45. Opsporing en bestrijding van online drugsmarkten

MR. DR. J.J. OERLEMANS EN DRS. R.S. VAN WEGBERG

Online drugsmarkten hebben zich in de afgelopen tien jaar flink geprofessionaliseerd. In dit artikel staat de vraag centraal hoe de opsporing en verstoring van online drugsmarkten in zijn werking gaat. Daarbij wordt extra aandacht besteed aan de digitale infiltratie-operatie van de online drugsmarkt 'Hansa' in mei 2017.

1. Inleiding

Tien jaar geleden (in 2008) zag een ondernemende Hagenees een gat in de drugsmarkt: de online verkoop van (soft) drugs. Waar je met een fysieke coffeeshop slechts klanten in de regio kunt bedienen, heb je via internet in potentie een wereldwijd bereik. Daarmee was 'Wolkenwietje.nl' geboren, vermoedelijk de eerste online webwinkel voor (soft) drugs uit Nederland. Al snel werd de website op verzoek van de politie offline gehaald.[1] Tot dusver krijgen online coffeeshops in Nederland geen gedoogvergunning. Een van de redenen is dat online coffeeshops praktisch gezien niet goed kunnen voldoen aan alle gedoogcriteria, zoals het controleren van de leeftijd en nationaliteit van de kopers en het verbod op adverteren via internet.[2]

Drie jaar later (in 2011) is de online drugsverkoop aanmerkelijk geprofessionaliseerd. Veel internetters maakten kennis met de online drugsmarkt *Silk Road*, na een veelbesproken interview met de eigenaar (de 'administrator') van de website *The Dread Pirate Roberts*.[3] Silk Road was een van de eerste echt succesvolle 'webshops voor drugs'.[4]

Dit type online anonieme markten kenmerken zich door (1) toegankelijkheid via het anonimiseringsnetwerk Tor[5], (2) betaling in een *cryptocurrency*[6], en (3) de levering van drugs via de post.[7]

Het verdienmodel bij deze moderne online drugsmarkten is doorgaans als volgt. Voor elke transactie tussen een koper (*buyer*) en verkoper (*vendor*) krijgt de beheerder van de 'webwinkel' een klein percentage in cryptocurrency. Na twee jaar werd Ross Ulbricht, de verdachte achter 'The Dread Pirate Roberts' door de Secret Service, DEA en FBI in San Francisco in de kraag gevat.[8] De 28 miljoen dollar aan Bitcoin op de digitale portemonnee van de verdachte werd via een veiling verkocht. Ross Ulbricht kreeg een levenslange gevangenisstraf opgelegd.[9]

In 2016 schatte onderzoeksbureau RAND, in opdracht van het WODC, dat maandelijks 14 tot 25 miljoen dollar aan drugs wordt omgezet op online anonieme markten. Uit het onderzoek kwam ook naar voren dat Nederlandse

1 'Politie sluit digitale coffeeshop', *Telegraaf*.nl, 19 maart 2008: *'De Boven Regionale Recherche Haaglanden-Hollands Midden heeft een 47-jarige Hagenaar aangehouden omdat hij via internet softdrugs verhandelde. Via zijn digitale coffeeshop verkocht de man onder meer hasj, hennep en joints. De pakketjes drugs werden na bestelling bij de klanten thuisbezorgd, zo liet een politiewoordvoerder woensdag weten.'*

2 Zie de Aanwijzing Opiumwet, *Stcrt.* 2015, 5391. Dat wil natuurlijk niet zeggen dat Nederlandse online drugswebshops niet bestaan. Zo adverteert de website 'Groentebezorgd' bijvoorbeeld met: *'Eenvoudig wiet kopen online en wiet bestellen via groenthuisbezorgd.com! Wiet kopen online is veilig en betrouwbaar. Bestel je wiet online en krijg het de volgende dag in huis. In plaats van het bezoeken van de coffeeshop kun je nu wiet kopen via internet.'*

3 Adrian Chen, 'The Underground Website Where You Can Buy Any Drug Imaginable', *Wired Magazine*, 1 juni 2011. Internetcriminelen gebruiken doorgaans pseudoniemen 'nicknames' om anoniemer te blijven.

4 Typering door Rechtbank Rotterdam in hun uitspraak in klare taal over een online drugsmarkt. Rb. Rotterdam 16 juli 2019, ECLI:NL:RBROT:2019:5630.

5 Tor staat voor 'The Onion Router', een anonimiseringsdienst die het internetverkeer langs een aantal servers stuurt en het netwerkverkeer versleuteld. Zie R. Dingledine, N. Mathewson & P. Syverson, 'Tor: The second-generation onion router', Naval Research Lab Washington DC 2004.

6 Cryptocurrencies, zoals Bitcoin en Monero, zijn virtueel geld dat is gebaseerd op cryptografische software, waarbij er geen centrale autoriteit is die toeziet op het beheer van het geld. Zie, o.a., J.J. Oerlemans e.a., 'Cybercrime en witwassen', WODC, nr. 319, Meppel: Boom Criminologie 2016.

7 Zie T. Verburgh, E. Smits & R.S. van Wegberg, 'Uit de schaduw: Perspectieven voor wetenschappelijk onderzoek naar dark markets', *Justitiële verkenningen* 2018, jrg. 44, nr. 5, p. 68-82.

