Artikel

In(ternet)filtratie: een roep om meer waarborgen?

Mr. S.B.H. van Overveld, mr. I.C. Smits en mr. C.M. Taylor Parkins-Ozephius*

1. Inleiding

Het is een groeiende vorm van criminaliteit: digitale criminaliteit. Niet langer worden enkel driehoog-achter, in louche 'winkels' illegale producten aan de consument aangeboden; tegenwoordig kan op illegale marktplaatsen – *dark markets* – op het wereldwijde illegale *dark web*, worden gehandeld in wapens, drugs en andere goederen en diensten.[1] Het *dark web* is de tegenhanger van het *surface web*. Op het *surface web* is alle inhoud van sites beschikbaar, die kan worden gevonden via bijvoorbeeld Google. Alle inhoud die daarentegen niet kan worden gevonden via de bekende zoekmachines, valt binnen het *dark web*.[2] Het opsporen van illegale, digitale marktplaatsen door de politie en het Openbaar Ministerie (hierna: OM) is lastig. Dit komt onder meer door de verschillende veiligheidsmaatregelen die het bestaan van *dark markets* mogelijk maken, zoals anonimiseringsprotocollen, cryptocurrency's, *escrow* en *review*systemen.[3] Anonimiseringsprotocollen en cryptocurrency's waarborgen de anonimiteit van zowel koper als verkoper. *Escrow* en *review*systemen zorgen ervoor dat koper en verkoper, ondanks de anonimiteit, weten dat ze elkaar kunnen vertrouwen. *Escrow* biedt bescherming aan de koper[4] en door middel van *review*-systemen kunnen gebruikers elkaar beoordelen.[5]

Dark markets zijn voor veel mensen onbekend terrein. Bovendien zitten *dark markets* zo ver verborgen in de krochten van het *dark web*, dat toegang krijgen tot deze *markets* als gebruiker al moeilijk is, laat staan dat ze gemakkelijk kunnen worden opgespoord en opgerold door politie en justitie. Desondanks is het de Nederlandse politie in juli 2017 gelukt om in samenwerking met de FBI twee van de grootste *dark markets* te sluiten: Alphabay en Hansa Market. Tijdens laatstgenoemde operatie, die later bekend werd als operatie Bayonet en resulteerde in de spraakmakende Hansa-zaak, wist de Nederlandse High Tech Crime Unit de ondergrondse website Hansa op baanbrekende wijze over te nemen. De FBI haalde allereerst Alphabay uit de lucht. Vervolgens nam de Nederlandse politie Hansa Market voor een maand over en hield de market draaiende, teneinde zoveel mogelijk informatie in te winnen over de gebruikers van deze *dark market*.[6] De politie baseerde de interventie op artikel 126h Wetboek van Strafvordering (hierna: Sv): de infiltratiebevoegdheid. *Digitale* infiltra-

* Mr. S.B.H. (Sophie) van Overveld is als docent Straf(proces)recht verbonden aan het Willem Pompe Instituut voor Strafrechtswetenschappen van de Universiteit Utrecht. Mr. I.C. (Isabel) Smits is als docent Straf(proces)recht verbonden aan het Willem Pompe Instituut voor Strafrechtswetenschappen van de Universiteit Utrecht. Mr. C.M. (Celine) Taylor Parkins-Ozephius is als docent Straf(proces)recht verbonden aan het Willem Pompe Instituut voor Strafrechtswetenschappen van de Universiteit Utrecht.

1. M.J. Barratt & J. Aldrigde, 'Everything you always wanted to know about drug cryptomarkets* (*but were afraid to ask)', *International Journal of Drug policy* 2016, afl. 35, p. 1.
2. T. Verburgh, E. Smits & R.S. van Wegberg, 'Uit de schaduw. Perspectieven voor wetenschappelijk onderzoek naar dark markets', *Justitiële verkenningen* 2018/55, nr. 5, p. 69.
3. Verburgh, Smits & Van Wegberg, *Justitiële verkenningen* 2018, p. 70-73.
4. In *escrow*-systemen wordt het te betalen bedrag door de marktplaats achtergehouden totdat de goederen of diensten door de koper zijn ontvangen.
5. Verburgh, Smits & Van Wegberg, *Justitiële verkenningen* 2018, p. 72-73.
6. Verburgh, Smits & Van Wegberg, *Justitiële verkenningen* 2018, p. 77.

doi: 10.5553/TBSenH/229567002020006005004

tie wordt echter niet expliciet in ons wetboek geregeld. Wel wordt in de memorie van toelichting bij de Wet bijzondere opsporingsbevoegdheden (hierna: Wet BOB) – waar artikel 126h Sv onderdeel van uitmaakt – aangegeven dat bij digitale infiltratie van dezelfde grondslag gebruik kan worden gemaakt als bij de 'klassieke' toepassing in de fysieke wereld.[7]

Toch stellen wij onszelf de vraag of deze wettelijke grondslag afdoende is voor infiltratie in de steeds sneller veranderende digitale wereld, zeker gezien de inbreuk die wordt gemaakt op niet alleen de persoonlijke levenssfeer van één verdachte, maar op die van duizenden gebruikers. De wetgever heeft wellicht dit soort grootschalige online infiltratiemogelijkheden ten tijde van het opstellen van de Wet BOB niet voor ogen gehad en daarom de wettelijke infiltratieregeling niet voorzien van voldoende waarborgen bij toepassing in een digitale context. Daarnaast lijkt digitale infiltratie ook nieuwe kansen te bieden. Zo is onlangs door de minister van Justitie en Veiligheid Grapperhaus en de staatssecretaris van Volksgezondheid, Welzijn en Sport Blokhuis een conceptwetsvoorstel om de Opiumwet te wijzigen in consultatie gebracht.[8] Dit conceptwetsvoorstel plaatst groepen designerdrugs op Lijst Ia, waarvan het gebruik tot op heden legaal is. Het OM zal, indien dit wetsvoorstel wordt aangenomen, in de toekomst mogelijk vaker gebruik willen maken van de mogelijkheid om digitaal te infiltreren op een *dark market*. Gezien de verschillen tussen de klassieke vorm van infiltratie en digitale infiltratie en de nieuwe mogelijkheden die de snel veranderende digitale wereld met zich brengt is een onderzoek naar de huidige regulering van deze nieuwe infiltratie praktijk onzes inziens noodzakelijk.

