WODC

5 | 18

Justitiële verkenningen

De digitalisering van georganiseerde misdaad

verschijnt 6 maal per jaar • jaargang 44 • oktober

JV

Boom juridisch

5 | 18

Justitiële verkenningen

De digitalisering van georganiseerde misdaad

Verschijnt 6 maal per jaar • jaargang 44 • oktober

Boomjuridisch

Wetenschappelijk Onderzoek- en Documentatiecentrum
Ministerie van Justitie en Veiligheid

Justitiële verkenningen is een gezamenlijke uitgave van het Wetenschappelijk Onderzoek- en Documentatiecentrum van het ministerie van Justitie en Veiligheid en Boom juridisch.

Redactiesecretariaat
tel. 070-370 65 54
e-mail infojv@minvenj.nl

Redactieadres
Ministerie van Justitie en Veiligheid, WODC
Redactie Justitiële verkenningen
Postbus 20301
2500 EH Den Haag
tel. 070-370 71 47
fax 070-370 79 48

WODC-documentatie
Voor inlichtingen: Infodesk WODC, e-mail: wodc-informatiedesk@minvenj.nl, internet: www.wodc.nl

Abonnementen
Justitiële verkenningen verschijnt zes keer per jaar. In digitale vorm is het tijdschrift beschikbaar op de website van het WODC, zie www.wodc.nl/publicaties/justitiele-verkenningen/index.aspx.
De abonnementsprijs bedraagt in 2018 € 164,00 (excl. btw) voor een online abonnement en € 219,00 (excl. btw, incl. verzendkosten) voor papier & online. Met een online abonnement heeft u toegang tot het volledige online archief en ontvangt u een e-mailattendering. Met papier & online ontvangt u tevens de gedrukte exemplaren.
Ga naar www.tijdschriften.boomjuridisch.nl voor meer informatie en om een abonnement af te sluiten. Hebt u vragen over de abonnementen? Neem dan contact op via tijdschriften@boomdistributiecentrum.nl of via 0522-23 75 55.

Abonnementen kunnen op elk gewenst tijdstip ingaan. Valt de aanvang van een abonnement niet samen met het kalenderjaar, dan wordt over het resterende gedeelte van het jaar een evenredig deel van de abonnementsprijs in rekening gebracht. Het abonnement kan alleen schriftelijk tot uiterlijk 1 december van het lopende kalenderjaar worden opgezegd. Bij niet-tijdige opzegging wordt het abonnement automatisch voor een jaar verlengd.

Uitgever
Boom juridisch
Postbus 85576
2508 CG Den Haag
tel. 070-330 70 33
e-mail info@boomjuridisch.nl
website www.boomjuridisch.nl

Ontwerp
Tappan, Den Haag

Coverfoto
Schermfoto van een door de politie gesloten dark market website

ISSN: 0167-5850

Inhoud

Inleiding

Het massale gebruik van internet brengt nieuwe mogelijkheden voor criminaliteit met zich mee. Dankzij internet, en ICT in bredere zin, kunnen daders afgeschermd met elkaar communiceren en kunnen capabele mededaders worden gevonden. Ook kunnen aanbieders en vragers van illegale goederen en diensten 'vanachter hun bureau' met elkaar zakendoen. Bovendien is het bereik aan potentiële slachtoffers voor bijvoorbeeld fraude met betalingsverkeer sterk toegenomen en zijn er nieuwe mogelijkheden voor het witwassen van criminele verdiensten. Deze digitalisering van zware en georganiseerde criminaliteit is het thema van dit nummer van *Justitiële verkenningen*.
De mogelijkheden die ICT daders biedt en vooral de gevaren die onder andere cybercriminaliteit voor de samenleving mee kan brengen, staan volop in de belangstelling. Toch is er nog relatief weinig empirisch onderzoek gedaan naar het gebruik van ICT door dadergroeperingen in de zware en georganiseerde criminaliteit. Dit themanummer biedt inzichten uit empirisch wetenschappelijk onderzoek én opsporingsonderzoek op dit terrein. Digitalisering biedt namelijk niet alleen daders nieuwe kansen en mogelijkheden. Elke modus operandi kent zwakke plekken en elke technologie brengt ook kansen voor politie en justitie met zich mee. Het opsporingsonderzoek tegen *Ennetcom* is hier een treffend voorbeeld van.
Ennetcom was een aanbieder van versleutelde communicatie die volgens het Openbaar Ministerie (OM) veelvuldig werd gebruikt door criminelen. In het opsporingsonderzoek kon een kopie worden gemaakt van de server waarop diensten van Ennetcom draaiden (2016). Daarmee bleek de *Pretty Good Privacy* (PGP) die gebruikers dachten te genieten toch niet zo sterk. Miljoenen versleutelde berichten konden worden ontcijferd, waarmee politie en justitie een ware goudmijn leken te hebben aangeboord.[1] Een ander voorbeeld zien we in het politieoptreden tegen *Hansa*. *Hansa* was een ondergrondse marktplaats, waarop kopers en verkopers van drugs elkaar troffen. In 2017 hield de politie niet alleen de beheerders van deze marktplaats aan, maar nam ook de servers in beslag. Bovendien hielden politie en

1 Zo is ontsleuteld berichtenverkeer via Ennetcom gebruikt in de zaak tegen een verdachte van een liquidatiepoging, die tot achttien jaar is veroordeeld (Rb. Amsterdam 19 april 2018, ECLI:NL:RBAMS:2018:2504).

doi: 10.5553/JV/016758502018044005001

OM de marktplaats voor een bepaalde periode operationeel. Zo zijn grote aantallen transacties én kopers en verkopers in beeld gekomen. In zeven artikelen wordt in dit themanummer zowel ingegaan op de daders en hun werkwijze als op het instrumentarium dat politie en justitie tegen gedigitaliseerde criminaliteit kunnen inzetten.

In het openingsartikel behandelen ***Geralda Odinot, Christianne de Poot*** en ***Maite Verhoeven*** de aard en samenwerkingsstructuur van georganiseerde cybercriminaliteit. Hoe gaan daders te werk? Welke structuur hebben de samenwerkingsverbanden die zich met georganiseerde cybercriminaliteit bezighouden, en hoe werken de daders daarbinnen samen? De auteurs gebruiken data die zijn verzameld in een door de EU gefinancierd onderzoek dat is uitgevoerd in Nederland (door onderzoekers van het WODC), Duitsland (Bundeskriminalamt) en Zweden (Swedish National Council for Crime Prevention). In elk van deze landen hebben wetenschappers opsporingsonderzoeken naar georganiseerde criminaliteit bestudeerd en hebben zij interviews afgenomen.

Elk crimineel bedrijfsproces, of het nu om grootschalige drugshandel gaat of banking malware, bestaat uit verschillende schakels. ***Edwin Kruisbergen, Rutger Leukfeldt, Edward Kleemans*** en ***Robby Roks*** stellen de vraag hoe daders binnen de georganiseerde criminaliteit ICT gebruiken in relatie tot een essentiële schakel binnen ieder 'bedrijfsproces', het regelen van de geldstromen. Ze richten zich daarbij niet uitsluitend op cybercrime, maar kijken juist ook naar hoe daders binnen 'traditionele' georganiseerde criminaliteit de mogelijkheden van ICT gebruiken. In hoeverre maken zij bijvoorbeeld gebruik van een digitale munteenheid als de bitcoin? Uit het door de auteurs bestudeerde casusmateriaal komt het beeld naar voren dat ICT inderdaad tot financiële innovatie heeft geleid, maar dat daders tegelijkertijd nogal eens vertrouwen op de oude zekerheid van contant geld. Digitalisering leidt zo ook tot een nieuwe flessenhals in het criminele bedrijfsproces; hoe wissel je digitale valuta veilig om in contanten?

Vervolgens wordt de aandacht verlegd naar een specifiek delict, kinderporno. De komst van het internet heeft de mogelijkheden voor het bekijken, verspreiden en produceren van kinderpornografisch materiaal sterk uitgebreid. ***Madeleine van der Bruggen*** doet promotieonderzoek naar dit onderwerp. In haar artikel gaat ze aan de hand van een literatuurstudie in op de vraag hoe de digitalisering het criminaliteitsbeeld van kinderporno heeft veranderd. Zij schetst eerst de historische

doi: 10.5553/JV/016758502018044005001

ontwikkeling van kinderporno op papier naar kinderporno in anonieme netwerken op het zogenoemde *darkweb*. Daarna bespreekt ze de gevolgen van het bestaan van dergelijke netwerken voor het criminaliteitsveld van kinderporno. Ze sluit af met aanbevelingen voor wetenschappelijk onderzoek en de opsporingspraktijk.

De digitalisering van criminaliteit leidt tot tal van interessante, zowel empirische als theoretische, onderzoeksvragen. Een zo'n vraag is of ons begrip van criminele actoren nog wel voldoet. Deze vraag is het uitgangspunt van het artikel geschreven door ***Wytske van der Wagen*** en ***Frank Bernaards***. Zij stellen dat met de komst van *botnets* een nieuw type criminele actor is geïntroduceerd. Een botnet is een netwerk van computers die, via kwaadaardige software en buiten medeweten van de eigenlijke gebruikers, onder controle staan van een dader die de *bots* bijvoorbeeld gebruikt voor aanvallen op een website. Een botnet is daarmee een criminele actor die mens noch machine is. Volgens de auteurs voldoet hierdoor de reguliere, mensgerichte criminologische benadering van criminele netwerken niet meer. Zij presenteren daarom een meer hybride perspectief, dat recht doet aan de centrale rol van technologie in cybercriminaliteit.

ICT-toepassingen hebben op verschillende terreinen tot vernieuwing van criminele werkwijzen geleid. Zo zijn er dankzij het internet nieuwe mogelijkheden ontstaan om vraag en aanbod op criminele markten bij elkaar te brengen. Zoals tweedehands fietsen worden verhandeld op bijvoorbeeld Marktplaats op het reguliere internet, zo vinden vraag en aanbod van bijvoorbeeld drugs elkaar op het *darkweb*, een min of meer afgeschermd deel van het internet. ***Thijmen Verburgh, Eefje Smits*** en ***Rolf van Wegberg*** stellen in hun bijdrage de vraag centraal wat de mogelijkheden zijn om onderzoek te doen naar illegale marktplaatsen. Zij beschrijven, mede aan de hand van de *Hansa*-casus, hoe politie-interventies tegen *darkweb markets* (of *dark markets*) een schat aan data kunnen blootleggen en hoe deze data door onderzoekers kunnen worden gebruikt.

Die *Hansa*-casus laat, zoals eerder beschreven, mooi zien dat het internet ook de politie mogelijkheden biedt, bijvoorbeeld om dekmanteloperaties uit te voeren. Dezelfde faciliteiten die het daders mogelijk maken om (in meer of mindere mate) online afgeschermd te opereren, geven opsporingsambtenaren de kans om onder een dekmantel die daders op te sporen.

doi: 10.5553/JV/016758502018044005001

De online toepassing van dekmanteloperaties staat centraal in het artikel van ***Jan-Jaap Oerlemans***. Hij beschrijft hoe de drie undercoverbevoegdheden uit het Wetboek van Strafvordering ook toepassingen in de online omgeving kennen en welke vragen dekmanteloperaties op het internet met zich meebrengen.
Waar Oerlemans ingaat op de toepassing van algemene (opsporings)bevoegdheden op het internet, daar bespreekt ***Bart Custers*** recente wetgeving die specifiek is gemaakt voor de digitale omgeving, de Wet computercriminaliteit III. Deze wet werd in juni 2018 aangenomen door de Eerste Kamer. De auteur schetst in het afsluitende artikel eerst de achtergrond van de cybercrimewetgeving in Nederland, die met de Wet computercriminaliteit (I) in 1993 van start ging. Daarna gaat hij dieper in op de Wet computercriminaliteit III, met name op de nieuwe strafbepalingen en de nieuwe opsporingsbevoegdheden. Wellicht de belangrijkste verandering die de wet introduceert, is de zogenoemde hackbevoegdheid. Opsporingsambtenaren mogen in bepaalde situaties 'inbreken' in computers en netwerken, waarbij ze bijvoorbeeld op afstand camera's en microfoons kunnen aanzetten of toetsaanslagen vastleggen (zogenoemde *keyloggers*). De auteur bespreekt de legitimiteit en noodzakelijkheid van deze bevoegdheid.

Edwin Kruisbergen [*]

* Gastredacteur dr. E.W. Kruisbergen is als onderzoeker verbonden aan het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) van het ministerie van Justitie en Veiligheid.

doi: 10.5553/JV/016758502018044005001

De aard en aanpak van georganiseerde cybercrime

Bevindingen uit een internationale empirische studie

Geralda Odinot, Christianne de Poot en Maite Verhoeven*

Ons dagelijks leven is enorm gedigitaliseerd en verweven met het internet. Deze ontwikkeling biedt allerlei nieuwe mogelijkheden voor het plegen van criminaliteit. Cybercriminaliteit is volgens McAfee[1] een *growth industry*, waar de opbrengsten hoog zijn en de pakkansen laag. De opkomst van cybercriminaliteit en de kans om hier slachtoffer van te worden zijn een zorg voor de samenleving, de rechtshandhaving en het beleid van het ministerie van Justitie en Veiligheid (J&V). Over de aard en de organisatie van deze criminaliteit is nog niet veel informatie beschikbaar, terwijl kennis hierover essentieel is om dit fenomeen aan te kunnen pakken. Wie zijn de daders van deze misdrijven en hoe gaan ze te werk? Hoe kan de politie deze criminaliteit opsporen en op welke manieren kan cybercriminaliteit worden tegengegaan?
Om antwoord te vinden op deze vragen hebben onderzoekers uit Duitsland, Zweden en Nederland de handen ineengeslagen en gezamenlijk onderzoek gedaan naar ernstige vormen van georganiseerde cybercriminaliteit.[2] Ten behoeve van dit onderzoek zijn in deze drie landen dossiers bestudeerd van opsporingsonderzoeken die gericht waren op ernstige vormen van georganiseerde cybercriminaliteit. Bij

* Dr. G. Odinot is wetenschappelijk onderzoeker en trainer forensisch interviewen How2Ask. Ten tijde van de uitvoering van het onderzoek waarop dit artikel is gebaseerd, was zij werkzaam als onderzoeker bij het WODC. Dr. C.J. de Poot is als senioronderzoeker verbonden aan het WODC. Zij is tevens hoogleraar Criminalistiek aan de Vrije Universiteit en lector Forensisch onderzoek aan de Hogeschool van Amsterdam en de Politieacademie. Dr. M.A. Verhoeven is als beleidsmedewerker Rechtshandhaving & Ketensamenwerking Cariben verbonden aan het ministerie van Justitie en Veiligheid. Ten tijde van de uitvoering van het onderzoek waarop dit artikel is gebaseerd, was zij werkzaam als onderzoeker bij het WODC.

1 Zie https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/McAfee%20and%20CSIS%20-%20Econ%20Cybercrime.pdf.

2 Zie voor het hele rapport: BKA, WODC & BRA (2016), *Cyber-OC … Scope and manifestations in selected EU member states* (HOME/2012/ISEC/AG/4000004382). Polizei + Forschung, 50.

doi: 10.5553/JV/016758502018044005002

de selectie van de dossiers is uitgegaan van de definities van georganiseerde misdaad van Europol.[3] Daarin wordt onder andere gesteld dat er sprake is van een crimineel samenwerkingsverband wanneer minimaal twee personen gedurende een langere periode samenwerken met als doel geldelijk gewin of macht. Daarnaast zijn enkele zaken geselecteerd die voldeden aan een van de vier categorieën van cybercrime, zoals omschreven door Wall (2007) en Martin (2013). Deze categorisering maakt een indeling die gebaseerd is op de rol die ICT en computers hebben bij het plegen van het delict.

In totaal werden er ten behoeve van dit onderzoek 44 zaken geselecteerd uit de periode 2009-2014, 18 uit Duitsland, 15 uit Zweden en 11 uit Nederland. Deze hadden betrekking op verschillende vormen van georganiseerde cybercriminaliteit, zoals het verspreiden van malware, hacking, het runnen van botnets, phishing, misbruik van het bankwezen, het (digitaal) witwassen van geld en illegale online handel. Alle geselecteerde zaken zijn bestudeerd met een Engelse vertaling van de checklist, die ontwikkeld is voor de Monitor Georganiseerde Criminaliteit (Kleemans e.a. 1998; Kleemans e.a. 2002; Van de Bunt & Kleemans 2007; Kruisbergen e.a. 2012). Ook zijn diepte-interviews gehouden met experts van politie en justitie,[4] zowel om beter zicht te krijgen op de concrete zaken als om meer algemene informatie te achterhalen over de aard en de aanpak van dit fenomeen.

Door de internationale samenwerking en de daarmee gepaard gaande gegevensverzameling in drie landen is een bijzondere en unieke dataset ontstaan waarmee het fenomeen cybercrime op basis van empirische gegevens vanuit een internationaal perspectief kan worden bestudeerd. Dit artikel is gebaseerd op de slotconclusie van het rapport, waarin alle bevindingen van de drie instituten zijn samengevoegd. De focus van dit artikel is gericht op de vraag of traditionele georganiseerde misdaad de weg naar het internet heeft weten te vinden. Gebeurt cybercrime in georganiseerd verband, en zo ja, hoe zien de organisatie en structuur van een dergelijke online organisatie er dan uit? Welke gevolgen heeft dit voor de opsporing van georganiseerde cybercriminaliteit?

3 Europols criteria voor 'organized criminal groups' (Doc 6204/2/97 ENFOPOL 35 Rev 2).

4 De bevindingen zijn ook voor elk land afzonderlijk beschreven. De resultaten en conclusies specifiek voor Nederland zijn te vinden in: Odinot e.a. 2017.

doi: 10.5553/JV/016758502018044005002

De modus operandi

Het internet heeft inmiddels een prominente plek ingenomen als plaats voor het plegen van criminaliteit. De terminologie waarmee verschillende vormen van cybercrime worden aangeduid, is niet altijd even duidelijk. In het Nederlands wordt vaak gesproken over cybercrime in ruime zin en cybercrime in enge zin.[5] Onder cybercrime in ruime zin wordt traditionele criminaliteit verstaan waarbij gebruik wordt gemaakt van computers of netwerken. Bij cybercrime in enge zin is ICT zowel het doel als het middel. Voor vormen van traditionele criminaliteit waarbij gebruik wordt gemaakt van ICT, zoals het verkopen van illegale spullen, oplichting of bedreiging via internet en het verspreiden van kinderporno, gebruikt Wall (2014) de term *cyber-enabled* criminaliteit. Vaak gaat het bij deze misdrijven om hybride vormen van criminaliteit waarbij het internet zorgt voor schaalvergroting van de afzetmarkt van traditionele misdaden. Daarnaast zorgt het internet ook voor het vergroten en verbreden van het criminele netwerk. Wanneer het internet weg zou vallen, zou de criminaliteit in een andere vorm blijven bestaan. Dit is niet het geval bij cybercrime in enge zin. Daarbij gaat het om criminaliteit die met computers tegen computers wordt gepleegd. Deze criminaliteit wordt door Wall aangeduid met de term *cyber-dependent* criminaliteit. Phishing, hacken, het verspreiden van ransomware en het opzetten, verhuren en/of beheren van een botnet zijn hier voorbeelden van.
Door de anonimiteit die het internet kan bieden is het opsporen van daders die zich schuldig maken aan dit soort delicten bijzonder moeilijk. Om ondervertegenwoordiging van bepaalde misdrijven te minimaliseren zijn daarom ook zaken opgenomen waarin slechts één van de betrokken verdachten kon worden geïdentificeerd en kon worden vervolgd. In dat geval bleek uit het dossier dat er sprake was van een samenwerkingsrelatie met personen van wie de identiteit in het onderzoek niet kon worden achterhaald, of van een misdrijf dat volgens de opsporingsexperts gezien de aard en omvang onmogelijk door één persoon kon worden gepleegd. Er bevinden zich voorbeelden van zowel georganiseerde *cyber-enabled* als van georganiseerde *cyber-dependent* criminaliteit in onze dataset. Daarmee hebben we ons gericht op alle vormen van ernstige georganiseerde cybercriminaliteit.

5 Zie bijv. Cybersecuritybeeld Nederland 2018 van de NCTV.

doi: 10.5553/JV/016758502018044005002

De cyber lift voor traditionele misdaad

De bestudeerde casussen laten zien dat het betreden van de digitale wereld en het samenwerken met ICT-specialisten de impact van traditionele misdaad vergroten. In meerdere casussen schakelen verdachten een ICT-specialist in om criminele activiteiten te kunnen plegen. Zo kwamen we een zaak tegen waarin een ICT-specialist samenwerkte met 'traditionele' drugshandelaren en voor hen een digitale marktplaats bouwde die bedoeld was om drugs op het darkweb te verkopen. Als de vakkundigheid en betrouwbaarheid van deze specialist worden gewaardeerd, leidt dit soms tot een intensievere samenwerking. Er zijn ook voorbeelden van zaken waarbij de ICT-specialist een cruciale rol speelde bij het uitvoeren van de criminele activiteiten en waarin deze persoon een significant deel van de opbrengst kreeg. Een mooi voorbeeld daarvan zagen we in een zaak waarin een technicus werd ingezet vanwege zijn specialistische kennis voor het aanpassen van chips in bankpassen. Er zijn echter ook casussen waarin een ICT-specialist voor een enkele dienst werd ingehuurd. In zo'n zaak werd een computersysteem in opdracht gehackt voor het achterhalen van specifieke informatie.

Er bleken echter ook casussen te zijn waarin georganiseerde misdaadgroepen, naast hun traditionele criminelen activiteiten, heel goed in staat bleken om zelf cyberdelicten te plegen die een hoge mate van (technologische) kennis vereisen. Zo wisten criminelen in een zaak zelf mailadressen buit te maken. Vervolgens stuurden ze een e-mail naar die adressen, waarmee de ontvangende computers met malware werden besmet. Deze malware zorgde ervoor dat betalingsverkeer werd omgeleid naar de rekening van de criminelen.

Zoals hierboven al werd beschreven, zorgen de mogelijkheden die ICT en het internet bieden niet alleen voor nieuwe vormen van criminaliteit, maar ook voor een transformatie van traditionele criminaliteit. Dit komt doordat het internet gebruikt kan worden om op een veel grotere schaal actief te zijn. De impact van misdaden als drugshandel, mensenhandel, afpersing, fraude, illegaal gokken en handel in namaakartikelen wordt daarmee groter. Zo kunnen illegale goederen wereldwijd worden verkocht en kan kennis wereldwijd worden uitgewisseld. Deze vergroting van scope, impact en mate van afscherming die de bestudeerde dossiers laten zien, wordt door Wall (2007) aangeduid met de term '*cyber lift*'.

doi: 10.5553/JV/016758502018044005002

Het plegen van cyberdelicten lijkt met de jaren eenvoudiger te zijn geworden. Het vereist minder technische kennis, omdat kennis over modus operandi via fora wordt gedeeld, en specifieke kennis eenvoudigweg kan worden gekocht. Dit leidt niet alleen tot een *lift* van traditionele misdrijven, maar heeft tevens tot gevolg dat traditionele georganiseerde misdaadgroepen ook betrokken raken bij *cybercrime in enge zin*. De dossiers laten zien dat deze groepen specialistische kennis inkopen door specialisten in te huren (*crime-as-a-service*), of door kant-en-klare doe-het-zelfpakketten aan te schaffen. *Crime-as-a-service* lijkt een lucratieve handel en kan als een opzichzelfstaand fenomeen worden gezien, hoewel recent onderzoek laat zien dat de omvang van deze markt beperkt is.[6] Door het gemak waarmee kennis kan worden ingekocht, wordt de drempel voor het plegen van cybercrime verlaagd en de criminele horizon op internet verruimd. Dit biedt kansen voor zowel traditionele georganiseerde misdaadgroepen als nieuwe spelers in het veld.

Benutten van de digitale infrastructuur

Traditionele vormen van georganiseerde misdaad kenmerken zich door complexe logistieke processen, waarbij toegang moet worden verkregen tot leveranciers, transporteurs en klanten. Vaak is hierbij sprake van transnationale contacten en handelsstromen, en in alle gevallen moeten verschillende activiteiten in tijd en ruimte op elkaar worden afgestemd. Dankzij het internet kunnen dit soort processen sterk worden vereenvoudigd. Daders van cybercrime kunnen in theorie achter hun computer blijven zitten om samen te werken, contacten te leggen met leveranciers en klanten, en om activiteiten te coördineren.
Uit de bestudeerde casussen bleek dat daders van *cyber-enabled crime* de infrastructuur die nodig is om deze misdrijven te kunnen plegen in het algemeen zelf opbouwen en beheren. Zo verlopen de koop en verkoop in deze zaken regelmatig via zelf gemaakte en beheerde websites en online fora.
Juist bij de technisch meer geavanceerde vormen van *cyber-dependent crime* ligt dit anders. De bestudeerde netwerken blijken voor het verrichten van hun misdrijven veelvuldig gebruik te maken van

6 Zie https://www.tudelft.nl/2018/tu-delft/eerste-grootschalige-marktanalyse-ondergrondse-cybercrime-economie/.

doi: 10.5553/JV/016758502018044005002

bestaande digitale infrastructuren van bedrijven en overheden. In de bestudeerde zaken vonden deze activiteiten vaak op en via het 'gewone' reguliere internet plaats en niet per se op afgeschermde duistere plaatsen van het net. Voor het verkrijgen van toegang tot databases of eigendommen van slachtoffers, door middel van een hack, hoeven niet per se eigen structuren of voorzieningen te worden ontwikkeld. In een van de bestudeerde dossiers werd bijvoorbeeld gebruikgemaakt van reclamefoto's op een bekende website om computers van nietsvermoedende klikkende bezoekers te besmetten met ransomware. Doordat de maatschappij verder is gedigitaliseerd, zijn er meer mogelijkheden ontstaan voor het plegen van transnationale georganiseerde cybercrime. Onervaren daders die niet beschikken over de netwerken, contacten en infrastructuur die nodig zijn voor het plegen van traditionele georganiseerde misdaad, kunnen hierdoor toch relatief eenvoudig in deze geavanceerde vormen van georganiseerde cybercrime instappen.

Facilitering van georganiseerde misdaad

Naast de digitale infrastructuur worden ook andere nieuwe gelegenheidsstructuren en faciliteringsmechanismen benut bij het plegen van cybercrime. Hierbij springt allereerst de manier waarop geld kan worden overgedragen en kan worden witgewassen via het internet in het oog (zie ook Oerlemans e.a. 2016). Door gebruik te maken van cryptovaluta's of van geldoverdrachten via webaccounts die als bankrekening kunnen worden gebruikt, is het relatief eenvoudig om wereldwijd afgeschermde geldoverdrachten uit te voeren. Uit de dossiers kon niet worden afgeleid op welke wijze het geld in specifieke zaken precies wordt overgedragen en witgewassen. Wel bleek uit het onderzoek dat het gebruik van cryptovaluta's nieuwe ondergrondse economische structuren met zich meebrengt, die moeilijk te beheersen zijn.
Parallel aan deze nieuwe economische structuren komen er ook nieuwe faciliteerders in beeld, zoals online financiële dienstverleners en handelaren in cryptovaluta's, die de criminele activiteiten bewust of onbewust met hun diensten ondersteunen.
Naast financiële dienstverleners springen in de door ons bestudeerde dossiers ook andere nieuwe faciliteerders in het oog die, al dan niet bewust, cybercrime faciliteren. Denk bijvoorbeeld aan hostingprovi-

doi: 10.5553/JV/016758502018044005002

ders waar dubieuze websites een plek hebben en online reclamebureaus die advertenties plaatsen met verborgen software. Maar ook webwinkels en koeriersdiensten die door verdachten worden gebruikt voor de distributie van goederen en van geld. Daarnaast zagen we ook faciliteerders die we kennen vanuit de traditionele vormen van georganiseerde misdaad, zoals dekmantelondernemingen die dienstbaar zijn bij het afschermen van zaken, geldhandelaren en geldezels die hun rekeningnummers ter beschikking stellen en cash innen.
Soms maken faciliteerders deel uit van het sociale netwerk van de verdachten, maar vaker komen verdachten via het internet met hen in contact. De meeste faciliteerders raken bewust betrokken bij de criminele activiteiten, maar het gebeurt ook onvrijwillig en onbewust. Lang niet alle faciliteerders lijken te weten dat zij met hun diensten criminele activiteiten mogelijk maken, en dat zij hiervoor door de verdachten worden gebruikt. Denk bijvoorbeeld aan koeriersdiensten die wereldwijd pakketten vervoeren en afleveren. Of de eigenaar/beheerder van de populaire website waarop een reclamebureau besmette foto's plaatste om bezoekers te infecteren met malware.

Structuur en organisatie van cybergroepen

De manier waarop verdachten in de bestudeerde zaken met elkaar samenwerken, komt deels overeen met wat we weten over samenwerking in de traditionele georganiseerde misdaad. Er is sprake van dynamische netwerken; veranderlijke samenwerkingsvormen die worden aangepast aan de criminaliteit die wordt gepleegd. Sociale relaties zijn hierbij van belang. In de bestudeerde casussen spelen familiebanden, vriendschappen, online en offline sociale contacten op allerlei manieren een rol: een bevinding die overeenkomt met eerder onderzoek waaruit bleek dat daders elkaar vaak persoonlijk kennen (Kruisbergen e.a. 2018).
De casussen laten zowel bestaande groepen als nieuwe groepen zien. Cybercrime in enge zin is meestal georganiseerd rond een harde kern, die eventueel ondersteuning zoekt voor zijn activiteiten bij een breed netwerk van mensen. Hierbij kan het gaan om het ronselen van mensen die virtueel geld willen omzetten naar cash, de geldezels, maar ook om het ronselen van mensen met de juiste ICT-vaardigheden, die via het internet gemakkelijk te vinden zijn. Er lijkt hierbij minder te

doi: 10.5553/JV/016758502018044005002

worden geïnvesteerd in relaties met mededaders dan bij traditionele vormen van georganiseerde misdaad. Als je weet waar je moet zoeken, zijn medeplegers met specifieke ICT-vaardigheden blijkbaar gemakkelijk te vinden en daardoor is het minder noodzakelijk om te investeren in bestaande relaties om deze ten behoeve van toekomstige activiteiten te behouden.
De wijze van samenwerking kan het best worden omschreven als losjes, flexibel en opportunistisch, en is minder dan bij traditionele georganiseerde misdaad gebaseerd op langdurige sociale relaties. De samenstelling van het samenwerkingsverband is afgestemd op de kennis en kunde die voor het plegen van een specifiek delict nodig zijn. Nieuwkomers in het veld treden vaak op als 'onderaannemers' of vormen een netwerk waar een persoon of groep weer mee in contact staat. Het wereldwijde karakter van het internet faciliteert het ontstaan van deze netwerken of schakels van mensen. De individuele leden die allen beschikken over specifieke kennis zijn niet per se in staat om de vaak technisch complexe delicten op te zetten en uit te voeren. Het is juist de samenwerking tussen deze individuen, die elkaar weten te vinden op het internet, die de criminele activiteiten mogelijk maakt. Fora, communicatieplatformen op internet, fungeren daarbij als ontmoetingsplaats (Soudijn & Monsma 2012**;** Wall & Williams 2014). Hier worden contacten gelegd en wordt informatie uitgewisseld. Op deze manier kunnen verdachten online relaties opbouwen, samenwerken en communiceren zonder elkaar offline te hoeven ontmoeten. Deze kanalen worden ook gebruikt voor de verkoop en het delen van kennis, software, scripts, goederen, producten en ruw materiaal. Het feit dat online communicatiediensten versleuteld zijn en de gebruiker vaak anoniem kan blijven door het gebruik van anonimiseringssoftware, blijkt een belangrijke motivatie te zijn om deze fora te verkiezen boven de meer traditionele communicatiekanalen. In de bestudeerde dossiers konden we constateren dat er vaak zonder terughoudendheid werd gecommuniceerd over uiteenlopende zaken.

Vertrouwen

Bij de losse, flexibele en opportunistische samenwerkingsverbanden die een deel van de dossiers te zien gaf, is de verantwoordelijkheid voor de uitvoering van een misdaad verspreid over meerdere personen. De rol die 'vertrouwen' speelt bij online samenwerkingsverban-

doi: 10.5553/JV/016758502018044005002

den krijgt hiermee een andere vorm dan die we kennen uit de traditionele georganiseerde misdaad. Bij traditionele georganiseerde misdaad zijn langdurige samenwerkingsverbanden en loyaliteit een belangrijk gegeven. In online criminele samenwerkingsverbanden zien we dit niet terug. Vaak zijn deze samenwerkingsverbanden gebouwd op *thin trust*; banden die niet zozeer gebaseerd zijn op sterke of zwakke interpersoonlijke relaties, maar op de reputatie of veronderstelde kwaliteiten van personen, die unieke toegang geven tot middelen en kansen die in de directe sociale kring niet aanwezig zijn (Khodayakov 2007). Terwijl sterke vertrouwensbanden typerend zijn voor de samenwerking binnen een criminele groep, is *thin trust* typerend voor virtuele samenwerking en voor samenwerking met experts die niet beschikbaar zijn in de eigen kring.
In de bestudeerde bestanden komen we zowel voorbeelden tegen van sterke samenwerkingsrelaties, gebaseerd op vertrouwen, loyaliteit en controle door middel van macht en geweld, als voorbeelden van losse, meer 'projectmatige' samenwerkingsrelaties, waarin vertrouwen een heel andere rol speelt. Partners worden in dat geval geselecteerd op grond van prestige en reputatie, die niet alleen gebaseerd zijn op kennis, kunde en eerdere prestaties, maar ook op de mate waarin men zich volgens de referenten aan afspraken houdt. Een goede reputatie wordt opgebouwd met recensies op het internet en met feedback over de geleverde diensten.
Door de anonimiteit van het internet kunnen subjecten op het internet met elkaar samenwerken en vertrouwelijke zaken met elkaar delen. Dit betekent echter niet dat zij elkaar ook in de offline wereld zouden vertrouwen. De anonimiteit van het internet biedt hun bescherming. Deze anonimiteit van het internet heeft echter ook gevolgen voor de wijze waarop mensen elkaars handelingen kunnen controleren, en voor de wijze waarop afspraken kunnen worden afgedwongen. Controle door middel van macht en geweld maakt plaats voor recensies en indien nodig ook cyberaanvallen. Zo hebben we in de dossiers gevallen gezien van verdachten die elkaar bestookten met DDoS-aanvallen.

Ketenstructuur

In een deel van de door ons bestudeerde cyberzaken wordt de samenwerking tussen verdachten gekenmerkt door een ketenstructuur. Met

doi: 10.5553/JV/016758502018044005002

name in de lossere netwerken krijgt de samenwerking tussen verdachten de vorm van een ketensamenwerking. Binnen zo'n keten zijn verschillende verdachten betrokken bij verschillende activiteiten, die pas na samenvoeging een strafbaar feit opleveren. In deze ketenstructuren werken verdachten wel met elkaar samen, maar zijn zij slechts verantwoordelijk voor een kleiner onderdeel van de gehele criminele activiteit. Als gevolg hiervan kunnen verdachten betrokken zijn bij georganiseerde criminaliteit, zonder precies te weten van welke misdaden hun activiteiten onderdeel uitmaken. Er kan zelfs ruime tijd zitten tussen de geleverde dienst en het uiteindelijke delict. Een voorbeeld hiervan is software die iemand geschreven heeft en te koop heeft aangeboden. Tussen de verkoop en de daadwerkelijke inzet kan langere tijd zitten.