8 Zie uitgebreid J. Bearman, 'The Rise and Fall of Silk Road', *Wired Magazine,* april 2015 en het interactieve achtergrond verhaal 'Marktplaats van de drugs. De opkomst en ondergang van de digitale drugsmarktplaats', *De Volkskrant* op https://www.volkskrant.nl/kijkverder/2015/.

9 S. Thielman, 'Silk Road operator Ross Ulbricht sentenced to life in prison', 29 mei 2015, *The Guardian*. De 144.336 bitcoins waren destijds meer dan 28 million dollar waard. Zie het persbericht, 'Manhattan U.S. Attorney Announces Forfeiture Of $28 Million Worth Of Bitcoins Belonging To Silk Road', 16 januari 2014, U.S. Department of Justice.

verkopers van drugs ruim vertegenwoordigd lijken te zijn op online drugsmarkten.[10] De Nederlandse politie speelt een voortrekkersrol in het opsporen en bestrijden van deze markten, mede vanwege de aanwezigheid van Nederlandse verkopers (of hen die zich als zodanig voordoen) en het feit dat regelmatig Nederlandse IT-infrastructuur betrokken is bij de hosting van drugsmarkten.

Dit artikel legt uit welke opsporingsmethoden worden gebruikt voor het verzamelen van bewijs in opsporingsonderzoeken naar online drugsmarkten en op welke wijze deze opsporingsmethoden zijn gereguleerd. Daarbij wordt extra aandacht besteed aan de rechtmatigheid van de digitale infiltratie-operatie van de online drugsmarkt 'Hansa' in 2017. Een nevendoel van de Hansa-operatie is het *verstoren* van online drugsmarkten. In dit artikel wordt uitgelegd hoe dat in deze casus in zijn werking is gegaan en wat de gedachten daarbij zijn geweest. Ook voor strafrechtjuristen is het van belang kennis te nemen van de tendens dat het verstoren van criminaliteit een prominente plek krijgt bij de bestrijding van gedigitaliseerde criminaliteit. Daarbij worden door de auteurs ook enkele juridische vragen geïdentificeerd die in de toekomst een rol kunnen spelen.[11]

Het artikel is als volgt opgebouwd. In paragraaf 2 wordt nagegaan welke opsporingsmethoden worden gebruikt bij het verzamelen van bewijs op online drugsmarkten en hoe deze opsporingsmethoden zijn genormeerd. In paragraaf 3 wordt aandacht besteed aan de strategie van het 'verstoren' op online drugsmarkten. In paragraaf 4 wordt het artikel afgesloten met een conclusie en een blik op de toekomst van online drugsmarkten.

2. Opsporing op online drugsmarkten

Online drugsmarkten zijn vrijwel alleen toegankelijk via het anonimiseringsnetwerk 'Tor'. Als gevolg daarvan kan enerzijds de webserver waar de website op draait vaak niet worden gelokaliseerd en wordt anderzijds het IP-adres van de bezoekers van de websites verhuld.[12] Door het gebrek aan een centrale organisatie die de activiteiten gebruikers van Tor bijhoudt, is het daar niet mogelijk gebruikersgegevens te vorderen. De beheerders van websites of andere diensten die via Tor bereikbaar zijn, kunnen door het verhullen van de IP-adressen vaak niet worden gelokaliseerd en zullen in de regel niet voldoen aan (buitenlandse) vorderingen van opsporingsautoriteiten.

Het volgen van IP-adressen en het vorderen van gegevens is daarmee geen bruikbare strategie bij de opsporing van de personen achter de drugsdelicten die via online drugsmarkten worden gepleegd. Het volgen van de digitale sporen die gebruikers van online drugsmarkten achterlaten, zoals 'nicknames', reviews en de interactie aangaan (onder dekmantel) met de kopers en verkopers op online drugsmarkten, biedt aanzienlijk meer kansen.

2.1 Openbronnenonderzoek op online drugsmarkten

Kopers en verkopers op online drugsmarkten laten digitale sporen na die bruikbaar zijn voor opsporingsinstanties. Kopers en verkopers gebruiken bijvoorbeeld een pseudoniem (*nickname*), teneinde hun anonimiteit te waarborgen. Het pseudoniem wordt over langere tijd en op meerdere markten gebruikt, mede omdat de verkopers van drugs worden beoordeeld via online *reviews* en daarmee een betrouwbare reputatie kunnen opbouwen.[13] Het is ook mogelijk dat een pseudoniem op andere plekken op internet wordt gebruikt, zoals een webforum waar wordt gediscussieerd over onderwerpen. Maar ook andere digitale sporen, zoals een 'handtekening' onder een profielnaam of een PGP-sleutel die wordt gebruikt voor het versleuteld versturen van berichten levert mogelijk een bruikbaar spoor op.