In deze bijdrage zullen wij allereerst de werkwijze van politie en justitie beschrijven in operatie Bayonet, waarbij ook wordt stilgestaan bij de rechterlijke toetsing van het opsporingsonderzoek. In paragraaf 3 zal de bevoegdheid tot infiltratie op grond van artikel 126h Sv worden uitgediept. Daarbij lichten wij tevens de verschillen tussen 'klassieke' infiltratie en 'digitale' infiltratie uit. In paragraaf 4 wordt de noodzaak tot een duidelijkere wettelijke grondslag voor infiltratie in de digitale wereld toegelicht en worden de kansen en uitdagingen voor de toekomst aangestipt. We besluiten in paragraaf 5 de bijdrage met een conclusie.

2. Operatie Bayonet en de gerechtelijke toetsing van het opsporingsonderzoek

In 2017 haalde de FBI Alphabay offline: een van de belangrijkere marktplaatsen op het dark web. Net voordat de marktplaats offline werd gehaald, kreeg het Team High Tech Security van de Nederlandse politie signalen door dat de FBI bezig was met een grote operatie rondom Alphabay. Dit moment greep de Nederlandse politie aan om direct actie te ondernemen en de operatie omtrent Alphabay te combineren met een onderzoek naar Hansa Market. De politie was op dat moment al bezig met onderzoek naar Hansa Market, omdat een server van deze dark market in Nederland stond en de Nederlandse politie derhalve jurisdictie had. Later bleek dat het hele systeem met servers verplaatst was naar Litouwen, maar door een samenwerking met de politie in Litouwen, kreeg de Nederlandse politie in één keer toegang tot alle informatie van Hansa Market. De twee (Duitse) beheerders van Hansa Market konden vervolgens worden aangehouden. Hansa Market direct offline halen was op dat moment het meest voor de hand liggend geweest. Toch koos het Team High Tech Security voor een andere route: de website werd gekopieerd, waardoor de politie continu een kopie in handen had van de database van Hansa Market. De dark market kon gewoon worden bezocht door kopers en verkopers. Zij zagen niet dat het beheer van Hansa Market was overgenomen door de politie. Op de gekopieerde website verwijderde de politie de complete foto-database, waardoor alle verkopers de foto's van producten die zij verkochten, opnieuw moesten uploaden. Ook verleidde de politie de gebruikers tot het downloaden van een Excel bestand, waardoor de IP-adressen van hen die dit bestand gedownload hadden zo binnenstroomden bij de politie. Verder kwamen alle berichten, wachtwoorden en transacties vanaf dat moment binnen op de computers van de politie. Het aantal bezoekers nam daarnaast nog eens een vlucht toen Alphabay werd gesloten. Kopers en verkopers die normaal gesproken actief waren op Alphabay, verplaatsten zich naar Hansa Market. Hierdoor konden nog meer bezoekers in de gaten worden gehouden. Sinds de overname van het beheer van Hansa Market zijn meer dan 50.000 transacties geteld. De meeste transacties betroffen de koop en verkoop van hard- en softdrugs. Na een maand haalde de politie Hansa Market offline. De val van Hansa Market was daarmee het sluitstuk van een omvangrijke digitale infiltratieoperatie.[9]

7. *Kamerstukken II* 1996/97, 25403, 3, p. 29 en 55.
8. Wetsvoorstel tot wijziging van de Opiumwet in verband met het toevoegen van een derde lijst met als doel het tegengaan van productie van en de handel in nieuwe psychoactieve stoffen en enkele andere wijzigingen (hierna: Wetsvoorstel tot wijziging van de Opiumwet).
9. https://www.politie.nl/nieuws/2017/juli/20/ondergrondse-hansa-market-overgenomen-en-neergehaald.html.

doi: 10.5553/TBSenH/229567002020006005004

In juli 2019 werden verschillende gebruikers van Hansa Market veroordeeld voor grootschalige drugshandel en witwassen.[10] Tevens is hierbij de rechtmatigheid van het aan operatie Bayonet ten grondslag liggende onderzoek '26Gravesac' aan bod gekomen. In de zaak van een van de verdachten, voerde de advocaat als verweer aan dat in dit onderzoek sprake was van vormverzuimen, waarbij doelbewust en met een grove veronachtzaming een ernstige inbreuk op het recht op een eerlijk proces van de verdachte heeft plaatsgevonden. Deze advocaat stelde dat de wettelijke grondslag ontbrak en dat het optreden van de opsporingsambtenaren niet voldoende inzichtelijk was. Door dit gebrek aan inzicht was het optreden van de opsporingsambtenaren niet controleerbaar op proportionaliteit en subsidiariteit.[11] De officier van justitie achtte artikel 126h Sv een voldoende wettelijke basis voor het overnemen en beheren van de market. Daarnaast was de infiltratie volgens hem in overeenstemming met de eisen van proportionaliteit en subsidiariteit.[12] De argumentatie die tot dit standpunt heeft geleid, is niet opgenomen in het vonnis.

