallen lijkt hiervan ook online sprake, bijvoorbeeld wanneer criminele netwerken proberen om de productie en distributie van goederen en diensten te controleren en te reguleren via online forums. Over het algemeen komen de auteurs echter tot de conclusie dat de operationalisering van 'organised crime as power' in het digitale domein niet opgaat, onder andere omdat er in het geval van de forums 'no system of enforcement, no opposition against competitors, and no control over distribution' is (Leukfeldt e.a. 2017, p. 296).
De relatie tussen cybercrime en georganiseerde criminaliteit wordt eveneens behandeld in het onderzoek van Odinot, De Poot en Verhoeven (2018) naar de aard en aanpak van georganiseerde cybercrime en de vijfde ronde van de Monitor Georganiseerde Criminaliteit (Kruisbergen, Leukfeldt, Kleemans & Roks, 2018). In die laatste studie stond de vraag centraal op welke manieren de georganiseerde criminaliteit in Nederland gebruik maakt van technologische ontwikkelingen. Daartoe werden 30 opsporingsonderzoeken bestudeerd: 23 die gekarakteriseerd kunnen worden als 'traditionele' vormen van georganiseerde criminaliteit, drie traditionele zaken waarin sprake was van een innovatieve ICT-component in de uitvoering of organisatie van criminele activiteiten en vier cybercrime zaken. Op basis van een analyse van deze zaken constateren de auteurs dat er in sommige gevallen sprake is van wezenlijke veranderingen in het criminele bedrijfsproces als gevolg van technologische ontwikkelingen. Hierbij valt te denken aan een criminele organisatie die zich bezighield met de invoer van verdovende middelen via de haven en de diensten van een ICT-specialist inschakelde om het systeem van een containerterminal te hacken, om zo de verdovende middelen ongezien van het haventerrein te kunnen halen. Odinot e.a. (2018) onderzochten een vergelijkbare casus waarin drugshandelaren een ICT-specialist inschakelden om een website te maken waarmee op het *darknet* drugs verkocht konden worden.
Daarnaast illustreren de studies van Kruisbergen e.a. (2018) en Odinot e.a. (2018) dat de manier van samenwerken tussen daders verandert als gevolg van technologische mogelijkheden. In plaats van offline, ontmoeten mensen elkaar op forums en maken ze gebruik van elkaars competenties en contacten om nieuwe criminele activiteiten te ontplooien. Odinot e.a. (2018, p. 16-17) laten daarbij in het bijzonder zien dat samenwerkingsverbanden in sommige gevallen niet langer gebaseerd zijn op sociale relaties, maar op de reputatie of veronderstelde kwaliteiten van personen. Deze vormen van 'thin trust' zijn volgens Odinot e.a. (2018) typerend voor virtuele samenwerkingsverbanden, in het bijzonder als het gaat om expertise die niet beschikbaar zijn in eigen kring.
De voornaamste conclusie van de analyse van Kruisbergen e.a. (2018) is echter dat er in het merendeel van de zaken door daders nog steeds vrij traditioneel te werk wordt gegaan. Zo vormt de fysieke wereld nog steeds de plek waar de meeste contacten tussen daders ontstaan, ook in gevallen waarin daders zich bezighouden met digitale vormen van criminaliteit. Deze lokale inbedding van cybercrime, en het belang van de 'human factor' meer in het algemeen, komt ook tot uitdrukking in het feit dat daders nog steeds elkaar fysiek lijken te willen ontmoeten, ondanks alle mogelijkheden en afscherming die digitale communicatiemiddelen hen bieden. Ten slotte komt het traditionele karakter ook terug in de manieren waarop de daders omgaan met geld. De opkomst van cryptogeld, en andere meer digitale en anonieme manieren van betalen ten spijt, in veel gevallen geldt nog steeds 'cash is king' (Kruisbergen e.a. 2018, p. 71).