Binnen deze ketenstructuren heeft elke verdachte in zekere zin macht, en heeft elke verdachte een bepaalde rol, maar tegelijkertijd lijkt iedereen of juist niemand verantwoordelijk te zijn voor de misdaad als geheel. Hierdoor is sprake van fragmentatie van het delict. Dit lijkt een nieuw kenmerk van georganiseerde cybercriminaliteit, en zou een verandering kunnen betekenen voor de inhoud van het concept georganiseerde criminaliteit.

In zo'n ketenstructuur kunnen de verschillende spelers voor zichzelf bezig zijn en individuele doelen hebben. Samen bereiken ze een georganiseerde vorm van criminaliteit, die niet zozeer van bovenaf georganiseerd is, maar veeleer vanuit een bottom-up proces is ontstaan. Op deze manier lijken zowel de criminele activiteiten als de groepen van samenwerkende personen min of meer op toevallige wijze te ontstaan en bepaalde vormen aan te nemen.

Deze ontwikkelingen maken dat georganiseerde cybercrime niet alleen kan worden gepleegd op basis van onderlinge afspraken tussen verdachten die elkaar kennen en samenwerken aan een bepaald project, op basis van een bepaalde verdeling van taken, maar ook in de vorm van de hierboven geschetste ketenstructuur, zonder duidelijke coördinatie. Er bestaat daarmee een diversiteit aan vormen, waardoor het moeilijk kan zijn om na te gaan wie wel en niet tot een criminele groep behoren en om criminaliteit aan specifieke criminele groepen of organisaties toe te schrijven. Ook wordt het daardoor moeilijk om te voorspellen hoe criminaliteitsvormen zich ontwikkelen.

doi: 10.5553/JV/016758502018044005002

Anonimiteit

Het internet biedt mogelijkheden om volledig anoniem te acteren. Uit de bestudeerde dossiers blijkt dat verdachten de identiteit van hun medeplegers daardoor niet altijd kennen. Dat geldt vooral voor de *cyber-dependent* zaken. Een verdachte van grootschalige DDoS-aanvallen was bijvoorbeeld zeer verbaasd dat zijn medepleger een 16-jarige jongen bleek te zijn. Ook tijdens verhoren verklaarden verdachten dat ze online contacten hadden, informatie uitwisselden en diensten kochten van personen die zij nooit persoonlijk hadden ontmoet. Dit geldt niet alleen voor kleine flexibele gelegenheidssamenwerkingsverbanden, maar ook voor groepen die langer bestaan en wel enigszins werken in een hiërarchische structuur. Bij *cyber-enabled crime* is er vaak sprake van een vermenging van ICT en traditionele georganiseerde misdaad. Dit brengt met zich mee dat daders van deze misdrijven elkaar vaak wel kennen en elkaar ook offline ontmoeten (Kruisbergen e.a. 2018). Echter, ook bij dit soort misdrijven hebben verdachten online contacten en wordt er ook samengewerkt met personen die ze niet kennen en met wie het nooit tot een fysieke ontmoeting komt. Een pakkend voorbeeld is een verdachte die samen met enkele bekenden een marktplaats wilde bouwen, nadat de website op het darkweb, waarvan hij medebeheerder was, door de eigenaar op non-actief was gesteld. De verdachte verklaarde dat hij deze eigenaar nog nooit had ontmoet en dat communicatie enkel via fora en via de mail verliep. De identiteit van de eigenaar van deze darkweb-marktplaats is nooit in beeld gekomen en het opsporingsteam veronderstelde dat hij zich in het buitenland bevond.
De inbedding van individuele anonieme verdachten in een keten van samenwerkende daders maakt het opsporen van complexe cybercriminaliteit niet eenvoudig. Het in kaart brengen van een samenwerkingsverband wordt verder bemoeilijkt doordat informatie over criminele activiteiten en over de daders gefragmenteerd is. Zoals eerder opgemerkt, speelt de loyaliteit van individuele leden naar een groep geen grote rol op internet en online samenwerkingsverbanden duren soms maar kort. Met het ontmantelen of uitschakelen van een individuele schakel loopt het voortbestaan van de ketenstructuur geen enkel gevaar. In de wereldwijde pool die het internet biedt, is snel doorschakelen mogelijk, hetgeen kenmerkend is voor deze online samenwerkingsverbanden.

doi: 10.5553/JV/016758502018044005002

Het is echter niet ondenkbaar dat bepaalde schakels essentieel zijn voor één of meer samenwerkingsverbanden. Dit zou met name kunnen gelden voor individuen die hoog in aanzien staan of over zeer schaarse kennis beschikken. In de bestudeerde casussen zijn we hiervan overigens geen voorbeelden tegengekomen. Focussen op zo'n specifieke schakel zou lonend kunnen zijn bij het verstoren van de activiteiten van misdaadgroepen. Tegelijkertijd is dit waarschijnlijk ook bijzonder moeilijk, omdat het gaat om individuen die zeer kundig zijn in datgene wat zij doen en daardoor mogelijk ongrijpbaar blijven.

Ten slotte

Door technologische ontwikkelingen die het mogelijk maken om steeds gemakkelijker anoniem op het internet te acteren vormt de aanpak van georganiseerde cybercrime een steeds groter probleem. Niet alleen omdat daders, bewijsmateriaal, opbrengsten en slachtoffers van georganiseerde cyberdelicten nog ongrijpbaarder worden dan ze al waren, maar vooral ook door de wijze waarop er op internet in de vorm van ketensamenwerking lijkt te worden geopereerd. Wanneer verschillende samenhangende stappen door verschillende mensen in een ketensamenwerking worden gezet, wordt het moeilijk om de aard van een misdrijf te begrijpen, om te zien hoe het misdrijf ontstaat, om de verdachten te identificeren die verantwoordelijk zijn voor stappen of voor het grotere geheel, en om het misdrijf met traditionele middelen op te sporen. De nieuwe Wet computercriminaliteit III,[7] die binnenkort in Nederland in werking treedt, zal de Nederlandse politie nieuwe onderzoeksinstrumenten bieden. Zo biedt deze wet de mogelijkheid om de toegang te krijgen tot systemen en data voordat deze versleuteld zijn. De toekomst zal uitwijzen of de verruimde opsporingsmogelijkheden de gewenste oplossingen kunnen bieden. Omdat een verdachte op het internet zich overal ter wereld kan bevinden, vergt het identificeren, lokaliseren, aanhouden, vervolgen en uiteindelijk berechten van verdachten vooral een intensieve internationale samenwerking. Om internationaal samen te kunnen werken hebben opsporingsinstanties nog steeds rechtshulpverzoeken nodig om de benodigde informatie of het benodigde bewijsmateriaal te

7 Besluit Wet computercriminaliteit III, *Kamerstukken* I 2017/18, 34372, https://www.eerstekamer.nl/wetsvoorstel/34372_computercriminaliteit_iii.

doi: 10.5553/JV/016758502018044005002

kunnen verkrijgen. Ons onderzoek liet zien dat deze verzoeken door lokale prioriteiten, ingewikkeld papierwerk en omslachtige procedures vaak worden behandeld met een tempo dat onverenigbaar is met de snelheid van het internet. Daarbij ontstaat dan tevens de vraag wáár de verdachte berecht moet worden, omdat een misdaad op internet niet altijd een fysieke locatie heeft. Overheden zullen daarom actief en creatief moeten nadenken over nieuwe manieren om deze moeilijk grijpbare vormen van criminaliteit te kunnen bestrijden. Begrijpen hoe georganiseerde cybercrime in elkaar zit en zich ontwikkelt, is een noodzakelijke eerste stap. We hopen dat het gezamenlijke onderzoeksrapport, geschreven door onderzoekers uit drie Europese landen, bijdraagt aan dit doel.

Literatuur

BKA, WODC & BRA 2016
BKA, WODC & BRA, *Cyber-OC – Scope and manifestations in selected EU member states* (HOME/2012/ISEC/AG/4000004382). Polizei + Forschung 2016, 50

Van de Bunt & Kleemans 2007
H.G. van de Bunt & E.R. Kleemans, m.m.v. C.J. de Poot, R.J. Bokhorst, M. Huikeshoven, R.F. Kouwenberg, M. van Nassou & R. Staring, *Georganiseerde criminaliteit in Nederland. Derde rapportage op basis van de Monitor Georganiseerde Criminaliteit*, Den Haag: Boom Juridische uitgevers 2007.

Khodayakov 2007
D. Khodayakov, 'Trust as a process: A three-dimensional approach', *Sociology* (41) 2007, p. 115-132.

Kleemans e.a. 1998
E.R. Kleemans, E.A.I.M. van den Berg & H.G. van de Bunt, m.m.v. M. Brouwers, R.F. Kouwenberg & G. Paulides, *Georganiseerde criminaliteit in Nederland. Rapportage op basis van de WODC-monitor*, Den Haag: WODC 1998.

Kleemans e.a. 2002
E.R. Kleemans, M.E.I. Brienen & H.G. van de Bunt, m.m.v. R.F. Kouwenberg, G. Paulides & J. Barensen, *Georganiseerde criminaliteit in Nederland. Tweede rapportage op basis van de WODC-monitor*, Den Haag: WODC 2002.

doi: 10.5553/JV/016758502018044005002

Kruisbergen e.a. 2012
E.W. Kruisbergen, H.G. van de Bunt & E.R. Kleemans, *Georganiseerde criminaliteit in Nederland. Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit*, Den Haag: Boom Lemma 2012.

Kruisbergen e.a. 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.

Martin 2013
J. Martin, 'Lost on the Silk Road: Online drug distribution and the "cryptomarket"', *Criminology and Criminal Justice* (14) 2013, afl. 3, 351-367, https://doi.org/10.1177/1748895813505234.

Odinot e.a. 2017
G. Odinot, M.A. Verhoeven, R.L.D. Pool & C.J. de Poot, *Organised cyber-crime in the Netherlands. Empirical findings and implications for law enforcement* (Cahier 2017-1), Den Haag: Boom juridisch 2017.

Oerlemans e.a. 2016
J.J. Oerlemans, B.H.M. Custers, R.L.D. Pool & R. Cornelisse, *Cybercrime en witwassen* (O&B 319), Den Haag: WODC 2016.

Soudijn & Monsma 2012
M.R.J. Soudijn & E. Monsma, 'Virtuele ontmoetingsruimtes voor cybercriminelen', *Tijdschrift voor Criminologie* (54) 2012, afl. 4, p. 349-360.

Wall 2007
D.S. Wall, *The transformation of crime in the information age*, Cambridge: Polity Press 2007.

Wall 2014
D.S. Wall, '"High risk" cybercrime is really a mixed bag of threats', 2014, https://theconversation.com/high-risk-cyber-crime-is-really-a-mixed-bag-of-threats-34091.

Wall & Williams 2014
D.S. Wall & M.L. Williams, *Policing cybercrime. Networked and social media technologies and the challenges for policing*, Oxon, VK: Routledge 2014.

doi: 10.5553/JV/016758502018044005002

Criminele geldstromen en ICT: over innovatieve werkwijzen, oude zekerheden en nieuwe flessenhalzen

Edwin Kruisbergen, Rutger Leukfeldt, Edward Kleemans en Robby Roks[*]

Criminele netwerken gebruiken ICT op tal van manieren: voor onderlinge communicatie, om capabele mededaders en 'tools' te vinden, om afzetmarkten te vergroten, om een groter aantal potentiële slachtoffers te bereiken, en ook om criminele geldstromen af te schermen. Het regelen en afschermen van geldstromen is een essentiële opgave voor daders in de georganiseerde criminaliteit. Georganiseerde criminaliteit is primair ingegeven door financieel gewin. Maar criminele verdiensten brengen risico's met zich mee, vooral als je succesvol bent en je criminele activiteiten grote opbrengsten genereren. Criminele verdiensten en de besteding daarvan kunnen immers tot aandacht van de autoriteiten leiden, met arrestatie en inbeslagname van vermogen als mogelijke gevolgen.

Dit artikel biedt empirisch inzicht in hoe daders binnen de georganiseerde criminaliteit ICT gebruiken voor het regelen van hun geldstromen. We richten ons daarbij niet uitsluitend op cybercrime, maar verkennen juist het gebruik van ICT én de consequenties daarvan voor een breder scala van soorten georganiseerde criminaliteit, dus ook 'traditionele' georganiseerde criminaliteit zoals drugssmokkel. De empirische data die aan dit artikel ten grondslag liggen, bestaan uit

* Dr. E.W. Kruisbergen is als onderzoeker verbonden aan het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) van het ministerie van Justitie en Veiligheid. Dr. R. Leukfeldt is senior-onderzoeker cybercrime bij het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving en lector Cybersecurity in het mkb bij de Haagse Hogeschool. Prof. dr. E.R. Kleemans is hoogleraar zware criminaliteit en rechtshandhaving aan de Vrije Universiteit Amsterdam. Dr. R. Roks is universitair docent aan de Erasmus Universiteit Rotterdam.

doi: 10.5553/JV/016758502018044005003

dertig grootschalige opsporingsonderzoeken die zijn bestudeerd voor de Monitor Georganiseerde Criminaliteit.[1]
Hieronder lichten we eerst de onderzoeksopzet en de gebruikte bronnen toe. Vervolgens bespreken we de empirische resultaten van onze studie. Daarbij gaan we in op de criminele verdiensten zelf, maar met name op de besteding ervan en het afschermen van criminele inkomsten. We eindigen het artikel met conclusies. Aan de ene kant leidt ICT ook wat betreft het beheer van criminele geldstromen tot nieuwe werkwijzen. Aan de andere kant laten analyses zien dat oude zekerheden nog steeds een prominente rol spelen in keuzes van daders. Zo blijkt contant geld nog steeds een dominante factor in criminele geldstromen, zowel bij traditionele georganiseerde criminaliteit als bij cybercriminaliteit. Bovendien blijkt het omwisselen van digitale valuta voor contant geld een belangrijke flessenhals te zijn voor het criminele bedrijfsproces van daders die online opereren.

Onderzoeksopzet en gebruikte bronnen

Aan de basis van dit artikel liggen uitgebreide zaaksbeschrijvingen die zijn gemaakt na analyse van dertig opsporingsonderzoeken in de meest recente, vijfde ronde van de Monitor Georganiseerde Criminaliteit.[2] Elk van de dertig zaken bevat informatie over verschillende, soms tientallen verdachten. De selectie van de dertig zaken kwam tot stand na een intensieve inventarisatie van zaken bij centrale, regionale en gespecialiseerde eenheden van de politie en het Openbaar Ministerie (zie kader). Bij die selectie speelden verschillende criteria een rol:
- Er is sprake van een crimineel samenwerkingsverband.
- Het opsporingsonderzoek is afgerond (de belangrijkste verdachten zijn aangehouden) in 2011 of later.
- De zaak is rijk aan informatie.
- De zaak heeft toegevoegde waarde; er moet spreiding zijn over verschillende delicttypen.

1 Dit artikel is gebaseerd op een rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit. Voor een uitgebreide bespreking van de onderzoeksmethode, de gebruikte bronnen en de uitkomsten van empirische analyses op drie verschillende deelthema's, zie Kruisbergen e.a. 2018.
2 Vijf zaken op het terrein van cybercrime/ICT-gerelateerde georganiseerde criminaliteit zijn ook geanalyseerd in onderzoek van Odinot e.a. (2017).

doi: 10.5553/JV/016758502018044005003

Voor iedere zaak is het volledige opsporingsdossier bestudeerd aan de hand van een uitgebreide checklist.[3] De zaken beslaan verschillende soorten georganiseerde criminaliteit, onder meer verschillende typen drugsproductie en -handel, mensensmokkel/-handel, witwassen en cybercriminaliteit. Op basis van de rol die ICT speelt binnen een zaak, onderscheiden we vier categorieën zaken. De eerste categorie bevat 23 zaken van *traditionele georganiseerde criminaliteit*, dat wil zeggen zaken zonder een sterke ICT-component. Het gaat dan om gevallen van offline drugshandel, mensenhandel/-smokkel en andere (combinaties van) misdrijven.

De tweede categorie betreft *traditionele georganiseerde criminaliteit met ICT als belangrijk vernieuwend element* in de modus operandi. Het gaat om drie zaken. De eerste zaak betreft een dadergroepering die door middel van een hack in het netwerk van een haventerminal de afhandeling van binnenkomende containers manipuleert. De tweede zaak draait om betrokkenen bij een online marktplaats (een *darknet market*) waarop onder meer drugs worden verhandeld. In de derde zaak staat een moderne variant van witwassen centraal: het omwisselen van met criminaliteit verdiende bitcoins voor contante euro's.

De derde categorie betreft twee zaken van *georganiseerde low-tech cybercriminaliteit*. De eerste zaak richt zich op een variant van *skimmen* (ook wel *shimmen* genoemd). In de tweede zaak staan *phishing-operaties* centraal, waarbij daders toegangsgegevens van slachtoffers voor internetbankieren proberen te verkrijgen.

De vierde categorie ten slotte omvat twee gevallen van *georganiseerde high-tech cybercriminaliteit*. Beide zaken draaien om *banking malware*, waarbij daders via kwaadaardige software betalingen via internetbankieren manipuleren.

Waar dat relevant is, maken we bij de bespreking van de onderzoeksuitkomsten onderscheid tussen de vier genoemde categorieën. Vanwege de beperkte ruimte die dit artikel heeft, zullen we echter lang niet alle zaken individueel kunnen bespreken.[4]

3 Voor meer informatie over de (selectie van) zaken, zie Kruisbergen e.a. 2018, p. 22-31. In dezelfde publicatie is de gebruikte checklist integraal opgenomen (als bijlage).

4 Er is enige overlap tussen de categorieën (traditionele georganiseerde criminaliteit, (low-tech/high-tech) cybercriminaliteit, etc.) enerzijds en het te analyseren vraagstuk (hoe gaan daders om met criminele geldstromen?) anderzijds. Bij cybercriminaliteit is immers het digitale aspect in de modus operandi tot op zekere hoogte een gegeven. Echter, dat het gronddelict (bijv. drugshandel of banking malware) al dan niet digitaal van aard is, betekent niet automatisch dat de financiële component dat ook in dezelfde mate is.

doi: 10.5553/JV/016758502018044005003

De zaken die voor de Monitor Georganiseerde Criminaliteit worden geanalyseerd, vormen geen aselecte steekproef van *de* georganiseerde criminaliteit in Nederland. Ten eerste is iedere mogelijke steekproef van gevallen van georganiseerde criminaliteit nu eenmaal afhankelijk van opsporingsactiviteiten van de politie, en daarmee per definitie niet aselect. Ten tweede bestaat er geen geschikt centraal overzicht van alle zaken die hebben gespeeld in Nederland, waarmee een steekproefkader dus ontbreekt (en wat de inventarisatie van zaken ook tijdrovend maakt). Ten derde is het ook onverstandig om een aselecte steekproef van zaken te analyseren. Zou dat wel gebeuren, dan is de kans namelijk groot dat vooral zaken worden bestudeerd die relatief weinig kennis over georganiseerde criminaliteit toevoegen, bijvoorbeeld omdat ze delicttypen betreffen waarover al veel bekend is (bepaalde vormen van drugshandel), of omdat de zaak heel klein is en er weinig is doorgerechercheerd. Voor de inventarisatie van zaken zijn gesprekken gevoerd met (landelijke) specialisten op het terrein van cybercrime, cocaïne en heroïne, synthetische drugs en hennep, fraude en witwassen, overvallen, ram- en plofkraken, mensenhandel en Hollandse netwerken. Verder zijn zaken geïnventariseerd bij (andere) regionale en landelijke eenheden. Uiteindelijk zijn behalve landelijke eenheden alle tien regio's van de politie/het Openbaar Ministerie (OM) bij de inventarisatie betrokken. De inventarisatie leidde tot een 'longlist' van ongeveer zeventig zaken, waarvan er dertig zijn geselecteerd.

Criminele verdiensten en besteding

Vragen naar (besteding van) criminele verdiensten behoren tot de moeilijkste onderzoeksvragen op het terrein van de georganiseerde criminaliteit, simpelweg omdat een goed zicht op de financiële positie van daders vaak ontbreekt (Kleemans e.a. 2002, p. 124). Dit laatste geldt grosso modo ook voor de dertig zaken uit de meest recente, vijfde ronde van de Monitor Georganiseerde Criminaliteit. Dit is waarschijnlijk enerzijds het gevolg van succesvolle pogingen van daders om hun verdiensten en vermogen te onttrekken aan het zicht van de opsporing. Zo vermoedt een zaaksofficier in een drugszaak dat veel criminele verdiensten naar het land van herkomst van de daders zijn gestroomd. Anderzijds zijn er ook zaken waarin informatie erop wijst dat daders (nog) weinig verdiensten hebben gegenereerd op het

doi: 10.5553/JV/016758502018044005003

moment dat de politie ingreep.[5] Hoewel de financiële positie van daders in de georganiseerde criminaliteit verre van transparant is, bieden de dertig bestudeerde zaken, dankzij de inzet van soms verregaande opsporingsinstrumenten, toch veel interessante inzichten. Waar besteden daders hun geld aan? Besteding valt grofweg uiteen in consumptie en investeringen. Op beide punten laten de analyses geen grote verschillen zien ten opzichte van eerder onderzoek (Kruisbergen e.a. 2015) en ook geen grote verschillen tussen traditionele en cybercriminaliteit. We beginnen met consumptie.

In verschillende zaken van offline en online criminaliteit zien we daders die er een uitbundige levensstijl en navenant uitgavenpatroon op na houden. Zo wordt in een van de casussen die zich op banking malware richten meer dan twee ton uitgegeven aan boten (casus 155).[6] Bij een crimineel samenwerkingsverband dat zich bezighoudt met het omwisselen van bitcoins voor euro's wordt informatie gevonden die wijst op verschillende grote uitgaven, onder meer aan auto's en helikoptervluchten (173). Er zijn echter ook daders bij wie er weinig of geen opvallende uitgavenposten worden vastgesteld. Sommigen lijken zelfs moeite te hebben om rond te komen. Dit laatste valt bijvoorbeeld af te leiden uit afgeluisterde gesprekken tussen twee verdachten in een drugszaak (casus 175).

Als een dader na consumptie en het voortzetten van criminele activiteiten geld over heeft van zijn criminele inkomsten, kan hij dat investeren in de reguliere economie.[7] Die investeringen in de legale economie zijn in zeker opzicht interessanter dan het consumptiepatroon van daders. De opbouw van posities in de reguliere economie, en meer in het algemeen de wisselwerking tussen 'onder-' en 'bovenwereld', vormt namelijk een belangrijke aanleiding tot beleidsmaatrege-

5 In verschillende zaken was het (financieel) onderzoek nog niet afgerond op het moment dat de zaak werd bestudeerd. Opsporingsonderzoeken waarin op het moment van bestuderen wel berekeningen waren gemaakt van de criminele verdiensten beslaan een grote bandbreedte: van een ton of enkele tonnen tot (vele) miljoenen.

6 De nummering is dezelfde als die is gebruikt in de monitorrapportage (Kruisbergen e.a. 2018). In die rapportage worden in een bijlage alle casussen afzonderlijk toegelicht. Omdat in de vijf rondes van de Monitor Georganiseerde Criminaliteit inmiddels 180 zaken zijn geanalyseerd, zijn de 30 zaken uit de vijfde ronde genummerd van 151 t/m 180.

7 Onder investeringen in de legale economie verstaan we onder meer onroerend goed, bedrijven, aandelen, obligaties en opties. Luxe goederen als auto's en horloges en andere juwelen hebben we in onze analyses niet meegenomen als investeringen. Ook het aanhouden van contant geld en tegoeden op bankrekeningen hebben we niet als investering meegenomen.

doi: 10.5553/JV/016758502018044005003

len tegen georganiseerde criminaliteit en tot antiwitwasbeleid in het bijzonder.

Voor de dertig zaken is gekeken naar bezittingen in de legale economie die aan daders zijn te relateren. Concreet gaat het daarbij om (gedeeltelijk) bezit van bedrijven en onroerend goed (al dan niet afgeschermd door bijvoorbeeld het gebruik van katvangers). Deze analyses zijn gebaseerd op alle informatie die in opsporingsdossiers aanwezig is over investeringen en bezittingen. Daarbij zijn de inbeslagnames meegenomen, maar ook informatie afkomstig uit andere bronnen, zoals bijvoorbeeld verhoren, observaties en undercoveroperaties.

Het patroon dat we in het grootste deel van de dertig zaken zien wat betreft de aard, omvang, plaats en het gebruik van de bezittingen in de legale economie komt overeen met het patroon dat werd gevonden bij eerdere analyses (Kruisbergen e.a. 2015). Dit investeringspatroon lijkt vrij conservatief, waarbij de fysieke en/of sociale afstand tussen een dader en zijn bezittingen vaak klein is. Zo investeren daders veel in het land waarin ze wonen en/of het land waar ze via een migratieachtergrond mee verbonden zijn. Verder investeren ze vooral in tastbare, 'bekende' vermogensbestanddelen, dat wil zeggen huizen en ander onroerend goed en bedrijven uit sectoren als groot-/detailhandel, horeca en transport. Ze gebruiken die bedrijven bovendien vaak ter ondersteuning van hun criminele activiteiten (zie Bruinsma & Bovenkerk 1996). Bedrijven worden daarbij ingezet voor logistieke doeleinden (zoals vervoer, opslag, ontmoetingen), voor het verhullen van criminele activiteiten (het bieden van een dekmantel van legaliteit voor illegale activiteiten) en voor witwasdoeleinden (door bijvoorbeeld te doen alsof inkomsten die feitelijk zijn verdiend met criminaliteit door legale bedrijfsactiviteiten zijn voortgebracht). De portfolio's van daders bestaan dus vooral uit onroerend goed en het genoemde type bedrijven. Daarentegen lijken minder tastbare, puur financiële bezittingen, zoals obligaties, opties en aandelen in bedrijven waarin daders níét persoonlijk betrokken zijn (bijvoorbeeld in beursgenoteerde bedrijven), veel minder vaak voor te komen. De zeven zaken van georganiseerde criminaliteit met een duidelijke ICT-component laten zoals gezegd geen grote verschillen zien met de andere, meer traditionele zaken.

doi: 10.5553/JV/016758502018044005003

Witwassen

Criminele geldstromen moeten worden afgeschermd. Wil een dader voorkomen dat zijn geld, en ook hijzelf, onderwerp van politieaandacht wordt, dan moeten dat geld en/of de illegale herkomst ervan verborgen blijven. Welke rol speelt ICT hierbij in de verschillende zaken?[8]

In hoe daders hun criminele inkomsten afschermen, zien we belangrijke verschillen tussen traditionele georganiseerde criminaliteit enerzijds en ICT-gerelateerde criminaliteit anderzijds. Bij de 23 zaken van traditionele georganiseerde criminaliteit zien we witwasmodaliteiten zoals die in eerdere publicaties zijn beschreven. Zo komen rudimentaire vormen voor als het verbergen en verplaatsen en het, al dan niet via stromannen of facilitators, uitgeven van grote bedragen aan contant geld aan bijvoorbeeld (het leasen van) auto's of het huren van onroerend goed (afgeschermde consumptie). Dit laatste zien we bijvoorbeeld in een zaak die draait om drugsproductie en -handel. De hoofdverdachte betaalt € 20.000 contant voor de huur van een Nederlands huis, betaalt meer dan € 20.000 contant voor de aankoop van een Mercedes, rekent vele duizenden euro's contant af voor de aanschaf van (water)scooters en laat een relatie bijna € 9.000 contant afrekenen voor een vakantiereis (casus 161). Ook meer complexe witwasconstructies worden in de zaken aangetroffen. Het gaat dan bijvoorbeeld om het fingeren van legale inkomsten uit dienstbetrekking of bedrijf, loan-backconstructies of het doorsluizen van geld via buitenlandse rechtspersonen.

Ook daders die zich bezighouden met traditionele georganiseerde criminaliteit zouden gebruik kunnen maken van nieuwe, door ICT mogelijk gemaakte betaal- en witwasmogelijkheden, zoals cryptovaluta. Een dader die bijvoorbeeld actief is in offline drugshandel zou de aanschaf van bitcoins kunnen gebruiken in een constructie om zijn geldstromen af te schermen, of als investering waarbij wordt gespeculeerd op

8 Voor een toelichting op wat witwassen is en welke varianten te onderkennen zijn, zie Kruisbergen & Soudijn 2015.

doi: 10.5553/JV/016758502018044005003

koersstijging.[9] In de 23 zaken van traditionele georganiseerde criminaliteit zien we echter nergens het gebruik van bitcoins of andere cryptovaluta. Wel wordt in een van de zaken geconstateerd dat daders gebruikmaken van prepaid cards, ook een zogenoemde *new payment method* (casus 165). De financiële innovatie van cryptovaluta ontbreekt dus in zaken van traditionele georganiseerde criminaliteit. Als het om witwaspatronen gaat, zijn de daders in deze 23 zaken van traditionele georganiseerde criminaliteit dus nog behoorlijk 'traditioneel'. Misschien zijn deze daders onbekend met de nieuwe mogelijkheden, zijn ze beducht voor de nadelen van cryptovaluta,[10] vinden ze het gewoonweg niet nodig om via ICT hun werkwijze drastisch te veranderen, of wist de politie het gebruik van virtuele munten niet op te sporen.

Bij ICT-gerelateerde criminaliteit zijn de opbrengsten, in tegenstelling tot veel vormen van traditionele georganiseerde criminaliteit, in eerste instantie vaak digitaal van aard. Drugshandelaren die actief zijn op een darknet market ontvangen de opbrengsten van hun handel vaak in een cryptomunteenheid zoals bitcoin. Bij bijvoorbeeld phishing- en malwareaanvallen verkrijgen daders door hun frauduleuze handelingen de controle over het online betalingsverkeer van hun slachtoffers, dat in digitale euro's verloopt. Casus 152 draait om online drugs- en wapenhandel via een darknet market. Online afgesloten drugstransacties worden betaald met bitcoins. In het opsporingsonderzoek wordt bij doorzoekingen beslag gelegd op honderden bitcoins, ter waarde van grofweg een half miljoen euro. Een van de moderators van de marktplaats handelt ook zelf in drugs. In het dossier wordt gemeld dat de genoemde moderator/drugshandelaar contacten heeft bij wie hij bitcoins kan omwisselen in fysieke euro's. Hij gaf er blijkbaar de voorkeur aan in ieder geval een deel van zijn verdiensten in fysieke euro's

9 Bitcoin is digitaal 'geld'. In tegenstelling tot reguliere munteenheden als de dollar en euro wordt deze cryptografische munteenheid niet uitgegeven, beheerd of gecontroleerd door een bank, overheid of een andere centrale actor. De creatie van bitcoins, aangeduid als *mining* (delven), verloopt decentraal, via een peer-to-peernetwerk, namelijk via computers van gebruikers. Zoals een bankbiljet wordt gedrukt en een munt wordt gesmeed, zo ontstaat een bitcoin door toepassing van een algoritme, oftewel een wiskundige formule. Bitcoins hebben geen fysieke vorm en worden bewaard in een *wallet*, een digitale portemonnee die online of bijvoorbeeld op een USB-stick wordt aangehouden (Kruisbergen & Soudijn 2015, p. 18-20).

10 Zoals het risico dat via het internet opgeslagen bitcoins kwijtraken of worden gestolen, de begrenzing van de anonimiteit waarmee bitcointransacties kunnen worden gedaan (Meiklejohn e.a. 2013; Ron & Shamir 2013; Oerlemans e.a. 2016), de extreem grillige koers en de geringe bruikbaarheid van bitcoin voor betalingen van reguliere goederen en diensten in de offline wereld.

doi: 10.5553/JV/016758502018044005003

aan te houden. Het omwisselen gebeurde via individuele bitcoinwisselaars met wie op openbare plekken werd afgesproken. Er zijn ook verschillende, gemakkelijk toegankelijke online *bitcoin exchanges*, maar wisseltransacties verlopen daar vaak via herleidbare kanalen, wat voor een drugshandelaar natuurlijk niet aantrekkelijk is. Omdat meer online handelaren hun bitcoins willen omwisselen in euro's, is de online handel in illegale goederen gepaard gegaan met een vraag naar bitcoinwisseldiensten, die met een grotere mate van anonimiteit worden aangeboden. Casus 173 richt zich op professionele facilitators die daarin voorzien.

> *De hoofdverdachten wisselen tegen betaling van een commissie aangeleverde bitcoins om voor contante euro's. Vermoedelijk is in ieder geval een deel van de door hen opgekochte bitcoins afkomstig van illegale handel op het darkweb. Aanwijzingen hiervoor zijn: de politie treft bij klanten van de bitcoinwisselaars voorwerpen aan die in verband staan met verzending van drugs; een bitcoin wallet van een klant is te relateren aan online drugshandel; klanten betalen voor het omwisselen een commissie van bijvoorbeeld 7%, veel hoger dan reguliere, online bitcoin exchangers rekenen.*
> *De bitcoinwisselaars ontmoeten hun klanten met name in lokale vestigingen van hamburger- of koffieketens (met wifi). Nadat een klant zijn bitcoins heeft overgeboekt naar een door de wisselaar gecontroleerde bitcoin wallet, krijgt de klant contant geld. De grote hoeveelheid bitcoins die de wisselaars aldus verkrijgen, levert voor henzelf ook een omwissel- en witwasprobleem op. De aangekochte bitcoins worden deels omgewisseld voor euro's bij reguliere bitcoin exchangers. Laatstgenoemden storten de euro's op rekeningen die onder controle staan van de wisselaars. Het geld wordt contant opgenomen en weer gebruikt voor de aankoop van bitcoins. In totaal zijn met de wisseldienst die de daders aanbieden miljoenen euro's gemoeid (casus 173).*

De zojuist besproken casussen 152 en 173 maken samen met casus 151 deel uit van de categorie traditionele georganiseerde criminaliteit met ICT als belangrijk vernieuwend element. Casussen 154 en 156 scharen we onder georganiseerde low-tech cybercriminaliteit. Ook hier zien we dat digitale valuta, in dit geval euro's, worden omgewisseld in fysieke, contante euro's. In casus 154, een al wat oudere zaak, manipuleren de daders kaartlezers van een grote Nederlandse bank om gegevens van rekeninghouders af te lezen. Met zelfgemaakte betaalpassen wordt vervolgens in meer dan tien verschillende landen

doi: 10.5553/JV/016758502018044005003

contant geld opgenomen, waarna het via fysiek vervoer of via *money transfers* wordt verplaatst. Casus 156 richt zich op daders die phishing-aanvallen uitvoeren. Daarbij wordt geld van de rekening van een slachtoffer overgeboekt naar de rekening van een zogenoemde *money mule*. Vervolgens wordt het geld contant opgenomen, door de money mule zelf of een ronselaar. Het gebruik van cryptovaluta, prepaidkaarten of andere innovaties zien we in de twee zaken niet.
Casussen 153 en 155 draaien beide om daders die betrokken zijn bij banking malware, hetgeen we als georganiseerde high-tech cybercriminaliteit hebben geclassificeerd. Het criminele samenwerkingsverband in casus 153 besmet computers en mobiele telefoons met software om banktransacties te manipuleren. De daders passen verschillende methoden toe om de criminele verdiensten af te schermen.[11] Zo wordt geld afkomstig van bankrekeningen van slachtoffers wel gebruikt om onder meer bitcoins, *WebMoney* en vouchers te kopen. De bitcoins worden vervolgens (ten dele) omgewisseld voor euro's. Een andere afschermingsmethode bestaat eruit dat met het geld online goederen zoals computers en telefoons worden aangekocht. Daarnaast komt het voor dat geld van de slachtoffers wordt overgeboekt naar rekeningen van money mules, waarna het contant wordt opgenomen.
In casus 155 gebruiken daders eveneens rekeningen van money mules en wordt geld vervolgens *gecasht*. Bovendien kopen ook deze daders bitcoins met een deel van het gestolen geld. Daarbij wordt bovendien een zogenoemde *bitcoin mixing service* gebruikt, om het spoor tussen zend- en ontvangstadres van een bitcoin te verhullen en aldus de identiteit van (in dit geval) de ontvanger te beschermen. In deze zaak wordt verder meer dan € 300.000 contant geld in beslag genomen. In deze twee zaken van cybercrime met een sterkere technische component (casus 153 en 155) worden dus wel 'nieuwe' betaalmethoden zoals bitcoins gebruikt. Tegelijkertijd zien we ook in deze zaken de centrale rol die contant geld speelt.