De rechtbank oordeelde dat de infiltratieactie onder de bijzondere opsporingsbevoegdheid als bedoeld in artikel 126h Sv valt.[13] Opvallend is dat de argumentatie die tot dit oordeel leidde in het vonnis ontbreekt. De rechtbank besteedde in het vonnis meer aandacht aan de verwerping van het verweer dat niet controleerbaar was of de digitale infiltratieactie voldeed aan de eisen van proportionaliteit en subsidiariteit. De rechtbank besprak in dit kader dat het dossier een aanvullend proces-verbaal bevatte, waarin de inzet van de digitale infiltratieactie uitvoerig beschreven werd. Deze beschrijving was naar het oordeel van de rechtbank voldoende. Hierbij nam de rechtbank in aanmerking dat het niet eerder was gelukt om een dark market effectief te verstoren. Daarnaast was volgens de rechtbank de aard en de ernst van de internationale onlinehandel in verdovende middelen van belang, de kennelijke onmogelijkheid om op andere wijze inzicht te verkrijgen in deze strafbare feiten, de identiteit van kopers en verkopers en de mogelijkheid om eventuele criminele tegoeden van hen in beslag te nemen. Dit alles maakte naar het oordeel van de rechtbank dat met de inzet van deze bijzondere opsporingsbevoegdheid gedurende een begrensde periode van iets langer dan een maand aan de eisen van proportionaliteit en subsidiariteit werd voldaan. Kortom, de rechtbank keurde de inzet van digitale infiltratie in deze specifieke zaak goed.[14]

Met de goedkeuring van de rechtbank leek operatie Bayonet een groot succes. De *dark market* werd effectief verstoord en zoals eerdergenoemd, werd een aantal gebruikers veroordeeld. Toch is volgens ons dit succes niet zonder haken en ogen. Zo is onzes inziens het vraagstuk over de wettelijke grondslag voor de infiltratieactie door de rechtbank niet overtuigend beantwoord en vragen wij ons af of de infiltratiebevoegdheid wellicht met meer waarborgen zou moeten worden omkleed, wanneer deze bevoegdheid wordt toegepast in het digitale domein. Wij zullen daarom in de volgende paragraaf stilstaan bij het wettelijk kader van de infiltratiebevoegdheid. Vervolgens zullen wij de verschillen tussen klassieke infiltratie en digitale infiltratie nader uitwerken en laten zien dat, ten aanzien van toepassing van de infiltratiebevoegdheid in de digitale wereld, mogelijk leemtes ontstaan in de wet. Hetgeen, zeker in het licht van het strafvorderlijk legaliteitsbeginsel, moet worden voorkomen.

3. (Digitale) infiltratie op grond van artikel 126h Sv

Het ontstaan en de ontwikkeling van de computer heeft ook gevolgen voor het strafrecht gehad. De Wet computercriminaliteit van 1993 was een eerste reactie vanuit de wetgever op deze ontwikkelingen. Dat de technologische ontwikkelingen na de invoering van deze wet het hoogtepunt nog niet hadden bereikt, was ook de wetgever niet ontgaan. In het bijzonder de toen nieuwe technologieën die het mogelijk maakten om (netwerken van) computers aan andere (netwerken van) computers te koppelen, boden (en bieden) burgers en overheden ongekende mogelijkheden tot overdracht, verkrijging en bewerking van informatie. Deze constatering van de wetgever leidde tot een vervolg op de Wet computercriminaliteit, te weten de Wet computercriminaliteit II.[15]

Nog voordat deze Wet computercriminaliteit II in werking trad, deed de Wet BOB zijn intrede in 2000.[16] Drie bijzondere opsporingsbevoegdheden met betrekking tot undercover opsporingsmethoden werden geïntroduceerd in het Wetboek van Strafvordering: pseudokoop- en dienstverlening, stelselmatige informatie-inwinning en infiltratie. Artikel 126h Sv regelt de bevoegdheid tot infiltratie.[17] Vanwege het ingrijpende karakter bevat artikel 126h Sv verschillende waarborgen. Zo is infiltratie alleen toegestaan in geval van verdenking van een misdrijf als omschreven in artikel 67 lid 1 Sv, waarbij

10. Zie onder meer Rechtbank Rotterdam 3 juli 2019, ECLI:NL:RBROT:2019:5339; Rechtbank Rotterdam 4 juli 2019, ECLI:NL:RBROT:2019:6049; Rechtbank Rotterdam 4 juli 2019, ECLI:NL:RBROT:2019:6050.
11. Rechtbank Rotterdam 3 juli 2019, ECLI:NL:RBROT:2019:5339, r.o. 4.1.
12. Rechtbank Rotterdam 3 juli 2019, ECLI:NL:RBROT:2019:5339, r.o. 4.2.
13. Rechtbank Rotterdam 3 juli 2019, ECLI:NL:RBROT:2019:5339, r.o. 4.3.
14. Rechtbank Rotterdam 3 juli 2019, ECLI:NL:RBROT:2019:5339, r.o. 4.3.
15. *Kamerstukken II* 1998/99, 26671, 3, p. 2.
16. *Stb*. 1999, 245.
17. Artikel 126p Sv betreft de vroegsporing-variant van de infiltratiebevoegdheid. De politie kan op bevel van de officier van justitie op grond van artikel 126p jo. artikel 126o Sv deelnemen of medewerking verlenen aan het georganiseerd verband, indien vermoed wordt dat misdrijven als omschreven in artikel 67 lid 1 Sv worden beraamd of gepleegd en die misdrijven gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren, *Kamerstukken II* 1996/97, 25403, nr. 3, p. 28. Wij zullen ons in deze bijdrage beperken tot artikel 126h Sv, omdat die bepaling, in tegenstelling tot artikel 126p Sv, de grondslag vormde in de Hansa-zaak.

doi: 10.5553/TBSenH/229567002020006005004

bovendien sprake moet zijn van een ernstige inbreuk op de rechtsorde die voortvloeit uit de aard van het misdrijf of de samenhang met andere door de verdachte begane misdrijven. Daarnaast mag pas worden geïnfiltreerd, indien het onderzoek dit dringend vordert. Met deze eis wordt de subsidiariteitstoets in de wettelijke bevoegdheid neergelegd. Artikel 126h Sv vereist ook dat de politiële infiltratie alleen mag worden uitgevoerd door opsporingsambtenaren die daartoe een bevel hebben gekregen van de officier van justitie. Met dit bevel verkrijgen de opsporingsambtenaren de toestemming van de officier om medewerking te verlenen aan een groep van personen waarbinnen naar redelijkerwijs wordt vermoed misdrijven worden beraamd of gepleegd. Tevens mogen de opsporingsambtenaren de verdachte of betrokkene op grond van lid 2 niet uitlokken tot het plegen van strafbare feiten, waarop zijn opzet tevoren niet was gericht (het zogenoemde 'Tallon-criterium'). Uit lid 3 blijkt dat aan het infiltratiebevel verschillende eisen worden gesteld om de kwaliteit van de infiltratie te bewaken en de infiltratie te controleren.[18] Zo dient de infiltratie aan een termijn te worden gebonden. De wettelijke regeling bevat geen maximumtermijn voor infiltratieacties, maar de officier van justitie wordt wel verplicht om een termijn van geldigheid te bepalen in het bevel.[19] Ten slotte dient de infiltratie getoetst te worden door het College van procureurs-generaal.[20]