Daders cybercrime

Een andere vraag die onlosmakelijk verbonden is met deze relatief nieuwe vorm van criminaliteit is: wie zijn de daders? Wat drijft deze personen, 'volgens het clichébeeld getooid met een hoodie te midden van rondzwevende groene cijfertjes in een donkere ruimte' (Verhagen 2019). Tot voor kort was het nog niet goed mogelijk – in elk geval niet op basis van empirisch onderzoek – om een antwoord op deze vraag te formuleren. Daar is recent verandering in gekomen, met het verschijnen van het proefschrift 'Cyber-offenders versus traditional offenders' van Marleen Weulen Kranenbarg (Vrije Universiteit Amsterdam) en iets eerder het WODC-rapport 'Jeugddelinquentie in een virtuele wereld. Een nieuw type daders of nieuwe mogelijkheden voor traditionele daders?'. Deze onderzoeken geven een interessante beschrijving van en inkijk in het leven

van cyber-daders, alsmede risicofactoren voor dit type criminaliteit.
Eerder (*DD* 2019/6) werd beschreven hoe Weulen Kranenbarg bestudeerde of, en zo ja hoe daders van cyber-afhankelijke delicten (cybercrime in enge zin) verschillen van traditionele delinquenten op verschillende criminologische domeinen, zoals de criminele carrière en motivaties. Zij ontdekte zowel overeenkomsten als verschillen; zo bleek het hebben van werk of het volgen van een opleiding geen effect te hebben op cybercrime, terwijl deze vormen van 'sociaal kapitaal' wel een verlagend effect hebben op traditionele criminaliteit. Anders dan de motivaties zoals gerapporteerd door traditionele delinquenten, bleken de cyber-delinquenten nauwelijks financiële motivaties te benoemen. Intrinsieke motivaties (iets willen leren, nieuwsgierigheid) waren veel belangrijker dan extrinsieke motivaties. Dit is een wezenlijk verschil met motivaties voor traditionele criminaliteit.
Het onderzoek dat in 2017 vanuit het WODC werd uitgevoerd had als doel om 'een beeld te krijgen van de kenmerken van jongeren die in de Monitor Zelfgerapporteerde Jeugdcriminaliteit (MZJ) hebben aangegeven online delicten te plegen'. De vraag die ook speelde, was in hoeverre delinquent gedrag van jongeren zich verplaatst naar de virtuele wereld. De focus in dit onderzoek lag op jongeren van 12 tot en met 22 jaar. De onderzoekers maakten voor het onderzoek gebruik van drie metingen van de MZJ, namelijk 2005, 2010, en 2015. Cybercrime werd vertaald naar 'online delinquentie', waarbinnen verder werd onderscheiden naar gedigitaliseerde delinquentie ('gedigitaliseerde daders') en cyberdelinquentie ('cyberdaders'). De eerste vorm heeft betrekking op traditionele delicten, waarbij nu gebruik wordt gemaakt van ICT. Bij de tweede vorm gaat het om delicten 'waarbij ICT zowel doel als middel is. Hieronder worden delicten als het versturen van virussen en het plegen van DDoS-aanvallen verstaan' (MJZ 2017, p. 5). Deze tweede categorie komt daarmee grofweg overeen met de cyber-afhankelijke delicten die later ook door Weulen Kranenbarg werden bestudeerd. Hoewel de indeling een iets andere precieze omschrijving kent, sluit deze aan bij de in de inleiding genoemde indeling.
De onderzoekers bekeken allereerst verschillen tussen cyberdaders en gedigitaliseerde daders, en maakten daarbij een indeling naar leeftijdscategorieën: 12 tot en met 17-jarigen, en 18 tot en met 22-jarigen. De jonge cyberdaders bleken vaker te gamen, offline delinquentie meer af te keuren, vaker zelf slachtoffer te zijn geweest van cyberdelicten, meer openheid naar hun ouders toe te geven en minder gedigitaliseerde delinquente vrienden te hebben dan gedigitaliseerde daders. In de oudere groep gingen de verschillen deels de andere kant op; in deze groep bleken cyberdaders *minder vaak* te gamen. Daarnaast hadden zij minder offline delinquente vrienden, en ook minder gedigitaliseerde delinquentie vrienden. Met name voor de jongvolwassenen concludeerden de onderzoekers dat de groep cyberdaders een minder risicovol profiel had dan de groep gedigitaliseerde daders (alsmede de daders die aangaven cyber- én gedigitaliseerde delicten te hebben gepleegd). Interessant is ten slotte de vergelijking tussen profielen van jongeren die geen delicten rapporteren, jeugdige online daders, jeugdige offline daders, en daders die zowel online als offline delicten zeggen te plegen. Niet geheel onverwacht blijkt dat jongeren die geen delicten rapporteren het minst risicovolle profiel hebben (veel beschermende factoren, weinig risicofactoren). Kijkend naar de jongste groep online daders (de eerdergenoemde categorieën samengenomen) en offline daders, blijkt er onder online daders minder drugsgebruik voor te komen, en keuren zij offline delinquentie meer af. In de oudere groep blijken online daders een hogere mate van zelfcontrole te hebben dan offline daders. Daarnaast rapporteren zij minder drugsgebruik, slachtofferschap van online delicten, en offline delinquente vrienden.