Cash is (still) king

Die centrale rol van contant geld is een overheersend, gemeenschappelijk kenmerk van veel van de door ons bestudeerde zaken, zowel op

11 Zie ook Oerlemans e.a. (2016, p. 78-79) voor een beschrijving van de werkwijze in deze zaak.

doi: 10.5553/JV/016758502018044005003

het terrein van traditionele als op het terrein van ICT-gerelateerde georganiseerde criminaliteit. Daders verbergen bijvoorbeeld contant geld of zorgen dat het in andere landen terechtkomt. Verder zagen we in ons casusmateriaal online drugshandelaren en daders van phishing- of banking-malwareaanvallen die hun digitale valuta omwisselen voor fysieke euro's (zie ook Leukfeldt 2014; Leukfeldt e.a. 2017; Oerlemans e.a. 2016; Europol 2015). Ten slotte gebruiken daders contant geld om kostbare goederen en diensten af te rekenen. Bij deze contante geldstromen maken daders gebruik van een breed scala aan dienstverleners, die onbewust, zonder veel vragen te stellen, of juist doelbewust daders helpen. Voor het verplaatsen van geld kunnen daders terecht bij ondergrondse bankiers of personen die gespecialiseerd zijn in de fysieke smokkel van geld. Voor het discreet omruilen van met drugshandel verdiende bitcoins voor contante euro's gebruiken daders bitcoinwisselaars. Dat deze dienstverleners waardevol zijn, komt terug in de prijs die hun klanten bereid zijn te betalen. Soudijn en Reuter (2016) berekenden de totale kosten voor cocaïnehandelaren van contant-geldsmokkel op 10 à 17% van het gesmokkelde bedrag. De prijs die klanten moeten betalen voor de diensten van de professionele bitcoinwisselaars die wij in casus 173 zagen, lijkt te variëren en ligt bijvoorbeeld op 7%, een stuk hoger dan bij reguliere bitcoin exchangers.[12]

Naast het verplaatsen en wisselen van criminele verdiensten is het accepteren van betalingen met contant geld een soort 'dienstverlening' die daders benutten. In de vijfde, maar ook in eerdere rondes van de monitor zien we aanbieders van goederen en diensten in de reguliere economie die schijnbaar zonder vragen te stellen contante betaling accepteren van (zeer) hoge bedragen (Kruisbergen e.a. 2012). Zij stellen daders in staat om hun criminele verdiensten ongestoord te consumeren. Het kan daarbij gaan om autobedrijven, aanbieders van woonruimte, elektronicawinkels, aannemers, reisbureaus en andere aanbieders van kostbare goederen en diensten.

12 Verder wordt, zoals we zagen, voor cashen van geld bij phishing- en banking-malwareaanvallen gebruikgemaakt van money mules. Zij zijn eerder katvangers dan professionele facilitators en hebben een meer inwisselbare positie in de periferie van criminele netwerken. Uit onderzoek blijkt dat ze vooral worden gerekruteerd onder jongvolwassenen uit armere wijken in stedelijke gebieden (Oerlemans e.a. 2016). Uit communicatie tussen daders in casus 155 komt naar voren dat zij money mules vooral zoeken onder gemakkelijk beïnvloedbare personen, die bijv. kampen met schulden, psychische problemen of drugsverslaving. In ons casusmateriaal zien we ook dat money mules de hun toegezegde vergoeding niet altijd krijgen (casus 156).

doi: 10.5553/JV/016758502018044005003

Discussie

In dit artikel bespraken we hoe daders binnen de georganiseerde criminaliteit ICT gebruiken voor het regelen van hun geldstromen. In ons casusmateriaal zagen we dat enerzijds gebruik wordt gemaakt van innovaties, zoals cryptovaluta en aanverwante diensten, maar dat anderzijds veel nog via traditionele patronen lijkt te verlopen, waarbij onder meer de dominante rol van contant geld opviel. Aan het slot van dit artikel benoemen we een aantal methodologische plus- en minpunten van ons onderzoek en gaan we kort in op de mogelijke implicaties van de uitkomsten.

Het onderzoek

Ons onderzoek is gebaseerd op de bestudering van dertig opsporingsonderzoeken. Opsporingsdossiers bevatten de verslaglegging van de inzet van de exclusieve opsporingsbevoegdheden die de politie heeft, zoals het afluisteren van gesprekken, de inbeslagname van goederen en de inzet van undercoveroperaties. Opsporingsdossiers bieden daarmee een rijk inzicht in onder andere de activiteiten van daders en de wijze waarop zij zich tot elkaar en hun omgeving verhouden. De uitgebreide verslagen die van deze opsporingsdossiers zijn gemaakt, stellen ons vooral in staat om onderbouwde, kwalitatieve uitspraken te doen over de *aard* van de georganiseerde criminaliteit in Nederland. Uitspraken over *hoe vaak* bijvoorbeeld een bepaalde werkwijze voorkomt, kunnen alleen binnen de context van de bestudeerde zaken worden gedaan; ze kunnen niet worden veralgemeniseerd naar *de* georganiseerde criminaliteit.[13]
Opsporingsdossiers vormen een rijke bron, maar kennen beperkingen. Zo zijn alleen gevallen van georganiseerde criminaliteit meegenomen die door Nederlandse autoriteiten zijn opgespoord en onder de door ons gehanteerde begripsomschrijving van georganiseerde criminaliteit vallen. Datgene wat buiten het zicht van de Nederlandse opsporings-

13 Wel is vanwege het grote aantal zaken dat inmiddels binnen de Monitor Georganiseerde Criminaliteit is bestudeerd (180, waarin informatie aanwezig is over in totaal honderden verdachten), het doen van kwantitatieve analyses op specifieke deelterreinen mogelijk, mits daarbij het genoemde voorbehoud wordt gemaakt. Voorbeelden hiervan zijn: de analyse van criminele carrières (Van Koppen 2013), analyse van investeringen van daders in de legale economie (Kruisbergen e.a. 2015), analyse van de rechtsgang en de incasso bij ontnemingsmaatregelen (Kruisbergen e.a. 2016) en de analyse van geëiste en opgelegde straffen (Van Wingerde & Van de Bunt 2017).

doi: 10.5553/JV/016758502018044005003

praktijk valt, blijft ook buiten het bereik van ons onderzoek. Voor cybercrime werkt deze beperking mogelijk sterker uit dan bij andere vormen van georganiseerde criminaliteit. Juist bij cybercrime kan in de modus operandi of dadergroepering namelijk sprake zijn van een internationale component en bovendien komen lang niet alle door politie en justitie gepleegde interventies tegen cybercrime uiteindelijk terecht in individuele opsporingsdossiers.[14]

Mogelijke beleidsimplicaties

Cryptovaluta vormen een belangrijke financiële innovatie. Het is ook een belangrijke, door technologie gedreven vernieuwing in de werkwijze bij witwassen. Samen met onder andere prepaidkaarten is het een van de weinige veranderingen binnen opgespoorde witwasvormen, die verder vooral door traditionele, beproefde werkwijzen worden gedomineerd. Dit zien we in ons casusmateriaal, maar komt ook naar voren uit een analyse van vier criminaliteitsbeeldanalyses op het terrein van witwassen, die tezamen een periode van twaalf jaar beslaan (Soudijn 2018).
Cryptovaluta zoals bitcoin zijn op dit moment grotendeels ongereguleerd. Ook aanverwante diensten vallen nu grotendeels buiten financiele regulering en toezicht, waardoor bijvoorbeeld bitcoin exchangers niet meldplichtig zijn in het kader van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). Nieuwe criminele werkwijzen, zoals het gebruik van bitcoin, roepen de vraag op of bestaande wet- en regelgeving voldoende is toegerust voor de nieuwe situatie. Met andere woorden, moeten cryptovaluta worden gereguleerd? Dit is natuurlijk een puur beleidsmatige, politieke keuze. Een voordeel van regulering is dat regulering en toezicht aangrijpingspunten kunnen bieden om witwassen via cryptovaluta tegen te gaan. Online wisselkantoren voor cryptovaluta zouden zo bijvoorbeeld onder het bereik van Nederlandse toezichthouders kunnen worden gebracht. Vanuit antiwitwasperspectief kan regulering echter ook nadelen hebben. De acceptatie van cryptovaluta in de reguliere economie lijkt op dit moment nog laag; wie een glas cola wil kopen, een nieuwe spijkerbroek, een auto of een huis, kan dit meestal niet met bitcoin doen. Regulering kan bijdragen aan normalisering van cryptovaluta en een

14 Voor een meer uitgebreide bespreking, zie Kruisbergen e.a. (2018, p. 24-31, 102-103).

doi: 10.5553/JV/016758502018044005003

hogere acceptatiegraad van deze nieuwe 'munten' als betaalmiddel. Daarmee zouden de mogelijkheden om op criminele wijze verdiende cryptovaluta in de reguliere economie om te zetten, wit te wassen, juist worden vergroot (zie ook Oerlemans e.a. 2016).
Ondanks de innovatie die cryptovaluta (samen met enkele andere vernieuwingen, zie Soudijn 2018) wel degelijk zijn, speelt contant geld nog steeds een hoofdrol in de criminele wereld, ook wanneer de criminelen zich met online activiteiten bezighouden (zie ook Europol 2015; Oerlemans e.a. 2016; Soudijn 2018). De prominente rol die contant geld speelt, biedt verschillende aanknopingspunten voor opsporing en beleid. Bij verschillende vormen van ICT-gerelateerde criminaliteit is het incasseren of omwisselen van de opbrengsten een fase waarin daders kwetsbaar zijn. Deze flessenhals in het criminele bedrijfsproces geldt bijvoorbeeld voor daders van banking malware en phishing die hun digitale euro's willen omwisselen in contanten. Hij doet zich ook voor bij de drugshandelaren die hun op het darknet verdiende cryptovaluta willen omruilen voor contante euro's. De flessenhals bestaat eruit dat daders in deze fase nogal eens, direct of indirect, in contact komen met de reguliere omgeving, zoals het reguliere bankverkeer. Dat biedt kansen voor detectie, opsporing en uiteindelijk preventie.[15]
Hebben daders eenmaal contant geld in handen – als directe opbrengst van bijvoorbeeld traditionele offline drugshandel, of indirect nadat daders hun digitale valuta voor fysiek geld hebben omgewisseld –, dan vindt het een bestemmingsdoel.[16] Ons casusmateriaal geeft aanleiding te vermoeden dat veel op criminele wijze verdiend geld in contante vorm zijn weg vindt in de reguliere economie. Ook andere studies tonen dit aan (Soudijn 2017; Kruisbergen e.a. 2012; Soudijn & Akse 2012). Daarbij gaat het om de dagelijkse uitgaven van daders (die al aanzienlijk kunnen zijn), maar ook om uitgaven aan onder meer reizen, auto's, inrichting en woonruimte. Bij dit (afgeschermd) consumeren kunnen daders gebruikmaken van stromannen of gespecialiseerde dienstverleners, die daders bijvoorbeeld in staat stellen om woonruimte of auto's te gebruiken zonder dat dit tot hun

15 Het *cashen* van geld bij bijv. banking malware via money mules houdt in dat deze money mules hun reguliere bankrekening beschikbaar stellen. Ook bij het omwisselen van bitcoins voor euro's kan (indirect) contact met het reguliere betalingsverkeer ontstaan. Dit is bijv. het geval wanneer een individuele bitcoinwisselaar de door hem opgekochte bitcoins zelf ook wil omwisselen en daarvoor (uiteindelijk) van een reguliere partij gebruikmaakt.
16 Die bestemming kan er ook uit bestaan dat het geld in eerste instantie wordt bewaard of verplaatst.

doi: 10.5553/JV/016758502018044005003

persoon herleidbaar is. Daders worden echter ook, bewust of onbewust, gefaciliteerd door verkopers die hun kostbare goederen of diensten zonder problemen contant laten betalen.
Vanwege de dominante rol die contant geld speelt in offline én online criminaliteit, kan ook de aanpak van cybercriminaliteit profiteren van generieke maatregelen tegen contante criminele geldstromen.[17] Het bemoeilijken van onder andere consumptie van criminele verdiensten, door bijvoorbeeld het verhogen van het bewustzijn of het uitbreiden van de meldingsplicht, kan hieraan een zinvolle bijdrage leveren.

Literatuur

Bruinsma & Bovenkerk 1996
G.J.N. Bruinsma & F. Bovenkerk (red.), *De georganiseerde criminaliteit in Nederland: de branches*, Den Haag: Sdu Uitgevers 1996.

Europol 2015
Europol, *Why is cash still king? A strategic report on the use of cash by criminal groups as a facilitator for money laundering*, Den Haag: European Police Office 2015.

Kleemans e.a. 2002
E.R. Kleemans, M.E.I. Brienen & H.G. van de Bunt, m.m.v. R.F. Kouwenberg, G. Paulides & J. Barensen, *Georganiseerde criminaliteit in Nederland. Tweede rapportage op basis van de WODC-monitor* (O&B 198), Den Haag: Boom Juridische uitgevers 2002.

Van Koppen 2013
M.V. van Koppen, *Pathways into organized crime: Criminal opportunities and adult-onset offending* (diss. Amsterdam VU), Alblasserdam: Haveka 2013.

Kruisbergen & Soudijn 2015
E.W. Kruisbergen & M.R.J. Soudijn, 'Wat is witwassen eigenlijk? Introductie tot theorie en praktijk', *Justitiële verkenningen* 41 2015, afl. 1, p. 10-23.

Kruisbergen e.a. 2012
E.W. Kruisbergen, H.G. van de Bunt & E.R. Kleemans, *Georganiseerde criminaliteit in Nederland. Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit* (O&B 306), Den Haag: Boom Lemma 2012.

17 Het gebruik van grote coupures door daders (en anderen) wordt op termijn bemoeilijkt doordat de ECB in 2018 zal stoppen met de productie van nieuwe € 500-biljetten.

doi: 10.5553/JV/016758502018044005003

Kruisbergen e.a. 2015
E.W. Kruisbergen, E.R. Kleemans & R.F. Kouwenberg, 'Profitability, power, or proximity? Organized crime offenders investing their money in legal economy', *European Journal on Criminal Policy and Research* (21) 2015, afl. 2, p. 237-256.

Kruisbergen e.a. 2016
E.W. Kruisbergen, E.R. Kleemans & R.F. Kouwenberg, 'Explaining attrition: Investigating and confiscating the profits of organized crime', *European Journal of Criminology* (13) 2016, afl. 6, p. 677-695.

Kruisbergen e.a. 2018
E.W. Kruisbergen, E.R. Leukfeldt, E.R. Kleemans & R.A. Roks, *Georganiseerde criminaliteit en ICT. Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit* (Cahier 2018-8), Den Haag: WODC 2018.

Leukfeldt 2014
E.R. Leukfeldt, 'Cybercrime and social ties: Phishing in Amsterdam', *Trends in Organized Crime* (17) 2014, afl. 4, p. 231-249.

Leukfeldt e.a. 2017
E.R. Leukfeldt, E.R. Kleemans & W.P. Stol, 'Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks', *British Journal of Criminology* 2017, DOI:10.1093/bjc/azw009.

Meiklejohn e.a. 2013
S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G.M. Voelker & S. Savage, *A fistful of bitcoins: Characterizing payments among men with no names*, San Diego: University of California 2013.

Odinot e.a. 2017
G. Odinot, M.A. Verhoeven, R.L.D. Pool & C.J. de Poot, *Organised cybercrime in the Netherlands: Empirical findings and implications for law enforcement*, Den Haag: WODC 2017.

Oerlemans e.a. 2016
J.J. Oerlemans, B.H.M. Custers, R.L.D. Pool & R. Cornelisse, *Cybercrime en witwassen: bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware* (O&B 319), Den Haag: Boom criminologie 2016.

Ron & Shamir 2013
D. Ron & A. Shamir, 'Quantitative analysis of the full bitcoin transaction graph', in: A.-R. Sadeghi (red.), *Financial cryptography and data security. Lecture notes in computer science* (Vol. 7859), Heidelberg: Springer 2013, p. 6-24.

Soudijn 2017
M.R.J. Soudijn, *Witwassen. Criminaliteitsbeeldanalyse 2016*, Zoetermeer: Politie, Landelijke Eenheid, Dienst Landelijke Informatieorganisatie 2017.

doi: 10.5553/JV/016758502018044005003

Soudijn 2018
M.R.J. Soudijn, 'Using police reports to monitor money laundering developments. Continuity and change in 12 years of Dutch money laundering crime pattern analyses', *European Journal on Criminal Policy and Research* 2018, DOI:10.1007/s10610-018-9379-0.

Soudijn & Akse 2012
M.R.J. Soudijn & Th. Akse, *Witwassen. Criminaliteitsbeeldanalyse 2012*, Driebergen: KLPD, Dienst Nationale Recherche 2012.

Soudijn & Reuter 2016
M.R.J. Soudijn & P. Reuter, 'Cash and carry: The high cost of currency smuggling in the drug trade', *Crime, Law and Social Change* (66) 2016, afl. 3, p. 271-290.

Van Wingerde & Van de Bunt 2017
C.G. van Wingerde & H.G. van de Bunt, *Geëiste en opgelegde straffen bij de strafrechtelijke afhandeling van georganiseerde criminaliteit. Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit*, Apeldoorn: Politie & Wetenschap 2017.

doi: 10.5553/JV/016758502018044005003

Georganiseerde kinderporno-netwerken op het darkweb

Madeleine van der Bruggen*

Sinds enkele jaren komen vanuit politieorganisaties en internationale media steeds meer signalen over grootschalige kinderpornonetwerken op het darkweb. Op deze darkweb-websites, oftewel forums, wordt niet alleen het uitwisselen van kinderpornografisch materiaal en informatie met betrekking tot kindermisbruik gefaciliteerd, maar ook de (technische) afscherming ervan.[1] Bovendien zijn deze websites tegenwoordig, in tegenstelling tot het recente verleden, toen deze nog voornamelijk werden bezocht door verdachten met uitzonderlijke technische kennis, ook eenvoudig bereikbaar voor de groep minder technisch geavanceerde verdachten. De veronderstelling bestaat dat dit een belangrijke oorzaak is van de toename van het volume van illegaal materiaal dat online uitgewisseld wordt (Europol 2016).
Psychologisch onderzoek naar het fenomeen kinderporno is omvangrijk; denk hierbij aan onderzoek naar het classificeren van kinderpornodaders op basis van type delict en motivatie (bijv. Merdian e.a. 2013; Shelton e.a. 2016) en onderzoek naar parafilieën en behandelwijzen (bijv. Krueger e.a. 2009; Seto & Ahmed 2014). Criminologisch onderzoek, en zeker onderzoek naar kinderporno op verborgen darkweb-netwerken, is minder omvangrijk. Het feit dat zowel psychologisch als criminologisch onderzoek grotendeels gebaseerd is op kinderpornoplatforms op het open internet, betekent dat de wetenschappelijke kennis over dit thema enigszins verouderd is. Een belangrijke verklaring hiervoor is dat data op dergelijke anonieme netwerken grotendeels illegaal van aard zijn, en daardoor moeilijk beschikbaar voor wetenschappers. Hiernaast baseert onderzoek zich overwegend op strafdossiers, en daarmee op de groep (ex-)veroordeelden zichtbaar

* M. van der Bruggen MSc MA is als promovendus verbonden aan de Universiteit Leiden en werkzaam bij de Dienst Landelijke Recherche van de Nationale Politie.

1 Zie https://www.europol.europa.eu/newsroom/news/major-online-child-sexual-abuse-operation-leads-to-368-arrests-in-europe?_sp=cb05b05e-de4a-4de3-96ac-7cb8a8da572f.1498809972275 en https://www.vg.no/spesial/2017/undercover-darkweb/?lang=en, geraadpleegd op 27 juni 2018.

doi: 10.5553/JV/016758502018044005004

voor de politie. De verborgen ontoegankelijke groepen als darkwebforumgebruikers, en zeker de technisch meest geavanceerde personen, zijn nog weinig onderzocht (Duijn & Klerks 2014; Westlake & Bouchard 2016; Zulkarnine e.a. 2016). Dit betekent dat de huidige kennis gebaseerd is op enkel een gedeelte van de volledige verdachtenpopulatie.
Dit artikel geeft suggesties voor onderzoek naar de meer verborgen netwerken en onbekende verdachten. Middels een literatuurstudie wordt de vraag beantwoord hoe de digitalisering het criminaliteitsgebied van de kinderporno heeft veranderd. Allereerst wordt een korte historische ontwikkeling geschetst van de ontwikkeling van kinderporno op papier naar kinderporno in illegale en anonieme digitale netwerken op het darkweb. Vervolgens komen de gevolgen van het bestaan van dergelijke netwerken voor het criminaliteitsbeeld van kinderporno aan de orde. Theoretisch wordt betoogd dat een ontwikkeling heeft plaatsgevonden van kinderporno als een overwegend individueel delict naar een delict gepleegd in georganiseerd verband binnen netwerken. Het artikel sluit af met aanbevelingen voor wetenschappelijk onderzoek en de opsporingspraktijk.

Een historische ontwikkeling van het criminaliteitsbeeld van de kinderporno

Kinderporno heeft met de komst van het digitale tijdperk grote ontwikkelingen doorgemaakt. De eerste mogelijkheden voor het vastleggen van kindermisbruik ontstonden met de uitvinding van de camera. Producenten van kinderporno waren echter nog steeds genoodzaakt om uit hun anonimiteit te treden om het materiaal te verkopen of te verspreiden, bijvoorbeeld met tussenkomst van een seksshop of via een postorderbedrijf (Van der Bruggen 2015; Oerlemans 2010). De groep die elkaar daadwerkelijk ontmoette en steun bij elkaar zocht, was logischerwijs klein, omdat dit in het fysieke leven plaats moest vinden (Owens e.a. 2016).
Aan het eind van de jaren negentig kwam het internet beschikbaar voor het grote publiek. Daarmee werden het gemak en de behoefte om zich te verenigen onder kinderpornoliefhebbers groter. Er vond met andere woorden een verplaatsing plaats van fysieke naar digitale ontmoetingsplekken (Felson 2006; Soudijn & Zegers 2012). Ook al veran-

doi: 10.5553/JV/016758502018044005004

derden de digitale locatie en vorm van dergelijke platforms door de jaren heen, vanaf het begin al lag de nadruk op het vormen van community's, gekenmerkt door het promoten en normaliseren van seks met kinderen en het delen van ervaringen en fantasieën (Durkin & Bryant 1999; O'Halloran & Quayle 2010). Dergelijke groepen waren in deze begintijd van het internet echter nog altijd slechts beschikbaar en bereikbaar voor een relatief kleine groep mensen. De nadruk lag niet op het plegen van strafbare feiten in de vorm van het delen van kinderpornografisch materiaal. Het hoofddoel van deze netwerken was daarentegen zelfhulp en het communiceren met gelijkgestemden. De internetactiviteiten van personen met een seksuele interesse in kinderen veranderden met de groei van het internet en het ontstaan van gedecentraliseerde en semianonieme *peer-to-peer* (p2p-)netwerken. Door de mogelijkheden om bestanden rechtstreeks te delen van computer naar computer zonder tussenkomst van een centrale server (Steel 2009) vond een transitie plaats naar nadruk op het uitwisselen van strafbaar materiaal. Daarnaast zorgde de toegenomen snelheid waarmee bijvoorbeeld foto's en video's gedeeld konden worden ervoor dat kinderpornocriminaliteit in een dynamiek van vraag en aanbod terechtkwam. Uit onderzoek is gebleken dat een percentage van 1 tot 3% van alle zoektermen op p2p-websites kinderpornogerelateerd is. Verder is de groep mensen die kinderpornografisch materiaal daadwerkelijk beschikbaar stelt, oftewel host, klein, maar heeft wel een enorm bereik (Hughes e.a. 2006; Steel 2009). Kortom: de vraag is groter dan het aanbod. Het gevaar van deze netwerken is derhalve niet alleen de normalisering van kindermisbruik, maar ook het beschikbaar zijn van kinderporno voor een grote groep potentieel nieuwsgierige en impulsieve gebruikers. De drempel tot het plegen van strafbare feiten wordt hiermee verlaagd. Binnen deze p2p-netwerken ligt de nadruk minder op het delen van ervaringen en gevoelens dan bij de vroegere zelfhulpgroepen. Wel hebben sommige van dergelijke websites rankingsystemen en geven ze deelnemers de mogelijkheid om het gedownloade materiaal te becommentariëren (Prichard e.a. 2011). Om deze reden kunnen p2p-netwerken worden gezien als een eerste stap richting illegale kinderpornonetwerken, aangezien het uitwisselen van kinderporno op grote schaal en op georganiseerde wijze gefaciliteerd wordt.

doi: 10.5553/JV/016758502018044005004

Kinderporno in illegale en anonieme netwerken op het darkweb

Op het darkweb kunnen tegenwoordig subculturen worden gevonden waarbinnen, in vergelijking met p2p-netwerken, intensief en gedetailleerd gecommuniceerd wordt. Kinderpornoforums op het darkweb zijn qua opbouw vrijwel identiek aan legale forums op het normale internet: leden melden zich aan door middel van het aanmaken van een *nickname* en wachtwoord en krijgen vervolgens toegang tot het publieke deel van het forum. Hierbinnen wordt met elkaar gecommuniceerd binnen *threads*: series van berichten gecentreerd rondom een bepaald thema. Voorbeelden van thema's: categorieën van kinderpornografisch materiaal (bijvoorbeeld jongens versus meisjes, *hardcore* versus *soft-core, teen* versus *pre-teen*), informatieve secties (bijvoorbeeld over technieken omtrent computerveiligheid en technische afscherming of het plegen van kindermisbruik) en secties met betrekking tot forumbeheer waar administrators leden welkom heten en de huisregels uitleggen (Van der Bruggen e.a. 2018; Goodman 2015; Moerenhout 2012). Leden kunnen een stelling poneren of een vraag stellen binnen passende forumonderdelen, waar andere leden vervolgens op reageren (Van Remunt & Van Wilsem 2016). De meeste forums kennen een hiërarchische structuur, waarbij leden een status (bijvoorbeeld *member, VIP member*, moderator) toegewezen krijgen afhankelijk van bijvoorbeeld de mate van activiteit, het type van gedeeld materiaal en de rol binnen het forum. Soms krijgen leden met een hogere status toegang tot verborgen delen op het forum, wat vaak gepaard gaat met een grotere mate van prestige en autoriteit (Bartlett 2014; Boerman e.a. 2017). Omdat veiligheid en anonimiteit cruciaal zijn voor het voortbestaan van illegale forums, kennen deze forums strikte veiligheidsvoorschriften, waarop wordt toegezien door de forumadministrators en -moderators. Wanneer forumregels worden overtreden, kunnen de administrators deze leden straffen of zelfs van het forum verwijderen. Informatie afkomstig van politiediensten en de media laat zien dat deze netwerken groeien en dat leden vaak gedurende lange tijd en ook op verschillende platforms tegelijk actief zijn (Europol 2016; Moerenhout 2012).[2]

2 Zie https://www.thelocal.de/20170706/police-bust-online-child-porn-ring-with-nearly-90000-members, geraadpleegd op 27 juni 2018, en https://www.europol.europa.eu/newsroom/news/major-online-child-sexual-abuse-operation-leads-to-368-arrests-in-europe?_sp=cb05b05e-de4a-4de3-96ac-7cb8a8da572f.1498809972275, geraadpleegd op 27 juni 2018.

doi: 10.5553/JV/016758502018044005004

Gevolgen voor het criminaliteitsbeeld

De toegenomen digitale mogelijkheden hebben grote gevolgen gehad voor het criminaliteitsbeeld en de opsporing van kinderporno. Hierin zijn drie parallel lopende ontwikkelingen te onderscheiden. Allereerst rapporteren opsporingsinstanties en media dat kinderpornoverdachten met enige technische basiskennis en belang hechtend aan technische veiligheid, zich verplaatst hebben naar anonieme websites op het darkweb. Het darkweb is daarom niet alleen maar beschikbaar voor de technisch meest geavanceerde verdachten; het gros van de kinderpornoliefhebbers en potentieel geïnteresseerden weet inmiddels zijn weg te vinden (Europol 2016; Goodman 2015).[3] Met de beschikbaarheid en toegankelijkheid van het volledig anonieme darkweb voor het grote publiek is de drempel tot het bekijken en verspreiden van kinderpornografisch materiaal verlaagd, wat mogelijk geleid heeft tot een verbreding van de daderpopulatie. Het is niet ondenkbaar dat mensen die voorheen vanwege de zichtbaarheid en de pakkans op het normale internet een rem voelden om kinderporno te downloaden, deze rem nu niet meer ervaren door de anonimiteit van het darkweb. Bovendien zetten forumdeelnemers elkaar actief aan tot het plegen van misbruik. Zo is een nieuw platform ontstaan waar seks met kinderen op grote schaal genormaliseerd en aangemoedigd wordt (Owens e.a. 2016; Shelton e.a. 2016).

Als tweede ontwikkeling bevorderen de anonimiteit en het feit dat de netwerken enkel bestaan uit gelijkgestemden het communityaspect: forumleden leren elkaar kennen als vrienden en ontwikkelen langdurige relaties (Boerman e.a. 2017; Goodman 2015). Communicatie wordt gekenmerkt door respect voor en erkenning van elkaars gevoelens. Dit gevoel van het deel uitmaken van een subcultuur heeft ertoe geleid dat er niet alleen actief over strafbaar kinderpornografisch materiaal gecommuniceerd wordt. Communicatie gaat ook over onderwerpen als seksualiteit, achtergronden en motivaties van verdachten, en over organisatorische onderwerpen zoals forummanagement en techniek. Het is op cybercriminele darkweb-forums dus vele malen makkelijker geworden om in contact te komen met mededaders, onder wie daders met bepaalde (technische) vaardighe-

3 Zie https://www.vg.no/spesial/2017/undercover-darkweb/?lang=en, geraadpleegd op 27 juni 2018, en https://www.thelocal.de/20170706/police-bust-online-child-porn-ring-with-nearly-90000-members, geraadpleegd op 27 juni 2018.

doi: 10.5553/JV/016758502018044005004

den, wat de criminele mogelijkheden van de groep vergroot (Leukfeldt e.a. 2017).
Ten derde heeft de toegenomen anonimiteit, en de hiermee gepaard gaande beperkte externe controle, ertoe geleid dat op deze forums de nadruk expliciet is gaan liggen op het plegen van strafbare feiten. In tegenstelling tot p2p-netwerken, die hoofdzakelijk gebruikt worden voor het downloaden van allerlei legaal materiaal (zoals muziek en films), zijn de duizenden tot honderdduizenden geregistreerde leden van darkweb-kinderpornoforums allemaal mensen die bewust op zoek zijn naar kinderporno en bereid om de grens van het strafbare te overschrijden (Van der Bruggen e.a. 2018). De (al dan niet terecht) ervaren garantie van anonimiteit, gecombineerd met het feit dat deze netwerken enkel bestaan uit gelijkgestemden, zorgt voor een extra drempelverlaging als het gaat om zowel het aanzetten tot en het plegen van strafbare feiten als het delen van persoonlijke fantasieën en ervaringen.
Bovenstaande ontwikkelingen hebben ertoe geleid dat het aantal daders dat samenkomt in darkweb-netwerken, vele malen groter is dan het aantal daders dat elkaar voorheen fysiek opzocht. Vanwege deze schaalvergroting hebben forums zich ontwikkeld tot georganiseerde en hiërarchische structuren met deelnemers met verschillende rollen en functies, waarin een bepaalde mate van sturing en toezicht noodzakelijk is geworden. Kinderpornonetwerken op het darkweb lijken hiermee veel op criminele structuren, oftewel criminele organisaties (Von Lampe 2016).

Georganiseerde kinderporno

Met kinderpornoforums op het darkweb is een professionele en georganiseerde modus operandi van kinderpornocriminaliteit ontstaan, waarbij geopereerd wordt binnen flexibele digitale structuren. Vooral de criminelen in de top van de netwerken werken in grote mate met elkaar samen binnen gelieerde forums, oftewel criminele verbanden. Hierbinnen worden langdurige relaties opgebouwd, rollen aangenomen en taakverdelingen op verschillende niveaus gemaakt. Op het darkweb zijn community's ontstaan, waarvan zowel producenten en consumenten als faciliteerders deel uitmaken. De ontstane situatie kent parallellen met de georganiseerde misdaad, waarvan volgens

doi: 10.5553/JV/016758502018044005004

Fijnaut (1996) sprake is wanneer (a) een groep mensen (b) systematisch misdrijven pleegt met ernstige gevolgen voor de samenleving en (c) deze misdrijven op effectieve wijze afschermt. Kinderporno op het darkweb voldoet echter niet volledig aan het laatste criterium van de georganiseerde misdaad volgens Fijnaut (1996): (d) primair gericht op illegaal gewin. Ook al zijn er aanwijzingen dat binnen kleine subgroepen sprake is van betalingen met bitcoins om toegang te krijgen tot unieker kinderpornografisch materiaal, in zijn algemeenheid lijkt kinderporno op het darkweb (nog) geen handel met primair een financieel oogmerk (Europol 2016).

Ergo: volgens deze traditionele en enge definitie van georganiseerde misdaad is kinderporno op het darkweb geen georganiseerde misdaad. Beargumenteerd kan echter worden dat deze conclusie geen recht doet aan de situatie, omdat het om ernstige misdrijven gaat en er wel degelijk sprake is van een bepaalde mate van organisatie. Theoretisch gezien past het fenomeen wel binnen het moderne analytische *framework* van de georganiseerde misdaad van Von Lampe (2016), die stelt dat groepen in verschillende maten georganiseerd kunnen zijn. Hij beschrijft georganiseerde criminaliteit als een flexibel en dynamisch fenomeen in verschillende contexten, en noemt kinderporno expliciet als voorbeeld hiervan. De operationalisering van georganiseerde misdaad bestaat uit het beschrijven van criminele organisaties aan de hand van hun criminele activiteiten, de criminele en sociale structuur die ten grondslag aan de organisatie ligt, en de buitenwettelijke zelfregulatie die binnen de organisatie plaatsvindt (Von Lampe 2016).