Ook al blijkt het niet met zoveel woorden uit de wettekst van artikel 126h Sv, volgens de memorie van toelichting bij de Wet BOB kan de infiltratiebevoegdheid ook worden ingezet in een digitale context.[21] Ook uit de memorie van toelichting bij de Wet computercriminaliteit II werd duidelijk dat de infiltratiebevoegdheid voor een onderzoek in een digitaal netwerk relevant kan zijn.[22] De wetgever opende hiermee de deur voor infiltratie in een digitale context, waardoor opsporingsambtenaren op grond van artikel 126h Sv óók kunnen deelnemen aan een groep van personen, die actief is op online fora en handelswebsites wanneer het vermoeden bestaat dat door die groep strafbare feiten worden beraamd of gepleegd.[23] Volgens Oerlemans en Wegberg wordt in een dergelijke digitale infiltratieoperatie door de opsporingsambtenaren daadwerkelijk geparticipeerd in een criminele organisatie, teneinde bewijsmateriaal over strafbare feiten te verzamelen.[24] Het risico bestaat hierbij dat, net als bij de klassieke infiltratie, de betrokken opsporingsambtenaar strafbare feiten moet plegen teneinde de dekmantel te behouden en het vertrouwen te winnen van leden van een criminele organisatie.[25]

18. *Kamerstukken II* 1996/97, 25403, 3, p. 30-31.
19. *Kamerstukken II* 1996/97, 25403, 3, p. 74-75.
20. *Kamerstukken II* 1996/97, 25403, 3, p. 31.
21. *Kamerstukken II* 1996/97, 25403, 3, p. 29 en 55.
22. *Kamerstukken II* 1998/99, 26671, 3, p. 36.
23. B.J. Koops & J.J. Oerlemans, *Strafrecht en ICT,* Monografieën recht en informatietechnologie, Den Haag: Sdu Uitgevers 2019, p. 201.
24. J.J. Oerlemans & R.S. van Wegberg, 'Opsporing en bestrijding van online drugsmarkten', *Strafblad* 2019/05, p. 28.
25. J.J. Oerlemans, *Normering van digitale opsporingsmethoden*, Breda: Nederlandse Defensie Academie 2017, p. 27.

Behalve het vergaren van bewijsmateriaal, is het verstoren van de online drugsmarkt een doel op zich.[26] Volgens de memorie van toelichting bij de Wet computercriminaliteit II gelden bij infiltratie in een digitale context dezelfde voorwaarden als bij de klassieke toepassing van de infiltratiebevoegdheid, zoals het doorlaatverbod (artikel 126ff Sv) en het eerdergenoemde Tallon-criterium (artikel 126h lid 2 Sv), *'tenzij de specifieke aard van het onderzoek in een geautomatiseerde omgeving om specifieke voorzieningen vraagt'*.[27] Door deze laatste zinssnede werd de deur naar digitaal infiltreren door de wetgever dus niet wagenwijd opengezet. Immers, wanneer de specifieke aard van het onderzoek om specifieke voorzieningen vraagt, kunnen andere voorwaarden gelden. Een nadere invulling van deze 'tenzij'-bepaling ontbreekt in de memorie van toelichting en in de overige Kamerstukken. Bij ons dient zich de vraag aan of een grootschalige infiltratie van een *dark market* kwalificeert als een geval, waarin dergelijke specifieke voorzieningen nodig zijn. In de volgende paragraaf zal dit nader worden toegelicht.

4. Infiltreren in een digitale context: een roep om meer waarborgen?

De Rechtbank Rotterdam kwam tot het oordeel dat de klassieke infiltratiebevoegdheid afdoende was voor de digitale infiltratieoperatie van Hansa Market. Gelet op hetgeen in bovenstaande paragraaf reeds naar voren is gebracht, trekken wij de gegrondheid van dit oordeel in twijfel. Onzes inziens kan een digitale infiltratieoperatie namelijk dusdanig anders van aard zijn dan een infiltratieoperatie in de fysieke wereld, dat de huidige regulering en de toepassing daarvan in het digitale domein dient te worden heroverwogen. Allereerst zullen we ingaan op de 'tenzij-bepaling': bovengenoemde zinsnede uit de memorie van toelichting bij de Wet computercriminaliteit II. Wij zullen onze interpretatie van deze tenzij-bepaling weergeven en toelichten en beoordelen of een infiltratieoperatie in een digitale context om specifieke voorzieningen vraagt. Daarnaast lichten wij het doorlaatverbod uit. Het doorlaatverbod is een regulering van de infiltratiebevoegdheid. Dit verbod zullen we bespreken in het kader van de vraag of op dit moment voldoende waarborgen zijn opgenomen om dit verbod ook in digitale context te kunnen handhaven. Tot slot gaan we in op het voorstel tot het opnemen van Lijst Ia in de Opiumwet. Tot op heden is, zover bekend, de digitale infiltratiebevoegdheid enkel in de Hansa-zaak aangewend. Door meer stoffen op te nemen in de Opiumwet zal het OM in de toekomst wellicht vaker gebruik willen maken van de bevoegdheid digitaal te infiltreren. Een met voldoende waarborgen omklede

26. Oerlemans & Van Wegberg, *Strafblad* 2019/05, p. 30.
27. *Kamerstukken II* 1998/99, 26671, 3, p. 36-37.

doi: 10.5553/TBSenH/229567002020006005004

bevoegdheid tot digitale infiltratie is dan ook in dit licht essentieel.