Het verzamelen van gegevens uit open bron wordt ook wel 'openbronnenonderzoek' genoemd. Daarbij kan onderscheid worden gemaakt tussen het 'handmatig verzamelen' van gegevens en 'geautomatiseerd verzamelen' van gegevens. Bij een handmatige verzameling van gegevens gaat een rechercheur aan de hand van een digitaal spoor zelf op zoek naar gerelateerde informatie. Nuttige informatie wordt vervolgens opgeslagen. Het is ook mogelijk door middel van software, zogenoemde *crawlers*, van tevoren alle beschikbare informatie te verzamelen op basis van bepaalde parameters. Vervolgens kan een rechercheur via een soort zoekprogramma bijvoorbeeld een pseudoniem intoetsen en alle beschikbare informatie krijgen die het programma heeft verzameld. Het is ook denkbaar dat daarbij verbanden worden gelegd: zoals één persoon die verschillende nicknames gebruikt, maar steeds dezelfde PGP-sleutel gebruikt voor het versturen van bericht of hetzelfde bitcoinadres gebruikt voor het overmaken van het geld. Andere software wordt gebruikt voor de analyse van bitcointransacties, met het doel om na te gaan wie de verzenders en ontvangers zijn van het geld of bijvoorbeeld van welke online drugsmarkt bepaalde transacties vandaan komen. Deze informatie kan worden gebruikt voor de iden-

10 Zie K. Kruithof e.a, 'Internet-facilitated drugs trade. An analysis of the size, the scope and the role of the Netherlands', Santa Monica/Cambridge: RAND, WODC 2016. Nederlandse verkopers waren naar schatting verantwoordelijk voor 8% van de totale drugsomzet op de acht geanalyseerde markten. Per hoofd van de bevolking is die omzet 2,4 keer zo groot als de omzet uit het Verenigd Koninkrijk en 4,5 keer zo groot als die van de Verenigde Staten.

11 In dit artikel wordt niet alle techniek achter de gebezigde systemen en opsporingsmethoden uitgelegd; in plaats daarvan ligt de nadruk op het informeren over de gebezigde opsporingsbevoegdheden, de innovatieve verstoringsstrategieën van de politie bij de bestrijding van online drugsmarkten en de juridische vragen daaromtrent. In voetnoten wordt naar bronnen verwezen met nadere uitleg en duiding van de techniek.

12 Het Tor-netwerk heeft geen centraal administratiesysteem waarin wordt bijgehouden welke computers via het netwerk verbinding maken. Het doel is juist anonimiteit te verschaffen.

13 Zie, o.a., R.S van Wegberg e.a, 'Plug and Prey? Measuring the Commoditization of Cybercrime via Online Anonymous Markets', in: *Proceedings of the 27th USENIX Security Symposium* (USENIX Security 18) (pp. 1009-1026), USENIX 2018.

tificatie van verdachten of voor het verzamelen van bewijs van het delict witwassen.

Openbronnenonderzoek door opsporingsinstanties vindt doorgaans plaats op basis van artikel 3 Politiewet. Al jaren woedt er een discussie of openbronnenonderzoek op enig moment een meer ernstige inbreuk op het recht op privacy maakt en daarom een bijzondere opsporingsbevoegdheid moet worden toegepast. Daarbij wordt de toepassing van de bijzondere bevoegdheden van stelselmatige observatie en stelselmatige informatie-inwinning geopperd.[14] Al in 1999 is door de wetgever opgemerkt dat opsporingsbevoegdheden, zoals observatie en infiltratie, onder gelijke voorwaarden in de digitale wereld kunnen worden toegepast.[15] Beide bevoegdheden lenen zich niet goed voor openbronnenonderzoek, maar de toepassing van een BOB-bevoegdheid biedt wel een belangrijke waarborg door het verplichte bevel van een officier van justitie met de daarbij horende proportionaliteits- en subsidiariteitstoets. Een interessante vraag is daarbij of de politie en het Openbaar Ministerie ook gebruikmaken van de software van commerciële instanties die mogelijk relevante informatie eerder hebben verzameld en zo ja, onder welke voorwaarden.

Wij bieden in dit overzichtsartikel geen antwoord op deze vraag. De vraag op welke wijze openbronnenonderzoek moet worden gereguleerd is uitgebreid aan bod gekomen in het onderzoek 'Strafvordering in het digitale tijdperk' door de Commissie-Koops, dat is uitgevoerd het kader van het project 'Modernisering Strafvordering'. De Commissie Koops stelt voor de nieuwe bijzondere opsporingsbevoegdheid tot het 'stelselmatig verzamelen van gegevens omtrent een persoon', zo spoedig mogelijk te reguleren. Toch wacht de wetgever de implementatie af van het wetsvoorstel tot wijziging van 'Boek 2: het opsporingsonderzoek' in het herziene Wetboek van Strafvordering (op zijn vroegst in 2023-2024).

2.2 Undercover interacties op online drugsmarkten

Voor opsporingsinstanties is het ook zeer interessant de interactie – onder dekmantel – aan te gaan met personen die actief zijn op online drugsmarkten. Net zoals het internet een grenzeloos medium biedt aan criminelen om met (relatieve) anonimiteit activiteiten te ontplooien, biedt het internet ook voor opsporingsinstanties interessante mogelijkheden. Opsporingsambtenaren kunnen net zo anoniem communiceren als de betrokkenen van het opsporingsonderzoek, zonder (direct) lijfelijk risico te lopen en zonder de bureaustoel te hoeven verlaten.