Aanpak cybercrime

Zoals hierboven al bleek, kent cybercrime vele gezichten. Buiten dat dadergroepen – alsook slachtoffers – aanzienlijk van elkaar verschillen, begeven daders zich in (relatieve) anonimiteit, tussen en over nationale grenzen, en in een zich snel ontwikkelend technologisch veld. Daar komt bij dat opsporings- en handhavende instanties in gevallen afhankelijk kunnen raken van private partijen (en hun infrastructuren) en soms ook de kennis en middelen ontberen om het zich snel ontwikkelende technologische veld bij te benen (Boes & Leukfeldt 2017; Holt 2018). Het aanpakken van cybercrime is dan ook geen sinecure; een *'kill switch'* (Wall 2017, p. 19), ofwel een pasklare oplossing, is er niet op basis van het voorgaande. In de literatuur worden wel verschillende (algemene) strategieën besproken, als uitgangspunt, die aanknopingspunten bieden om voorgenoemde moeilijkheden te benaderen. Hieronder worden er twee besproken: publiek-private samenwerking en het stimuleren van *resilience*.
Het belang van publiek-private samenwerking om tot een aanpak van cybercrime te komen wordt niet enkel in de wetenschappelijke discours herkend. Ook in Tweede Kamerstukken wordt opgeroepen om 'in samenspraak met de private sector te komen tot een integraal plan van aanpak voor cybercrime', waarbij 'het voorkomen van dader- en slachtofferschap, opsporing en vervolging [en] het terugdringen van recidive' het doel zijn (*Kamerstukken II*, 2017/18, 28684, 522, p. 1). Hetgeen Jewkes en Wall reeds in 2008 (p. 582) stelden, lijkt nu dan ook algemeen geaccepteerd:

'[t]he scope, scale, and structure of the internet outstrops the capacity of any single enforcement of regulatory body.'

De voetbal metafoor van Hans Boutellier (2005), toegepast op cybercriminaliteit zoals in Boes en Leukfeldt (2017), vormt een toegankelijke illustratie. Een voetbalteam bestaat doorgaans uit een voorhoede, een middenveld en een verdediging. In Boes en Leukfeldt (2017) bestaat de voorhoede uit de burger, het middenveld uit organisaties die betrokken zijn bij cybersecurity, maar van wie het niet de primaire taak is. De defensie bestaat uit organisaties van wie de primaire taak wel 'de veiligheid' betreft; 'police, prosecutors, or private security companies' (p. 186). Aan de hand van dit model kunnen we denken in acties van 'de linies' als zodanig. Zo kunnen burgers virusscanners en firewalls installeren, zich informeren over

de risico's in het digitale domein en daaraan gekoppeld nadenken over hun online gedragingen. Maar met een spreekwoordelijke voorzet vanuit het middenveld of de defensie is het natuurlijk gemakkelijker 'scoren'. Denk aan beleid op *awareness* campagnes, en 'built in' en/of optionele (betaalbare) beveiliging bij het afnemen van internetdiensten, zoals online winkelen. Boes en Leukfeldt (2017, p. 195) stellen meer algemeen dat 'vertrouwen, kennis, communicatie en het vermogen tot samenwerken' de belangrijkste succes factoren zijn binnen publiek-private samenwerking.
Te constateren valt tegelijk dat een aanzienlijk deel van wetenschappelijke literatuur zich met name richt op 'de defensie' (vaak, de politie), en de (on)mogelijkheden die 'deze spelers' hebben om cybercrime te voorkomen (preventie), op te sporen en te vervolgen. Detectie van cybercrime (zie ook hierboven) vormt daar een eerste, belangrijk probleem. Slechts het topje van de ijsberg wordt bekend bij de politie, zoals hiervoor al uiteengezet. Tegelijkertijd zien we het belang van een integrale aanpak ook hier terug. Nauwe(re) samenwerking en het delen van informatie kan zo bijdragen aan een duidelijker beeld van de problematiek (zie ook Wall 2017). Een gevolg van het voorgaande is uiteraard ook dat maar een zeer beperkt aandeel binnen de strafrechtsketen geraakt. Meer algemeen wordt kennis binnen de organisatie besproken als belangrijk struikelblok (Holt, 2018). Hierop wordt gereageerd door middel van educatie en 'good practice guides' (Boes & Leukfeldt 2017, p. 190), maar ook door het oprichten van speciale cyber eenheden (Holt 2018): 'Het Team High Tech van de Landelijke eenheid van de politie is inmiddels 120 personen sterk. Daarnaast werkt de politie aan de opbouw van cybercrimeteams in de regionale eenheden' (*Kamerstukken II*, 2017/18, 28684, 522 p. 5).
Tegelijkertijd suggereert Wall (2017) dat het oprichten van intelligence/cybereenheden niet afdoende zal zijn. In zijn onderzoek constateert hij dat onder de huidige omstandigheden 'de politie' (te) veel tijd kwijt is aan wat hij 'cyber incivilities' noemt, waardoor de beschikbare capaciteit om zwaardere dreigingen (zie ook hierboven) en/of delicten op te pakken beperkt blijft. Het belang van 'nettiquette' wordt daarbij niet onderkend – te meer omdat deze (zo lijkt) sterk bijdraagt aan een 'cyber reassurance gap' – maar gepleit wordt voor een verandering in aanpak. Een aanpak die zich nader richt op 'wat normaal' is binnen (vooral) de jeugdige doelgroep, en hun gebruik van digitale netwerken en *devices* (zie ook Holt, Brewer & Goldsmith 2018). Wall (2017) suggereert bijvoorbeeld dat een 'tussenpersoon/positie' soelaas zou kunnen bieden met oog op het vergroten van inzicht en een rol als 'gatekeeper':

> 'developing roles like the police school liason officer as key players in the resolution of cybercrime, rather than just developing specialist cybercrime units' (p. 15).

Een andere literatuur richt zich op (cyber) *resilience* (Chmutina, Lizarralde, Dainty & Bosher 2016); een belangrijke vraag die in deze literatuur gesteld wordt is hoe, op het moment dat een (cyber)incident plaatsvindt, een slachtoffer (in deze context, vaak een bedrijf of organisatie) zo goed en snel mogelijk terug kan keren naar de 'normale functie' van voor het cyber incident. Dat er inmiddels behoorlijk geïnvesteerd wordt op het vergroten van de 'veerkracht' is onder andere af te leiden uit verschillende gesubsidieerde projecten gericht op de cyberveiligheid 2019 (CCV 2019). Buiten dat het van belang wordt geacht slachtofferschap te voorkomen, daders op te sporen en te vervolgen, wordt hier dus ook aangespoord 'uit te gaan' van een incident, en na te gaan of en hoe het slachtoffer/organisatie deze (zo goed mogelijk) kan 'doorstaan'.