Specifieke voorzieningen

Wanneer in een digitale context wordt geïnfiltreerd, kunnen de gegevens van soms wel duizenden gebruikers van een platform worden verkregen. Zoals we hebben gezien zijn zowel Alphabay als Hansa Market succesvol verstoord en zijn meer dan 50.000 transacties geteld in de korte tijd dat de market was overgenomen. Daarbij heeft de politie informatie over 420.000 gebruikers van Hansa Market verkregen.[28] Hoewel de klassieke bevoegdheid van artikel 126h Sv ook gebruikt kan worden in het onderzoek naar grote criminele organisaties, is de omvang en impact van een digitaal onderzoek volgens ons geenszins te vergelijken met een klassieke infiltratie. Immers, de politie kreeg tijdens operatie Bayonet in slechts 27 dagen de beschikking over informatie van duizenden gebruikers, waaronder zelfs de woonadressen van minstens 10.000 gebruikers.[29] Uit bovenstaande volgt dat bij een digitale infiltratieactie in een betrekkelijk kort tijdsbestek relatief veel informatie over duizenden gebruikers wordt verkregen. De specifieke aard van dit onderzoek kan onzes inziens bij uitstek vallen onder de eerdergenoemde tenzij-bepaling uit de memorie van toelichting. Soortgelijke grootschalige infiltratieoperaties zouden dan ook moeten worden voorzien van specifieke voorzieningen.

Gedacht kan worden aan een extra waarborg die erin voorziet dat de officier van justitie voor de inzet van de bevoegdheid over een machtiging van de rechter-commissaris (hierna: R-C) dient te beschikken. Zolang – zoals nu het geval is – geen toepassing wordt gegeven aan de tenzij-bepaling, is overeenkomstig artikel 126h Sv de officier van justitie bevoegd tot het afgeven van een bevel tot politiële digitale infiltratie. De officier van justitie dient hiertoe een afweging te maken in het licht van de proportionaliteit en de subsidiariteit van de inzet van de bevoegdheid. Oerlemans werpt in zijn noot bij de Hansa-zaak de vraag op hoe de noodzaak tot de inzet van de bijzondere opsporingsbevoegdheid van infiltratie opweegt tegen de privacy-inbreuk van duizenden betrokkenen.[30] Zoals aangegeven kan bij digitale infiltratie in korte tijd veel informatie worden ingewonnen. Dit betreft dan niet zeer diepgaande informatie over het privéleven van één persoon, zoals we vaak zien bij de inzet van andere bijzondere opsporingsbevoegdheden, maar juist minder diepgaande informatie over heel veel verschillende personen. Zo zijn bij de infiltratie van Hansa Market de woonadressen van 10.000 gebruikers onderschept. Gezien de snelle ontwikkelingen is het nog maar afwachten welke gegevens bij een volgende grootschalige digitale infiltratieactie kunnen worden onderschept. De beschreven aard van de digitale infiltratiebevoegdheid eist volgens ons een machtiging van de R-C als specifieke voorziening. De R-C dient hierbij te toetsen of het bevel aan alle wettelijke eisen voldoet en oordeelt over de proportionaliteit en subsidiariteit van het specifieke onderzoek.[31] In dat geval vindt eerst een uitgebreide interne toetsing plaats door de Centrale Toetsingscommissie (hierna: CTC), gevolgd door de toetsing van een onafhankelijke rechter. Pas dan is de procedure voor het verlenen van toestemming voor de inzet van de bevoegdheid met voldoende waarborgen omkleed.

Voorts is het relevant om naar de betrokkenheid van de R-C te kijken vanuit het perspectief van het Europees Hof voor de Rechten van de Mens (hierna: EHRM).[32] Het EHRM benadrukt in *Miliniene tegen Litouwen* dat in het geval van een *'veiled system of investigation'* rechterlijk toezicht meer gepast is.[33] Ook in *Furcht tegen Duitsland* kaart het EHRM aan dat *'judicial supervision'* wordt gezien als het meest geschikte middel bij undercover infiltratieoperaties.[34] Uit verschillende arresten van het EHRM volgt derhalve dat het EHRM toezicht door een onafhankelijke rechter prefereert boven toezicht door de officier van justitie.[35] Indien bij digitale infiltratieoperaties als Operatie Bayonet een vergaande inbreuk wordt gemaakt op de privacy van duizenden betrokkenen, geven wij, net als het EHRM, de voorkeur aan rechterlijk toezicht bij digitale infiltratieoperaties. Uit de rechtspraak van het EHRM vloeit echter niet voort dat een infiltratieoperatie altijd onder rechterlijk toezicht moet staan. Ook zonder het toezicht van een onafhankelijke rechter kan de infiltratiebevoegdheid rechtmatig worden aangewend.[36] Het is dan de officier van justitie die adequaat toezicht dient te houden op de infiltratieoperatie. Het EHRM acht enkel toezicht van een officier van justitie geschikt als er voldoende procedures en (procedurele) waarborgen zijn.[37] De enkele (procedurele) waarborg ter bescherming van de integriteit van het onder-