Opsporingsambtenaren kunnen tot op zeker hoogte onder dekmantel interacteren met verdachten op basis van de algemene bevoegdheid in 3 Politiewet jo 141-142 Sv om gegevens te verzamelen in het kader van een opsporingsonderzoek.[16] De begrenzing ligt daar waar het onderzoek een 'min of meer volledig beeld van bepaalde aspecten van het privéleven van de betrokkene' met zich meebrengt en de opsporingsmethode daarmee een meer dan geringe privacy-inbreuk met zich meebrengt. Om te bepalen of daarvan sprake is kunnen de (reeds bekende) volgende factoren behulpzaam zijn: (1) de duur, (2) plaats, (3) intensiteit, (4) frequentie en (5) het gebruik van een technisch hulpmiddel.[17]

De Context-zaak is vooralsnog het enige arrest dat iets zegt over de rechtmatigheid van het aanmaken van een fictief account met de intentie om de interactie met de verdachte aan te gaan op sociale media, door zich toe te voegen als vriend aan de verdachte op Facebook.[18] De Rechtbank Den Haag wees er in eerste aanleg op dat het wenselijk is de bijzondere bevoegdheid tot stelselmatige-inwinning in te zetten aan de *voorkant* van een dergelijke undercoveractie, omdat dan de inschatting kan worden gemaakt dat het onderzoek stelselmatig van aard wordt (omdat een min of meer volledig beeld van bepaalde aspecten van het privéleven van de betrokkene wordt verkregen).[19] Voor zover de opsporingshandeling niet stelselmatig is, kan de informatie-inwinning worden gestoeld op de algemene bevoegdheid.

De interactie onder dekmantel met een verdachte kan ook bestaan uit de aankoop van een product, waarvoor de toepassing van de pseudokoop als bijzondere opsporingsbevoegdheid geschikt is. Het is ook mogelijk onder dekmantel privéberichten te versturen naar de koper of verkoper van drugs. Een interessante vraag is of als dekmantel het account van een bestaand persoon mag worden gebruikt (de 'accountovername' als opsporingsmethode). Eerder heeft Oerlemans betoogd dat de accountovername als opsporingsmethode mogelijk is met de toepassing van de bijzondere opsporingsbevoegdheid van stelselmatige informatie-inwinning, voor zover een verdachte of informant vrijwillig meewerkt en zijn inloggegevens met opsporings-

14 Zie, o.a., J.J. Oerlemans & B.J. Koops, 'Surveilleren en opsporen in een internetomgeving', *Justitiële verkenningen* 2012, jrg. 38, nr. 5, p. 35-49 en M. Feenstra, 'Opsporingsmiddelen in ontwikkeling. Open-bronnenonderzoek als de nieuwe 'tap'', *PROCES* 2018, nr. 6, p. 367-375.

15 Zie *Kamerstukken II* 1998/99, 26671, nr. 3, p. 36.

16 Zie, o.a., HR 19 december 1995, ECLI:NL:HR:1995:ZD0328, *NJ* 1996/249, m. nt. Schalken, *Kamerstukken II* 1996/97, 25403, nr. 3, p. 110 en 115 en HR 20 januari 2009, ECLI:NL:HR:2009:BF5603, *NJ* 2009/225, m.nt. Borgers, HR 13 november 2012, ECLI:NL:HR:2012:BW9338, *NJ* 2013/413, m.nt. Borgers en HR 1 juli 2014, ECLI:NL:HR:2014:1562, *NJ* 2015/115, m.nt. P.H.P.H.M.C. van Kempen.

17 Zie *Kamerstukken II* 1996/97, 25403, nr. 3, p. 26-27 en *Kamerstukken II* 1998/99, 26671, nr. 7, p. 46. Hoewel de factoren zijn geformuleerd voor de bevoegdheid van stelselmatige observatie, wordt er vanuit gegaan dat de factoren ook van toepassing zijn bij de bijzonder opsporingsbevoegdheid van stelselmatige informatie-inwinning.

18 Zie 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*-zaak).

19 Zie uitgebreid: J.J. Oerlemans, '"Facebookvrienden worden met de verdachte": Over undercoverbevoegdheden op internet', *Justitiële Verkenningen* 2018, jrg. 44, nr. 5, p. 83-99.

autoriteiten deelt.[20] Als daarbij een strafbaar feit wordt gepleegd, zoals het delen van strafbaar materiaal of het leveren van een illegale dienst, moet de BOB-bevoegdheid van infiltratie worden toegepast. Als de accountovername heimelijk plaatsvindt is dat wellicht mogelijk op basis van een netwerkzoeking of door toepassing van de hackbevoegdheid.[21]

2.3 Infiltratie op online drugsmarkten

Infiltratieoperaties onderscheiden zich van stelselmatige inwinning van informatie in de zin dat bij infiltratieoperaties wordt *geparticipeerd* in een criminele organisatie teneinde bewijsmateriaal over strafbare feiten te verzamelen.[22] 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.[23] De Hansa-operatie vormt een uitstekend voorbeeld van de toepassing van infiltratie als opsporingsbevoegdheid in een digitale context.

De Hansa-operatie

Van 20 juni tot 20 juli 2017 heeft de Nederlandse politie de online drugsmarktplaats 'Hansa' overgenomen. Tijdens de overname vonden meer dan 50.000 transacties plaats. Meer dan 500 Nederlandse afleveradressen zijn gemeld bij post- en koeriersbedrijven, met de bedoeling de leveringen tegen te houden. Ongeveer 10.000 buitenlandse adressen van kopers op Hansa Market zijn doorgegeven aan Europol.[24] Een van de verkopers op Hansa Market is op 3 juli 2019 door de Rechtbank Rotterdam tot vijf jaar gevangenisstraf veroordeeld voor het witwassen van bitcoins voor in totaal meer dan € 800.000. Ook heeft de verdachte samen met anderen meer dan 22.000 drugsbestellingen afgeleverd.[25]