Tot slot

Geconcludeerd kan worden dat er de afgelopen vijf jaar diverse ontwikkelingen hebben plaatsgevonden op het gebied van cybercrime; zowel in termen van onderzoek als de aanpak van cybercrime. Het voorgaande laat echter ook zien dat er nog genoeg vragen onbeantwoord zijn en dat er ook diverse nieuwe vragen ontstaan. Een eerste vraag is of de juridische kwalificaties van dader nog wel voldoen in het cyberdomein. In het geval van phishing zaken zijn de 'money mules', veelal kwetsbare (jonge)mannen en vrouwen die hun bankpassen- en gegevens ter beschikking stellen aan anderen, naast dader in juridische zin ook slachtoffer (van oplichting) door de ronselpraktijken van daders die buiten beeld blijven van politie en justitie. Daarnaast is er een aantal cyberdaders dat zichzelf niet als dader ziet. Naast de wat beter bekende voorbeelden van mensen die illegaal films of muziek downloaden, kan hierbij in het bijzonder gedacht worden aan (ethische) hackers. De studie van Van der Wagen, Althoff en Van Swaaningen (2016) toont dat deze 'cybercriminelen' hun activiteiten zien als positief voor bedrijven en de samenleving in het algemeen: ze leggen kwetsbaarheden bloot en brengen daarmee niet, of maar in beperkte mate schade aan computersystemen aan. Ten slotte illustreren Van der Wagen en Bernaards (2018) dat technologie in toenemende mate opereert als dader. Het gaat daarmee om 'niet-menselijke entiteiten, zoals computerprogramma's, exploit kits, systemen, servers en beheerpanelen, die een sleutelrol spelen in het criminele proces' (p. 63). Naast de coördinatie en uitvoering, zou technologie ook een rol spelen in het mede vormgeven van het criminele proces.
Met andere woorden; voortzetting van onderzoek is noodzakelijk. Het probleem cybercrime is ingewikkeld en grensoverschrijdend. Niet in de laatste plaats is de aanpak van cybercrime ook een uitdaging door een beperkte kennis van de omvang van cybercrime. Door snelle technologische ontwikkelingen loopt de aanpak (denk hierbij ook aan de wetgeving) vaak achter de feiten aan. Ook is nog weinig bekend over de vraag in hoeverre de speciale eenheden bij de politie die worden ingericht tegen cybercrime deze ontwikkelingen kunnen bijbenen, hoe zij cybercrime proberen tegen te gaan, hoe zij functioneren en welke knelpunten daarbij optreden.
Deze constateringen maken cybercrime een complex en uitdagend fenomeen. Daar komt nog bij dat ICT in ons dagelijks

leven niet meer is weg te denken en we er in steeds grotere mate van afhankelijk zijn. In toenemende mate is bijvoorbeeld onze huishoudelijke apparatuur uitgerust met functies die afhankelijk zijn van het internet en waarbij steeds meer gegevens over ons doen en laten worden verzameld. Deze verwevenheid van ICT met ons dagelijks leven maakt ons kwetsbaar omdat het ons leven plat kan leggen.
De ontwikkeling van cybercrime dient (en zal) in de komende jaren nauwgezet in de gaten te worden gehouden. Aangezien het hier een relatief nieuwe vorm van criminaliteit betreft, kan worden verwacht dat het fenomeen cybercrime er over vijf jaar anders uitziet dan nu. Interessant is daarbij of cybercrime daadwerkelijk een (groter) deel van de offline criminaliteit gaat vervangen, zoals nu regelmatig door experts wordt voorspeld.

R. Salet, *J. Brands*, *E. Rodermond* & *R. Roks*

Literatuur:

Boes & Leukfeldt 2017
S. Boes & E.R. Leukfeldt, 'Fighting cybercrime: A joint effort', in: R.M. Clark & S. Hakim (Eds.) *Cyber-Physical Security,* Cham: Springer 2017: 185-203.

Boutellier 2005
H. Boutellier, *Meer dan veilig. Over bestuur, bescherming en burgerschap.* Den Haag: Boom Juridische Uitgevers 2005.

CBS 2017
CBS, *Veiligheidsmonitor 2017*, Den Haag: Centraal Bureau voor de Statistiek 2017.

CCV 2019
CCV, Projecten Cyberveiligheid 2019, https://hetccv.nl/fileadmin/Bestanden/Onderwerpen/Cybercrime/Projecten_Cyberveiligheid_obv_subsidie_JenV_2019.pdf.

Chmutina, Lizarralde, Dainty & Bosher 2016
K. Chmutina, G. Lizarralde, A. Dainty & L. Bosher, 'Unpacking resilience policy discourse', *Cities58*, 2016, p. 70-79.

Clough 2015
J. Clough, *Principles of Cybercrime*, Cambridge: Cambridge University Press 2015.

Holt, Brewer & Goldsmith 2018
T.J. Holt, R. Brewer & A. Goldsmith, 'Digital drift and the "sense of injustice": Counter-productive policing of youth cybercrime', *Deviant Behavior*, 2018, p. 1-13.

Holt 2018
T.J. Holt, 'Regulating Cybercrime through Law Enforcement and Industry Mechanisms', *The ANNALS of the American Academy of Political and Social Science*, *679*(1), 2018, p. 140-157.

Jewkes & Yar 2008
Y. Jewkes & M. Yar, 'Policing cybercrime in the twenty-first century', in: T. Newburn (red.), *Handbook of policing*, Cullompton, UK: William 2008, p. 280-607.

Kruisbergen, Leukfeldt, Kleemans & Roks 2018
E.W. Kruisbergen, E.R. Leukfeldt, E.R. Kleemans & R.A. Roks, *Georganiseerde criminaliteit en ICT. Vijfde ronde Monitor Georganiseerde Criminaliteit* (Cahier 2018-8), Den Haag: WODC 2018.

Leukfeldt, Lavorgna & Kleemans 2017
E.R. Leukfeldt, A. Lavorgna & E.R. Kleemans, 'Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime', *European Journal on Criminal Policy and Research* 23(3) 2017, p. 287-300.

Leukfeldt & Weulen Kranenbarg 2017
R. Leukfeldt & M. Weulen Kranenbarg, 'De menselijke factor in cybercrime', *Tijdschrift voor Criminologie* (59) 3 2017, p. 282-290.

Odinot, De Poot & Verhoeven 2018
G. Odinot, C. de Poot & M. Verhoeven, 'De aard en aanpak van georganiseerde cybercrime: Bevindingen uit een internationale empirische studie', *Justitiële Verkenningen* (44)5 2018, p. 9-22.

Rokven, Weijters & Van der Laan 2017
J.J. Rokven, G. Weijters & A.M. van der Laan, *Jeugddelinquentie in de virtuele wereld. Een nieuw type daders of nieuwe mogelijkheden voor traditionele daders?*, Den Haag: WODC, 2017.

Verhagen 2019

L. Verhagen, ‘Ook cybercrimineel ontdekt aantrekkelijke kant van kunstmatige intelligentie – hoe zorgwekkend is dat?’, *De Volkskrant*, 11 januari 2019.

Van der Wagen & Bernaards 2018
W. van der Wagen & F. Bernaards, ‘De ‘non-human (f)actor’ in cybercrime: Cybercriminele netwerken beschouwd vanuit het ‘cyborg crime’-perspectief’, *Justitiele Verkenningen* 44(5) 2018, p. 54-67.

Van der Wagen, Althoff & Van Swaaningen 2016
W. van der Wagen, M. Althoff & R. van Swaaningen, ‘De andere ‘anderen’: een exploratieve studie naar processen van othering van, door en tussen hackers’, *Tijdschrift over Cultuur en Criminaliteit* 6(1) 2016, p. 27-41.

Wall 2017
D.S. Wall, Crime, ‘Security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing’, in: R. Brownsword, E. Scotford and K. Yeung (Eds.) *The Oxford Handbook on the Law and Regulation of Technology*, Oxford: Oxford University Press 2017, p. 1075-1096.

Wall 2007
D.S. Wall, *Cybercrime*, Cambridge: Polity Press 2007.

Wall 2005/15
D.S. Wall, ‘The Internet as a Conduit for Criminals’, in: A. Pattavina (red.), *Information Technology and the Criminal Justice System,* Thousand Oaks, CA: Sage 2005/15 (ook beschikbaar via https://ssrn.com/abstract=740626).

Weulen Kranenbarg 2018
M. Weulen Kranenbarg, *Cyber-offenders versus traditional offenders: An empirical comparison* (diss. Amsterdam VU), Amsterdam: Vrije Universiteit 2018.

Yar & Steinmetz 2019
M. Yar & K.F. Steinmetz, *Cybercrime and Society,* Los Angeles: Sage, 2019.