28. A. Greenberg, 'Operation Bayonet: inside the sting that hijacked an entire dark web drug market', Wired.com, 3 augustus 2018.
29. J.J. Oerlemans, annotatie bij Rb. Rotterdam 3 juli 2019, ECLI:NL:RBROT:2019:5339, *Computerrecht* 2019/178, afl. 5, p. 345; Greenberg, Wired.com, 3 augustus 2018.
30. J.J. Oerlemans, annotatie bij Rb. Rotterdam 3 juli 2019, ECLI:NL:RBROT:2019:5339, *Computerrecht* 2019/178, afl. 5, p. 345-346.
31. Vgl. 126m Sv. In de memorie van toelichting is hieromtrent het volgende overwogen: 'Voorts is bij de ingrijpende bevoegdheden van de telefoontap en het opnemen van vertrouwelijke communicatie (waaronder is begrepen het direct afluisteren) voorgeschreven dat de officier een machtiging van de rechter-commissaris moet verkrijgen. Deze machtiging wordt voorgesteld omdat ik eraan hecht dat, alvorens deze bevoegdheden worden gehanteerd, een rechter controleert of aan de wettelijke voorwaarden en de ongeschreven beginselen van een behoorlijke procesorde is voldaan, zoals de beginselen van proportionaliteit en subsidiariteit.' Zie *Kamerstukken II* 1996/97, 25403, 3, p. 15.
32. Zie ook J.J. Oerlemans, annotatie bij Rb. Rotterdam 3 juli 2019, ECLI:NL:RBROT:2019:5339, *Computerrecht* 2019/178, afl. 5, p. 345-346.
33. EHRM 24 juni 2008, appl.nr 74355/01, par. 39 (*Miliniene/Litouwen*).
34. HRM 23 oktober 2014, appl. nr. 54648/09, par. 53 (*Furcht/Duitsland*).
35. EHRM 4 november 2010, appl. nr. 18757/06, par. 50 (*Bannikova/Rusland*).
36. Hof 's-Hertogenbosch 25 april 2005, ECLI:NL:GHSHE:2005:AT5241, r.o. 6; EHRM 9 juni 1998, appl.nr. 25829/94, par. 37-38 (*Teixeira de Castro/Portugal*).
37. J.J. Oerlemans, annotatie bij Rb. Rotterdam 3 juli 2019, ECLI:NL:RBROT:2019:5339, *Computerrecht* 2019/178, afl. 5, p. 345-346; zie tevens EHRM 4 november 2010, appl. nr. 18757/06, par. 50 (*Bannikova/Rusland*); EHRM 23 oktober 2014, appl. nr. 54648/09, par. 53 (*Furcht/Duitsland*); EHRM 28 juni 2018, appl. nr. 31536/07, par. 45.

zoek kan onzes inziens worden gevonden in de omstandigheid dat het voornemen van de officier van justitie om van de bevoegdheid tot digitale infiltratie gebruik te maken ter toetsing moet worden voorgelegd aan het College van procureurs-generaal. Dit college laat zich adviseren door de CTC. Uit de wetsgeschiedenis volgt dat deze toetsing door het College van procureurs-generaal kan worden voorgeschreven en berust op de interne gezagsverhoudingen binnen het OM.[38] Deze toets door het college van procureurs-generaal biedt in de klassieke context van de infiltratiebevoegdheid voldoende waarborgen, bij toepassing van de infiltratiebevoegdheid in het digitale domein is dat nog de vraag.

Kortom, uit zowel de memorie van toelichting als uit de rechtspraak van het EHRM blijkt volgens ons dat het karakter van digitale undercoveroperaties vraagt om de betrokkenheid van de rechter-commissaris bij de toepassing van de infiltratiebevoegdheid in een digitale context. Het wettelijk verankeren van de voorafgaande machtiging van de rechter-commissaris in plaats van enkel een bevel van de officier van justitie, biedt meer waarborgen en doet daarmee recht aan de mate van inbreuk op de privacy van de (mogelijk) duizenden betrokkenen.

Voor wat betreft de termijn voor de inzet van de bevoegdheid vraagt digitale infiltratie onzes inziens ook om specifieke voorzieningen. Bij een aantal bijzondere opsporingsbevoegdheden is een specifieke maximumtermijn (met verlengingsmogelijkheid) in de wet vastgelegd. Zo kan bijvoorbeeld een bevel tot observatie (artikel 126g Sv) worden gegeven voor een termijn van ten hoogste drie maanden. De wettelijke regeling voor infiltratieacties bevat geen maximumtermijn. Uit de memorie van toelichting van de Wet BOB volgt hieromtrent dat naar de aard van de infiltratiemethode een redelijke termijn nodig zal zijn om alleen al enige contacten te leggen met de organisatie waarom het gaat. Dientengevolge zou volgens de wetgever een wettelijke termijn *of* zó lang moeten zijn, dat er geen waarborgfunctie van uitgaat, *of* zó kort, dat om de haverklap verlengingen moeten worden afgegeven, terwijl de omstandigheden maar heel langzaam wijzigen.[39] Wel wordt de officier van justitie verplicht om een termijn van geldigheid te bepalen in het bevel.[40]

Wederom is het hier van belang om op te merken dat digitale infiltratie geenszins vergelijkbaar is met klassieke infiltratie. Het is dan ook de vraag of de redenering van de wetgever dat naar de aard van de infiltratiemethode een redelijke termijn nodig zal zijn om enige contacten te leggen met de organisatie, ook standhoudt in het geval van digitale infiltratie. Zoals blijkt uit de beschrijving van operatie Bayonet wordt bij de digitale infiltratieacties door de politie toegang verkregen tot de market, waardoor de politie in één keer toegang heeft tot alle informatie van de market. Het beheer van de market komt vervolgens, nadat de website is gekopieerd, te liggen in handen van de politie, zonder dat de kopers en verkopers hiervan op de hoogte zijn. Er is dan ook, in tegenstelling tot klassieke infiltratie, geen redelijke termijn nodig om enige contacten te leggen met de organisatie. Bovendien is geen sprake van het leggen van contacten met de organisatie zoals gebruikelijk is bij klassieke infiltratie, nu de digitale infiltratieactie anoniem wordt uitgevoerd en de opsporingsambtenaren volledig buiten het zicht van de gebruikers van de market opereren. De argumentatie van de wetgever om de wettelijke regeling van infiltratie niet te voorzien van een maximumtermijn, houdt voor de digitale variant geen stand.

Er kan onzes inziens juist worden beargumenteerd digitale infiltratieacties te voorzien van een wettelijke maximumduur, nu de mate van inbreuk groot kan zijn en het daarom van belang is dat de infiltratieactie niet langer duurt dan strikt noodzakelijk. In overeenstemming met het door de wetgever zelf geformuleerde uitgangspunt, moet deze termijn zodanig zijn dat daadwerkelijk gebruik kan worden gemaakt van de methode, maar dat ook een hernieuwde toetsing van de methode mogelijk wordt.[41] De – zojuist geïntroduceerde – rechter-commissaris is de aangewezen autoriteit om te oordelen over de duur van de inzet en over de vraag of na ommekomst van deze termijn verlenging mogelijk is.

In aanvulling op het voorgaande, kan het opnemen van een maximumduur worden aangemerkt als een waarborg die eraan bijdraagt dat de bevoegdheid op een proportionele wijze wordt ingezet. Om te voldoen aan de eisen van proportionaliteit is het voorts van belang dat deze maximale termijn alleen mag worden gebruikt, indien het onderzoek dit dringend vordert. Hiertoe zal tijdens een infiltratieoperatie een afweging gemaakt moeten worden of de noodzaak tot de inzet van de bijzondere opsporingsbevoegdheid van infiltratie opweegt tegen de privacy-inbreuk van die duizenden betrokkenen, en, zo ja, voor de duur van welke (binnen de maximumduur vallende) termijn. Op deze manier wordt daadwerkelijk invulling gegeven aan de eis van proportionaliteit.

Het doorlaatverbod

Het doorlaatverbod biedt verschillende uitdagingen in het geval van digitale infiltraties, zoals bij Hansa Market. Het doorlaatverbod uit artikel 126ff Sv verplicht de opsporingsambtenaar die handelt ter uitvoering van een bevel als omschreven in de titels IVa tot en met V en Vb van het Wetboek van Strafvordering, de hem in de wet verleende inbeslagnemingsbevoegdheden te gebruiken, indien hij door de uitvoering van het bevel de vindplaats weet van voorwerpen waarvan het aanwezig hebben of voorhanden hebben ingevolge de wet verboden is vanwege hun schadelijkheid voor de volksgezondheid of hun gevaar voor de veiligheid. Dit doorlaatverbod en daarmee de verplichting tot inbeslagneming is in begin-

38. *Kamerstukken II* 1996/97, 25403, 3, p. 15 en 31.
39. *Kamerstukken II* 1996/97, 25403, 3, p. 74-75.
40. *Kamerstukken II* 1996/97, 25403, 3, p. 75.
41. *Kamerstukken II* 1996/97, 25403, 3, p. 104.

doi: 10.5553/TBSenH/229567002020006005004

sel ook van toepassing op de opsporingsambtenaren die door middel van de infiltratiebevoegdheid de vindplaats van verboden voorwerpen en middelen weten. Deze inbeslagneming mag volgens de tweede volzin van artikel 126ff Sv uitgesteld worden met het oogmerk om op een later tijdstip daartoe over te gaan; van uitstel komt dus geen afstel. Het tweede lid van artikel 126ff Sv biedt wel de mogelijkheid van de verplichting tot inbeslagneming af te zien op bevel van de officier van justitie, indien hij dit beveelt op grond van een zwaarwegend opsporingsbelang. Dit criterium biedt enkele ruimte om illegale goederen alsnog door te laten gaan. Hierbij wordt meegewogen of het opsporingsbelang groter is dan het onmiddellijk gevaar dat door het doorlaten van de voorwerpen ontstaat.[42] Dit laatste is volgens de Commissie Kalsbeek mede afhankelijk van de hoeveelheid door te laten voorwerpen.[43] Een verzoek tot het doen van een dergelijk bevel dient ingevolge artikel 140a Sv jo. artikel 131 lid 5 RO via de centrale toetsingscommissie ter goedkeuring te worden voorgelegd aan het College van procureurs-generaal en de minister van Justitie en Veiligheid.

Wanneer een opsporingsambtenaar door het gebruik van de infiltratiebevoegdheid inlichtingen verkrijgt over de locatie waar verboden voorwerpen zich bevinden, is hij aldus verplicht deze voorwerpen in beslag te nemen. Op *dark markets* worden veel verboden voorwerpen verhandeld en deze voorwerpen worden doorgaans via de post verstuurd. Het handhaven van het doorlaatverbod kan grote gevolgen hebben voor de infiltratie van een *dark market*. Zo is het denkbaar dat wanneer de opsporingsambtenaren alle verboden voorwerpen direct onderscheppen, dit snel de ronde zal doen waardoor meerdere gebruikers hiervan op de hoogte zijn. Nu het de politie en het OM eenmaal is gelukt om een *dark market* over te nemen zal de kennis over de grootschalige inbeslagneming mogelijk gebruikers doen vermoeden dat ook de door hen gebruikte *dark market* is overgenomen. De gebruikers kunnen vervolgens overstappen naar een andere website of hun zaken op een andere manier regelen. De andere mogelijkheid, het uitstellen van het inbeslagnamemoment, lijkt geen goede oplossing te zijn. Als het pakket eenmaal op de plaats van bestemming is aangekomen, is het immers niet bekend wat er met het verboden voorwerp zal gebeuren. Er lijkt aldus een beperkte termijn te zijn waarin de voorwerpen in beslag genomen kunnen worden. De omvang van de *dark markets* biedt hierbij een extra uitdaging. Het kan immers gaan om duizenden gebruikers die allen proberen verboden voorwerpen en middelen te verhandelen op een eigen manier.

De inzet van de infiltratiebevoegdheid is op dit moment omkleed met verschillende (wettelijke) waarborgen. Het doorlaatverbod is een van deze waarborgen. Grootschalige digitale infiltratie brengt nieuwe uitdagingen met zich mee op het gebied van het doorlaatverbod. Het is niet duidelijk op welke wijze de politie en het OM bij de overname van Hansa Market met het doorlaatverbod zijn omgegaan. Is het handhaven van het doorlaatverbod wel realistisch bij dit soort grootschalige digitale infiltratieacties? Gedurende de overname van Hansa Market zijn meer dan 50.000 transacties geteld. Stel dat slechts van één procent van deze transacties de vindplaats van het verhandelde verboden voorwerp bekend is geworden bij de opsporingsambtenaar, dan gaat het alsnog om meer dan 5.000 pakketten. Gezien de mogelijke problemen is het daarom wenselijk, al dan niet noodzakelijk, dat hier voorafgaand aan de inzet van deze opsporingsbevoegdheid goed over wordt nagedacht en dat hier concrete en controleerbare plannen voor worden gemaakt.

Wetsvoorstel tot opnemen 'Lijst Ia' in de Opiumwet

Een met meer waarborgen omkleedde bevoegdheid tot infiltratie in een digitale context is tevens relevant in de context van een recent conceptwetsvoorstel. Minister Grapperhaus en staatssecretaris Blokhuis hebben op 6 maart 2020 een conceptwetsvoorstel in consultatie gebracht. In dit voorstel wordt een verbod neergelegd om een middel dat deel uitmaakt van een stofgroep, opgenomen in de nieuwe Lijst Ia, binnen of buiten het grondgebied van Nederland te brengen, te bereiden, te bewerken, te verwerken, te verkopen, af te leveren, te verstrekken of te vervoeren, aanwezig te hebben of te vervaardigen.[44] Door risicovolle stofgroepen onder de Opiumwet te plaatsen, wordt het produceren, het voorhanden hebben en transporteren van alle substanties die vallen onder de chemische basisstructuur van een bepaalde stof in één klap verboden. Zo krijgt een hele groep designerdrugs bij voorbaat geen kans, ongeacht de specifieke samenstelling. In Duitsland en België wordt al gewerkt met een dergelijk verbod.[45] Het wetsvoorstel heeft enerzijds tot doel de volksgezondheid te beschermen en anderzijds de productie en handel in deze schadelijke stoffen tegen te gaan. Bovendien kan internationaal meer gezamenlijk worden opgetrokken en worden voldaan aan rechtshulpverzoeken uit andere landen waar deze stoffen al wel verboden zijn. Dit is volgens ons een goede ontwikkeling in het licht van de bestrijding van deze (ondermijnende) criminaliteit. Toch zal dit wetsvoorstel, mocht het door de Tweede en Eerste Kamer worden aangenomen, er vermoedelijk voor zorgen dat meer handel zal plaatsvinden op *dark markets* dan voorheen. Alle stofgroepen die thans nog legaal verkrijgbaar zijn, zullen dan illegaal verhandeld worden op het *dark web*. Hoe meer verhandeld wordt op *dark markets*, hoe vaker de digitale infiltratiebevoegdheid gebruikt zal moeten worden. Ook in dit licht is het onzes inziens

42. *Kamerstukken II* 1998/99, 26269, 5, p. 211.
43. *Kamerstukken II* 1998/99, 26269, 5, p. 211.
44. Artikel 2a conceptwetsvoorstel.
45. Rijksoverheid.nl, https://www.rijksoverheid.nl/actueel/nieuws/2020/03/06/wetsvoorstel-blokhuis-en-grapperhaus-plaatst-groepen-designerdrugs-op-lijst-ia-van-de-opiumwet#:~:text=stofgroepen%20te%20verbieden.-,Lijst%20Ia,stof%20in%20%C3%A9%C3%A9n%20klap%20verboden.

doi: 10.5553/TBSenH/229567002020006005004

wenselijk een duidelijke wettelijke grondslag op te nemen voor digitale infiltratie.

5. Conclusie

Het binnendringen en oprollen van de grote *dark market* Hansa was een baanbrekende operatie. Niet eerder had de Nederlandse politie in samenwerking met internationale politie- en justitiediensten een illegale marktplaats met de omvang van Hansa Market ontmanteld. Artikel 126h Sv bood aan de Nederlandse politie de bevoegdheid om de *dark market* te infiltreren. Anders dan artikel 126h Sv doet vermoeden, geeft deze bepaling volgens de memorie van toelichting bij de Wet BOB ook een bevoegdheid tot infiltreren in een groep van personen die digitaal opereert. Onzes inziens komt echter bij een digitale infiltratieoperatie meer kijken dan bij infiltratie in de fysieke wereld, onder meer doordat gegevens van duizenden personen in één klap kunnen worden verzameld. Dit levert niet slechts een inbreuk op het recht op privacy op van één persoon, maar op die van heel veel personen. De vraag wat vervolgens met alle verkregen informatie dient te worden gedaan is ook niet gemakkelijk te beantwoorden. Zo vereist artikel 126ff Sv dat illegale voorwerpen waarvan de locatie bekend is geworden door een opsporingsbevoegdheid als infiltratie, vervolgens ook in beslag worden genomen. Gezien de aard van de infiltratie, waarbij de opsporingsambtenaren enige tijd anoniem aan het roer trachten te staan van een *dark market*, kleven er risico's aan het direct in beslag nemen van alle voorwerpen. De inbeslagneming uitstellen lijkt daarentegen ook geen bevredigende mogelijkheid, nu de locatie van de verboden voorwerpen slechts gedurende een beperkte tijd bekend is. Daarnaast is onlangs door minister Grapperhaus en staatssecretaris Blok een wetsvoorstel in consultatie gebracht, waarmee wordt beoogd een nieuwe Lijst Ia op te nemen in de Opiumwet. Door het strafbaar stellen van het handelen in designerdrugs, zullen stoffen die tot op heden via het *surface web* verkrijgbaar zijn, na invoering van de wetswijziging worden aangeboden op het *dark web*. Kort gezegd zal de criminaliteit door dit wetsvoorstel toenemen, waardoor behoefte ontstaat aan een duidelijk omschreven bevoegdheid tot (digitale) infiltratie.

Wij achten het om verschillende redenen aldus noodzakelijk dat de bevoegdheid tot infiltratie met meer waarborgen wordt omkleed, wanneer deze bevoegdheid wordt aangewend in de digitale wereld. De wetgever heeft de deur naar specifieke voorzieningen in het geval van digitale infiltratie op een kier gezet, door in de memorie van toelichting omtrent klassieke infiltratie te overwegen dat het denkbaar is dat '*de specifieke aard van het onderzoek in een geautomatiseerde omgeving om specifieke voorzieningen vraagt*'.[46] