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