De rechtbank legt in het vonnis uit dat onder het bevel van een officier van justitie de infiltratiebevoegdheid van art. 126h Sv is ingezet. De (a) overname van de technische infrastructuur, (b) het fungeren als beheerder van Hansa Market, (c) het reageren op verzoeken van kopers, (d) deelname aan berichtenverkeer, (e) het onderhouden van contacten en (f) het verrichtten van een aantal pseudokopen, zijn daarbij allemaal onder de bijzondere opsporingsbevoegdheid van infiltratie geschaard. De rechtbank is daarbij summier in haar motivering. Onduidelijk blijft bijvoorbeeld in hoeverre en onder welke voorwaarden en grondslag het account van de oude beheerders (de *administrators*) van de drugsmarkt is overgenomen. Ook is het opvallend dat bijvoorbeeld geen verweer is gevoerd met betrekking tot het doorlaatverbod.[26]

De Rechtbank Rotterdam overweegt wel of er sprake is van uitlokking. De rechtbank past daarbij de gebruikelijke toets toe of de verkopers en kopers door het onderzoeksteam door de overname niet tot andere strafbare feiten zijn gebracht, dan die waarop hun opzet reeds was gericht.[27] Met de geruisloze overname van Hansa Market heeft het onderzoeksteam de bestaande situatie in zoverre ongewijzigd voortgezet. Niet is gebleken dat verkopers (of kopers) door de overname, dan wel door het handelen van het onderzoeksteam, zijn gebracht tot het begaan van andere strafbare feiten dan waarop hun opzet reeds van tevoren was gericht. Het toelaten van nieuwe vendors en het aanbieden van een korting bij personen bij wie al het opzet bestond om te handelen in verdovende middelen op deze specifieke en verborgen website, past volgens de rechtbank eveneens in dit kader en kan dan ook niet worden gekwalificeerd als uitlokking.

Het Europees Hof voor de Rechten van de Mens prefereert overigens de betrokkenheid van een rechter bij infiltratie-acties.[28] Toch is voor de toepassing van de bijzondere opsporingsbevoegdheid tot infiltratie, zelfs in grootschalige operaties met verstrekkende gevolgen zoals in deze, slechts een bevel van een officier van justitie vereist. De Centrale Toetsingscommissie van het Openbaar Ministerie adviseert over voorgenomen infiltratieoperaties.

2.4 Jurisdictie

Tijdens een opsporingsonderzoek naar een online drugsmarkt kunnen jurisdictievraagstukken opspelen. Het internet is een grenzeloos medium, waardoor de opsporing ook eenvoudig de territoriale grenzen van staten overgaat. Opsporing door overheidsinstanties mag niet over de territoriale grenzen van een staat plaatsvinden, zonder

20 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.

21 Hof Den Haag 19 december 2018, ECLI:NL:GHDHA:2018:3529, *Computerrecht* 2019/51, m.nt. J.J. Oerlemans.

22 Zie *Kamerstukken II* 1996/97, 25403, nr. 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'.

23 Zie *Kamerstukken II* 1996/97, 25403, nr. 3, p. 28.

24 H. Modderkolk, 'Zo nam de Nederlandse politie een online drugsmarkt over', *De Volkskrant*, 19 augustus 2017. Zie ook Andy Greenberg, 'Operation Bayonet: inside the sting that hijacked an entire dark web drug market', *Wired.com*, 3 augustus 2018.

25 De drugs werden verstopt in speciaal met 3D-printers geprinte verpakkingen als make-updoosjes. Twee medeverdachten zijn ook veroordeeld, zie Rb. Rotterdam 4 juli 2019, ECLI:NL:RBROT:2019:6049 en ECLI:NL:RBROT:2019:6050.

26 Zie voor een uitgebreide bespreking van de zaak: Rb. Rotterdam 3 juli 2019, ECLI:NL:RBROT:2019:5339, *Computerrecht* 2019/178, m.nt. J.J. Oerlemans.

27 Zie HR 29 juni 2010, ECLI:NL:HR:2010:BL0613. Zie voor uitgebreide overwegingen omtrent het uitlokkingsverbod, mede in relatie tot EHRM-jurisprudentie, HR 20 juni 2017, ECLI:NL:PHR:2017:878, concl. A-G Knigge.

28 Zie, o.a., EHRM 4 november 2010, ECLI:CE:ECHR:2010:1104JUD001875706, par. 50, *EHRC* 2011/9, m.nt. Ölçer (*Bannikova/Rusland*), EHRM 23 oktober 2014, ECLI:CE:ECHR:2014:1023JUD005464809, par. 53, *EHRC* 2015/1, m.nt. F.P. Ölçer (*Furcht/Duitsland*) en EHRM 28 juni 2018, ECLI:CE:ECHR:2018:0628JUD003153607, par. 45 (*Tchokhonelidze/Georgië*).

toestemming van de betrokken staat of verdragsbasis.[29] Het systeem van rechtshulp wordt gezien als het geëigende instrument om bewijs op buitenlands territorium te verzamelen. De opsporing en vervolging van personen wordt namelijk gezien als de exclusieve taak van een staat.[30] Het zonder toestemming overnemen van die taak wordt gezien als een schending van de soevereiniteit van de betrokken staat. Dat kan gevolgen met zich meebrengen, onder andere op diplomatiek gebied. In Nederland heeft de vermeende unilaterale opsporing van de Amerikanen bijvoorbeeld geleid tot Kamervragen.[31]

Wel kan worden beargumenteerd dat in de context van drugsmarktplaatsen via Tor, de locatie van de verdachten en de digitale infrastructuur niet met een redelijke inspanning is vast te stellen en daarom unilaterale (digitale) opsporing tot op zeker hoogte toelaatbaar is.[32] De mogelijke schending van de soevereiniteit van de betrokken staat leidt overigens niet tot gevolgen in het strafproces, omdat het geen beschermd belang van de verdachte is dat leidt tot de sanctie van een vormverzuim in de zin van art. 359a Sv.[33]

Het valt te bezien of hierover in internationaal verband nadere afspraken worden gemaakt. Europol merkt in haar jaarlijkse cybercrimerapport uit 2019 op dat 'de coördinatie en standaardisatie van undercover online onderzoeken zijn vereist om dark web-onderzoeken te 'deconflicteren'.' Europol stelt dat het huidige juridische instrumentatrium van rechtshulp in de EU ('Mutual Legal Assistance') onvoldoende is voor digitale opsporingsonderzoeken.[34]

3. Verstoren op online drugsmarkten

Vanaf het moment dat politiediensten zich bewust werden van het bestaan van online anonieme markten als een prominente ontmoetings- en handelsplaats voor criminelen, hebben politiediensten over de hele wereld verschillende operaties uitgevoerd om deze criminele ondernemingen te sluiten. [35] Daarbij zijn met name traditionele onderzoeksmethoden gebruikt, zoals infiltratie op de markt en het onderscheppen van fysieke pakketten. In toenemende mate wordt dit traditionele politiewerk gecombineerd met technische onderzoekstechnieken, zoals de inzet van eerdergenoemde crawlers, *scrapers*[36], en het benutten van (server-) misconfiguraties of andere kwetsbaarheden, die gericht zijn op het achterhalen van de locaties van de servers van deze markten. Het gebruik van een combinatie van traditionele en technische opsporingsmethoden maakt het mogelijk de infrastructuur van deze markten over te nemen, de administrators buiten te sluiten en vervolgens de markt ontoegankelijk te maken – terwijl men in bezit blijft van de gehele administratie op de inbeslaggenomen servers.

Op basis van de inzichten die zijn verkregen van eerdere *take downs* – zoals de Silk Road 1.0 en 2.0 – weten we dat een 'eenvoudige' take down vaak resulteert in de migratie van gebruikers naar andere markten en op deze nieuwe markten hun illegale activiteiten voortzetten. Dit betreft het klassieke 'waterbedeffect', ofwel criminaliteit die zich verplaatst, in plaats van zich iets aan de te trekken van overheidsoptreden. Onderzoekers van de Carnegie Mellon University bestudeerden het totale handelsvolume op online anonieme markten in het ecosysteem vóór, tijdens en na beide Silk Road take downs. [37] Hoewel de handelsvolumes na beide take downs veranderden, nam het handelsvolume toe in plaats van af. Het ecosysteem herstelt niet alleen van een interventie, maar blijft groeien. Opmerkelijk zijn de inzichten van de socioloog Ladegaard, die de media-aandacht voor beide take downs koppelt aan dit toegenomen verkoopvolume.[38]

De Nederlandse politie lijkt vastbesloten met het waterbedeffect en de groei van online drugsmarkten te breken en hun interventiestrategieën te wijzigen om deze ongewenste bijwerking aan te pakken. Verstoring als 'alternatieve interventie' staat al enige tijd hoog op de agenda bij politie en het OM, maar sinds Prinsjesdag 2019 ook nadrukkelijk in Den Haag. [39] Het Ministerie van Justitie en Veiligheid neemt alternatieve interventies in 2020 bovendien mee als prestatie-indicator voor de politie in haar beoordeling van de bestrijding van digitale criminaliteit. De Nederlandse

29 Zie de S.S. 'Lotus'-zaak (*Frankrijk t. Turkije*), *PCIJ Reports*, Series A, nr. 10, 7 september 1927, p. 18-19.

30 Zie, o.a. Schmidt (red.), Tallinn Manual 2.0, Cambridge: Cambridge University Press 2017, p. 21.

31 Zie 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 antwoord op Kamervragen over het mediabericht 'FBI agenten hacken mee met Nederlandse politie en detentieomstandigheden VS' van 15 april 2013, *Aanhangsel Handelingen II* 2012/13, 2001.

32 Zie o.a., J.J. Oerlemans, *Investigating Cybercrime* (diss. Leiden), Amsterdam: Amsterdam University Press 2017, p. 297 en M.F.H. Hirsch Ballin, 'De rol van grenzen bij opsporing: grenzeloze inzet van opsporingsbevoegdheden?', *Ars Aequi* 2018, afl. 6, p. 462-467. Deze redenering wordt al aangehouden bij de mogelijk grensoverschrijdende toepassing van de hackbevoegdheid uit art. 126nba Sv. Zie ook de 'Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv', *Stcrt*. 2019, 10277.

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

34 Zie Europol, 'Internet Organised Threat Assessment', Den Haag 2019, p. 46.

35 Zie o.a., P.H. Hartel & R.S. van Wegberg, 'Crime and Online Anonymous Markets' in: M. Nataragan (red.), *International and Transnational Crime and Justice*, Cambridge: Cambridge University Press 2019, p. 67-72.

36 Een scraper onderscheid zich van een crawler, in de zin bij een scraper de gegevens ook direct worden gedownload en verder worden verwerkt door een systeem.

37 Zie K. Soska & N. Christin, 'Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem', in: *Proceedings of the 24th USENIX Security Symposium* (USENIX Security 15) (pp. 33-48), USENIX 2015.