Het eerste kenmerk van de georganiseerde misdaad volgens Von Lampe (2016) betreft de criminele activiteiten. De kern hiervan is in het geval van kinderpornonetwerken op het darkweb door de jaren heen niet veel veranderd. Werden vroeger kinderpornografische afbeeldingen uitgewisseld middels p2p-netwerken of papieren kopieën, thans is het uitwisselingsmedium gemoderniseerd. Het financiële gewin dat de traditioneel georganiseerde misdaad kenmerkte, wordt binnen deze netwerken niet zichtbaar in de vorm van geldelijk gewin, maar in de non-monetaire uitwisseling van illegale commoditeiten (Von Lampe 2016). Met andere woorden: de 'economische' functie van de criminele activiteiten bestaat uit het genereren van materieel gewin in de vorm van het verkrijgen en delen van nieuwer en uniek materiaal, wat de onderhandeling voor zowel aanbieder

doi: 10.5553/JV/016758502018044005004

als afnemer lucratief maakt. Binnen kinderpornonetwerken op het darkweb zijn echter een zekere variatie, continuïteit en complexiteit zichtbaar wat betreft deze criminele activiteiten. Naast illegaal materiaal wordt op grote schaal relevante informatie gedeeld ten behoeve van het uitbreiden van de criminele activiteiten en het behouden en verbeteren van de criminele netwerken, resulterend in 'criminal social capital' (McCarthy & Hagan 2001). Hierbij valt te denken aan informatie met betrekking tot het misbruiken van kinderen (waar zelfs handleidingen voor beschikbaar zijn),[4] de meest (technisch) veilige manieren om kinderporno te maken en verspreiden, en de technische afscherming van criminele activiteiten om zich te beschermen tegen interventie van politie en justitie (Boerman e.a. 2017; Europol 2016; Goodman 2015; Moerenhout 2012; VG 2017).

Het tweede kenmerk volgens Von Lampe (2016) betreft de criminele en sociale structuur die ten grondslag aan de organisatie ligt. Bovengenoemde intensieve communicatie heeft er niet alleen toe geleid dat kinderpornonetwerken op het darkweb gebruikt worden voor het plegen van strafbare feiten (criminele activiteiten), maar ook dat er met deze forums sociale verenigingen of platforms zijn ontstaan waar gelijkgestemden elkaar vinden. Deze platforms worden gekenmerkt door een hiërarchie en rolverdeling die ondersteunend zijn voor de criminele activiteiten en deze in stand houden en promoten. De sociale en emotionele functie bestaan eruit dat binnen de netwerken seks met kinderen expliciet genormaliseerd en zelfs gepromoot wordt. Dit leidt ertoe dat de band tussen mensen met een seksuele interesse in kinderen versterkt wordt, en er een groepsgevoel gecreëerd wordt waarin deviante normen en waarden prevaleren (Europol 2016; O'Halloran & Quayle 2010; Prichard e.a. 2011; Westlake & Bouchard 2016). Netwerkleden kúnnen nog altijd autonome beslissingen nemen in het plegen van strafbare feiten, maar de verleiding hiertoe wordt wel expliciet aangemoedigd. Hieraan ligt een bepaalde mate van vertrouwen ten grondslag, zich uitend in loyaal, respectvol en vriendelijk gedrag richting de community. Behalve crimineel sociaal kapitaal wordt dus ook emotioneel kapitaal gehaald binnen dergelijke netwerken, omdat het groepsgevoel sterk aanwezig is (Prichard e.a. 2011).

4 Over dit zogenoemde 'pedohandboek' worden in 2018 Kamervragen gesteld aan de minister van Justitie en Veiligheid, waarop door de minister wordt geantwoord op 15 juni 2018 middels Kamerstuknr. 2018Z05871, p. 1–4.

doi: 10.5553/JV/016758502018044005004

Tot slot het derde kenmerk volgens Von Lampe (2016): de buitenwettelijke zelfregulatie die binnen de organisatie plaatsvindt. Ook deze is goed zichtbaar binnen de strikt hiërarchische kinderpornonetwerken op het darkweb: de autoriteit en de bevoegdheid tot het maken van interne beleidsmatige keuzes worden uitgeoefend door 'admins' en 'moderators'. Ook al wordt het darkweb, en meer specifiek kinderpornonetwerken op het darkweb, door burgers en media soms omschreven als platform zonder regels, waar alle criminaliteit is toegestaan, niks is minder waar. De meeste kinderpornonetwerken hebben een bepaalde focus: er wordt controle gehouden op het delen van een bepaald soort kinderpornografisch materiaal. Hierbij valt te denken aan het al dan niet toestaan van beeldmateriaal met gewelddadige handelingen of marteling en het al dan niet toestaan van materiaal met slachtoffers van beide geslachten. Grenzen, regels en interne discipline zijn dus duidelijk omschreven en staan onder controle. Juist omdat binnen kinderpornonetwerken ten behoeve van regulering geen legaal centraal gezag aanwezig is, is een bepaalde mate van zelfregulatie noodzakelijk. 'Admins' en 'moderators' schrijven expliciete en strikte gedragsregels voor en kunnen maatregelen treffen wanneer netwerkleden zich niet houden aan de interne regels (Europol 2016; Goodman 2015; Moerenhout 2012; VG 2017). Ook lossen zij eventuele conflicten tussen leden onderling op, wanneer het risico bestaat dat die het netwerk in gevaar brengen. Het uiteindelijke doel is dus om het netwerk te laten voortbestaan en te beschermen tegen interventie van politie en justitie of actoren met kwade bedoelingen. De rollen en taken, en daarmee de macht en status, zijn duidelijk verdeeld, waarbij bepaalde vaardigheden dus noodzakelijk zijn voor het voortbestaan ervan.

Conclusie: kinderpornoforums op het darkweb kennen een hoge mate van organisatie en bieden een platform waar in relatieve anonimiteit illegale activiteiten kunnen worden ontplooid, waar criminele en sociale verenigingen worden gevormd, en waar de top van het netwerk zorgt voor de regulering van zijn criminele organisatie (Von Lampe 2016).

doi: 10.5553/JV/016758502018044005004

Tot slot

Samenvattend kan worden geconcludeerd dat de digitalisering en het ontstaan van kinderpornoforums op het darkweb grote veranderingen hebben meegebracht voor het criminaliteitsbeeld van de kinderporno. Er is een grotere mate van professionaliteit zichtbaar en een transitie van overwegend individuele verdachten naar verdachten die gezamenlijk en anoniem opereren in netwerken. Dit heeft ertoe geleid dat de beschikbaarheid van het illegale materiaal vergroot en de drempel tot het downloaden ervan verlaagd is binnen groepen waarin daderschap actief aangemoedigd en gefaciliteerd wordt (Bartlett 2014; Boerman e.a. 2017; Westlake & Bouchard 2016). De uitwisseling van kinderporno via het internet is op zichzelf niet nieuw en het zoeken naar gelijkgestemden, de bevestiging en het uiten van fantasieën evenmin. De combinatie van de expliciete focus op het plegen van strafbare feiten en de communicatieve openheid in het delen van ervaringen en onderlinge advisering op deze grote schaal, en de mate van organisatie en professionaliteit die hier noodzakelijkerwijs aan ten grondslag ligt, is echter wel nieuw. Voornamelijk de buitenwettelijke zelfregulatie die darkweb-kinderpornoforums kenmerkt, heeft ertoe geleid dat het proces van verzamelen en verspreiden van kinderporno steeds meer trekken gekregen heeft van georganiseerde misdaad. De relatief eenvoudige dynamiek van vraag en aanbod is met andere woorden vervangen door een modus operandi met georganiseerde en sociale structuren.

Criminologisch wetenschappelijk onderzoek heeft nog niet voldoende meebewogen met deze ontwikkelingen. Data van kinderpornonetwerken op het darkweb zijn voor veel onderzoekers ontoegankelijk vanwege hun illegale aard. Daarom is samenwerking van academische onderzoekers met toegepaste onderzoekers werkend in de opsporingspraktijk noodzakelijk. Daarnaast kunnen bijvoorbeeld cybercrime- en *data science*-onderzoek een bijdrage leveren. Kinderpornonetwerken moeten worden gezien als omgevingen met rijke informatie over criminele verbanden en processen. Netwerken bestaan uit veelomvattende relatie- en communicatiedata, die gebruikt kunnen worden om kennis te verzamelen over de werking en de onderliggende structuren van de community's. Derhalve biedt dit mogelijkheden voor automatische en kwantitatieve netwerkanalyses en het detecte-

doi: 10.5553/JV/016758502018044005004

ren van *key players* (Van der Bruggen e.a. 2018; Duijn & Klerks 2014; Frank e.a. 2010; Van Remunt & Van Wilsem 2016; Zulkarnine e.a. 2016).

De realiteit is dat in de fysieke wereld kinderen misbruikt worden, mede omdat op het darkweb criminele organisaties in stand gehouden moeten worden, en gevoed moeten blijven met nieuw en uniek kinderpornografisch materiaal. Tegenwoordig is het devies voor de opsporing om minder te zoeken naar individuele daders, maar om op zoek te gaan naar de *key players* die de criminele organisatie draaiend houden. Dat is weliswaar gecompliceerd en tijdrovend, maar wanneer deze verdachten aangehouden worden zal de organisatie naar verwachting maximaal verstoord worden. Hierbij dient bovendien rekening te worden gehouden met de bevinding dat samenwerkingsverbanden flexibel zijn, en dat criminele partners elkaars rollen kunnen overnemen. Meer kennis over deze samenwerkingsverbanden kan leiden tot een sterkere informatiegestuurde en effectieve opsporing, waarin tactische keuzes gemaakt worden, gevoed door wetenschappelijke kennis.

Literatuur

Bartlett 2014
J. Bartlett, *The Dark Net: Inside the digital underworld*, Portsmouth, UK: William Heinemann 2014.

Boerman e.a. 2017
F. Boerman, M. Grapendaal, F. Nieuwenhuis & E. Stoffers, *Nationaal dreigingsbeeld 2017: georganiseerde criminaliteit*, Driebergen: Dienst Landelijke Informatieorganisatie (Politie) 2017.

Van der Bruggen 2015
M. van der Bruggen, 'Een beschouwing van de ontwikkeling van het internet en cybercriminaliteit en de gevolgen hiervan voor de internationale bestrijding van digitale kinderporno', *Tijdschrift voor Criminologie* (57) 2015, afl. 2, p. 240-257.

Van der Bruggen e.a. 2018
M. van der Bruggen. A. van Bunningen. P. Talens & I. van Balen, 'Kinderporno vanuit netwerkperspectief', *Het Tijdschrift voor de Politie* (80) 2018, afl. 4, p. 26-28.

doi: 10.5553/JV/016758502018044005004

Duijn & Klerks 2014
P. Duijn & P. Klerks, 'De brug tussen wetenschap en opsporingspraktijk. Onderzoek naar de toepassing van sociale netwerkanalyse in de opsporing', *Tijdschrift voor Criminologie* (56) 2014, afl. 4, p. 39-70.

Duijn e.a. 2014
P. Duijn, V. Kashirin & P. Sloot, 'The relative ineffectiveness of criminal network disruption', *Scientific Reports* (4) 2014, p. 1-15.

Durkin & Bryant 1999
K.F. Durkin & C.D. Bryant, 'Propagandizing pederasty: A thematic analysis of the on-line exculpatory accounts of unrepentant pedophiles', *Deviant Behavior* (20) 1999, afl. 2, p. 103-127.

Europol 2016
Europol, *IOCTA 2016: Internet Organised Crime Threat Assessment*, Den Haag: European Police Office 2016.

Felson 2006
M. Felson, *The ecosystem for organized crime* (HEUNI-paper nr. 26), Helsinki: HEUNI 2006.

Fijnaut 1996
C.J.C.F. Fijnaut, 'Georganiseerde criminaliteit in Nederland. De rol van autochtone criminele groepen', in: M. van Traa (red.), *Deel 1 onderzoeksgroep Fijnaut: Autochtone, allochtone en buitenlandse criminele groepen*, Den Haag: Sdu Uitgevers 1996, p. 3-57.

Frank e.a. 2010
R. Frank, B. Westlake & M. Bouchard, 'The structure and content of online child exploitation networks', *Workshop on Intelligence and Security Informatics* 2010, p. 1-9.

Goodman 2015
M. Goodman, *Future crimes: Inside the digital underground and the battle for our connected world*, Londen: Transworld Publishers 2015.

Hughes e.a. 2006
D. Hughes, J. Walkerdine, G. Coulson & S. Gibson, 'Is deviant behavior the norm on p2p file-sharing networks?', *IEEE Distributed Systems Online* (7) 2006, afl. 2, https://ieeexplore.ieee.org/abstract/document/1610578

Krueger e.a. 2009
R. Krueger, M. Kaplan & M. First, 'Sexual and other Axis I diagnoses of 60 males arrested for crimes against children involving the internet', *The International Journal of Neuropsychiatric Medicine* (14) 2009, afl. 11, p. 623-631.

Von Lampe 2016
K. von Lampe, *Organized crime: Analyzing illegal activities, criminal structures, and extra-legal governance*, Londen: SAGE Publications 2016.

doi: 10.5553/JV/016758502018044005004

Leukfeldt e.a. 2017
E.R. Leukfeldt, E.R. Kleemans & W.P. Stol, 'Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks', *The British Journal of Criminology* (57) 2017, afl. 3, p. 704-722.

McCarthy & Hagan 2001
B. McCarthy & J. Hagan, 'When crime pays: Capital, competence, and criminal success', *Social Forces* (79) 2013, afl. 3, p. 1035-1060.

Merdian e.a. 2013
H.L. Merdian, C. Curtis, J. Thakker, N. Wilson & D.P. Boer, 'The three dimensions of online child pornography offending', *Journal of Sexual Aggression* (19) 2013, afl. 1, p. 121-132.

Moerenhout 2012
L. Moerenhout, *Kinderpornografie: verslag van een onderzoek voor het Nationaal dreigingsbeeld 2012*, Zoetermeer: Dienst IPOL 2012.

Oerlemans 2010
J.J. Oerlemans, 'Een verborgen wereld: kinderpornografie op internet', *Tijdschrift voor Familie- en Jeugdrecht* (10) 2010, p. 236-243.

O'Halloran & Quayle 2010
E. O'Halloran & E. Quayle, 'A content analysis of a "boy love" support forum: Revisiting Durkin and Bryant', *Journal of Sexual Aggression* (16) 2010, afl. 10, p. 71-85.

Owens e.a. 2016
J. Owens, J. Eakin, T. Hoffer, Y. Muirhead & J. Shelton, 'Investigative aspects of crossover offending from a sample of FBI online child sexual exploitation cases', *Aggression and Violent Behavior* (30) 2016, p. 3-14.

Prichard e.a. 2011
J. Prichard, P. Watters & C. Spiranovic, 'Internet subcultures and pathways to the use of child pornography', *Computer Law & Security Review* (27) 2011, p. 585-600.

Van Remunt & Van Wilsem 2016
T. van Remunt & J. van Wilsem, 'Wat wordt er nu eigenlijk gezegd? Een verkennend onderzoek naar communicatiepatronen op het Darkweb', *Proces* (95) 2016, afl. 1, p. 24-39.

Seto & Ahmed 2014
M.C. Seto & A.G. Ahmed, 'Treatment and management of child pornography use', *Psychiatric Clinics of North America* (37) 2014, afl. 2, p. 207-214.

doi: 10.5553/JV/016758502018044005004

Shelton e.a. 2016
J. Shelton, J. Eakin, T. Hoffer, Y. Muirhead & J. Owens, 'Online child sexual exploitation: An investigative analysis of offender characteristics and offending behaviour', *Aggression and Violent Behavior* (30) 2016, p. 15-23.

Soudijn & Zegers 2012
M. Soudijn & B. Zegers, 'Cybercrime and virtual offender convergence settings', *Trends in Organized Crime* (15) 2012, afl. 2/3, p. 111-129.

Steel 2009
C. Steel, 'Child pornography in peer-to-peer networks', *Child Abuse & Neglect* (33) 2009, p. 560-568.

VG 2017
VG, 'VG exposed the largest child sexual abuse forum. It was run by the police', 1 november 2017, https://www.vg.no/spesial/2017/undercover-darkweb/?lang=en.

Westlake & Bouchard 2016
B. Westlake & M. Bouchard, 'Liking and hyperlinking: Community detection in online child sexual exploitation networks', *Social Science Research* (59) 2016, p. 23-36.

Zulkarnine e.a. 2016
A. Zulkarnine, R. Frank, B. Monk, J. Mitchell & G. Davies, 'Surfacing collaborated networks in Dark Web to find illicit and criminal content', in: *IEEE Conference on Intelligence and Security Informatics (ISI)*, 2016, p. 1-6.

doi: 10.5553/JV/016758502018044005004

De 'non-human (f)actor' in cybercrime

Cybercriminele netwerken beschouwd vanuit het 'cyborg crime'-perspectief

Wytske van der Wagen en Frank Bernaards*

> 'De Nederlandse politie heeft dinsdag een netwerk opgerold van waaruit zes miljoen webaanvallen zijn gelanceerd. Met het platleggen van de site webstresser.org en de arrestatie van de vermoedelijke beheerders zou de grootste veroorzaker van wereldwijde ddos-aanvallen uit de lucht gehaald zijn.'[1]

Cybercrime en de bestrijding ervan hebben de afgelopen jaren steeds meer prioriteit gekregen voor politie en justitie. Hoewel de bestrijding flink is geïntensiveerd, blijft het voorlopig een uitdaging om daders op te sporen en te vervolgen. Een belangrijk streven is om een 'fysieke persoon', een mens van vlees en bloed, voor het gerecht te slepen (Aalbers 2016), of liever nog een geheel crimineel netwerk op te rollen. Echter, bij cybercrime gaat dit gepaard met tal van complexe technische, geografische en juridische obstakels (Koops 2010). Daders beschikken bijvoorbeeld over diverse tools waarmee ze relatief onzichtbaar en anoniem kunnen opereren en hun sporen kunnen uitwissen (Van Hardeveld e.a. 2017). Als het dan uiteindelijk wel lukt om daders aan te houden, is het maar de vraag of hiermee 'de kous af is'. Naast het feit dat hun positie mogelijk snel door een andere cybercrimineel kan worden ingenomen, speelt er nog iets anders. De bestrijding van cybercrime vereist in veel gevallen dat niet alleen de (mense-

* Dr. W. van der Wagen is als universitair docent verbonden aan de Erasmus School of Law (sectie Criminologie). In juni 2018 promoveerde zij aan de Rijkuniversiteit Groningen op het proefschrift *From cybercrime to cyborg crime: An exploration of high-tech cybercrime, offenders and victims through the lens of actor-network theory.* F. Bernaards LLM is werkzaam als operationeel specialist bij Team High Tech Crime van de Dienst Landelijke Recherche.

1 Zie https://www.nrc.nl/nieuws/2018/04/25/politie-legt-groot-netwerk-achter-webaanvallen-plat-a1600763.

doi: 10.5553/JV/016758502018044005005

lijke) dader(s), maar juist ook de (kwaadaardige) infrastructuur en de individuele besmettingen worden gestopt, wat bijvoorbeeld duidelijk naar voren komt bij de ontmanteling van zogenaamde botnets, netwerken van geïnfecteerde computers (Schless & Vranken 2013; Van der Wagen & Pieters 2015). In de *Webstresser*-zaak (zie het citaat bovenaan) was een belangrijk doel van de politie om de technologie uit te schakelen door de servers achter de website inactief, ontoegankelijk en onbereikbaar te maken. Pas toen dat gelukt was, werd er gekeken naar de beheerders van Webstresser en diens klanten. Om dit soort criminaliteit te kunnen bestrijden, dient de politie zich als het ware steeds meer te (be)wapenen tegen kwaadaardige netwerken van mensen en technologieën (Van der Wagen & Pieters 2015).

Deze ontwikkeling roept de vraag op of we in de criminologie mogelijk met een andere bril naar de organisatiestructuur van cybercriminele netwerken moeten kijken. Kunnen bestaande benaderingen de prominente rol van technologie voldoende ondervangen of duiden? Zouden we niet naar een meer hybride benadering moeten toe gaan, die zich nadrukkelijk of nadrukkelijker (ook) richt op de rol en positie van technologische 'nodes' in een crimineel netwerk?

In deze bijdrage presenteren wij een alternatieve criminele netwerkbenadering, die een actievere rol toekent aan niet-menselijke actoren, zoals technologische infrastructuren, objecten, software en tools, in de uitvoering en totstandkoming van criminele handelingen en hun gevolgen. Deze op actor-netwerktheorie (Latour 1996, 2005; Mol 2010) gestoelde benadering, ook wel het 'cyborg crime'-perspectief genoemd (Van der Wagen 2018a, 2018b), conceptualiseert criminele netwerken niet uitsluitend als menselijk aangestuurde netwerken, maar als hybride netwerken van mens en technologie. Dit perspectief wordt vervolgens afgezet tegen bevindingen uit een reeds afgerond verkennend onderzoek naar cybercriminele (actor-)netwerken (Van der Wagen & Dimitrova 2017). Dit betrof een kwalitatieve analyse van chatgesprekken tussen cybercriminelen die een rol vervullen bij het plegen van diverse cybercriminele activiteiten, waaronder botnets, het schrijven en verspreiden van malafide software en de inzet van *money mules*. In deze bijdrage staan we stil bij de belangrijkste uitkomsten van dit onderzoek, waarbij het accent vooral zal liggen op de 'non-human (f)actor' in een crimineel netwerk.

doi: 10.5553/JV/016758502018044005005

Netwerken van mensen of van machines?

> 'In the cyberworld, strength is in software, not in numbers of individuals.' (Brenner 2002, p. 27)

ICT is in toenemende mate een belangrijk, zelfs onmisbaar onderdeel geworden van georganiseerde misdaad. Enerzijds hebben we te maken met traditionele groepen die steeds meer gebruikmaken van ICT, zoals het gebruik van gecrypte telefoons voor afgeschermde communicatie rondom liquidaties en drugshandel, of de handel in illegale wapens en drugs via *dark markets* op het internet. Anderzijds zijn er de afgelopen jaren groepen ontstaan die zich exclusief richten op vormen van hightech cybercriminaliteit, zoals grootschalige bankfraude via malware (Kruisbergen e.a. 2018; Leukfeldt e.a. 2016; Odinot e.a. 2016). Deze groepen verschillen in meerdere opzichten van traditionele criminele groepen. Zo is er bijvoorbeeld in mindere mate sprake van vaste groepen, maar werken daders in kleine, flexibele, diffuse en steeds wisselende formaties samen (Choo 2008; Yip e.a. 2013). Specialisaties zijn hierbij van groot belang. Zo zijn er actoren die de code van de kwaadaardige software schrijven (individuen met de technologische skills) en weer andere actoren die er vervolgens gebruik van maken (Monsma e.a. 2010; Odinot e.a. 2016). Actoren die bijvoorbeeld de controle hebben over een botnet, kunnen volgens Mielke en Chen (2008) hun macht flink laten gelden in cyberspace. Ze zijn een onmisbare schakel voor tal van lucratieve activiteiten, zoals de verspreiding van spam, DDoS-aanvallen en bankfraude, en kunnen het bereik van deze activiteiten (en dus de schade) ook aanzienlijk vergroten. Zoals in het citaat van Brenner (2002) al wordt aangestipt: in cyberspace draait het niet alleen om 'sociale' (lees: menselijke) banden, maar ook om de juiste technologische connecties. Veel taken worden niet zozeer uitgevoerd door mensen, maar geautomatiseerd, door machines. Van der Wagen (2018a) pleit dan ook voor een alternatieve conceptualisering van cybercrime, waarbij hightech verschijnselen zoals botnets als hybride criminele netwerken worden beschouwd. We gaan nu nader op dit perspectief in en staan daarbij stil bij de vraag hoe dit perspectief een bredere toepassing kan hebben.

doi: 10.5553/JV/016758502018044005005

Het 'cyborg crime'-perspectief

Het 'cyborg crime'-perspectief is het resultaat van een theoretisch exploratief promotieonderzoek naar cybercrime, waarbij de actor-netwerktheorie (hierna: ANT) is toegepast op verschillende vormen van cybercrime (Van der Wagen 2018a). Belangrijk om te benadrukken is dat het 'cyborg crime'-perspectief (net als ANT) geen theorie is die iets wil verklaren, maar veeleer een lens of denkkader is dat de onderzoeker op een bepaalde manier naar fenomenen laat kijken. Hierbij kunnen twee kernaspecten worden onderscheiden (zie voor een uitgebreide beschrijving: Van der Wagen 2018a).

Ten eerste bedeelt het perspectief een actieve rol toe aan niet-menselijke entiteiten in acties en beschouwt het de mens niet a priori als de centrale en enige actor die ertoe doet. Het erkent wel dat mens en machine verschillend zijn, maar stelt dat ze een vergelijkbare rol kunnen spelen in situaties, handelingen, gebeurtenissen, enzovoort. Zo kunnen objecten of technologieën op basis van hun 'script' (handelingsprogramma) een bepaald gebruik uitnodigen (goed of kwaad), en kunnen ze handelingen ook mede mogelijk maken, vormgeven, reguleren, in stand houden en/of verstoren. Volgens deze mediërende visie op de mens-techniekrelatie kunnen mens en technologie elkaar ook wederzijds beïnvloeden, waardoor het onderscheid tussen doel (mens) en middel (ding) vervaagt (zie ook Verbeek 2014). Technologie is dan ook niet slechts een passief instrument dat onder de volledige controle staat van de mens.

Ten tweede, samenhangend met het voorgaande punt, heeft het 'cyborg crime'-perspectief een hybride en relationele opvatting van de compositie van criminele actoren en netwerken. Het veronderstelt dat actoren pas significant (belangrijk) worden in relatie tot andere actoren, als collectief, niet op zichzelf. Vanuit deze zienswijze zou je als onderzoeker moeten kijken naar het *netwerk* van elementen of actoren (groot, klein, menselijk, technisch, virtueel, enz.) dat een handeling of gebeurtenis in werking stelt of mogelijk maakt, alsmede naar de actoren die juist weerstand bieden. Cybercrime, zowel dader- als slachtofferschap, wordt op zijn beurt beschouwd als het product van een complexe wisselwerking tussen menselijke, niet-menselijke en virtuele (inter)acties.

Wat betekent de toepassing van een dergelijk perspectief dan voor de criminologische analyse van cybercriminele netwerken? Het belang-

doi: 10.5553/JV/016758502018044005005

rijkste uitgangspunt is dat er evenredige aandacht moet zijn voor de rol die menselijke en niet-menselijke entiteiten spelen als we (criminele) handelingen en processen willen analyseren. Het stelt de vraag: welk deel van het criminele proces wordt uitgevoerd door welke actor (menselijk of niet-menselijk), en hoe geeft de actor vorm aan dit proces? In dit kader verschilt het perspectief dan ook van een klassieke 'crime script'-analyse. Deze benadering of methode tracht ook het criminele proces (uitvoering en organisatie) en de betrokken actoren in kaart te brengen (bijv. Hancock & Laycock 2010), maar duidt de rol van technologie vooral in functionele en dus passieve termen. Ook in (andere) gelegenheidsbenaderingen wordt het verloop van het criminele proces voornamelijk toegeschreven aan menselijke (rationele) keuzes die worden gemaakt (zie ook Demant & Dilkes Frayne 2015), waarmee mogelijk bepaalde interacties buiten beeld blijven in de analyse die juist van belang zijn bij cybercrime (Van der Wagen 2018a).

Korte beschrijving van het geanalyseerde empirische materiaal

In het verlengde van het promotieonderzoek van de eerste auteur is het 'cyborg crime'-perspectief ook toegepast op ander empirisch materiaal. Voor dit onderzoek (Van der Wagen & Dimitrova 2017) is een dataset geanalyseerd bestaande uit een omvangrijke hoeveelheid chatgesprekken, voornamelijk in de Russische taal.[2] De dataset omvat ongeveer 5.700 unieke nicknames en maar liefst 45 miljoen chatregels van voornamelijk criminele aard, waarvan we voor dit project een beperkt deel hebben kunnen analyseren. De geanalyseerde gesprekken zijn in de periode november 2015 tot en met september 2016 gevoerd. De gesprekken zijn daarmee van recente datum en ook niet eerder voor wetenschappelijk onderzoek gebruikt. De dataset biedt veel gedetailleerde informatie. Daar het privégesprekken betrof tussen daders onderling, gaven ze in detail bloot hoe en met wie de actoren criminele handelingen uitvoeren en organiseren, hoe ze met elkaar communiceren en handel drijven, en welke obstakels zich hierbij voordoen. Dergelijke informatie is bijvoorbeeld in mindere mate beschikbaar bij de analyse van forumdata. Daar wordt wel contact gelegd met mededaders, geadverteerd en kennis uitgewisseld, maar de

2 De tweede onderzoeker beheerst de Russische taal volledig.

doi: 10.5553/JV/016758502018044005005

deals zelf worden doorgaans via de chat afgehandeld. We hadden daarmee als onderzoekers gedetailleerd en uniek materiaal tot onze beschikking, dat zich goed leent voor wetenschappelijk onderzoek en de toepassing van het 'cyborg crime'-perspectief. Tegelijkertijd was het materiaal complex en uitdagend. Dit had vooral te maken met de vaak zeer technische aard van de gesprekken, (gedeeltelijke) versleuteling van de gesprekken en het gebruik van slang.
Tijdens het onderzoek hebben we ons vooral gericht op de analyse van gesprekken over het gebruik van *botnets* voor financieel gewin en de (deel)activiteiten die hiermee verbonden zijn. Voor de verschillende deelactiviteiten is in kaart gebracht welke menselijke en niet-menselijke actoren betrokken zijn (zie figuur 1) en hoe zij in relatie tot elkaar staan. Een korte beschrijving van deze activiteiten, zoals we dat ook in de gesprekken konden waarnemen, volgt hieronder.

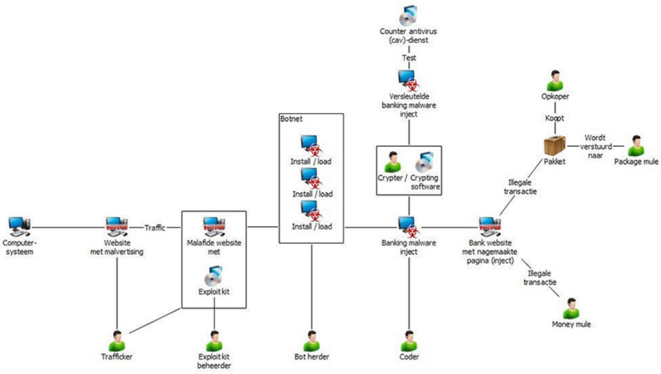
Een crimineel netwerk van interafhankelijke scripts

Een botnet is een netwerk van aan het internet verbonden gecompromitteerde (computer)systemen, die op afstand kunnen worden aangestuurd. De beheerder van een botnet wordt ook wel een *bot herder* genoemd; hij kan zijn botnet zelf gebruiken of aan anderen verhuren voor allerlei (malafide) activiteiten. Om (computer)systemen te compromitteren, en zo zijn of haar botnet op te bouwen, kan de herder gebruikmaken van een *exploit kit*. Dergelijke kits draaien op een website en scannen de (computer)systemen van websitebezoekers op kwetsbaarheden om uit te buiten. Voor de beheerder van een exploit kit is het uiteraard van belang dat er daadwerkelijk bezoekers op de website afkomen, waar de exploit kit op draait. Het verkeer naar een website met een exploit kit wordt ook wel *traffic* genoemd, een specialisme dat verzorgd wordt door *traffickers*.
Traffic wordt onder meer gegenereerd door *malvertising*: hierbij laat de trafficker een advertentie verspreiden onder bezoekers van een (legitieme) website. De advertentie leidt de gebruiker vervolgens naar een malafide website, waar de exploit kit het omgeleide (computer)systeem opwacht. Een exploit kit-beheerder wil vaak specifieke traffic hebben, zodat de kit vanuit zijn perspectief de meeste kans op succes heeft. Afhankelijk van het type exploit kit is hij bijvoorbeeld vooral geïnteresseerd in traffic van (computer)systemen met een spe-

doi: 10.5553/JV/016758502018044005005

cifieke *user agent* (kenmerken van het betreffende systeem), waaruit blijkt dat gebruiker mogelijk een besturingssysteem heeft met kwetsbaarheden die door de exploit kit kunnen worden uitgebuit. Een uiteindelijk succesvol geïnfecteerd (computer)systeem wordt ook wel een *install* of *load* genoemd.

Figuur 1 Schematische weergave van een botnet



Vanuit een botnet kan kwaadaardige software, ofwel *malware*, worden verspreid. Indien deze erop gericht is om banktransacties af te vangen, is er sprake van *banking malware*. Hiermee kunnen transacties op het internet (semi)automatisch worden doorgesluisd naar tussenrekeningen. Een cybercrimineel die het gemunt heeft op banktransacties kan bijvoorbeeld gebruikmaken van *injects*. Hiermee wordt code bedoeld die in de browser wordt 'geïnjecteerd' en de gebruiker een nagemaakte bankpagina toont. De schrijver, ofwel *coder*, en/of de gebruiker van banking malware willen niet dat hun malware ontdekt wordt door antivirusprogramma's. Om die reden huren ze *crypters* in, die ervoor zorgen dat een bestand zo wordt ingepakt of versleuteld dat een virusscanner het bestand niet kan detecteren. Om vervolgens te testen of het gecrypte bestand daadwerkelijk niet gedetecteerd zal worden door virusscanners, kan er gebruik worden gemaakt van een *counter antivirus* (cav)-dienst. Aanbieders van cav maken het mogelijk om een bestand tegen een hele verzameling aan virusscanners aan te houden om te bezien of er detectie plaatsvindt. Overigens zijn virusscanners constant in ontwikkeling, waardoor een crypt geen onbeperkte 'levensduur' zal hebben. Alleen na een succesvolle test zal de

doi: 10.5553/JV/016758502018044005005

gecrypte malware geschikt zijn voor daadwerkelijk gebruik. Er zijn crypters die hier garanties en support op afgeven, maar daar moet dan ook een hogere prijs voor betaald worden.
De crimineel die investeert in deze deelactiviteiten wil uiteindelijk natuurlijk winst maken. Dat doet hij door gebruik te maken van diverse tussenstappen, bijvoorbeeld door een organisatie in te schakelen die *money mules* of *package mules* in dienst heeft. Money mules zijn mensen die hun bankrekening ter beschikking stellen om geld op te ontvangen en weer door te sturen. Bij package mules gaat het om personen, ook wel *drops* genoemd, die pakketten ontvangen met (dure) goederen die gekocht zijn via illegale transacties. Zij sturen die pakketten weer door naar zogenoemde *opkopers*, die het goed te gelde kunnen maken.