38 Zie I. Ladegaard,'We know where you are, what you are doing and we will catch you: Testing deterrence theory in digital drug markets', *The British Journal of Criminology* 2017, 58(2), 414-433.

39 Zie Rijksbegroting 2020 Justitie en Veiligheid (*Kamerstukken II* 2019/20, 35300-VI, nr. 2, p. 21)

politie kan sinds 2017 gezien worden als een voortrekker in alternatieve interventies gericht op online drugsmarkten.[40]

3.1 Verstoring op Hansa-markt

Operatie 'Bayonet' is een nog niet eerder vertoonde, gecoördineerde politie interventie. Daarbij zijn twee toonaangevende online anonieme markten – *AlphaBay* en Hansa Market – door de FBI en Team High Tech Crime (THTC) van Nederlandse politie offline gehaald. Het lukte de FBI om AlphaBay neer te halen, terwijl THTC de controle over Hansa Market overnam en bijna een maand lang exploiteerde als beheerder om vervolgens Hansa Market definitief offline te halen (zie ook paragraaf 2.3). De onverwachte en onaangekondigde take down van AlphaBay zorgde ervoor dat kopers en verkopers in onzekerheid en wanhoop achterbleven, terwijl de FBI – in tegenstelling tot pronkerige persconferentie bij eerdere take downs – volledig zweeg over hun betrokkenheid.

Veel AlphaBay-gebruikers zochten hun toevlucht tot Hansa Market, dat op dat moment werd geëxploiteerd door THTC. Daarom waren de politiediensten in een perfecte positie om niet alleen het ecosysteem te verstoren door wantrouwen te creëren bij gebruikers op deze anonieme markten, maar ook waardevolle gegevens van duizenden gebruikers te verzamelen. THTC had zelfs in een gedurfde actie de codering van persoonlijke berichten op Hansa weten uit te schakelen, waardoor ze via de site persoonlijke informatie, zoals postadressen, konden volgen. Op de dag van take down van Hansa Market, liet de FBI weten een maand eerder verantwoordelijk te zijn geweest voor de take down van AlphaBay.

De planning van de Hansa-overname – ook wel operatie 'Gravesac' genoemd – startte al lang voor de zomer van 2017. Het idee tot overname kwam voort uit een tip over de locatie van de server. Deze tip leidde tot een jaar lang onderzoek dat uiteindelijk eindigde met de arrestatie van de administrators in Duitsland en de politie die de inbeslaggenomen servers in Litouwen kon migreren naar Nederland. Dit vormde de start voor het tweede bedrijf: het THTC als *dark market administrator*. Maar had deze verstoringstactiek nu daadwerkelijk een ander effect dan eerdere operaties tegen online drugsmarkten?

3.2 Meten is weten

Van Wegberg & Verburgh deden eerder onderzoek naar de effecten van *Operation Bayonet*.[41] Zij onderzochten daarbij de migratiepatronen vanaf de door de politie gesloten dark markets, Alphabay en Hansa Market, naar *Dream Market*. Dream Market werd na operatie Bayonet de grootste online anonieme markt. Ten eerste stelde de auteurs zich de vraag: vond er ook na de operatie een verplaatsingseffect plaats? Maar vooral, vroegen zij zich af: was er een verschil in gedrag voor- en nadat deze hele operatie in de openbaarheid kwam. Met behulp van crawlers zijn gegevens vergaard van de nieuwe registraties op het Dream Market-forum over de periode januari tot en met september 2017 om te bepalen wat de toestroom van gebruikers naar Dream Market was ten tijde van de operatie. Dit resulteerde in een eerste, maar te verwachten, inzicht: van de nieuwe forum registraties bleek dat er een aanzienlijk grotere instroom was na Operation Bayonet dan daarvoor.

Om te kunnen bepalen of verkopers ook de overstap waagden naar Dream Market en zo ja, wanneer en op welke wijze, was het voor de onderzoekers noodzakelijk nieuwe gebruikers terug te kunnen traceren aan eerdere activiteiten op AlphaBay of Hansa Market. Deze traceerbaarheid werd onder vastgesteld door de geregistreerde PGP-gegevens en de username van de verkoper in een dark web database – genaamd *Grams* – op te zoeken. Deze (inmiddels verdwenen) zoekmachine, gaf gebruikers van online anonieme markten de mogelijkheid om de reputatie van verkopers na te gaan, door eerdere activiteiten in kaart te brengen, zoals: 'verkoper X was eerder actief op markt Y en had daar reputatie Z'. Op deze wijze konden de onderzoekers nagaan of nieuwe verkopers op Dream Market eerder actief waren op AlphaBay, Hansa Market, of beide marktplaatsen.

Van Wegberg & Verburgh concluderen dat verkopers van Hansa Market minder migreerden naar Dream Market, of in ieder geval minder vaak onder hun eigen naam, dan vanaf AlphaBay. Gelet op het feit dat verkopers in een anonieme omgeving juist hun reputatie (hun eerdere activiteiten) in ere willen houden en daarnaast vindbaar willen zijn voor nieuwe klanten, is dit een interessante bevinding. Waarschijnlijk hebben meer verkopers op Hansa Market zich teruggetrokken uit de markt, vergeleken met AlphaBay verkopers. De onderzoekers concluderen daarom dat de Hansa Market-overname het vertrouwen van de gemeenschap in online drugsmarkten meer heeft geschaad, dan bij andere interventies.