Technologie meer dan een instrument? Een reflectie op de bevindingen

Zoals uit de chatgesprekken blijkt, zijn de samenwerkingsconstructies verbonden met bovenstaande activiteiten zeer flexibel en fluïde. Er lijkt sprake te zijn van een wereld of marktplaats waarin diverse actoren actief zijn (met een eigen of gedeeld handelingsprogramma) en van elkaar afhankelijk zijn voor bepaalde diensten, producten of vaardigheden. Dergelijke fluïditeit hangt samen met de digitale omgeving waarin de actoren manoeuvreren, maar zeker ook met de technologische aard van de delicten. Dit brengt ons bij het (uitgangs)punt dat ook niet-menselijke actoren (software, malware, tools, panelen, enz.) een belangrijke positie kunnen innemen in een cybercrimineel netwerk en/of van invloed zijn op hoe een crimineel netwerk ontstaat en zich ontwikkelt. In het nu volgende gaan we in op hoe de mediërende rol van technologie concreet gestalte kan krijgen, en refereren daarbij naar enkele bevindingen uit het onderzoek.
Allereerst zien we in de gesprekken terug dat technologie als een belangrijke verbindende schakel kan fungeren. Laten we hierbij de exploit kit – in de gesprekken ook wel als 'svjazka' (= verbinding) aangeduid – als voorbeeld nemen. Feitelijk gezien gaat het daarbij om technologie die gebruikmaakt van technologie om andere technologie aan te vallen. Een exploit kit bestaat namelijk uit verschillende soorten afzonderlijke *exploits*: programma's die zoeken naar kwetsbaarheden

doi: 10.5553/JV/016758502018044005005

op een (computer)systeem. De exploit kit staat aan de voor- en achterkant weer in verbinding met andere technologie. Zo is er aan de voorkant traffic benodigd om bezoek naar de exploit kit te genereren en komt een succesvol besmet (computer)systeem in een botnet terecht, waar het vervolgens voor allerlei doeleinden gebruikt kan worden. Ditzelfde voorbeeld laat tevens zien dat sommige technologieën vaak pas betekenis c.q. een malafide werking krijgen wanneer zij deel uitmaken van of in verbinding staan met andere technologie.

Een hiermee verbonden punt is dat, in tegenstelling tot traditionele criminaliteit, de tools die gebruikt worden om cybercrime te plegen geen statisch karakter hebben. Ze moeten worden onderhouden en/of steeds vernieuwd (bijvoorbeeld 'gerecrypt' worden), want anders worden ze onbruikbaar. Met andere woorden: de technologie is ook *tijdens* het criminele proces steeds in beweging en in ontwikkeling, wat ook continue interactie vraagt tussen kopers en afnemers en tussen mens en machine. Dit verklaart mogelijk ook dat er over technologie wordt gesproken alsof het om levende wezens gaat. Zo heeft men het over het 'levend houden' van een crypt, waarbij verwezen wordt naar de tijd die een crypt (gegarandeerd) onder de radar van antivirusprogramma's kan blijven. De termen 'levend' en 'dood' zien we op andere vlakken ook terug, bijvoorbeeld als het gaat om (computer)systemen in een botnet die wel of niet nog steeds gebruikt kunnen worden om (bank)gegevens af te vangen, of als het gaat om money mules die wel of niet nog steeds gebruikt kunnen worden.

Daarnaast zien we dat technologie een schakel kan zijn tussen mensen. In de gesprekken lezen we terug dat de afnemers en gebruikers van exploit kits en andere technologieën de werking daarvan vaak niet (geheel) begrijpen, bijvoorbeeld omdat ze de skills niet hebben om de technologie (effectief) in te zetten. Deze actoren zijn dan genoodzaakt om relaties met anderen aan te gaan om te communiceren over de werking en ondersteuning van de technologie, of om met iemand samen te werken die de technologie wel beheerst. In dit kader zien we dat actoren regelmatig een afweging moeten maken tussen een dienst afnemen (en daarvoor betalen) of de activiteit zelf (geautomatiseerd) uitvoeren met een bepaalde tool. In plaats van een (menselijke) crypter in te huren gaan ze bijvoorbeeld crypting software gebruiken. Ook bij illegale banktransacties zagen we terug dat de transacties zowel door mensen als door machines gedaan kunnen worden, wat bijgevolg

doi: 10.5553/JV/016758502018044005005

zijn weerslag heeft op de organisatiestructuur: wordt er samengewerkt met een mens of een machine?
Tot slot zien we dat technologie de rol van een *hub* of centraal punt in het criminele netwerk kan innemen, degene die alles en iedereen bij elkaar houdt. Een voorbeeld hiervan is het beheerpaneel dat gebruikt wordt bij *mule handling*. Hoewel dergelijke panelen in beginsel misschien instrumenteel van aard lijken, blijken ook deze een meer wezenlijke rol te spelen in het cybercriminele proces dan wellicht gedacht. Ze zijn een belangrijke plaats waar informatie samenkomt om activiteiten te stroomlijnen en uit te voeren. Een ander voorbeeld is de rol van servers die de basis vormen van de criminele infrastructuur. Als deze uit het netwerk worden gehaald, bijvoorbeeld door organisaties zoals Spamhaus of Dr Web, dan lijken er daadwerkelijk problemen in de uitvoering en organisatie te ontstaan. Zo klagen coders en gebruikers van injects over de werking van de technologie van dergelijke organisaties. Doordat IP-adressen op een *black list* van Spamhaus voorkomen, kunnen hun injects moeilijk of niet worden ingezet.

Cybercriminele netwerken: een complex samenspel van mens en technologie

In deze bijdrage is bepleit dat de 'non-human (f)actor' meer aandacht moet krijgen in de criminologische analyse van cybercriminele netwerken. In dit kader is een alternatief perspectief gepresenteerd, beter bekend als het 'cyborg crime'-perspectief, dat een hybride en complexe opvatting heeft van de formatie en compositie van criminele netwerken en daarbij ook een actievere rol toekent aan de technologie. In dit kader is gereflecteerd op de bevindingen uit een reeds afgerond onderzoek, waarbij conversaties tussen cybercriminelen zijn geanalyseerd en op basis waarvan actoren in kaart zijn gebracht die een rol spelen bij botnets en aanverwante activiteiten. Het onderzoek heeft laten zien dat niet-menselijke entiteiten, zoals computerprogramma's, exploit kits, systemen, servers en beheerpanelen, een sleutelrol spelen in het criminele proces. Ze zijn uiteraard van belang op het gebied van de coördinatie en uitvoering van criminele activiteiten, maar de bevindingen suggereren dat hun rol mogelijk ook fundamenteler van aard is en dat zij het criminele proces ook mede vormgeven. Door vanuit deze bril naar het fenomeen te kijken kunnen we mogelijk een breder palet

doi: 10.5553/JV/016758502018044005005

aan actoren, relaties, interacties en connecties blootleggen, waaronder ook die tussen mens en machine. Met het oog op de steeds verdergaande digitalisering en automatisering van criminaliteit concluderen we dan ook dat criminologen hun begrip van criminele netwerken moeten aanpassen door ook technologie als wezenlijk onderdeel van een crimineel netwerk te zien. Het 'cyborg crime'-perspectief biedt hier een passend kader en startpunt voor.

Ter afsluiting willen we nog graag stilstaan bij eventuele juridische implicaties van het perspectief. Het toekennen van actorschap aan technologie heeft natuurlijk ook consequenties voor het strafrecht. Denk bijvoorbeeld aan het verdachte-begrip, zoals gedefinieerd in artikel 27 Wetboek van Strafvordering. Indien technologische entiteiten daaronder kunnen worden geschaard, zouden bijzondere opsporingsbevoegdheden kunnen worden ingezet op belangrijke actoren zonder dat daarbij een mens in beeld is. Het 'cyborg crime'-perspectief kan daarmee ook handvatten bieden voor nieuwe inzichten over de verstoring en bestrijding van cybercriminele netwerken. Zo kan de aanpak zich bijvoorbeeld richten op het uitschakelen van panelen of andere onderdelen van de infrastructuur. Tevens zouden er maatregelen kunnen worden genomen die zich richten op het inperken van de toegang tot tools die gebruikt kunnen worden voor cybercrime, zoals tools die voor DDoS kunnen worden gebruikt (zie het citaat boven aan de bijdrage), of tools (zoals exploit kits) die een sleutelrol spelen in de (geautomatiseerde) verspreiding van malware.

Als we vervolgens kijken naar daderschap, schuld en causaliteit rijst de vraag in welke mate een strafbare gedraging aan iemand, maar ook aan iets, toegerekend kan worden. Hoe zit het bijvoorbeeld met malware die meer of andersoortige gegevens binnenhaalt dan beoogd in de programmatuur? En hoe zit het met de afnemer van een crypt en de huurder van een botnet die zelf misschien vrijwel niks begrijpt van de technologie die hij afneemt? Kortom, ook in juridisch opzicht dienen zich allerlei nieuwe vraagstukken aan. Misschien moeten we als cyber- of *cyborg*-criminologen wel het voortouw nemen in deze discussie.

doi: 10.5553/JV/016758502018044005005

Literatuur

Aalbers 2016
H. Aalbers, 'Tegenhouden in cyberspace', *het Tijdschrift voor de Politie* (78) 2016, afl. 9/16, p. 18-23.

Brenner 2002
S.W. Brenner, 'Organized cybercrime. How cyberspace may affect the structure of criminal relationships', *North Carolina Journal of Law & Technology* (4) 2002, afl. 1, p. 1-50.

Choo 2008
K.K. Choo, 'Organized crime groups in cyberspace: A typology', *Trends in Organized Crime* 2008, afl. 11, p. 270-295.

Demant & Dilkes Frayne 2015
J. Demant & E. Dilkes Frayne, 'Situational crime prevention in nightlife spaces', in: D. Robert & M. Dufrese (red.), *Actor-network theory and crime studies. Explorations in science and technology*, Londen/New York: Ashgate 2015, p. 5-19.

Hancock & Laycock 2010
G. Hancock & G. Laycock. 'Organised crime and crime scripts: Prospects for disruption', in: K. Bullock, R.V. Clarke & N. Tilley (red.), *Situational prevention of organised crime*, Devon: Willan Publishing 2010, p. 172-192.

Van Hardeveld e.a. 2017
G.J. van Hardeveld, C. Webber & K. O'Hara, 'Deviating from the cybercriminal script: Exploring tools of anonymity (mis)used by carders on cryptomarkets', *American Behavioral Scientist* (61) 2017, afl. 11, p. 1244-1266.

Koops 2010
B.J. Koops, 'The internet and its opportunities for cybercrime', in: M. Herzog-Evans (red.), *Transnational criminology manual*, Nijmegen: Wolf Legal Publishers 2010, p. 735-754.

Kruisbergen e.a. 2018
E.W. Kruisbergen, E.R. Leukfeldt, E.R. Kleemans, R.A. Roks e.a., *Georganiseerde criminaliteit en ICT. Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Misdaad* (Cahier 2018-8), Den Haag/Amsterdam: WODC/NSCR 2018.

Latour 1996
B. Latour, 'On Actor Network Theory. A few clarifications', *Soziale Welt – Zeitschrift für sozialwissenschaftliche Forschung und Praxis* (47) 1996, afl. 4, p. 369-381.

Latour 2005
B. Latour, *Reassembling the social. An introduction to actor-network-theory*, New York: Oxford University Press 2005.

doi: 10.5553/JV/016758502018044005005

Leukfeldt e.a. 2016
E.R. Leukfeldt, E.R. Kleemans & W.P. Stol, 'Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks', *British Journal of Criminology* (57) 2016, afl. 3, p. 704-722.

Mielke & Chen 2008
C.J. Mielke & H. Chen, 'Botnet and the cybercriminal underground', in: *IEEE International Conference on Intelligence and Security Informatics*, 2008, p. 206-211.

Mol 2010
A. Mol, 'Actor-network theory: Sensitive terms and enduring tensions', *Kölner Zeitschrift für Soziologie und Sozialpsychologie* (50) 2010, afl. 1, p. 253-269.

Monsma e.a. 2010
E. Monsma, V. Buskens, M. Soudijn & P. Nieuwbeerta, 'Partners in cybercrime: An online forum evaluated from a social network perspective', *ISCORE Papers* 2010, afl. 285, p. 1-28.

Odinot e.a. 2016
G. Odinot, M.A. Verhoeven, R.L.D. Pool & C.J. de Poot, 'Chapter II. Cyber-OC in the Netherlands', in: G. Bulanova-Hristova e.a. (red.), *Cyber-OC – Scope and manifestations in selected EU member states*, Bundeskriminalamt – Criminalistic Institute 2016, p. 15-99.

Schless & Vranken 2013
T. Schless & H. Vranken, 'Counter botnet activities in the Netherlands. A study on organization and effectiveness', in: *IEEE International Conference for Internet Technology and Secured Transactions*, 2013, p. 437-442.

Verbeek 2014
P-P. Verbeek, 'Some misunderstandings about the moral significance of technology', in: P. Kroes & P-P. Verbeek (red.), *The moral status of technical artefacts*, Dordrecht: Springer 2014, p. 75-88.

Van der Wagen 2018a
W. van der Wagen, *From cybercrime to cyborg crime: An exploration of high-tech cybercrime, offenders and victims through the lens of actor-network theory* (diss. Groningen), 2018.

Van der Wagen 2018b
W. van der Wagen, 'Het "cyborg crime"-perspectief. Theoretische vernieuwing in het digitale tijdperk', *Tijdschrift over Cultuur en Criminaliteit* (8) 2018, afl. 1, p. 19-34.

Van der Wagen & Dimitrova 2017
W. van der Wagen & E. Dimitrova, *Mission cyborg: op naar een hybride kijk op de bestrijding van cybercriminele (actor-)netwerken*, Driebergen: Dienst Landelijke Recherche 2017.

doi: 10.5553/JV/016758502018044005005

Van der Wagen & Pieters 2015
W. van der Wagen & W. Pieters, 'From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks', *British Journal of Criminology* (55) 2015, afl. 3, p. 578-595.

Yip e.a. 2013
M. Yip, N. Shadbot & C. Webber, 'Structural analysis of online criminal social networks', in: *IEEE International Conference on Intelligence and Security Information*, 2013, p. 60-65.

doi: 10.5553/JV/016758502018044005005

Uit de schaduw

Perspectieven voor wetenschappelijk onderzoek naar dark markets

Thijmen Verburgh, Eefje Smits en Rolf van Wegberg*

Digitale criminaliteit is een groeiende vorm van criminaliteit en heeft een grote maatschappelijke impact: van onbereikbare bankwebsites die bezwijken onder DDoS-aanvallen tot drugshandel via anonieme markten op het *dark web*. Een vorm van digitale criminaliteit zijn de zogeheten *dark markets*, een plek op het *dark web* waar online en anoniem wordt gehandeld in diverse goederen en diensten. In dit artikel laten we zien zien hoe op *dark markets* het samenspel van technische en sociale aspecten online anonieme handel in wapens, drugs en cybercrimegereedschap, zoals DDoS-aanvallen, mogelijk maakt. Sinds het ontstaan van *dark markets* wordt er onderzoek gedaan naar deze markplaatsen en de onderliggende mechanismen. Vooralsnog blijven veel kansen voor wetenschappers onbenut. Een nog grotendeels onbekend terrein is bijvoorbeeld het onderzoek naar politie-interventies zoals operatie Bayonet, waarbij twee van de grootste dark markets door de FBI en de Nederlandse politie gesloten werden. In deze bijdrage gaat de aandacht vooral uit naar verschillende manieren van onderzoek doen naar *dark markets*. Allereerst kijken we naar de belangrijkste kenmerken van *dark markets*. Daarna staan we stil bij het bestaande onderzoek naar *dark markets* om vervolgens in te gaan op de potentiële kansen voor onderzoek naar politie-interventies op *dark markets*.

* T. Verburgh MSc is als onderzoeker verbonden aan TNO. E. Smits MSc is werkzaam als onderzoeker bij TNO. R. van Wegberg MSc is als onderzoeker verbonden aan TNO en de Technische Universiteit Delft.

doi: 10.5553/JV/016758502018044005006

Figuur 1 **Dark markets en dark web ten opzichte van het internet**

Dark markets: definitie en karakteristieken

Om het concept *dark markets* beter te kunnen duiden, is het van belang om te weten hoe *dark markets* zich verhouden tot het gehele world wide web. Het gehele web is daarbij alle content die beschikbaar is via internetbrowsers. Binnen deze content vallen twee categorieën te onderscheiden: het *surface web* en het *deep web*. Content van sites die beschikbaar is via zoekmachines, zoals Google, vallen onder de categorie *surface web*. Dat wat niet doorzoekbaar is middels zoekmachines, valt onder de categorie *deep web*. Een klein deel van de content op het *deep web* is enkel toegankelijk wanneer gebruik wordt gemaakt van een speciaal anonimiseringsprotocol.[1] Dit gedeelte wordt het *dark web* genoemd (Barratt & Aldridge 2016). Een *dark market* is een ontmoetingsplaats of handelssite op het zogenoemde *dark web* waar gebruikers virtueel bijeenkomen om producten en/of diensten te kopen en/of verkopen.

1 Technologieën die het mogelijk maken om anoniem op het web te surfen en anonieme sites te hosten worden ook wel aangeduid met de term anonimiseringsprotocollen/darknets.

doi: 10.5553/JV/016758502018044005006

Het befaamde Silk Road 1.0[2] was niet de allereerste *dark market*[3], maar door de professionaliteit van de site, de positieve feedback van gebruikers en de media-aandacht werd Silk Road 1.0 al snel de grootste *dark market* (Buxton & Bingham 2015). Als gevolg van een grootschalige politieactie werd Silk Road 1.0 na ongeveer twee jaar gesloten. Al spoedig echter ontstonden nieuwe markten. De goederen die op *dark markets* worden aangeboden, zijn meestal illegaal van aard, waarbij drugs het meest worden verhandeld (Soska & Christin 2015). Tegenwoordig is de gemiddelde *dark market* groter dan Silk Road 1.0 was en wordt bij de grootste *dark markets* meer dan $ 200.000 per dag omgezet (Soska & Christin 2015).
Aldridge en Décary-Hétu (2016) stellen dat *dark markets* niet zozeer een nieuwe technologie hebben ontwikkeld, maar dat ze enkele bestaande veiligheidsmaatregelen hebben gecombineerd. Het gaat daarbij om vier onderliggende veiligheidsmaatregelen die *dark markets* mogelijk maken: anonimiseringsprotocollen, cryptocurrencies, *escrow* en *review*systemen, begrippen die hieronder nader worden uitgelegd. Aan deze veiligheidsmaatregelen liggen twee faciliterende principes ten grondslag die de kracht van het businessmodel van *dark markets* bepalen: anonimiteit en vertrouwen (Mounteney e.a. 2016; Cox 2016; Aldrigde & Décary-Hétu 2016; Tzanetakis e.a. 2016). Anonimiteit en vertrouwen zorgen ervoor dat *dark markets* bestaansrecht hebben en bestand zijn tegen externe invloeden van bijvoorbeeld politie, maar ook van overige externe actoren zoals rivaliserende sites die graag de concurrentie dwars zouden willen zitten. In de volgende paragrafen laten we zien op welke wijze anonimiteit en vertrouwen op dark markets worden gefaciliteerd.

Anonimiteit

Aangezien de meeste producten illegaal zijn, is anonimiteit van groot belang op een *dark market*. Hieronder wordt ingegaan op de verschillende technieken en voorzieningen die deze anonimiteit bevorderen: anonimiseringsprotocollen, cryptocurrencies, data-

2 Silk road 1.0 werd in 2011 opgericht en in 2013 gesloten door de FBI. Silk Road 1.0 staat bekend als de eerste moderne dark market, waar o.a. bitcoin gebruikt werd.
3 Andere initiatieven waren The Drugstore, AFOYI, BBS, TLG en OVDB (Buxton & Bingham, 2015).

doi: 10.5553/JV/016758502018044005006

encryptie en het gebruikmaken van post- en pakketdiensten. Met behulp van deze vier maatregelen worden vier belangrijke onderdelen afgedekt: 'ontmoeten', 'betalen', 'communiceren' en 'bezorgen'.

Ontmoeten

Technologieën die het mogelijk maken om anoniem op het web te surfen en anonieme sites te hosten worden ook wel aangeduid met de term anonimiseringsprotocollen/*darknets*. Deze technologie stelt gebruikers in staat om een ontmoetingsplek te creëren waarbij elke partij anoniem is; zowel de koper, verkoper als de eigenaar van de site. Het meest bekende en meest gebruikte anonimiseringsprotocol[4] dateert uit 2002 en wordt The Onion Router (TOR) genoemd. Er zijn echter ook andere protocollen beschikbaar zoals I2P & FREENET. In het geval van TOR wordt een speciale browser gebruikt, die openbaar beschikbaar is.[5]

Betalen

Silk Road 1.0 liet een duidelijke ontwikkeling zien ten opzichte van eerdere online drugsmarkten. Daar waar de voorgaande markten allemaal gebruikmaakten van het anonimiseringsprotocol TOR, was Silk Road 1.0 de eerste site die TOR combineerde met het gebruik van de cryptocurrency bitcoin. Dit maakte het mogelijk om tamelijk anoniem betalingen te verrichten, wat een enorme sprong voorwaarts betekende (Buxton & Bingham 2015). Bitcoin is op dit moment de populairste cryptocurrency voor *dark markets* (Matanovic 2017). Een andere cryptocurrency die ook regelmatig wordt gebruikt is Monero (Matanovic 2017).

Communiceren

Een andere techniek die wordt gebruikt op *dark markets* en die de anonimiteit vergroot, is Pretty Good Privacy (PGP) (Buxton & Bingham 2015). PGP geeft gebruikers de mogelijkheid om bestanden of teksten

4 Het TOR-protocol geleidt het internetverkeer langs meerdere TOR nodes en versleutelt het netwerkverkeer daartussen waardoor het originele IP-adres niet geopenbaard wordt (Dingledine, Mathewson & Syverson, 2004). Hierdoor maakt TOR het mogelijk om te surfen op internet zonder het openbaren van het IP-adres van de gebruikte computer.

5 Zie www.torproject.org

doi: 10.5553/JV/016758502018044005006

te versleutelen, zodat deze enkel door de zender en ontvanger kunnen worden gelezen. Door PGP op *dark markets* te gebruiken weten criminelen zeker dat de politie of administrators niet bij de inhoud van hun berichten kunnen, zoals het afleveradres van het pakketje. Omdat de berichten via PGP door slechts één entiteit kunnen worden ontsleuteld, wordt PGP ook gebruikt als een soort identiteitsbewijs. Door te controleren of iemand op verschillende momenten dezelfde PGP-gegevens gebruikt, kan bepaald worden of je contact hebt met dezelfde persoon.

Bezorgen

Gelet op het postgeheim dat in veel landen geldt, kunnen illegale goederen per post anoniem worden verstuurd. Het postsysteem stelt verkopers in staat een grotere klantenkring te bereiken en hun afzetmarkt te vergroten. Ook kunnen verkopers hun producten leveren op lastig te bereiken locaties. Bovendien werkt het postsysteem risicoreducerend aangezien er geen ontmoetingen plaatsvinden tussen koper en verkoper, waardoor geweld vermeden kan worden (Van Hout & Bingham 2013). Postverzending heeft echter ook zwakheden: pakketjes kunnen worden onderschept en autoriteiten controleren bij de landsgrenzen scherp op illegale goederen (Aldridge & Decary-Hetu 2016; Aldridge & Askew 2017).

Vertrouwen

Voor *dark markets* geldt dat iedereen anoniem is. Daarom dienen er veiligheidsmaatregelen te worden ontwikkeld om elkaar desondanks te kunnen vertrouwen. Anonimiteit leidt immers tot een paradijs voor oplichters, die dan ook in significante mate aanwezig zijn op *dark markets*. Voordat criminelen onderling handel drijven moet er enige vorm van vertrouwen bestaan in de markt, andere gebruikers op de markt en de financiële afwikkeling. De onderdelen *escrow, finalize early* en het *review*systeem (zie hieronder) hebben invloed op aspecten als 'bescherming' en 'reputatie', beide van groot belang voor het vertrouwen in de markt.

doi: 10.5553/JV/016758502018044005006

Bescherming

Bij de koop en verkoop van goederen is een systeem nodig om het vertrouwen tussen koper en verkoper te versterken. De verkoper wil erop kunnen vertrouwen dat hij het geld krijgt, de koper wil erop kunnen vertrouwen dat hij het bestelde product krijgt. Er zijn twee soorten bescherming mogelijk die het vertrouwen vergroten, namelijk *escrow* en *finalize early* (*FE*). *Escrow* biedt bescherming voor de koper doordat de betaling van de koper door de marktplaats achtergehouden wordt totdat de goederen in goede orde ontvangen zijn. Wanneer dit het geval is, wordt het bedrag van de koop overgemaakt naar de verkoper. *Finalize early* is een bescherming voor verkopers waarbij de verkoper de garantie krijgt dat hij uitbetaald wordt. Hij krijgt namelijk uitbetaald voordat de koper de producten in ontvangst heeft genomen. Bij beide systemen is de marktplaats de 'objectieve' derde partij die bemiddelt wanneer onenigheid bestaat tussen de koper en verkoper (Aldridge & Askew 2017; Afilipoaie & Shortis 2015). Het geld is in beheer van de marktplaats, wat betekent dat je als koper of verkoper niet meer elke individuele 'zakenrelatie' hoeft te vertrouwen. Je hoeft alleen maar één marktplaats te vertrouwen om garanties te krijgen.

Reputatie

Een andere manier waarop het vertrouwen op *dark markets* wordt vergroot, is door gebruik te maken van een *review*systeem dat vergelijkbaar is met de beoordelingssystemen van legale verkoopwebsites als Ebay en Amazon. Het *review*systeem is opgezet om intrinsieke risico's op oplichting te verminderen (Décary-Hétu & Dupont 2013; Holt e.a. 2015). De basis van het systeem is dat er vertrouwen wordt gecreëerd door informatiedeling. Dit betreft natuurlijk niet data die de anonimiteit in geding brengt, zoals geo-locatie. Het gaat juist om publieke informatiedeling aangezien de community toegang moet hebben tot de informatie voordat het vertrouwen kan worden gecreëerd. Er wordt gebruikgemaakt van een *review*systeem waar zowel de verkopers als de kopers kunnen worden beoordeeld, waardoor het vertrouwen groeit.

doi: 10.5553/JV/016758502018044005006

Onderzoek naar dark markets

De grote toegankelijkheid, het mondiale karakter en het solide businessmodel van *dark markets* zorgen ervoor dat interventies van opsporingsinstanties niet eenvoudig uit te voeren zijn. Het achterhalen van de locatie van een server of de identiteit van een crimineel is een grote uitdaging. Wetenschappelijk onderzoekers ondervinden minder hinder van deze barrières, omdat het voor onderzoekers niet gaat om het achterhalen van een specifieke identiteit of locatie. Voor onderzoekers gaat het om trends en ontwikkelingen, waarbij het gebruik van afgeleiden voldoende is. De omvang van een marktplaats wordt bijvoorbeeld geschat op basis van het aantal *listings* (advertenties) dat een *dark market* heeft. Daarnaast kunnen onderzoekers in verschillende gevallen juist profiteren van het feit dat *dark markets* een businessmodel hebben waarbij anonimiteit en vertrouwen centraal staan. Omdat niemand elkaar kent, noch weet waar iemand zich bevindt, vindt veel van de communicatie, en dus informatie-uitwisseling, plaats op de platformen zelf. Alle interactie met de site of elkaar zijn mogelijke datapunten die gebruikt kunnen worden voor onderzoek. Hierbij moet men zich wel realiseren dat criminelen buiten de platformen om contact kunnen hebben of elkaar fysiek kunnen ontmoeten, waardoor er ook een *dark number*[6] is.
Middels het bestuderen van *dark market*s kunnen zowel criminele fenomenen alsook interventies worden onderzocht. Bij fenomeenonderzoek kan bijvoorbeeld inzicht worden verschaft in de criminele werkwijze en trends die zichtbaar zijn op een *dark market*. Bij onderzoek naar interventies kijkt men juist naar de impact van een interventie op het ecosysteem van de *dark market*. Voor beide typen research geldt dat dit zowel kwalitatief als kwantitatief onderzoek kan betreffen.

Fenomeenonderzoek dark markets

Fenomeenonderzoek is gericht op een misdaadveld of criminele markt, waarbij wordt gekeken naar aard, omvang, trends en ontwikkelingen. Onderzoeksgegevens kunnen worden vergaard door middel van observatie, participatie of via interventies. Bij data uit observatie worden onderzoeksgegevens vaak met behulp van *scraping*

6 Aantal criminelen dat buiten de steekproef valt en daardoor de conclusies van het onderzoek kan beïnvloeden.

doi: 10.5553/JV/016758502018044005006

en *crawling* vergaard. *Scraping* en *crawling* zijn technieken waarmee het mogelijk is op een geautomatiseerde wijze de content van webpagina's op te slaan (Christin 2013b; Spitters e.a. 2015; Van Remunt & Van Wilsem 2016). Hierbij wordt van elke pagina van de site een soort *snapshot* gemaakt. Dit leidt ertoe dat kwantitatief onderzoek vaak gemakkelijk uit te voeren is, omdat er vaak grotere datasets beschikbaar zijn. Bij het observeren van *dark markets* probeert men periodiek zo veel mogelijk data van de grootste marktplaatsen te verzamelen. Anders zouden namelijk alle data verloren gaan als een marktplaats plotseling wordt opgeheven.

Bij participatie wordt deelgenomen aan de criminele activiteiten op *dark markets*. Van Wegberg e.a. (2018b) pasten deze methode toe op bitcoinmixers.[7] Het onderzoek was niet alleen gericht op het bestuderen van witwassen (door verschillende bitcoinmixers te gebruiken), maar ook op het *review*systeem van mixerdiensten. Het interveniëren op een *dark market* door politieacties levert in sommige gevallen ook toegang op tot data die beschikbaar zijn op de server. Hierdoor wordt het mogelijk inzicht te krijgen in de omvang van de daadwerkelijke handel en de achterliggende transacties. Deze schat aan data kan niet alleen tot nieuwe inzichten leiden, maar ook bestaande onderzoeken met data uit observaties valideren. Het onderzoeken van een marktplaats middels observatie maakt veelal gebruik van afgeleiden. Dit lijkt een valide methodologie, maar vraagt wel om toetsing. Om bijvoorbeeld het aantal *reviews* als afgeleide te gebruiken voor een inschatting van de totale transacties kan deze naast het daadwerkelijke aantal transacties gelegd worden. De daadwerkelijke transacties kunnen bijvoorbeeld worden onderzocht met behulp van de *back-end* van een site. In de *back-end*, ofwel de server waarop de website draait, staat de database die onder andere transactie- en registratiedata bevat.

Vooral de inzet van technieken als *scraping* en *crawling* levert potentieel grote datasets op met de mogelijkheid om een volledige historie in te zien. Dit maakt het mogelijk om het fenomeen *dark market* over een langere periode beter in kaart te brengen. Zo bestudeerde Christin (2013) binnen een tijdsperiode van drie maanden de producten die verhandeld werden op Silk Road 1.0. Hij onderzocht wat de omzet was van de verkopers en de omvang van de totale commissie die de administrators ontvingen. Andere onderzoeken brachten meerdere markt-

7 Mixerservices zorgen dat de traceerbaarheid van bitcoins wordt bemoeilijkt (Van Wegberg e.a. 2018).

doi: 10.5553/JV/016758502018044005006

plaatsen in kaart (Soska & Christin 2015; Kruithof e.a. 2016; Van Wegberg e.a. 2018). Aldrigde en Décary-Hétu (2014) onderzochten welk type koper actief was op Silk Road 1.0. Daarbij keken ze naar omvang en prijs van de transacties en de handel met behulp van *review*data. Zij concludeerden dat er niet enkel sprake was van *business-to-consumer* handel, maar dat er ook sprake was van *business-to-business* handel waarbij (offline) kopers drugs online kopen om hun eigen voorraad aan te leggen.

Onderzoek naar interventies op dark markets

Interventies op *dark markets* kunnen worden uitgevoerd door drie partijen, namelijk de marktplaats zelf, een private partij of een overheidsinstantie zoals de politie (zie volgende paragraaf). Hoewel het onlogisch klinkt dat een marktplaats zelf een interventie uitvoert, zijn er voorbeelden die dit illustreren. Zo zijn er voorbeelden van marktplaatseigenaren die ervandoor gaan met alle bitcoins die zij op dat moment in beheer hebben, ook wel een *exit scam* genoemd. Interventies gepleegd door een private partij zijn directe of indirecte acties uitgevoerd door derde partijen die de modus operandi van digitale criminaliteit veranderen. Zo kan een private partij stoppen met het aanbieden van haar diensten in het algemeen of voor specifieke locaties. Karami e.a. (2015) bestudeerden bijvoorbeeld de effecten van de interventie gepleegd door PayPal waarbij accounts gerelateerd aan een aantal specifieke booter-sites[8] werden bevroren.

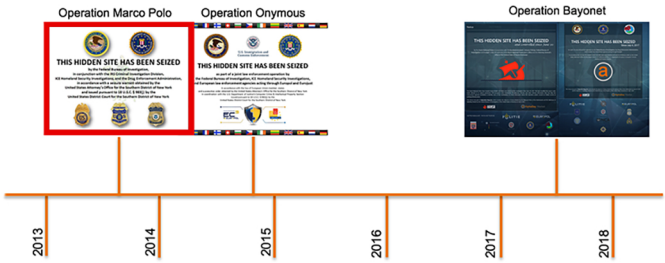
Onderzoek naar politie-interventies

De allereerste grote mondiale politieoperatie betreft Operatie Marco Polo, die in 2013 leidde tot sluiting van het befaamde Silk Road 1.0 en arrestatie van de administrator Ross Ulbricht. Operatie Onymous was de tweede mondiale operatie, deze leidde in 2014 tot de sluiting van meerdere sites op het *dark web*. Silk Road 2.0 was één van deze sites. De meest recente en laatste mondiale operatie betreft die van Operatie Bayonet in 2017. Deze operatie leidde tot de sluiting van de twee grootste markplaatsen van dat moment, namelijk Alphabay en Hansa

8 Platformen waar DDoS-aanvallen te koop zijn (Karami e.a 2015).

doi: 10.5553/JV/016758502018044005006

Figuur 2 Politie-interventies Marco Polo, Onymous en Bayonet



market. Alphabay werd hierbij als eerste door de FBI uit de lucht gehaald. Vervolgens werd Hansa market door de Nederlandse politie overgenomen en voor een maand draaiende gehouden. Dit heeft ertoe geleid dat veel data konden worden verzameld. Na een maand is ook Hansa market door de Nederlandse politie uit de lucht gehaald.
Onderzoek naar politie-interventies kan voor opsporingsdiensten potentieel van groot belang zijn. Met opgedane inzichten over de impact van operaties kunnen er immers verbeteringen worden gerealiseerd. Er zijn slechts enkele wetenschappelijke studies waarin onderzoek is gedaan naar of inzicht wordt verschaft in de effecten van politie-interventies.
Soska en Christin (2015) maken duidelijk dat *dark markets* in zekere mate bestand zijn tegen de tot nu toe ingezette interventies. Deze auteurs hebben over een langere periode onderzoek verricht naar de dagelijkse omzet binnen een aantal prominente marktplaatsen. Hoewel het onderzoek primair niet als doel had om interventies en de effectiviteit ervan te meten, konden zij daar uiteindelijk wel het een en ander over zeggen, omdat in de onderzoeksperiode zowel operatie Marco Polo als operatie Onymous plaatsvond. Uit dit onderzoek blijkt dat interventies slechts tijdelijk invloed hadden op de totale dagelijkse omzet van alle markten. De destijds overgebleven *dark markets* vulden namelijk het gat van de gesloten marktplaatsen snel op en maakten zelfs een significante groei door. Ook Décary-Hétu & Giommoni (2017) zagen slechts een gelimiteerd effect van operatie Onymous. Zo werd de prijs van de producten op de *dark markets* niet beïnvloed. Op de marktplaatsen in hun steekproef zagen ze daarnaast dat er voor een periode van een maand een daling te zien was van het totale aantal

doi: 10.5553/JV/016758502018044005006

verkopers en *listings*[9] in de steekproef (waaronder de sites die door operatie Onymous gesloten waren), maar dat deze aantallen na een maand weer aantrokken.

Van Wegberg en Verburgh (2018) deden onderzoek naar operatie Bayonet. Ze onderzochten daarbij specifiek de migratiepatronen vanaf de door de politie gesloten *dark market*s Alphabay en Hansa Market naar Dream Market. Dream Market werd na operatie Bayonet de grootste *dark market*. Om de instroom van criminelen naar Dream market te bepalen, werd met behulp van *scraping* en *crawling* data vergaard van de nieuwe registraties op het forum.[10] De registraties op de marktplaats zijn niet publiekelijk zichtbaar. Nieuwe kopers en verkopers zijn hierdoor niet goed te onderscheiden van de al aanwezige kopers en verkopers. Dit is omdat je alleen hun eerste publieke activiteit kunt meten, bijvoorbeeld een verkoper die zijn eerste advertentie plaatst. Een koper is niet verplicht een review achter te laten. Kopers en verkopers kunnen dus al langer actief zijn op de marktplaats, maar nog nooit eerder zichtbare datapunten hebben achtergelaten. Hoewel een eerste reviewscore of eerste advertentie mogelijke afgeleiden zijn voor nieuwe instroom, zijn deze variabelen – voorzover de onderzoekers kunnen nagaan – nog niet getest op validiteit. Door te kijken naar de registratie op het forum weten we zeker dat dit nieuwe kopers en verkopers zijn. Als onderzoeker mis je dan echter de groep die zich niet registreert op het forum. Het selecteren van de juiste variabelen is vaak een grote uitdaging en vergt een creatieve kijk op data. Onze ervaring is dat het combineren van technische en sociale invalshoeken het beste werkt om achterliggende concepten zoals identiteit en in- en uitstroompatronen het best te kunnen meten.

Uit de resultaten van de nieuwe forumregistraties bleek dat er een aanzienlijk grotere instroom was na operatie Bayonet dan daarvoor (Van Wegberg & Verburgh 2018). De traceerbaarheid werd onder andere bepaald door de geregistreerde PGP-gegevens en door de username van de verkoper in een *dark web*-database[11] op te zoeken.

9 Advertenties op een dark market.

10 De gemiddelde marktplaats bestaat uit een forum en een marktplaats. Voor het forum moet je je apart registreren. Hierbij zijn de exacte datum en het exacte tijdstip zichtbaar als deze wordt gescraped en crawled.

11 De *dark web*-zoekmachine Grams had een database waarbij de PGP-gegevens, username(s) en beoordelingen van verkopers van verschillende marktplaatse bijgehouden werden. Hierdoor konden kopers buiten de marktplaatsen op eenvoudige wijze controleren hoe betrouwbaar een verkoper was. Grams is in 2017 gestopt en is niet meer beschikbaar.

doi: 10.5553/JV/016758502018044005006

Zo kon worden achterhaald of de nieuwe verkoper eerder actief was op Alphabay, Hansa Market of beide marktplaatsen. Het bleek dat verkopers minder migreerden, of in ieder geval minder traceerbaar waren, vanaf Hansa Market dan vanaf Alphabay. Ervan uitgaande dat verkopers in een anonieme setting juist traceerbaar willen blijven, zodat ze vindbaar blijven voor hun cliënten, indiceren deze uitkomsten dat de verkopers op Hansa market zich meer terugtrokken uit de markt, of in ieder geval de traceerbaarheid verminderden, dan op Alphabay. De verkopers vertoonden dus een heftiger reactie op de interventie op Hansa Market.

Het voornaamste verschil tussen deze twee interventies is dat bij Alphabay de stekker eruit werd getrokken en dat Hansa nog een maand werd gerund door de Nederlandse politie alvorens de politie deze marktplaats opdoekte. De criminele gemeenschap op *dark markets* was bekend met het risico van een 'gewone' sluiting van een marktplaats zoals Silk Road 1.0 en Silk Road 2.0. De criminelen waren echter onbekend met het risico van een overname en wisten niet welke gegevens de politie van hen had weten te bemachtigen. De Hansa-overname heeft daarmee het vertrouwen van de gemeenschap in de onderliggende faciliterende principes van *dark markets* meer geschaad dan andere interventies. Dit was ook het doel van de overname. Een interessante vraag is of het effect bij een volgende overname net zo groot zal zijn of dat de impact hiervan afneemt.

Dit onderzoek is de eerste stap richting nieuwe onderzoeksaanpakken die zich richten op de gedragseffecten na politieacties. Bij deze methode geldt het voorbehoud dat er enkel uitspraken gedaan kunnen worden over de instroom en niet over de groep verkopers die zich voorafgaand aan de politieactie al hadden verplaatst over meerdere marktplaatsen. Sommige verkopers verspreiden zich proactief over meerdere marktplaatsen als strategie om businesscontinuïteit te behouden (Soska & Christin, 2015). Daarnaast zorgt men er op deze wijze voor dat de eigen username niet door anderen gebruikt kan worden op andere platformen. Hiermee dammen verkopers niet alleen potentiële reputatieschade in, maar is het voor verkopers ook gemakkelijker om te migreren naar een andere marktplaats als de huidige verdwijnt.

doi: 10.5553/JV/016758502018044005006

Tot slot

In dit artikel hebben we aangegeven welke mogelijkheden er zijn voor onderzoek naar *dark markets*. Soms moeten onderzoekers creatief zijn bij het vergaren van data en bij het meten van constructen, waarbij sociale en technische invalshoeken worden gecombineerd. Om zeker te weten dat er gemeten wordt wat men wil weten, is het essentieel dat er goed begrip is van de werkzame mechanismen op een *dark market*. Of de omvang van een marktplaats kan worden bepaald aan de hand van het totale aantal advertenties, moet nog worden getoetst. De data die voorkomen uit operatie Bayonet zijn van grote waarde hiervoor en vormen een goudmijn voor (Nederlandse) wetenschappers die *dark markets* onderzoeken. Met deze data kunnen afgeleide variabelen getoetst worden door ze af te zetten tegen de werkelijke waarden. Door in onderzoeken aandacht te besteden aan interventies op *dark markets* kan allereerst de effectiviteit van interventies worden beoordeeld. Bij een volgende operatie kan worden geprofiteerd van inzicht in de succesvolle en minder succesvolle elementen van eerdere politieacties. Met het schetsen van de context rondom de impactstudie van operatie Bayonet (Van Wegberg & Verburgh 2018) is getracht een nieuwe invalshoek weer te geven. Deze invalshoek richt zich op het bestuderen van de gedragseffecten van interventies. Onderzoek naar *dark market*-interventies staat echter nog in de kinderschoenen en initiatieven om creatief te interveniëren en dit te onderzoeken moedigen wij ten zeerste aan.

Literatuur

Afilipoaie & Shortis 2015
A. Afilipoaie & P. Shortis, *From Dealer to Doorstep – how Drugs are sold on the dark net. GDPO Situation Analysis*. Swansea: Swansea University, 2015.

Aldrigde & Décary-Hétu 2016
J. Aldridge & D. Décary-Hétu, 'Cryptomarkets and the future of illicit drug markets', in: EMCDDA *The Internet and Drug Markets*, 2016, p. 23-32.

doi: 10.5553/JV/016758502018044005006

Aldrigde & Askew 2017
J. Aldridge & R. Askew, 'How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement', *International Journal of Drug Policy* 2017, afl. 41, p. 101-109.

Barratt & Aldrigde 2016
M. Barratt & J. Aldridge, 'Everything you always wanted to know about drug cryptomarkets (but were afraid to ask)', *International Journal of Drug Policy* 2016, afl. 35, 1-6.

Buxton & Bingham 2015
J. Buxton & T. Bingham, *The rise and challenge of dark net drug markets,* Policy Brief, Swansea: Swansea University 2015.

Christin 2013
N. Christin, 'Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace', *World Wide Web* 2013, Conference Proceedings, p. 213–224.

Cox 2016
J. Cox, 'Staying in the shadows: the use of bitcoin and encryption in cryptomarkets', in: *EMCDDA, The Internet and Drug Markets*, 2016, p. 41-47.

Décary-Hétu & Dupont 2013
D. Décary-Hétu & B. Dupont, 'Reputation in a dark network of online criminals', *Global Crime* (14) 2013, afl. 2/3, p. 175–196.

Décary-Hétu & Giommoni 2017
D. Décary-Hétu & L. Giommoni, 'Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous', *Crime, Law and Social Change* 2017 afl. 67, p. 55–75.

Van Hout & Bingham 2013
M.C. van Hout &T. Bingham, "'Surfing the Silk Road': A study of users' experiences', *International Journal of Drug Policy* (24) 2013, afl. 6, p. 524-529.

Holt e.a. 2015
T.J. Holt, O. Smirnova, Y.T. Chua & H. Copes, 'Examining the risk reduction strategies of actors in online criminal markets', *Global Crime*, (16) 2015, afl. 2, p. 81–103.

Karami e.a. 2015
M. Karami, Y. Park & D. McCoy, 'Stress testing the Booters: Understanding and undermining the business of DDoS services', *Arxiv* 2015, p. 1033–1043.

Kruithof e.a. 2016
K. Kruithof, J. Aldrigde, D. Décary-Hétu, M. Sim e.a., *Internet-facilitated drugs trade. An Analysis of the size, scope and the role of the Netherlands*, Santa Monica: RAND Europe 2016

doi: 10.5553/JV/016758502018044005006

Matanovic 2017
A. Matanovic, Blockchain/cryptocurrencies and cybersecurity. Threats and opportunities' *The 9 th International Conference on Business Information Security (BISEC-2017)* 2017, conference proceedings, p. 11-15.

Mounteney e.a.
J. Mounteney, A. Oteo & P. Griffiths, 'The internet and drug markets: shining a light on these complex and dynamic systems', in: *EMCDDA, The Internet and Drug Markets* 2016, p. 13-17.

Van Remunt & Van Wilsem 2016
T. van Remunt, & J. van Wilsem, 'Wat wordt er nu eigenlijk gezegd? Een verkennend onderzoek naar communicatiepatronen op het Darkweb', *PROCES* (95) 2016, afl. 1, p. 24–39.

Soska & Christin 2015
K. Soska, & N. Christin, 'Measuring the longitudinal evolution of the online anonymous marketplace ecosystem', *24th USENIX Security Symposium (USENIX Security 15)* 2015, conference proceedings, p. 33–48.

Spitters e.a. 2015
M. Spitters, F. Klaver, G. Koot & M. van Staalduinen, 'Authorship analysis on dark marketplace forums', *Intelligence and Security Informatics Conference (EISIC)* 2015, conference proceedings, p. 1–8.

Tzanetakis e.a. 2016
M. Tzanetakis, G. Kamphausen, B. Werse & R. von Laufenberg, 'The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets', *The International Journal on Drug Policy* (35) 2016, afl. 1, p. 58-68.

Van Wegberg e.a. 2018a
R.S. van Wegberg, S. Tajalizadehkhoob, K. Soska, U. Akyazi e.a.'Plug and Prey? Measuring the Commoditization of Cybercrime via Online Anonymous Markets', *27th USENIX Security Symposium (USENIX Security 18)* 2018, conference proceedings, p. 1009–1026.

Van Wegberg e.a. 2018b
R.S. van Wegberg, J. Oerlemans & M.O. Deventer, 'Bitcoin money laundering: mixed results?', *Journal of financial crime* (2) 2018, afl. 2, p. 419-435.

Van Wegberg & Verburgh 2018
R.S. Van Wegberg & T. Verburgh, 'Lost in the fream? Measuring the effects of Operation Bayonet on vendors migrating to Dream Market', *Websci* 2018, conference paper.

doi: 10.5553/JV/016758502018044005006

Facebookvrienden worden met de verdachte

Over undercoverbevoegdheden op internet

Jan-Jaap Oerlemans*

Online undercoverbevoegdheden bieden de mogelijkheid onder dekmantel bewijs te verzamelen op internet. De anonimiteit en (potentieel) grensoverschrijdende toepassing bieden vanuit opsporingsperspectief belangrijke voordelen. Opsporingsambtenaren kunnen bijvoorbeeld onder dekmantel chatten met een verdachte of zichzelf toevoegen als 'vriend' aan het Facebookaccount van de verdachte.
Voor de toepassing van undercoveropsporingsbevoegdheden bestaat een gedetailleerd juridisch kader vanwege de Wet bijzondere opsporingsbevoegdheden (Wet BOB).[1] Deze wet is een nasleep van de IRT-affaire en bestaat onder andere ter regulering van controversiële undercover opsporingsmethoden, die eind jaren tachtig en negentig intensiever werden gebruikt ter bestrijding van de georganiseerde drugscriminaliteit (Commissie-Van Traa 1996).[2]
Met de Wet BOB zijn de volgende drie bijzondere opsporingsbevoegdheden met betrekking tot undercoveropsporingsmethoden in het Wetboek van Strafvordering (Sv) geïntroduceerd:
1. pseudokoop en pseudodienstverlening;
2. stelselmatige informatie-inwinning;
3. infiltratie.

Voor de toepassing van deze bijzondere opsporingsbevoegdheden in een online context is het van belang dat in de wetsgeschiedenis al in 1999 is opgemerkt dat opsporingsbevoegdheden, zoals observatie en infiltratie, onder gelijke voorwaarden in de digitale wereld kunnen

* Mr. dr. J.J. Oerlemans is als onderzoeker verbonden aan eLaw, het Centrum voor Recht en Digitale Technologie van de Universiteit Leiden.
1 *Stb.* 1999, 245.
2 De Wet BOB is gebaseerd op de aanbevelingen van de commissie-Van Traa.

doi: 10.5553/JV/016758502018044005007

worden toegepast.[3] De reikwijdte van undercoveropsporingsbevoegdheden is binnen een online context echter niet altijd duidelijk. De memorie van toelichting reflecteert heel summier op de concrete toepassing van de bijzondere opsporingsbevoegdheden in de 'digitale wereld', waarbij de context waarbinnen deze bevoegdheden worden ingezet snel verandert. In 1999 kon de wetgever bijvoorbeeld de ontwikkeling van sociale media nog niet overzien. Daarbij kan het onduidelijk zijn of het bestaand juridisch kader nieuwe toepassingen van bijzondere opsporingsbevoegdheden in een online context nog 'dekt'. De vraag is bijvoorbeeld in hoeverre de 'accountovername' als undercoveropsporingsmethode mag worden ingezet.
In dit artikel worden de mogelijkheden van online undercoveropsporingsbevoegdheden in kaart gebracht, aan de hand van de wet, literatuur en actuele jurisprudentie.[4] Het artikel is opgehangen aan de bespreking van de drie bijzondere opsporingsbevoegdheden van pseudokoop, stelselmatige informatie-inwinning en infiltratie in een online context. De tussenconclusie geeft antwoord op de vraag welke meerwaarde deze online undercoverbevoegdheden bieden voor de opsporing. Het artikel sluit af met een bespreking van het jurisdictievraagstuk bij de toepassing van online undercoverbevoegdheden, omdat er spanning bestaat tussen de praktische mogelijkheid grensoverschrijdend via internet op te sporen, terwijl het internationaal recht dit slechts onder strikte voorwaarden toelaat.

Pseudokoop

De bijzondere opsporingsbevoegdheid van een pseudokoop kan ook plaatsvinden op internet, zoals een online marktplaats, waarbij een undercoveragent de aankoop doet van een goed (zoals drugs of wapens) of gegeven[5] (zoals gestolen persoonsgegevens). De online

3 Zie *Kamerstukken II* 1998/99, 26671, 3, p. 36. Zie ook Siemerink 2000b.
4 Dit artikel bouwt voort op de resultaten van mijn proefschrift (Oerlemans 2017). Ter beperking van de omvang van het artikel wordt slechts de politiële inzet van de bijzondere opsporingsbevoegdheden besproken. Voor de inzet van burgers zijn andere bijzondere opsporingsbevoegdheden onder grotendeels gelijke voorwaarden van toepassing, maar gelden aanvullende specifieke regels op basis van de Aanwijzing opsporingsbevoegdheden (*Stcrt.* 2014, 24442). Dit artikel concentreert zich op de relevante bepalingen in het Sv en de reikwijdte van deze bevoegdheden in een online context.
5 Sinds 2006 kunnen door de bekrachtiging van de Wet computercriminaliteit II ook *gegevens* worden gekocht bij een pseudokoop, in plaats van alleen goederen. Zie *Kamerstukken II* 1998/99, 26671, 3, p. 36-37.

doi: 10.5553/JV/016758502018044005007

pseudokoop wordt in de strafrechtpraktijk veelvuldig toegepast (Kruisbergen & De Jong 2010, p. 216).[6] Gepubliceerde uitspraken laten bijvoorbeeld zien dat de bijzondere opsporingsbevoegdheid in artikel 126i Sv wordt toegepast voor de aankoop van drugs, vuurwapens, vuurwerk en gestolen goederen op Marktplaats.nl en van ivoor van bedreigde diersoorten via internet.[7]

De online pseudokoop biedt opsporingsautoriteiten de mogelijkheid na te gaan wie het pakketje met het goed of de gegevens verzendt en waar het wordt afgeleverd. Als de verdachte de verzending van het pakketje zelf heeft verzorgd, dan geeft hij of zij mogelijk identificerende gegevens vrij. Een pakketje met drugs kan bijvoorbeeld vingerafdrukken bevatten of DNA-materiaal (via een postzegel), op basis waarvan verder onderzoek kan plaatsvinden. Bij de aankoop van goederen of gegevens via internet gaat soms online communicatie vooraf. Tijdens deze communicatie is het wellicht mogelijk identificerende gegevens van een verdachte te achterhalen, zoals een naam, telefoonnummer en/of e-mailadres. Deze gegevens bieden mogelijkheden voor andere opsporingshandelingen, zoals het vorderen van gegevens bij aanbieders van communicatiediensten.

De opsporingsbevoegdheid van de pseudokoop mag worden toegepast nadat een bevel van een officier van justitie is afgegeven een goed of gegevens aan te kopen in opsporingsonderzoeken met betrekking tot misdrijven zoals omschreven in artikel 67 Sv. Hoewel een algemeen verbod tot uitlokking altijd al van toepassing is, wordt in artikel 126i lid 2 Sv er nogmaals op gewezen dat 'een persoon er niet toe mag worden bewogen om een delict te plegen dat hij niet voornemens was'.[8] Indien een persoon een vermoedelijk illegaal goed of gegevens op internet

6 De pseudoverkoop of -dienstverlening wordt – op basis van gepubliceerde uitspraken – in een online context bijna nooit toegepast (zie alleen Hof Amsterdam 31 mei 2013, ECLI:NL:GHAMS:2013:2090). Deze opsporingsmethode wordt daarom buiten beschouwing gelaten.

7 Zie bijv. Rb. Roermond 4 maart 2009, ECLI:NL:RBROE:2009:BH4757 (online pseudokoop van gestolen goederen op Marktplaats.nl), Rb. Zutphen 28 januari 2011, ECLI:NL:RBZUT:2011:BP2308 (online pseudokoop van illegale wapens), Rb. Oost-Brabant 6 mei 2013, ECLI:NL:RBOBR:2013:BZ9467 (online pseudokoop van illegaal vuurwerk), Rb. Rotterdam 8 mei 2014, ECLI:NL:RBROT:2014:3504 (online pseudokoop van drugs op Silk Road), Rb. Overijssel 18 april 2016, ECLI:NL:RBOVE:2016:1323 (online pseudokoop van ivoor van bedreigde diersoorten), Rb. Rotterdam 11 augustus 2017, ECLI:NL:RBROT:2017:6830 (aankoop vuurwapen op het 'dark web') en Rb. Den Haag 17 mei 2018, ECLI:NL:RBDHA:2018:5775 (online pseudoaankoop creditcardgegevens van LizardSquad-verdachte).

8 Zie verder over het uitlokkingsverbod HR 4 december 1979, ECLI:NL:HR:1979:AB7429, *NJ* 1980/356, m.nt. Th.W. van Veen (*Tallon*-zaak) en in het bijzonder EHRM 4 november 2010, 18757/06, *EHRC* 2011/9, m.nt. Ölçer (*Bannikova t. Rusland*) over uitlokking in de context van art. 6 EVRM. Zie ook *Kamerstukken II* 1996/97, 25403, 3, p. 31.

doi: 10.5553/JV/016758502018044005007

aanbiedt en een opsporingsambtenaar koopt vervolgens het aangeboden goed of gegeven, dan zal van uitlokking niet snel sprake zijn. De opsporingshandelingen in undercoveroperaties moeten zorgvuldig worden geverbaliseerd, zodat ter zitting kan worden nagegaan of er sprake is van uitlokking en of het recht op een eerlijk proces van artikel 6 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) niet is geschonden.

Stelselmatige informatie-inwinning

Via internet kunnen opsporingsambtenaren onder dekmantel *interacteren* met een verdachte en personen in diens omgeving. Deze interacties vinden bijvoorbeeld plaats in de vorm van communicatie op chatkanalen, online discussie- of handelsfora of door 'vrienden' te worden met de verdachte (of diens vrienden) op sociale media.
De bijzondere opsporingsbevoegdheid van stelselmatige informatie-inwinning kan bij bovengenoemde voorbeelden van toepassing zijn. Het is voor de bevoegdheid kenmerkend dat een actieve interventie in het leven van de verdachte plaatsvindt; het gaat verder dan louter het (passief) observeren van gedrag van personen of zaken.[9] In cybercrimezaken is de undercoveropsporingsmethode bijzonder waardevol, omdat een *nickname* en andere '*online handle*', zoals een e-mailadres, belangrijke digitale sporen zijn op basis waarvan bewijs kan worden verzameld.[10]
De wetgever heeft bij de Wet BOB expliciet aangegeven dat stelselmatige informatie-inwinning ook op internet kan worden toegepast.[11] De toepassing van stelstelmatige informatie-inwinning in een online context is bijzonder interessant, omdat opsporingsambtenaren met dezelfde anonimiteit als andere internetgebruikers met betrokkenen in een opsporingsonderzoek kunnen interacteren. Ook is het – praktisch gezien – mogelijk grensoverschrijdend via internet op te treden (daarover meer in de laatste paragraaf over jurisdictie). In deze paragraaf worden de vier mogelijke toepassingen van de bevoegdheid van

9 Zie *Kamerstukken II* 1996/97, 25403, 3, p. 35.
10 Zie uitgebreid Oerlemans 2017, p. 30-36.
11 Zie *Kamerstukken II* 1996/97, 25403, 3, p. 34. Zie ook *Kamerstukken II* 1998/99, 26671, 3, p. 37.

doi: 10.5553/JV/016758502018044005007

stelselmatige informatie-inwinning besproken. Eerst wordt nog het juridisch kader kort uiteengezet.

Juridisch kader

De juridische basis voor de interactie met verdachten in een opsporingsonderzoek onder dekmantel is artikel 3 van de Politiewet 2012 of artikel 126j Sv als de opsporingsmethode door een opsporingsambtenaar wordt uitgevoerd. Artikel 3 Polw 2012 voldoet voor zover de opsporingsmethode niet op stelselmatige wijze wordt toegepast. Artikel 126j Sv vormt de basis voor de inzet van de bijzondere opsporingsbevoegdheid van 'stelselmatige informatie-inwinning'.
Er is sprake van stelselmatigheid als een 'min of meer volledig beeld van bepaalde aspecten van iemands privéleven' wordt verkregen.[12] Uit de memorie van toelichting kunnen vijf factoren worden afgeleid om te bepalen of een opsporingsmethode op *stelselmatige* wijze wordt toegepast. Dit zijn: (1) de duur, (2) de plaats, (3) de intensiteit, (4) de frequentie en (5) het gebruik van een technisch hulpmiddel.[13] Deze factoren lijken oorspronkelijk geformuleerd voor stelselmatige observatie en niet expliciet voor stelselmatige informatie-inwinning. Toch kan worden aangenomen dat deze factoren ook voor deze bijzondere opsporingsbevoegdheid zijn geformuleerd.[14] Welke grondslag ook wordt toegepast, het is van belang dat opsporingsinstanties de opsporingshandelingen voldoende vastleggen (mogelijk met behulp van software), zodat de verdediging en rechter kunnen nagaan of van stelselmatigheid sprake is en het uitlokkingsverbod niet wordt geschonden.
Voor de toepassing van de bijzondere opsporingsbevoegdheid is een bevel van een officier van justitie vereist. Artikel 126j Sv kan worden ingezet bij de opsporing van elk misdrijf voor een (verlengbare) periode van drie maanden. De inzet is daarmee niet beperkt tot opsporingsonderzoeken naar bepaalde delicten. In het kader van het project Modernisering Strafvordering zijn er plannen om de toepassing van de bijzondere opsporingsbevoegdheid te beperken tot mis-

12 Zie *Kamerstukken II* 1996/97, 25403, 3, p. 26-27.
13 Zie *Kamerstukken II* 1996/97, 25403, 3, p. 26-27 en *Kamerstukken II* 1998/99, 26671, 7, p. 46.
14 Zie ook Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, *Computerrecht* 2016/46, m.nt. J.J. Oerlemans en Hof Den Haag 25 mei 2018, ECLI:NL:GHDHA:2018:1248 (*Context*).

doi: 10.5553/JV/016758502018044005007

drijven met ten minste een maximale gevangenisstraf van een jaar.[15] De inzet van de bijzondere opsporingsbevoegdheid kan ingrijpend zijn voor de betrokkene in het opsporingsonderzoek, omdat de undercoveragent in een langdurig traject een relatie met de verdachte kan opbouwen. Het is goed mogelijk dat de verdachte in de veronderstelling is een innige vriendschappelijke band te hebben, waarna blijkt dat hij is 'verraden' door de undercoveragent (zie ook Kruisbergen & De Jong 2012, p. 51). Daarnaast bestaan er bij undercoveroperaties bepaalde risico's omtrent de integriteit van het onderzoek. Extra waarborgen zijn op hun plaats om bijvoorbeeld het risico te beperken dat een undercoveragent zich met criminele activiteiten bezighoudt die verder gaan dan oorspronkelijk met een officier van justitie zijn afgesproken. In mijn proefschrift heb ik zelfs de betrokkenheid van een rechter-commissaris bij de toepassing van stelselmatige informatie-inwinning aanbevolen, onder verwijzing naar jurisprudentie van het Straatsburgse Hof, dat ook de betrokkenheid van een rechter bij undercoverbevoegdheden prefereert (Oerlemans 2017, p. 241).[16]

Online communiceren met de verdachte

Opsporingsambtenaren kunnen met de inzet van de bijzondere opsporingsbevoegdheid van stelselmatige informatie-inwinning onder dekmantel communiceren met verdachten op bijvoorbeeld een chatkanaal, online forum of online marktplaats. Met behulp van anonimiseringstechnieken kan het IP-adres van de politieorganisatie worden verhuld en onder een nickname (pseudoniem) met dezelfde anonimiteit als andere internetgebruikers worden gecommuniceerd. Cybercriminelen communiceren bijvoorbeeld veel met elkaar in chatkanalen, via online forums of via chatprogramma's zoals Jabber. Opsporingsinstanties kunnen daar handig op inspelen. In de praktijk moet op grond van de Aanwijzing opsporingsbevoegdheden overigens in de meeste gevallen de unit 'Werken Onder Dekmantel' (WOD) worden ingezet. Uiteraard is ook bij deze afdeling voldoende kennis van de subcultuur op internet noodzakelijk om voldoende overtuigend over te komen (Siemerink 2000a, p. 145).

15 Zie het discussiestuk over de regulering van bijzondere opsporingsbevoegdheden van 6 juni 2014, p. 26.

16 Zie bijv. EHRM 24 juni 2008, 74355/01 (*Milinienè/Litouwen*), EHRM 4 november 2010, 18757/06, *EHRC* 2011/9, m.nt. Ölçer (*Bannikova/Rusland*) en EHRM 23 oktober 2014, 54648/09, *EHRC* 2015/1, m.nt. F.P. Ölçer (*Furcht/Duitsland*).

doi: 10.5553/JV/016758502018044005007

De accountovername als opsporingsmethode

Een bijzonder interessante toepassing van de opsporingsmethode is de 'accountovername'. Uit jurisprudentie blijkt bijvoorbeeld dat Zwitserse opsporingsautoriteiten het account van een Zwitserse zedenverdachte hebben overgenomen.[17] De Zwitsers hebben daarmee vervolgens ingelogd op het peer-to-peerprogramma GigaTribe.[18] Via GigaTribe is contact gelegd met een Nederlandse GigaTribe-gebruiker en zijn via het programma bestanden met kinderpornografie uitgewisseld. Het is denkbaar dat de opsporingsmethode van de accountovername ook in Nederland wordt toegepast. Omdat in de *GigaTribe*-zaak de Zwitserse autoriteiten het bewijs hadden verzameld en hebben overgedragen aan de Nederlandse autoriteiten, is op grond van het vertrouwensbeginsel de opsporingsmethode niet aan de Nederlandse wetgeving getoetst.[19]

Het kan bijzonder waardevol zijn door de ogen van de verdachte of informant op besloten internetomgevingen rond te kijken en bewijs te verzamelen ten behoeve van een opsporingsonderzoek. In een online context is het daarmee mogelijk bewijs te verzamelen uit besloten netwerken, forums, accounts en andere plekken waar degene toegang toe heeft, van wie het account wordt overgenomen. Uiteraard mag bij de accountovername (en overige undercoveropsporingsmethoden) geen uitlokking plaatsvinden; de verdachte mag er niet toe worden bewogen een strafbaar feit te plegen dat hij niet voornemens was. Bij de *GigaTribe*-zaak lijkt daar bijvoorbeeld geen sprake van te zijn, omdat de desbetreffende GigaTribe-gebruikers bewust kinderpornobestanden met elkaar uitwisselden en de verdachte niet is bewogen tot het uitwisselen van de illegale bestanden nadat is gecommuniceerd met een opsporingsambtenaar onder dekmantel.

Naar mijn mening is de accountovername als opsporingsmethode mogelijk met toepassing van de bijzondere opsporingsbevoegdheid van stelselmatige informatie-inwinning als een verdachte of informant vrijwillig meewerkt en zijn inloggegevens met opsporingsautoriteiten

17 Zie Rb. Noord-Nederland 27 juli 2017, ECLI:NL:RBNNE:2017:2882, *Computerrecht* 2018/6, m.nt. J.J. Oerlemans en Rb. Amsterdam 22 november 2017, ECLI:NL:RBAMS:2017:8564.

18 GigaTribe is eigenlijk een '*friend-to-friend*'-programma, omdat het alleen verbindt met toegevoegde contacten van de gebruiker.

19 Zie Rb. Noord-Nederland 27 juli 2017, ECLI:NL:RBNNE:2017:2882.

doi: 10.5553/JV/016758502018044005007

deelt.[20] Opsporingsambtenaren kunnen vervolgens kennisnemen van informatie in deze besloten omgevingen en daarbij gegevens overnemen. Met de inzet van undercoverbevoegdheid kunnen zij onder dekmantel uit naam van die verdachte of informant communiceren met betrokkenen in het opsporingsonderzoek. Als daarbij een strafbaar feit wordt gepleegd, zoals het delen van kinderpornomateriaal als in bovengenoemde zaak, moet de BOB-bevoegdheid van infiltratie worden toegepast. Zonder informatie hierover in een openbare richtlijn van het Openbaar Ministerie of jurisprudentie waarbij de rechtmatigheid van de opsporingsmethode aan de Nederlandse wetgeving wordt getoetst, kan niet met 100% zekerheid worden gesteld dat deze toepassing inderdaad onder Nederlandse wetgeving mogelijk is. Het is uiteraard van belang dat afspraken worden gemaakt over hoe ver de opsporingsautoriteiten mogen gaan uit naam van degene die zijn account beschikbaar heeft gesteld.

De lokpuber

Na implementatie van de Wet computercriminaliteit III[21] kunnen opsporingsambtenaren zich ook voordoen als minderjarige (de 'lokpuber') en chatten met andere internetgebruikers. Deze opsporingsmethode kan waardevol zijn bij de opsporing van het delict grooming en ontucht.
Grooming is kort gezegd de strafbare gedraging waarbij een meerderjarige via internet met een minderjarige een afspraak maakt om seks te hebben.[22] Eerder heeft een dergelijke undercoveroperatie tot vrijspraak geleid, omdat voor de delictsomschrijving is vereist dat daadwerkelijk met een *minderjarig persoon* wordt afgesproken.[23] De tekst van artikel 248e (grooming) en artikel 248a van het Wetboek van Strafrecht (Sr) (ontucht) wordt nu aangepast, waardoor het volstrekt helder

20 Zie mijn annotatie bij Rb. Noord-Nederland 27 juli 2017, ECLI:NL:RBNNE:2017:2882 in *Computerrecht* 2018/6. De commissie-Koops (2018) merkt in haar rapport op dat opsporingsambtenaren soms ook actief inloggen op een account van een verdachte, waarbij de inloggegevens zijn verkregen na de inbeslagname van een gegevensdrager. De commissie stelt voor deze opsporingsbevoegdheid mogelijk te maken door deze onder de reikwijdte van de netwerkzoeking onder te brengen. In het hier besproken geval komt daar nog bij dat onder het account van de betrokkene met anderen wordt gecommuniceerd, waardoor de inzet van een undercoverbevoegdheid voor de hand ligt.
21 De Wet computercriminaliteit III is op 26 juni 2018 door de Eerste Kamer aangenomen.
22 Grooming is strafbaar gesteld in art. 248e Sr.
23 Zie Hof Den Haag 25 juni 2013, ECLI:NL:GHDHA:2013:2302.

doi: 10.5553/JV/016758502018044005007

wordt dat ook van grooming en ontucht sprake kan zijn als een meerjarige opsporingsambtenaar of zelfs een computerprogramma met de verdachte onder dekmantel communiceert, vanwege de toevoeging in de delictsomschrijving:

> 'of iemand zich, al dan niet met een technisch hulpmiddel, waaronder een virtuele creatie van een persoon die de leeftijd van achttien jaren nog niet heeft bereikt, voordoet als een persoon die de leeftijd van achttien jaren nog niet heeft bereikt'.[24]

In de memorie van toelichting van de Wet computercriminaliteit III wordt opgemerkt dat de inzet van de lokpuber plaatsvond op basis van de algemene taakstellende bepalingen van opsporingsambtenaren, dat wil zeggen artikel 3 Polw jo. artikel 141-142 Sv.[25] Hierbij sluit de wetgever kennelijk aan bij de lokfiets, die volgens jurisprudentie kan worden neergezet op basis van artikel 3 Polw.[26] Toch is het de vraag of de 'lokpuber' en 'lokfiets' over één kam kunnen worden geschoren. Bij de lokfiets ontstaat weinig zicht op het privéleven van de verdachten of derden. Terwijl bij de lokpuber en webcamseks het gespreksonderwerp intiem (seksueel) van aard is. Bovendien worden persoonsgegevens of een opname opgeslagen in politiesystemen ter bewijsvoering van grooming of webcamseks. Bij grooming is bovendien mogelijk sprake van een langere duur van het gesprek of een hogere frequentie van gesprekken. De vraag is of de grondslag van artikel 3 Polw dan wel voldoet. Voor de zekerheid kan daarom beter de bijzondere opsporingsbevoegdheid van stelselmatige informatie-inwinning worden ingezet.

24 Uit het citaat blijkt tevens dat de aanpassing ook is geïnspireerd door de actie van Terres des Hommes met het 'Sweetie project', waarmee met een virtueel meisje webcamseks aan de kaak is gesteld (zie uitgebreid Schermer e.a. 2016). Zie voor kritiek op de formulering van deze nieuwe strafbaarstelling o.a. De Hingh 2018 en over de precaire grens met het uitlokkingsverbod ook Ölçer 2014, p. 18.

25 *Kamerstukken II* 2015/16, 34372, 3, p. 72. In dezelfde zin *Kamerstukken II* 2016/17, 34372, 6, p. 115.

26 Zie HR 28 oktober 2008, ECLI:NL:HR:2008:BE9817 (*lokfiets*) en HR 23 januari 2018, ECLI:NL:HR:2018:62.

doi: 10.5553/JV/016758502018044005007

Facebookvrienden worden met de verdachte

Kunnen opsporingsambtenaren ook 'Facebookvrienden' worden met de verdachte? Het antwoord op deze vraag luidt bevestigend, zo blijkt uit de '*Context*-zaak'.[27] In deze zaak hebben opsporingsambtenaren een fictief profiel opgesteld en zichzelf als vriend toegevoegd aan het profiel van de verdachte op Facebook. Daarnaast hebben ze deelgenomen aan een Facebookgroep waarvan werd gedacht dat deze zich bezighield met jihadistische activiteiten.
In de *Context*-zaak hadden de opsporingsambtenaren het bevel van de officier van justitie voor stelselmatige informatie-inwinning pas later tijdens de undercoveroperatie verkregen. De rechters waren echter van mening dat al vóór het aanmaken van een profiel het bevel tot stelselmatige informatie-inwinning noodzakelijk was.[28] Dit is mijns inziens terecht, omdat bij het toevoegen van een nepprofiel aan het profiel van een verdachte er een grote kans is dat een 'min of meer volledig beeld van bepaalde aspecten van iemands privéleven' wordt verkregen. De inschatting of daarvan sprake is, moet voorafgaand aan de inzet van de opsporingsmethode plaatsvinden. Op Facebookprofielen zetten mensen in de regel veel privégegevens online, zoals foto's, geboortedatum, interesses en informatie over relaties. Daarnaast is het gehele online sociale netwerk van de betrokkene met betrekking tot die dienst zichtbaar. Daarom wordt al snel bij de inzet van het BOB-middel op Facebook aan het criterium voldaan.
Uit de *Context*-zaak bleek ook dat er sprake was van gebrekkige vastlegging van de opsporingshandelingen.[29] Hier kan nog een les uit worden getrokken voor toekomstige zaken: de verslaglegging van dit type opsporingshandelingen in strafzaken is essentieel.

27 Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, *Computerrecht* 2016/46, m.nt. J.J. Oerlemans en Hof Den Haag 25 mei 2018, ECLI:NL:GHDHA:2018:1248 (*Context*).
28 Zie Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, r.o. 5.26-5.27. Zie de bevestiging van deze zaak in het arrest van Hof Den Haag 25 mei 2018, ECLI:NL:GHDHA:2018:1248 (*Context*).
29 Zie Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, r.o. 5.27. Het maken van een proces-verbaal is hier verplicht, omdat de opsporingshandelingen mogelijk relevant tijdens het proces kunnen zijn. De vormverzuimen hebben niet geleid tot een sanctie. Het vormverzuim is daarmee dus 'gerelativeerd'.

doi: 10.5553/JV/016758502018044005007

Infiltratie

Infiltratieoperaties onderscheiden zich van stelselmatige inwinning in de zin dat bij infiltratieoperaties wordt *geparticipeerd* in een criminele organisatie teneinde bewijsmateriaal over strafbare feiten te verzamelen.[30] Het is daarbij mogelijk dat (geautoriseerde) strafbare feiten worden gepleegd. De Nederlandse wetgever gaf in de memorie van toelichting van de Wet BOB aan dat door middel van infiltratieoperaties bewijs kan worden verzameld over de strafbare feiten die in georganiseerd verband worden gepleegd (of worden gepland) en met de opsporingsmethode inzicht kan worden verkregen in de modus operandi van de verdachten.[31] Een infiltratieoperatie mag alleen worden gestart nadat een bevel is verkregen van een officier van justitie in opsporingsonderzoeken naar misdrijven zoals omschreven in artikel 67 Sv. Bovendien moet sprake zijn van een ernstige schending van de rechtsorde.[32] Als intern controlemechanisme moet ook de Centrale Toetsingscommissie van het Openbaar Ministerie verplicht advies geven over de inzet van infiltratieoperaties.
Infiltratieoperaties kunnen ook in een online context worden ingezet, zoals op online fora of handelswebsites waarbij het vermoeden bestaat dat strafbare feiten in georganiseerd verband worden gepleegd. Het ligt bijvoorbeeld voor de hand dat bij de eerder in dit nummer beschreven *Hansa-operatie* de bijzondere opsporingsbevoegdheid van infiltratie is ingezet. Het is daarbij spannend om te zien hoe rechters omgaan met het doorlaten van de drugs of de uitgestelde inbeslagneming daarvan; door het runnen van de website wordt immers drugshandel gefaciliteerd, hetgeen een van de gevoeligheden bij de IRT-affaire was.
Uit gepubliceerde jurisprudentie blijkt dat opsporingsinstanties eerder hebben geprobeerd in de hiërarchie van een online drugsmarktplaats op te klimmen door middel van een online infiltratieoperatie.[33] De opsporingsambtenaren hadden in deze zaak onder andere het doel de

30 Zie *Kamerstukken II* 1996/97, 25403, 3, p. 28–29. Zie ook de brief van de minister van Veiligheid en Justitie van 8 oktober 2014 (nr. 571620) over het juridische verschil tussen 'informanten' en 'individuen die infiltreren binnen een opsporingsonderzoek'.
31 Zie *Kamerstukken II* 1996/97, 25403, 3, p. 28.
32 Zie art. 126h Sv.
33 Rb. Midden-Nederland 9 oktober 2014, ECLI:NL:RBMNE:2014:4790 en ECLI:NL:RBMNE:2014:4792. Vermoedelijk ging het hier om de online marktplaatsen '*Black Market Reloaded*' en '*Utopia*'. Zie ook ANP, 'OM wil tot zeven jaar cel voor internetdealers', Nu.nl 23 september 2014.

doi: 10.5553/JV/016758502018044005007

positie van 'moderator' te verwerven. Moderators managen de dagelijkse taken van een forum en controleren de naleving van interne regels door de gebruikers van een forum. In die positie kan een goed beeld van de gebruikers van het criminele forum worden verkregen. Ter uitvoering van de operatie werd de bijzondere opsporingsbevoegdheid van infiltratie ingezet. Het is de opsporingsambtenaren uiteindelijk niet gelukt zelf moderator te worden op het forum. Zij wisten echter wel het vertrouwen te winnen van een van de moderators op het forum. Door middel van een pseudokoop werden drugs aangekocht (de moderator verkocht zelf ook drugs) en voor de aflevering werd een afspraak in de fysieke wereld gemaakt. Na de aankoop van de drugs is de verdachte gevolgd tot zijn woonhuis door een observatieteam, waarvoor de bijzondere bevoegdheid van systematische observatie was ingezet. De verdachte werd later gearresteerd. De advocaat van de verdachte protesteerde tegen het feit dat de operatie zowel in de fysieke wereld als 'virtueel' had plaatsgevonden. De rechter keurde deze hybride toepassing van de bijzondere opsporingsbevoegdheid van infiltratie goed.[34] Toch is het opvallend dat maar één zaak over de toepassing van een online infiltratie beschikbaar is. Meer jurisprudentie is noodzakelijk om de reikwijdte van de toepassing van de bijzondere opsporingsbevoegdheid in een online context voldoende te bepalen.

Tussenconclusie

Online undercoverbevoegdheden bieden een meerwaarde voor de opsporing, omdat zij naast de fysieke undercoveroperaties de mogelijkheid bieden ook in een online context onder dekmantel bewijs te verzamelen. In dit artikel is nagegaan welke toepassingsmogelijkheden er zijn met betrekking tot de pseudokoop, stelselmatige informatie-inwinning en infiltratie.
De verstrekte voorbeelden van de inzet van de bijzondere opsporingsbevoegdheden in dit artikel hebben voornamelijk betrekking op opsporingsonderzoeken naar cybercriminaliteit. In reguliere opspo-

34 Zie Rb. Midden-Nederland 9 oktober 2014, ECLI:NL:RBMNE:2014:4790 en ECLI:NL:RBMNE:2014:4792. Siemerink (2000b, p. 144) gaf in 2000 al aan dat deze hybride toepassing veel zal voorkomen. Net als in het normale leven beginnen interacties soms op internet en kunnen deze leiden tot ontmoetingen in de fysieke wereld.

doi: 10.5553/JV/016758502018044005007

ringsonderzoeken (geen cybercrime) waarbij verdachten online actief zijn, biedt de toepassing van online undercoverbevoegdheden echter ook additionele mogelijkheden ten opzichte van de bevoegdheden die in de fysieke wereld kunnen worden toegepast.
In cybercrimezaken kunnen online undercoveroperaties een effectief opsporingsmiddel zijn om bewijs te verzamelen met een online handle als digitaal spoor, zoals een nickname, e-mailadres of profiel op sociale media. Onder de omstandigheid dat verdachten consistent gebruik maken van anonimiseringstechnieken die het IP-adres verhullen van het netwerk waar zij gebruik van maken, is de toepassing van online undercoveropsporingsmethoden een van de weinige middelen om bewijs te verzamelen in opsporingsonderzoeken met betrekking tot cybercriminaliteit.
Een bijkomend voordeel van de *online* toepassing van undercover-opsporingsbevoegdheden is dat opsporingsambtenaren net zo anoniem kunnen communiceren als de betrokkenen van het opsporingsonderzoek, zonder (direct) lijflijk risico en zonder de bureaustoel te hoeven verlaten, met een wereldwijd bereik van de opsporingsmethode. Dat wereldwijde bereik levert echter wel een jurisdictievraagstuk op, dat in de volgende paragraaf wordt geadresseerd.

Het jurisdictievraagstuk

Opsporingsbevoegdheden, inclusief undercoveropsporingsbevoegdheden, mogen niet over de territoriale grenzen worden toegepast zonder toestemming van de betrokken staat of verdragsbasis.[35] Nederland heeft vele bilaterale en multilaterale verdragen met andere staten afgesloten, waarin onder andere rechtshulp wordt geregeld. Over de toelaatbaarheid van de grensoverschrijdende *online* toepassing van undercoverbevoegdheden wordt daarin met geen woord gerept. Dit roept de vraag op in hoeverre opsporingsambtenaren de bovengenoemde bijzondere opsporingsbevoegdheden unilateraal (dus zonder

35 Zie de *S.S. 'Lotus'*-zaak (*Frankrijk/Turkije*), *PCIJ Reports*, Series A, nr. 10, 7 september 1927, p. 18-19: 'The first and foremost restriction imposed by international law upon a State is that – failing existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.' Zie ook 'Rule 11' uit de Tallinn Manual 2.0 (Schmidt 2017, p. 66).

doi: 10.5553/JV/016758502018044005007

toestemming van een betrokken staat) en grensoverschrijdend mogen toepassen.

In de praktijk worden online undercoveroperaties dikwijls unilateraal uitgevoerd. De eerder in dit nummer beschreven *Hansa*-zaak is daar een voorbeeld van. Naar goed gebruik worden de autoriteiten van de betrokken staat van de operatie op de hoogte gesteld en vaak wordt het bewijsmateriaal aan de betrokken autoriteiten overgedragen, zodat zij zelf handhavend kunnen optreden. Uit nieuwsberichten en jurisprudentie blijkt ook dat Amerikaanse autoriteiten via internet Nederlandse ingezetenen hebben benaderd en pseudokopen op online handelsplaatsen hebben uitgevoerd (zie bijvoorbeeld Kreling & Modderkolk 2016; Lensink & Vuijst 2013).[36] Het is niet helemaal duidelijk of de Amerikanen wisten dat het Nederlandse ingezetenen waren die zij benaderden. Als een drugsverkoper bijvoorbeeld van de anonimiseringsdienst TOR gebruik maakt en zijn handel op een online drugsmarktplaats in de Engelse taal aanbiedt, dan is zijn IP-adres en daarmee – na de vordering van gebruikersgegevens – het woonadres van de abonneehouder niet vast te stellen. In deze situatie is het verdedigbaar dat een undercoveroperatie unilateraal wordt uitgevoerd, omdat de opsporingsautoriteiten van de onderzoekende staat dan niet redelijkerwijs kunnen vaststellen waar de verdachte zich bevindt (Oerlemans 2017, p. 338). Opsporingsautoriteiten bewegen zich echter internationaalrechtelijk gezien op glad ijs als ze gericht een buitenlandse ingezetene via internet benaderen en op unilaterale wijze undercoverbevoegdheden toepassen.

De opsporing en vervolging van personen worden namelijk gezien als de exclusieve taak van een staat (Schmidt 2017, p. 21). Het zonder toestemming overnemen van die taak is dan een schending van de soevereiniteit van de betrokken staat.[37] Dat kan gevolgen met zich meebrengen, bijvoorbeeld op diplomatiek gebied. In Nederland heeft de vermeende unilaterale opsporing van de Amerikanen geleid tot Kamervragen.[38] Ook vanuit het perspectief van de burger zijn vraagtekens te zetten bij unilaterale digitale opsporing. Opsporingsinstanties over de hele wereld kunnen praktisch gezien met toepassing van hun eigen

36 Zie bijv. Rb. Rotterdam 11 augustus 2017, ECLI:NL:RBROT:2017:6830.

37 Overigens kan de betrokken staat achteraf alsnog toestemming geven.

38 Zie het antwoord op Kamervragen over de uitlevering van een Nederlandse hacker aan de VS door Roemenië van 7 juli 2012, *Aanhangsel Handelingen II* 2011/12, 3160 en het antwoord op Kamervragen over 'FBI agenten hacken mee met Nederlandse politie en detentieomstandigheden VS' van 15 april 2013, *Aanhangsel Handelingen II* 2012/13, 2001.

doi: 10.5553/JV/016758502018044005007

lokale wetgeving – zowel voor de strafbaarstellingen als voor opsporingsbevoegdheden – via internet opsporen, terwijl deze buitenlandse wetgeving niet kenbaar is voor de verdachte. Dat is een rechtsstatelijk probleem. Juist die kennis over de omstandigheden en onder welke voorwaarden opsporingsautoriteiten hun zwaardmacht mogen uitoefenen, is een kernprincipe van het leven in een rechtsstaat (Oerlemans 2017, p. 297). De mogelijke schending van de soevereiniteit van de betrokken staat leidt overigens niet tot gevolgen voor het strafproces, omdat hiermee geen beschermd belang van de verdachte gemoeid is dat zou leiden tot de sanctie van een vormverzuim in de zin van artikel 359a Sv.[39]

Hirsch Ballin (2018) schreef recentelijk in *Ars Aequi* een interessant artikel waarin zij pleit voor de mogelijkheid tot unilaterale online opsporing. Dit is op het eerste gezicht radicaal vanuit internationaalrechtelijk perspectief, maar zij merkt in het artikel meteen op dat daarvoor internationale afspraken noodzakelijk zijn. Voor online undercoveroperaties is het misschien mogelijk tot een EU-verdrag te komen. Europol is in het 'Internet Organised Crime Threat Assessment' (IOCTA)-rapport (2016, p. 14) over de noodzaak daarvan in ieder geval helder:

> 'The difficulties faced by law enforcement operating lawfully in the Darknet are clear, with many jurisdictions restricted by national legislation. A harmonised approach to undercover investigations is required across the EU.'

Tot op heden zijn hier nog geen initiatieven op EU-niveau voor geweest. Het is een grote stap voor staten ook formeel digitale unilaterale vormen van opsporing toe te staan en daarover afspraken te maken met andere staten. De stormachtige ontwikkeling van cybercriminaliteit en de noodzakelijke inzet van digitale opsporingsbevoegdheden om bewijs te verzamelen laten hun echter geen keuze.

39 Met andere woorden: de 'Schutznorm' is niet van toepassing. Zie HR 7 maart 2000, *NJ* 2000/539, m.nt. Sch.

doi: 10.5553/JV/016758502018044005007

Literatuur

Commissie-Koops 2018
Commissie-Koops (Commissie modernisering opsporingsonderzoek in het digitale tijdperk), *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018.

Commissie-Van Traa 1996
Commissie-Van Traa, *Inzake opsporing. Enquête opsporingsmethoden*, Den Haag: Sdu Uitgevers 1996.

Europol 2016
Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, Den Haag: European Police Office 2016.

De Hingh 2018
A.E. de Hingh, 'Grooming in het wetsvoorstel Computercriminaliteit III. Over het verbod op sexchatten met kinderen, robots en politieambtenaren', *Computerrecht* 2018, afl. 4, p. 208-215.

Hirsch Ballin 2018
M.F.H. Hirsch Ballin, 'De rol van grenzen bij opsporing: grenzeloze inzet van opsporingsbevoegdheden?', *Ars Aequi* 2018, afl. 6, p. 462-467.

Kreling & Modderkolk 2016
T. Kreling & H. Modderkolk, 'De dealer die in de Amerikaanse val werd gelokt', *de Volkskrant* 7 juni 2016.

Kruisbergen & De Jong 2010
E.W. Kruisbergen & D. de Jong, *Opsporen onder dekmantel. Regulering, uitvoering en resultaten van undercovertrajecten*, Den Haag: WODC/Boom Juridische uitgevers 2010.

Kruisbergen & De Jong 2012
E.W. Kruisbergen & D. de Jong, 'Undercoveroperaties: een noodzakelijk kwaad? Heden, verleden en toekomst van een omstreden opsporingsmiddel', *Justitiële verkenningen* (38) 2012, afl. 3, p. 50-67.

Lensink & Vuijst 2013
H. Lensink & F. Vuijst, 'Geen krediet voor David S.', *Vrij Nederland* 16 maart 2013.

Oerlemans 2017
J.J. Oerlemans, *Investigating cybercrime* (diss. Leiden), Amsterdam: Amsterdam University Press 2017.

Ölçer 2014
F.P. Ölçer, 'De lokmethode bij de opsporing van grooming', *Computerrecht* 2014, afl. 1, p. 10-19.

Schermer e.a. 2016
B.W. Schermer, I.N. Georgieva, S. van der Hof & B.J. Koops, *Legal aspects of Sweetie 2.0*, Leiden/Tilburg: Center for Law and Digital Technologies (eLaw)/Tilburg Institute for Law Technology and Society (TILT) 2016.

doi: 10.5553/JV/016758502018044005007

Schmidt 2017
M.N. Schmitt (red.), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge: Cambridge University Press 2017.

Siemerink 2000a
L.A.R. Siemerink, 'Bob logt in: infiltratie en pseudokoop op internet', *Computerrecht* 2000, afl. 3, p. 141-147.

Siemerink 2000b
L.A.R. Siemerink, *De wenselijkheid en mogelijkheid van infiltratie en pseudokoop op het internet* (ITeR-reeks, deel 30), Deventer: Kluwer 2000.

doi: 10.5553/JV/016758502018044005007

Nieuwe online opsporingsbevoegdheden en het recht op privacy

Een analyse van de Wet computercriminaliteit III

Bart Custers*

De criminaliteitscijfers in westerse landen zijn al jaren dalende (Van Dijk e.a. 2012), maar cybercrime lijkt een uitzondering te vormen op deze tendens. Cybercrime is de laatste jaren aan een flinke opmars bezig (Europol 2017). Bijvoorbeeld met banking malware en ransomware kunnen cybercriminelen grote hoeveelheden geld verdienen (Oerlemans e.a. 2016).[1] Cybercrime ontwikkelt zich snel en opsporingsbevoegdheden zijn niet altijd toegesneden op deze nieuwe ontwikkelingen. Als gevolg van deze ontwikkelingen kunnen politie en justitie druk ervaren van de politiek en het publiek om cybercrime stevig aan te pakken en tegelijkertijd het gevoel hebben onvoldoende te zijn toegerust voor deze taak. Teneinde de positie van opsporingsdiensten te verstevigen heeft de regering in het verleden regelmatig nieuwe wetgeving ontwikkeld met nieuwe strafbaarstellingen en nieuwe opsporingsbevoegdheden op het terrein van cybercrime. De meest recente wetgeving is de Wet computercriminaliteit III, die in juni 2018 werd aangenomen door de Eerste Kamer (en eerder al door de Tweede Kamer). De belangrijkste nieuwe bevoegdheden in deze wet zijn de hackbevoegdheid (waarbij de politie onder bepaalde omstandigheden computers van verdachten mag hacken en spyware mag installeren) en het Notice and Take Down (NTD)-bevel (de bevoegdheid bestanden te vernietigen of toegang daartoe onmogelijk te maken).
In deze bijdrage zal worden ingegaan op de achtergrond en inhoud van de Wet computercriminaliteit III. Eerst worden de (achtergronden

* Mr. dr. ir. B.H.M. Custers is associate professor en onderzoeksdirecteur bij eLaw, het Centrum voor Recht en Digitale Technologie van de Universiteit Leiden.

1 De omzet op online anonieme marktplaatsen op het darkweb (zoals Silk Road en Alpha Bay) lijkt daarentegen juist beperkt. Zie Van Wegberg e.a. 2018.

doi: 10.5553/JV/016758502018044005008

van de) Wet computercriminaliteit I en II besproken en daarna de aanleiding voor de Wet computercriminaliteit III. Vervolgens wordt dieper ingegaan op de inhoud van de Wet computercriminaliteit III, in het bijzonder de nieuwe strafbepalingen en de nieuwe opsporingsbevoegdheden die daarin zijn opgenomen. Daarna volgt een discussie over de legitimiteit en noodzakelijkheid van de hackbevoegdheid, de belangrijkste verandering die de Wet computercriminaliteit III met zich meebrengt en mogelijk ook de meest ingrijpende bevoegdheid als het gaat om het recht op privacy.

Achtergrond van de Wetten computercriminaliteit

Het internet biedt tal van mogelijkheden voor grensoverschrijdende criminele activiteiten. Dit komt doordat het internet geografische jurisdicties overschrijdt, flexibel is en zich zeer snel ontwikkelt (Denning & Baugh 2000; Goodwin & Koops 2015). In deze paragraaf wordt de cybercrimewetgeving in Nederland besproken, voor beter begrip van de Wet computercriminaliteit III.

Wet computercriminaliteit I (1993)

De introductie van de Wet computercriminaliteit[2] in 1993 markeert het begin van de cybercrimewetgeving in Nederland.[3] Vanaf dat moment werd voor het eerst wetgeving opgesteld die specifiek is gericht op computercriminaliteit, al bestonden verschillende vormen van computercriminaliteit al langer. De Wet computercriminaliteit 1993 en ook de daarop volgende Wet computercriminaliteit II en III betreffen in feite aanpassingswetgeving: ze passen het Wetboek van Strafrecht (Sr) en het Wetboek van Strafvordering (Sv) aan, voornamelijk door verschillende extra bepalingen in te voegen die specifiek zijn gericht op cybercrime, en door enkele bestaande bepalingen aan te passen, zodat ze ook vormen van cybercrime omvatten.

2 *Kamerstukken II* 1989/90, 21551, 1-3.

3 De term cybercrime komt in de Nederlandse wetgeving niet voor. Anglicismen worden door de wetgever sowieso graag vermeden, maar toen de voorbereidingen voor de eerste Wet computercriminaliteit werden gestart in de jaren tachtig, werd de term cybercrime ook nog niet gebruikt (Brenner 2007). In deze bijdrage worden de termen cybercrime en computercriminaliteit als synoniemen gebruikt.

doi: 10.5553/JV/016758502018044005008

De Wet computercriminaliteit 1993 vloeide onder meer voort uit een advies van de Commissie computercriminaliteit in 1985, ook bekend als de commissie-Franken. Deze commissie publiceerde in 1987 een uitgebreid rapport met aanbevelingen (Franken e.a. 1987). Als gevolg hiervan werd de eerste Wet computercriminaliteit in 1990 door de regering bij de Tweede Kamer ingediend. Deze wet volgde in grote lijnen de aanbevelingen van de commissie, behalve voor bevoegdheden voor doorzoekingen en inbeslagname. De Wet computercriminaliteit 1993 reguleert opsporing van digitale informatie en computernetwerken. Zij stelt onder meer computervredebreuk (in de volksmond ook wel 'hacken' genoemd) voor het eerst strafbaar (in art. 138ab Sr), evenals illegaal aftappen en afluisteren (art. 139a- 139c Sr), vernieling en beschadiging van computers of netwerken (art. 161sexies en 161septies Sr), het vervalsen van betaalkaarten (art. 232 Sr), het wissen en wijzigen van digitale gegevens (art. 350a Sr) en het openlijk aanprijzen van afluisterapparatuur (art. 441a Sr). Voor de opsporing is onder meer het woord 'telefoongesprekken' vervangen door 'niet voor het publiek bestemd gegevensverkeer via de telecommunicatie-infrastructuur', zodat ook andere vormen van communicatie, zoals Skype en e-mail hieronder vallen. Verder wordt in het Wetboek van Strafvordering het bevel tot toegang tot gegevens en het doorzoeken van computers tijdens huiszoekingen geregeld. Na verschillende aanpassingen en debatten in het parlement leidde dit tot de definitieve versie van deze wet, die op 1 maart 1993 van kracht werd.

Tijdens de parlementaire debatten was er veel aandacht voor de juridische kwalificatie van gegevens. Een typisch voorbeeld is de strafbaarstelling van diefstal (art. 310 Sr): 'hij die enig goed dat geheel of ten dele aan een ander toebehoort wegneemt, met het oogmerk om het zich wederrechtelijk toe te eigenen, wordt, als schuldig aan diefstal, gestraft met gevangenisstraf van ten hoogste vier jaren of een geldboete van de vierde categorie'. Bij gegevensdiefstal zijn er twee problemen met deze strafbepaling. Ten eerste is de vraag of gegevens vanuit strafrechtelijk perspectief gelden als 'object'. Historisch gezien ziet de diefstalbepaling op unieke, fysieke voorwerpen, hoewel in het verleden ook jurisprudentie is ontstaan met betrekking tot niet-tastbare goederen, zoals elektriciteit[4] en giraal geld.[5] Recenter zijn ook bel-

4 HR 23 mei 1921, NJ 1921/564.
5 HR 11 mei 1982, ECLI:NL:PHR:1982:AC1987.

doi: 10.5553/JV/016758502018044005008

tegoed (*Belminuten*-arrest[6]) en virtuele objecten in games (*Runescape*-arrest[7]) onder deze diefstalbepaling geschaard, maar over bijvoorbeeld virtueel geld, zoals bitcoins, heeft de rechter zich nog niet uitgesproken. Ten tweede is de vraag of bij gegevensdiefstal sprake is van 'wegnemen' – immers, doorgaans gaat het om een kopie van de gegevens en blijven de originele gegevens gewoon bij de oorspronkelijke eigenaar. Uiteindelijk heeft de Hoge Raad pas in 1996 vastgesteld dat gegevens strafrechtelijk gezien *geen* goed zijn.[8] Gegevensdiefstal kan dus niet worden vervolgd en bestraft via de reguliere diefstalbepaling.

Wet computercriminaliteit II (2006)

De Wet computercriminaliteit van 1993 werd gevolgd door de Wet computercriminaliteit II, die in 1999 door de regering bij de Tweede Kamer werd ingediend.[9] Deze wet was bedoeld om de eerdere cybercrimewetgeving verder uit te werken en te actualiseren. Opnieuw werden wijzigingen in het Wetboek van Strafrecht en het Wetboek van Strafvordering voorgesteld. De parlementaire behandeling ging gelijk op met de ontwikkeling van het Cybercrimeverdrag, ook wel het Verdrag van Boedapest genoemd.[10] Het Cybercrimeverdrag is het eerste internationale verdrag voor criminaliteit die via het internet wordt gepleegd. Het wetsvoorstel Computercriminaliteit II liep daardoor vertraging op, omdat de regering er uiteindelijk voor heeft gekozen in deze wetgeving tevens het Cybercrimeverdrag te implementeren. In 2005 werden verschillende herzieningen van het wetsvoorstel ingediend bij de Tweede Kamer.[11] Uiteindelijk werd de wet in september 2005 aangenomen door de Tweede Kamer en in mei 2006 door de Eerste Kamer. Op 1 september 2006 trad de wet in werking. In de tussentijd was ook het Cybercrimeverdrag goedgekeurd en aangenomen. De Wet computercriminaliteit II voorziet in een uitbreiding van de definitie van hacken (er is ook sprake van computervredebreuk als daarbij geen beveiliging wordt doorbroken) en virussen en malware (het gaat om het aanrichten van schade en niet langer om het zichzelf

6 HR 31 januari 2012, ECLI:NL:PHR:2012:BQ6575.
7 HR 31 januari 2012, ECLI:NL:PHR:2012:BQ9251.
8 HR 3 december 1996, ECLI:NL:HR:1996:ZD0584.
9 *Kamerstukken II* 1998/99, 26671, 1-3.
10 Voluit: Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken van 23 november 2001.
11 *Kamerstukken II* 2004/05, 26671, 7 (tweede nota van wijziging), 11 (derde nota van wijziging) en 17 (vierde nota van wijziging).

doi: 10.5553/JV/016758502018044005008

vermenigvuldigen). Het toepassen van *denial of service attacks*[12] is verboden en het afluisteren van netwerkverkeer door netwerkaanbieders is strafbaar gesteld (art. 273d Sr). Ook *grooming*, het via internet regelen van een seksuele ontmoeting met een minderjarige of seksuele afbeeldingen van die minderjarige, is strafbaar gesteld (art. 248e Sr). Verder verhoogt deze wet de strafmaxima voor veel delicten en kan een verdachte hiervoor in voorlopige hechtenis worden genomen. Als gevolg van het Cybercrimeverdrag zijn de meeste vormen van computercriminaliteit ook strafbaar in Nederland als een Nederlander ze in het buitenland begaat.
Strafprocesrechtelijk gezien is de Wet computercriminaliteit II belangrijk omdat het gebruik van de internettap (daterend van de Wet bijzondere opsporingsbevoegdheden uit 2000) wordt aangescherpt (art. 126la-126nb Sv), evenals het vorderen van gegevens (daterend van de Wet bevoegdheden vorderen gegevens uit 2005) (art. 126nc-126ni Sv). Voor meer details, zie Oerlemans 2017a.

Wet computercriminaliteit III (2018)

Cybercrime ontwikkelt zich aan de hand van nieuwe technologieën.[13] Het is duidelijk dat het strafrecht en het strafprocesrecht steeds in lijn moeten zijn met deze ontwikkelingen om cybercrime adequaat aan te kunnen pakken. Om de cybercrimewetgeving verder te actualiseren en het hoofd te kunnen bieden aan de nieuwste vormen van cybercrime diende de regering in december 2015 daarom de Wet computercriminaliteit III in bij de Tweede Kamer.[14] De Wet computercriminaliteit III is op 20 december 2016 aangenomen door de Tweede Kamer en op 26 juni 2018 aangenomen door Eerste Kamer. De totstandkoming van de wet was nogal een zware bevalling, met name vanwege politiek-bestuurlijke gevoeligheden. De Raad van State had vanaf het eerste moment veel kritiek op het wetsvoorstel, onder meer omdat de voorwaarden voor onderzoek op afstand in een computer niet differentieren naar de mate van inbreuk op de privacy, omdat structureel systeemtoezicht op de nieuwe opsporingsbevoegdheden onvoldoende was en omdat de noodzaak en effectiviteit van het decryptiebevel (ont-

12 Een *denial of service attack* is een aanval op een computersysteem, waarbij getracht wordt deze computer plat te leggen, doorgaans via overbelasting.
13 Voor recente ontwikkelingen, zie Europol 2017.
14 *Kamerstukken II* 2015/16, 34372, 2.

doi: 10.5553/JV/016758502018044005008

sleutelplicht) niet overtuigend waren. Ook in de Tweede Kamer was er veel debat. In totaal zijn er meer dan twintig amendementen ingediend en verschillende moties (zowel in de Eerste als in de Tweede Kamer), al zijn de meeste amendementen en moties uiteindelijk niet aangenomen. Waarschijnlijk wordt de wet per 1 januari 2019 van kracht.

De grootste problemen waar de opsporingsinstanties tegenaan lopen, zijn het gebruik van (1) versleuteling van gegevens, (2) draadloze netwerken en (3) cloudcomputingdiensten.[15] Het gebruik van encryptie is problematisch voor het gebruik van zowel doorzoekings- als aftapbevoegdheden. Met andere woorden, het versleutelprobleem kan zich zowel bij gegevens in opslag als bij gegevens in transport voordoen. Het probleem bij opslag is dat opsporingsdiensten zonder de sleutel (zonder het wachtwoord) niet meer bij de gegevens kunnen. Het probleem bij transport is dat opsporingsdiensten zonder de sleutel de onderschepte gegevens niet meer kunnen uitlezen.