Kortom, vergeleken met take down van AlphaBay, lijken de effecten van de sluiting van Hansa Market op verkopers aanzienlijk anders. Verkopers lijken minder vaak bereid elders verder te gaan met hun criminele activiteiten na de sluiting van de Hansa Market. Weinigen bleken te zijn overgestapt naar Dream Market, diegenen die wel overstapten namen veelvuldig voorzorgsmaatregelen, zoals het veranderen van hun gebruikersnaam en/of PGP-sleutel. Velen begonnen opnieuw met een schone lei; waardoor hun vroegere reputatie volledig werd gewist en waarschijnlijk met pijnlijke gevolgen voor hun (digitale) portemonnee.

4. Conclusie

In dit artikel is hopelijk duidelijk geworden dat inmiddels substantieel veel drugshandel via online drugsmarkten

40 Zie o.a. A. Greenberg, 'Operation Bayonet: inside the sting that hijacked an entire dark web drug market', *Wired.com*, 3 augustus 2018.

41 Zie R.S. van Wegberg & T. Verburgh, 'Lost in the Dream? Measuring the effects of Operation Bayonet on vendors migrating to Dream Market', in: *Evolution of the Darknet Workshop at the Web Science Conference* (WebSci 18) (pp. 1-5), ACM 2018.

plaatsvindt. Maar: fysieke drugshandel is vooralsnog veel grootschaliger.[42] Tegelijkertijd krijgt fysieke drugshandel wel vaker een digitaal tintje mee, omdat via *Whatsapp* en *Telegram* prijslijsten met drugs in omloop zijn en de drugs op verzoek door een koerier aan het huis wordt geleverd. Hier is relatief weinig over bekend en liggen legio mogelijkheden voor nader onderzoek.

In dit artikel is ook duidelijk gemaakt dat online drugsmarkten bepaalde kansen en uitdagingen bieden voor de politie en het Openbaar Ministerie. Online undercoveroperaties bieden interessante mogelijkheden voor opsporingsinstanties, met name vanwege de mogelijkheden tot misleiding en interactie met verdachten op afstand. Digitale undercoveroperaties worden zeker herhaald in de toekomst, al dan niet door of in gezamenlijkheid met buitenlandse opsporingsinstanties. Het is belangrijk dat advocaten en rechters blijven toetsen hoe de gebezigde opsporingsmethoden zich tot de wet verhouden. In de Hansa-zaak heeft de verdediging enkele voor de hand liggende verweren laten liggen, zoals het doorlaatverbod en de toepassing van andere opsporingsbevoegdheden dan infiltratie. Ook verdient het nader onderzoek of de ontwikkeling van internationale verdragen noodzakelijk zijn voor het in goede banen leiden van online operaties van opsporingsautoriteiten.

De Hansa-operatie had nadrukkelijk ook de verstoring van de online drugsmarkt als doel, naast het vergaren van bewijs. Verstoring met als nevendoel 'zo effectief mogelijk handhaven', lijkt op het eerste gezicht door de beugel te kunnen. Toch verdient dit onderwerp ook vanuit juridisch perspectief nadere bestudering, met name op het gebied van toezicht op de rechtmatigheid van dergelijke operaties. Zo komen de betrokkenen van een verstoringsactie meestal niet voor een rechter, waardoor de rechtmatigheid van een operatie niet achteraf wordt getoetst.

Dit artikel laat ten slotte zien dat digitale verstoringsacties mooie kansen bieden voor onderzoek. Het meetbaar maken van politie interventies in het digitale domein biedt nieuwe inzichten op eerder onbeantwoordbare vragen rondom de effectiviteit van deze interventies. Het is daarnaast een handvat voor toekomstig optreden. Immers, wanneer een interventie ontworpen wordt die gebruikmaakt van eerdere, bewezen resultaten, kan daarmee de politiële slagkracht worden vergroot zonder extra middelen of capaciteit.

Waar de politie innoveert, staan de ontwikkelingen in de online drugsmarkten ook niet stil. Een recente ontwikkeling is bijvoorbeeld het ontstaan van *single vendor shops*, waarbij een succesvolle online drugsverkoper zijn eigen marktplaats begint. De recente take down van de webshop *DutchMagic* in mei 2019 is daarbij illustratief.[43] Het is ook denkbaar dat online drugsmarkten exclusiever worden (slechts toelating op uitnodiging of na een ballotage). Ten slotte is het interessant te zien in hoeverre online drugsmarkten in andere talen (zoals Cyrillisch, Spaans of Mandarijn) zich ontwikkelen.[44] Kortom, online drugshandel is een vorm van criminaliteit dat inmiddels op de radar staat en nog jaren een prominente vorm van gedigitaliseerde criminaliteit blijft voor politie en justitie.

Over de auteurs

Mr. dr. J.J. Oerlemans
is als onderzoeker verbonden aan eLaw, het centrum voor Recht en Digitale Technologie van de Universiteit Leiden.

Drs. R.S. van Wegberg
is als postdoc verbonden aan de TU Delft en is daarnaast werkzaam als cybercrime-onderzoeker bij TNO.

42 Zie K. Kruithof e.a, 'Internet-facilitated drugs trade. An analysis of the size, the scope and the role of the Netherlands', Santa Monica/Cambridge: RAND, WODC 2016.

43 Politie.nl, 'Politie en OM halen grootste coffeeshop op darkweb offline', 9 mei 2019.

44 Zie ook Europol, 'Internet Organised Threat Assessment', Den Haag 2019, p. 45.