In Nederland wordt ruim gebruik gemaakt van de internettap (Odinot e.a. 2012; Van de Pol 2006).[16] Bij het gebruik van encryptie van het internetverkeer wordt het voor opsporingsinstanties onmogelijk mee te kijken bij de onderschepte gegevensstromen. Veel communicatiediensten, zoals Twitter, WhatsApp en Gmail, gebruiken standaard encryptie. Andere diensten, zoals Facebook en Hotmail, bieden encryptie als optie aan voor hun gebruikers. Het gebruik van een internettap gaat via de aanbieder van een communicatiedienst, een Internet Service Provider (art. 126m Sv). Echter, het kan zijn dat de Internet Service Provider de gegevensstroom ook niet kan ontsleutelen (ondanks de verplichting in art. 126m lid 6 Sv). Ook komt het voor dat de tussenliggende diensten niet vallen onder het tapbevel en de ontsleutelplicht, of dat de diensten in het buitenland gevestigd zijn en niet kunnen worden verplicht tot medewerking. Verder noemt de memorie van toelichting het gebruik van TOR (The Onion Router)-netwerken. Dit is software die het mogelijk maakt voor gebruikers om anoniem op het internet te surfen: websites worden indirect bezocht, via een serie virtuele IP-adressen, zodat de privacy van gebruikers

15 MvT, p. 7-15.

16 Sinds de invoering van een nieuwe interceptiestandaard wordt door justitie geen onderscheid meer gemaakt tussen een telefoontap en een internettap, waardoor sinds 2014 geen afzonderlijke cijfers voor internettaps meer beschikbaar zijn. Zie *Kamerstukken II* 2013/14, 33930 VI, 1, bijlage, p. 17.

doi: 10.5553/JV/016758502018044005008

wordt gewaarborgd, aangezien er geen directe link is tussen de gebruikers en de websites die ze bezoeken.
Draadloze netwerken zijn tegenwoordig vrijwel overal (vaak gratis) beschikbaar in openbare ruimtes, in treinen en in de horeca. Internetgebruik via draadloze netwerken is voor opsporingsdiensten problematisch omdat interceptie van de communicatie lastig is. Ook andere vormen van communicatie, zoals optische communicatie, vormen een uitdaging voor interceptie (Custers 2008). Een internettap wordt afgegeven voor een specifiek IP-adres en een gebruiker kan niet worden getraceerd wanneer hij verbinding maakt met een andere router. Zodoende zijn opsporingsbevoegdheden grotendeels beperkt tot interceptie van het gegevensverkeer bij internettoegangs- en -knooppunten. Interceptie van communicatie via de ether is uiteraard technisch gezien wel mogelijk, maar dat kan alleen ter plaatse.
Cloudcomputing, bijvoorbeeld door het gebruik van diensten als Dropbox en Google Drive, is problematisch voor opsporingsdiensten omdat vaak onduidelijk is waar de servers zich bevinden. Via cloudcomputing kunnen gegevens op servers in een datacentrum ergens op de wereld worden opgeslagen en/of verwerkt, maar de locatie van de gegevens is vaak onduidelijk, soms ook voor de aanbieders van cloudcomputingdiensten zelf. Technisch gezien kunnen bestanden zelfs over meerdere servers in meerdere landen verspreid zijn opgeslagen. Als de opslag ergens in het buitenland is, is bovendien problematisch dat de opsporingsbevoegdheden zich niet uitstrekken tot computers en netwerken in het buitenland. Rechtshulpverzoeken zijn dan nodig, hetgeen vaak vertraging met zich meebrengt of op niets uitloopt.

Inhoud van de Wet computercriminaliteit III

De Wet computercriminaliteit III is vooral bekend vanwege de (strafprocesrechtelijke) bevoegdheden die opsporingsinstanties krijgen om te hacken en spyware te installeren (Kwakman & Buwalda 2014; Muijen 2016; Aink 2016). Daarnaast zijn ook enkele nieuwe strafbaarstellingen in de wet opgenomen, die hieronder kort worden besproken. Daarna komen de strafprocesrechtelijke onderdelen (het NTD-bevel en de hackbevoegdheid) aan bod. Voor een meer gedetailleerde bespreking, zie Oerlemans 2017a).

doi: 10.5553/JV/016758502018044005008

Strafrechtelijke onderdelen

De Wet computercriminaliteit III past het Wetboek van Strafrecht aan door een aantal artikelen te veranderen of in te voegen. In artikel 138c Sr wordt het overnemen van niet-openbare gegevens strafbaar gesteld. Volgens de memorie van toelichting gaat het hier om 'verduistering' van gegevens, naar analogie van de bepalingen voor 'diefstal' van gegevens.[17] Het overnemen moet dan wel opzettelijk ('willens en wetens') en wederrechtelijk (bijvoorbeeld zonder toestemming) zijn gebeurd. Denk bijvoorbeeld aan werknemers die bedrijfsgevoelige informatie op een draagbare gegevensdrager mee naar huis nemen of naar hun privémailadres sturen. Om niettemin ruimte te bieden aan klokkenluiders en ethische hackers die misstanden willen blootleggen, is in de memorie van toelichting aangegeven dat de wederrechtelijkheid vervalt indien hogere belangen een inbreuk rechtvaardigen en het handelen proportioneel en subsidiair is.
Omdat gegevens strafrechtelijk gezien in beginsel niet als goed worden beschouwd, is ook heling van gegevens niet strafbaar onder artikel 416 Sr (analoog aan de eerdergenoemde diefstal- en verduisteringsbepalingen). De Wet computercriminaliteit III introduceert daarom ook een strafbaarstelling voor de heling van gegevens in artikel 139g Sr. De verdachte moet dan ten tijde van zijn handelingen vermoeden dat de gegevens door een misdrijf zijn verkregen. Met deze strafbaarstelling moet het makkelijker worden gestolen persoonsgegevens of creditcardgegevens aan te pakken.
In artikel 248a Sr is het uitlokken van een minderjarige tot ontucht strafbaar gesteld en via artikel 248e is *grooming*. Via de Wet computercriminaliteit III worden deze artikelen zodanig gewijzigd dat het seksueel benaderen van kinderen door volwassenen via internet ook (duidelijker) strafbaar is gesteld. Door de wijziging is niet alleen het uitlokken van een minderjarige tot ontucht strafbaar, maar ook het uitlokken van iemand die zich voordoet als minderjarige tot ontucht strafbaar. Hierdoor ontstaat ruimte voor de inzet van zogeheten 'lokpubers', personen die zich als minderjarige voordoen (Ölçer 2014). Dit biedt meer ruimte voor het aanpakken van webcamseks met minderjarigen en *sextortion* (afpersing waarbij groomers met eerder beeldmateriaal het slachtoffer onder druk zetten om steeds opnieuw voor de

17 Art. 321 Sr over verduistering is niet toepasbaar omdat gegevens in het strafrecht niet als goed worden beschouwd. Zie de eerdere discussie over diefstal van gegevens.

doi: 10.5553/JV/016758502018044005008

camera te komen of steeds verder gaande seksuele handelingen te verrichten). Hieraan hebben opsporingsinstanties behoefte, omdat op deze manier daders op heterdaad kunnen worden betrapt tijdens de online communicatie (Lindenberg & Van Dijk 2016). Ook kan onder de nieuwe strafbaarstelling gebruik worden gemaakt van virtuele lokpubers, zoals Sweetie, een op basis van *cyber agent technology* zeer realistisch vormgegeven 10-jarig meisje dat op internet conversaties kan aangaan met verdachte personen die interesse tonen voor kinderen (Schermer e.a. 2016; Custers 2017).
Tot slot wordt via de Wet computercriminaliteit III een nieuw artikel 326d Sr ingevoegd, dat ziet op online handelsfraude. Dit fenomeen, ook wel 'Marktplaatsoplichting' genoemd, bestaat uit het aanbieden van producten of diensten via internet, zonder de intentie tot (volledige) levering van deze producten of diensten, terwijl wel de betaling ervan wordt opgestreken. Het klassieke oplichtingsartikel (art. 326 Sr) is onvoldoende om dit aan te pakken, omdat hiervoor sprake moet zijn van het aannemen van een valse naam of valse hoedanigheid, listige kunstgrepen of een samenweefsel van verdichtsels. Dat hoeft bij Marktplaatsoplichting niet het geval te zijn – daar is meer voor nodig, zoals het opzettelijk foute namen en e-mailadressen hanteren om de mogelijkheden tot verhaal te bemoeilijken (Oerlemans 2017a). Met de nieuwe strafbepaling kan dit beter worden geadresseerd, al zullen conflicten over het niet leveren van producten of diensten eerst en vooral via civielrechtelijke weg moeten worden opgelost.

Strafprocesrechtelijke onderdelen

De Wet computercriminaliteit III past ook het Wetboek van Strafvordering aan op twee belangrijke punten, door de introductie van het zogeheten NTD-bevel en de hackbevoegdheid. Het NTD-bevel, opgenomen in een nieuw artikel 125p Sv, houdt in dat de officier van justitie in bepaalde gevallen een aanbieder van een communicatiedienst kan bevelen om terstond bepaalde informatie ontoegankelijk te maken, ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten. Daartoe moet de officier van justitie eerst een machtiging vorderen bij de rechter-commissaris. Er bestaat al sinds 2008 een NTD-gedragscode onder internetaanbieders om op verzoek strafbaar of onrechtmatig materiaal te verwijderen van het internet, maar dit is op vrijwillige basis. Deze gedragscode blijft gewoon van

doi: 10.5553/JV/016758502018044005008

kracht en wordt als eerste, vrijwillige stap gebruikt. Pas als aanbieders niet meewerken of niet zijn aangesloten bij deze gedragscode, wordt de tweede, verplichtende stap ingezet.
Hoe bepaald materiaal ontoegankelijk moet worden gemaakt, laat de nieuwe wet in het midden. Volgens de memorie van toelichting kan dit via hardware (ontoegankelijk maken van ingangen van computers, afsluiten van servers) of via software (internetfilters, gegevens versleutelen/wissen) en moet per geval worden bekeken welke maatregel het meest effectief is, rekening houdend met proportionaliteit en subsidiariteit.
Met behulp van het NTD-bevel kunnen *botnets* beter worden bestreden. Dit zijn netwerken van computers die zijn besmet met malware (kwaadaardige software) waarvan cybercriminelen op afstand misbruik kunnen maken. Voorbeelden zijn onder meer het gebruik van botnets voor bitcoin mining, het versturen van grote hoeveelheden spam, het verzamelen van bedrijfsgeheimen en andere vertrouwelijke informatie, het uitvoeren van DDoS-aanvallen[18] en het verspreiden van banking malware en ransomware.
De hackbevoegdheid, opgenomen in een nieuw artikel 126nba Sv, houdt in dat opsporingsambtenaren onder bepaalde omstandigheden mogen binnendringen in computers en netwerken, al dan niet met een technisch hulpmiddel. Na inzet van deze bevoegdheid kunnen vervolgens andere opsporingsbevoegdheden worden ingezet, zoals het vastleggen van gegevens, het uitvoeren van (stelselmatige) observatie, het direct afluisteren en het ontoegankelijk maken van gegevens (Oerlemans 2017b).
Het gebruik van technische hulpmiddelen betreft doorgaans software die wordt beschreven als *spyware* (in deze context ook wel *policeware* genoemd) en heeft functionaliteiten zoals het op afstand aanzetten van camera's, microfoons en GPS, het vastleggen van toetsaanslagen (zogeheten *keyloggers*), het maken van *screenshots* en het doorzoeken van bestanden op de betreffende computers.
Het mag duidelijk zijn dat de inzet van de hackbevoegdheid een ernstige inbreuk op het recht op privacy met zich meebrengt (zie hieronder). Om die reden is de inzet van de hackbevoegdheid afgebakend en zijn extra waarborgen aangebracht. Zo is de inzet van de hackbe-

18 Een DDoS-aanval (Distributed Denial of Service) is een aanval op een computersysteem vanuit een grote hoeveelheid andere computers, teneinde het systeem plat te leggen (bijv. door doelbewuste overbelasting).

doi: 10.5553/JV/016758502018044005008

voegdheid alleen toegestaan in zaken waar het gaat om ernstige of zeer ernstige misdrijven en moet de inzet bovendien dringend zijn in het opsporingsonderzoek. Daarnaast mag deze bevoegdheid alleen worden ingezet nadat de officier van justitie dit heeft gevorderd bij de rechter-commissaris en vervolgens machtiging daartoe heeft verkregen. Bovendien is als extra waarborg ingebouwd dat ook de Centrale Toetsingscommissie van het Openbaar Ministerie wordt geraadpleegd in elke zaak waarin de hackbevoegdheid wordt ingezet.

Legitimiteit en noodzakelijkheid

De Wet computercriminaliteit III biedt opsporingsdiensten vergaande bevoegdheden voor hacken en de inzet van spyware. De inzet van zulke bevoegdheden brengt inbreuken op het recht op privacy met zich mee. Volgens de Hoge Raad speelt bij het beoordelen van inbreuken op het recht op privacy artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) een fundamentele rol.[19] Het recht op privacy is niet absoluut: inbreuken kunnen gerechtvaardigd zijn, mits die inbreuken bij wet zijn voorzien, voor legitieme doeleinden zijn (legitimiteit) en noodzakelijk in een democratische samenleving (noodzakelijkheid). Hier wordt ingegaan op de criteria van legitimiteit en noodzakelijkheid van de hackbevoegdheid in relatie tot het recht op privacy. Voor een meer gedetailleerde analyse, zie Pool en Custers (2017).

Het legitimiteitscriterium vereist dat voor het gebruik van opsporingsbevoegdheden een duidelijke wettelijke basis aanwezig is. Het is om deze reden dat de Nederlandse overheid de hackbevoegdheid in de wet wil vastleggen. Hoewel deze bevoegdheid al in zekere mate bestond (Oerlemans 2017b), wordt met de nieuwe wet voorzien in een expliciete(re) wettelijke basis. Ook het beoogde doel van de Wet computercriminaliteit III is legitiem, namelijk het bestrijden van cybercrime, hetgeen in lijn is met de belangen van nationale veiligheid, openbare veiligheid en het voorkomen van strafbare feiten. Kortom, aan het legitimiteitscriterium wordt goed voldaan.

Het noodzakelijkheidscriterium ligt ingewikkelder. Hoe noodzakelijkheid moet worden afgewogen tegen privacyinbreuken is niet zonder

19 HR 9 januari 1987, NJ 1987/928.

doi: 10.5553/JV/016758502018044005008

meer duidelijk, omdat het in beginsel ongelijke grootheden zijn. Bij dit criterium kan onder meer worden gekeken naar effectiviteit (wordt met de hackbevoegdheid het doel überhaupt bereikt, en zo ja, in welke mate?), proportionaliteit (is de inbreuk op rechten van de verdachte en anderen in redelijke verhouding tot de beoogde doelen van de hackbevoegdheid?) en subsidiariteit (kunnen de beoogde doelen wellicht ook op een andere, minder ingrijpende wijze worden bereikt?).
Uit eerder onderzoek bleek dat het niet altijd een gebrek aan opsporingsbevoegdheden was dat de politie hinderde bij de aanpak van criminaliteit, waaronder cybercrime (Custers 2012). Integendeel, het leek erop dat de politie onvoldoende gebruik maakte van bestaande opsporingsbevoegdheden, onder meer door gebrek aan operationele capaciteit, controle en situationeel bewustzijn (Prins 2011). De regering heeft eerder zelfs toegegeven dat de beschikbare kennis en capaciteit onvoldoende zijn om cybercrime effectief te kunnen aanpakken.[20] Waarschijnlijk is er bij de reguliere politiediensten sindsdien weinig veranderd, maar daar staat tegenover dat er de afgelopen jaren flink is geïnvesteerd in meer kennis en mensen, onder meer bij het High Tech Crime-team van de politie.
De vraag is of de hackbevoegdheid de beoogde doelen kan realiseren, namelijk het oplossen van problemen met betrekking tot encryptie, draadloze netwerken en cloudcomputing (Moitra 2003). Bij versleutelde opslag kan hacken een oplossing bieden via online doorzoeking (het zich op afstand toegang verschaffen tot een computer en eventueel gegevens kopiëren voor bewijsmateriaal). Ook kan zogeheten *spyware* of *policeware* (Jacobs 2012) worden geïnstalleerd om daarmee bijvoorbeeld wachtwoorden te onderscheppen of gegevens terug te sturen naar de politie. Bij versleuteld transport kan hacken een oplossing bieden door voor of achter de *end-to-end encryption* mee te kijken. Door een account te hacken of spyware te plaatsen op de computer van de verdachte kan bijvoorbeeld een microfoon op afstand worden ingeschakeld om gesprekken af te luisteren dan wel screenshots worden gemaakt of toetsaanslagen worden geregistreerd (met een zogeheten *keylogger*) om de communicatie op afstand te onderscheppen. In beginsel kan de hackbevoegdheid ook worden gebruikt om het cloudcomputingprobleem aan te pakken, omdat de politie zich op afstand toegang kan verschaffen tot een computer en vervolgens

20 *Kamerstukken II* 2012/13, 29911, 79.

doi: 10.5553/JV/016758502018044005008

gegevens kan kopiëren. Zo kan bijvoorbeeld in een online account van de verdachte worden ingelogd en op afstand bewijs worden verzameld. In theorie zijn er dus voldoende manieren waarop de hackbevoegdheid effectief kan zijn. In de memorie van toelichting wordt echter nergens aangegeven hoe opsporingsdiensten in concrete zaken baat zouden hebben of hebben gehad bij de inzet van hackbevoegdheden.

Bij proportionaliteit moet zowel worden gekeken naar de opbrengsten van de hackbevoegdheid (dus de hierboven beschreven effectiviteit) als naar de inbreuken op privacy en vervolgens worden afgewogen. In feite worden appels en peren vergeleken, want het gaat om ongelijke, onvergelijkbare grootheden. De proportionaliteitsvraag wordt regelmatig behandeld door het Europese Hof van Justitie. In 2014 zette dit Hof een streep door de Europese Dataretentierichtlijn uit 2006, waarbij grote hoeveelheden verkeersgegevens van telefoon- en internetgebruikers werden opgeslagen voor opsporingsdoeleinden.[21] Als reden werd gegeven dat de richtlijn fundamentele rechten schond op te algemene en allesomvattende wijze en daarmee disproportioneel was. In feite was het een carte blanche zonder duidelijke afbakening. Om een vergelijkbaar scenario te voorkomen zijn in elk geval extra voorwaarden aan de hackbevoegdheid verbonden, waaronder een Centrale Toetsingscommissie, specifieke normering van technische hulpmiddelen en beperking van het aantal delicten waarbij de hackbevoegdheid kan worden ingezet.[22] Tegelijkertijd brengt het gebruik van de hackbevoegdheid ook risico's met zich mee, zoals bijvoorbeeld misbruik van bevoegdheden (*function creep*), uitlokking (en vervagende grenzen tussen observatie en interactie) en identiteits- en aansprakelijkheidsvraagstukken (onduidelijk wie wat doet en wie verantwoordelijk is voor schade).

Bij subsidiariteit moet worden onderzocht of er alternatieven zijn die minder inbreuk maken op het recht op privacy. Met internettaps kan tot zekere hoogte vergelijkbare informatie worden verzameld, maar bij encryptie kan een internettap onvoldoende opleveren. Via rechtshulpverzoeken kan tot op zekere hoogte ook vergelijkbare informatie

21 EU Court of Justice (2014) Judgment of the ECJ in Digital Rights Ireland data retention challenge, Joined Cases C-293/12 (Digital Rights Ireland) and C-594/12 (Seitlinger), *Official Journal of the European Union* 8 april 2014.

22 Overigens is de hackbevoegdheid niet slechts beperkt tot bepaalde vormen van cybercrime. Ook bij verdenking van bepaalde 'gewone' delicten, zoals drugsgerelateerde criminaliteit, kan de hackbevoegdheid worden ingezet.

doi: 10.5553/JV/016758502018044005008

worden verzameld, maar daarbij kunnen Nederlandse opsporingsdiensten stuiten op landen die niet willen of kunnen meewerken. Zelfs als dat geen probleem is, kunnen rechtshulpverzoeken bijzonder veel vertraging opleveren, hetgeen zich slecht verhoudt tot de snel veranderende wereld van cybercriminaliteit. Tegelijkertijd lijkt de memorie van toelichting vooral gericht op efficiëntievoordelen: door het gebruik van de hackbevoegdheid kan de politie cybercrime aanpakken met minder kosten, tijd, mankracht en andere inspanningen. Volgens de memorie van toelichting kan worden verwacht dat de hackbevoegdheid mogelijk ook andere vormen van politie-inzet kan vervangen, waarmee middelen kunnen worden bespaard. Deze bewering wordt echter nergens verder onderbouwd en het valt te bezien of dit werkelijk het geval is.
Veel opsporingsinstanties in binnen- en buitenland geven aan dat er een gebrek aan expertise is als het gaat om de inzet van technologie in de opsporing, vervolging en berechting van criminaliteit (Custers 2012; Custers & Vergouw 2015). Het valt te bezien of de hackbevoegdheid in de Wet computercriminaliteit III, een instrument dat veel technische expertise behoeft, niet op dezelfde problemen zal stuiten. Het punt dat veel opsporingsbevoegdheden onvoldoende en suboptimaal worden ingezet, geeft te denken over de nieuwe bevoegdheden die nu aan de lijst worden toegevoegd.

Conclusie

Nederland behoort tot de koplopers op het gebied van cybercrimewetgeving. Inmiddels is al de derde Wet computercriminaliteit door het parlement geloodst. Bij alle opeenvolgende wetten zijn nieuwe vormen van cybercrime strafbaar gesteld, nieuwe opsporingsbevoegdheden geïntroduceerd en bestaande bepalingen aangescherpt, opdat ze beter zijn toegesneden op technologische ontwikkelingen. De meest recente wetgeving, de Wet computercriminaliteit III, introduceert nieuwe strafbepalingen en opsporingsbevoegdheden die technologische uitdagingen als versleuteling van gegevens en cloudcomputing te lijf gaan. In het Wetboek van Strafrecht worden, naar analogie van gegevensdiefstal, ook verduistering en heling van gegevens strafbaar gesteld. Daarnaast worden grooming, sextortion en online handelsfraude steviger aangepakt. In het Wetboek van Strafvordering worden

doi: 10.5553/JV/016758502018044005008

het NTD-bevel en de hackbevoegdheid als nieuwe opsporingsbevoegdheden geïntroduceerd.
Met name de hackbevoegdheid is een ingrijpende bevoegdheid, die de opsporingsinstanties in de gelegenheid stelt spyware te installeren op computers, om vervolgens bestanden van verdachten in te zien en mee te luisteren en/of te kijken door bijvoorbeeld op afstand microfoons en camera's aan te zetten of toetsaanslagen te registreren. Gebruik van de hackbevoegdheid brengt aanzienlijke inbreuken op het recht op privacy met zich mee. Hoewel de Wet computercriminaliteit III daarvoor een expliciete en legitieme basis neerlegt, is niet overduidelijk dat de bevoegdheid in alle opzichten voldoet aan de eisen van effectiviteit, proportionaliteit en subsidiariteit. De hackbevoegdheid kan bijdragen aan het oplossen van versleutelproblemen en cloudcomputingproblemen in de opsporing, maar vereist grondige technische en juridische kennis (iets waarin momenteel nog wordt geïnvesteerd door opsporingsdiensten) voordat er resultaten mee kunnen worden geboekt. De memorie van toelichting is weinig overtuigend in het aantonen van de toegevoegde waarde van de hackbevoegdheid. Nergens wordt duidelijk hoe opsporingsdiensten in concrete zaken baat zouden hebben of hebben gehad bij de inzet van hackbevoegdheden. Ook de onderbouwing van het efficiëntieargument is dun: onduidelijk blijft hoe de hackbevoegdheid mogelijk ook andere vormen van politie-inzet kan vervangen en daarmee middelen kunnen worden bespaard.
Tegelijkertijd brengt de hackbevoegdheid ook risico's met zich mee, zoals function creep, uitlokking en identiteits- en aansprakelijkheidsvraagstukken. Deze risico's worden maar beperkt afgedekt. Vooraf moet toestemming worden verkregen van de rechter-commissaris en achteraf is er toezicht door de Inspectie Justitie en Veiligheid op het volgen van de procedures. Een rechtmatigheidstoets achteraf kan in de rechtszaal plaatsvinden, maar voor zaken die uiteindelijk niet worden vervolgd, ontbreekt dan enige vorm van toetsing. Dat is problematisch, omdat niet transparant is hoe en hoe vaak opsporingsinstanties de bevoegdheid zullen toepassen. Niet uitgesloten is dat de hackbevoegdheid uiteindelijk een vergelijkbaar lot is beschoren als de eerdere Dataretentierichtlijn, die door het Europese Hof van Justitie ongeldig werd verklaard vanwege schending van fundamentele rechten op te algemene en allesomvattende wijze en daarmee disproportioneel was.

doi: 10.5553/JV/016758502018044005008

Literatuur

Aink 2016
J.R.J. Aink, 'Het wetsvoorstel Computercriminaliteit III. Een high tech inhaalslag?', *TPWS* 2016/46.

Brenner 2007
S.W. Brenner, 'History of computer crime', in: K. de Leeuw & J. Bergstra (ed.), *The history of information security*, Amsterdam: Elsevier 2007, p. 705-721.

Custers 2008
B.H.M. Custers, 'Tapping and data retention in ultrafast communication networks', *Journal of International Commercial Law and Technology* (3) 2008, p. 94-100.

Custers 2012
B.H.M. Custers, 'Technology in policing: Experiences, obstacles and police needs', *Computer law & security report (1)*, 2012, p. 62-68.

Custers 2017
B.H.M. Custers, *Cyber agent technology en de Wet op de Inlichtingen- en Veiligheidsdiensten (WIV)*, Universiteit Leiden 2017.

Custers & Vergouw 2015
B. Custers & B. Vergouw, 'Promising policing technologies: Experiences, obstacles and police needs regarding law enforcement technologies', *Computer Law & Security Review* (31) 2015, p. 518-526.

Denning & Baugh 2000
D.D. Denning & W.E. Baugh Jr, 'Hiding crimes in cyberspace', in: D. Thomas & B.D. Loader (red.), *Cybercrime: Law enforcement, security and surveillance in the information age*, London: Routledge 2000, p. 105-131.

Van Dijk e.a. 2012
J. van Dijk, A. Tseloni & G. Farrell, *The international crime drop*, Londen: Palgrave Macmillan 2012.

Europol 2017
Europol, *The Internet Organised Crime Threat Assessment (IOCTA)*, Den Haag: European Police Office 2017.

Franken e.a. 1987
H. Franken e.a., *Informatietechniek & strafrecht* (Rapport van de Commissie Computercriminaliteit), Den Haag: Staatsuitgeverij 1987.

Goodwin & Koops 2015
M.E.A. Goodwin & B.J. Koops, *Cyberspace, the cloud and cross-border criminal investigation. The limits and possibilities of international law*, Den Haag: WODC 2015.

Hyman 2013
P. Hyman, 'Cybercrime: It's serious, but exactly how serious?', *Communications of the ACM* (56) 2013, p. 18-19.

doi: 10.5553/JV/016758502018044005008

Jacobs 2012
B.P.F. Jacobs, 'Policeware', *Nederlands Juristenblad* 2012, p. 2761-2764.
Kerr 2013
O. Kerr, 'Fascinating new case on legal standards for searching a remote computer with unknown location', 2013, http://volokh.com/2013/04/26/fascinating-new-case-on-legal-standards-for-searching-a-remote-computer-with-unknown-location/.
Kwakman & Buwalda 2014
N.J.M. Kwakman & M.E. Buwalda, 'Het ontwerp wetsvoorstel Computercriminaliteit III', *Ars Aequi* 2014, p. 9-18.
Lindenberg & Van Dijk 2016
K. Lindenberg & A.A. van Dijk, *Herziening van de zedendelicten?* Den Haag: WODC 2016.
Moitra 2003
S.D. Moitra, 'Developing policies for cybercrime', *European Journal of Crime, Criminal Law and Criminal Justice* (13) 2003, p. 435-464.
Muijen 2016
P.J.D.J. Muijen, 'Wet computercriminaliteit III. To boldly go where no man has gone before', *Privacy & Informatie* 2016, p. 104-110.
Odinot e.a. 2012
G. Odinot, D. de Jong, J.B.J. van der Leij, C.J. de Poot e.a., *Het gebruik van de telefoon- en internettap in de opspring*, Den Haag: Boom Lemma 2012.
Oerlemans 2017a
J.J. Oerlemans, 'De Wet computercriminaliteit III: meer handhaving op internet', *Strafblad* 2017, p. 350-359.
Oerlemans 2017b
J.J. Oerlemans, *Investigating cybercrime* (diss. Leiden), Amsterdam: Amsterdam University Press 2017.
Oerlemans e.a. 2016
J.J. Oerlemans, B.H.M. Custers, R.L.D. Pool & R. Cornelisse, *Cybercrime en witwassen: bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware*, Den Haag: Boom criminologie 2016.
Ölçer 2014
F.P. Ölçer, 'De lokmethode bij de opsporing van grooming', *Computerrecht* 2014/3.
Van de Pol 2006
W. van de Pol, *Onder de tap. Afluisteren in Nederland*, Amsterdam: Uitgeverij Balans 2006.

doi: 10.5553/JV/016758502018044005008

Pool & Custers 2017
R.L.D. Pool & B.H.M. Custers, 'The police hack back. Legitimacy, necessity and privacy implications of the next step in fighting cybercrime', *European Journal of Crime, Criminal Law and Criminal Justice* 2017, p. 123-144.

Prins 2011
R. Prins, 'Polderen tegen cybercrime', *Security Management* (6) 2011, p. 28.

Schermer e.a. 2016
B.W. Schermer, I. Georgieva, S. van der Hof & B.J. Koops, *Legal aspects of Sweetie 2.0*, Leiden/Tilburg: Center for Law and Digital Technologies (eLaw)/Tilburg Institute for Law Technology and Society (TILT) 2016.

Van Wegberg e.a. 2018
R. van Wegberg, S. Tajalizadehkhoob, K. Soska, U. Akyazi e.a., 'Plug and prey? Measuring the commoditization of cybercrime via online anonymous markets', *Proceedings of the 27th USENIX Security Symposium*, Baltimore, 15-17 augustus 2018, p. 1009-1026.

doi: 10.5553/JV/016758502018044005008

Summaries

Justitiële verkenningen (Judicial explorations) is published six times a year by the Research and Documentation Centre of the Dutch Ministry of Security and Justice in cooperation with Boom juridisch. Each issue focuses on a central theme related to judicial policy. The section Summaries contains abstracts of the internationally most relevant articles of each issue. The central theme of this issue (no. 5, 2018) is *The digitalization of organized crime.*

The effect of the internet on the structure of organized cybercrime. Findings from an international empirical study

Geralda Odinot, Christianne de Poot and Maite Verhoeven

Worldwide, the digitalization of society is proceeding rapidly and this brings new forms of crime. The threats arising from different types of cybercrime are real and constantly evolving, as the internet with its anonymity and borderless reach, provides new opportunities for criminal activities. This article describes some results from an international empirical study aimed to gather more insight on the link between cybercrime and organized crime as well as on the question whether cybercrime is organized. It shows how cybercriminals cooperate with each other and what this organization structure looks like.

Criminal money flows and IT. On innovative modi operandi, old certainties, and new bottlenecks

Edwin Kruisbergen, Rutger Leukfeldt, Edward Kleemans and Robby Roks

In this article we analyze how organized crime offenders use IT to handle their money flows. How and to what extent do offenders use IT-facilitated possibilities, such as bitcoin, to launder their money? The empirical data consist of thirty large-scale police investigations. These thirty cases are part of the Organized Crime Monitor, an ongoing research project into the nature of organized crime in the Netherlands. One of the most striking findings is the fact that cash is still king – even for online drug dealers who get paid in digital currencies.

Organized child pornography networks on the Dark Web

Madeleine van der Bruggen

The emergence of Dark Web child pornography forums and their availability to large offender communities has enabled a professional form of child pornography distribution as well as an increased exchange of criminal and social capital. Offenders have access to a new platform in which strong ties and long-lasting relationships with co-offenders are formed. Moreover they could be classified as organized crime, because child pornography Dark Web forums are characterized by a hierarchical order, a clear role division and illegal power structures that regulate the illegal activities. The implications from a law enforcement as well as from scientific perspective are discussed.

The non-human (f)actor in cybercrime. Cybercriminal networks seen from a cyborg crime perspective

Wytske van der Wagen and Frank Bernaards

Botnets, banking malware and other high-tech crimes are increasingly analyzed by criminological scholars. Their distributed and automated nature poses however various theoretical challenges. This article presents an alternative approach, denoted as the 'cyborg crime' perspective, which adopts a more hybrid view of networks and also assigns an active role to technology. The value of this approach is demonstrated by reflecting on findings from earlier empirical work that analyzes conversations between cybercriminals involved in botnets and related activities. The research shows that technological nodes can take an important position in the organizational structure of cybercriminal networks and do not merely have a functional role. Viewing technology as an actor within a criminal network might offer new criminological insights in both the composition of these networks and how to disrupt them.

Out of the shadow. Opportunities for researchers in studying dark markets

Thijmen Verburgh, Eefje Smits and Rolf van Wegberg

In this article the authors present the lessons learned from previous research efforts into dark markets. First the important features of dark markets are discussed, i.e. anonymity and trust, as well as the question how data on dark markets can be collected. Next, the authors illustrate

how this data can be used to study the phenomenon of dark markets itself as well as the impact of police interventions on dark markets.

Befriending a criminal suspect on Facebook. Undercover powers on the Internet

Jan-Jaap Oerlemans

This article investigates which online undercover investigative methods are applied in practice and how they fit in the Dutch legal framework. In particular, the three special investigative powers of a pseudo purchase, systematic information gathering and infiltration are examined. Investigative powers cannot be applied unilaterally (across state borders). When law enforcement officials cannot reasonably determine the location of the suspect, the online unilateral application of undercover investigative powers is allowed. However, there is still a risk that diplomatic tensions arise with the involved state. States should agree in treaties under which circumstances cross-border online undercover operations are allowed.

New investigative powers and the right to privacy. An analysis of the Dutch Cybercrime III Act

Bart Custers

In 2018 the Dutch parliament accepted new cybercrime legislation (the Cybercrime III Act) that creates several new online criminal offences and gives law enforcement agencies new investigative powers on the Internet. This article describes the background of Dutch cybercrime legislation and the contents of the Cybercrime III Act. The newly introduced cybercrimes are discussed as well as the new investigative competences. Particularly the legitimacy and the necessity of the investigative power of the police to hack computer systems of suspects may significantly interfere with the right to privacy.

Congresagenda

6 november	Huwelijksdwang en familie-eer (Tilburg) www.avans.nl/onderzoek/expertisecentra/veiligheid/evenementen/onderzoek/kennismiddag-familie-eer
8 november	Multiprobleemgezinnen (Amsterdam) https://leidscongresbureau.nl/event/multiprobleemgezinnen
9 november	Big Data & Crime (Den Haag) https://bit.ly/2NYIHyE
14-17 november	ASC Annual Conference (Atlanta, GA) www.asc41.com/annualmeeting.html
16 november	Drugbeleid voor festivals (Brussel) www.politiestudies.be/vrij.cfm?Id=425
19-20 november	Challenge accepted! Exploring pathways to civil justice in Europe (Rotterdam) www.eur.nl/esl/evenementen/challenge-accepted-exploring-pathways-civil-justice-europe-2018-11-19
22 november	Jaarcongres huiselijk geweld (Ede) www.huiselijkgeweldcongres.nl
29 november	De aanpak van witwassen (Breukelen) www.kerckebosch.nl
30 november	Niets dan de waarheid: getuigenbewijs in strafzaken (Breukelen) www.kerckebosch.nl
13 december	De aanpak van problematische schulden (Utrecht) www.kerckebosch.nl
14 december	Democratie: nieuwe ontwikkelingen (Rotterdam) www.eur.nl/esl/evenementen/staatsrechtconferentie-democratie-nieuwe-ontwikkelingen-14-december-2018-eur-2018-12-14
20 december	Sociale veiligheid en digitalisering (Den Bosch) www.avans.nl

Het volgende nummer van *Justitiële verkenningen* (Jv 6) is gewijd aan:

Dreiging en onveiligheidsgevoelens

Nadere informatie bij de redactie.

doi: 10.5553/JV/016758502018044005009

Wetenschappelijk Onderzoek- en
Documentatiecentrum
Ministerie van Justitie en Veiligheid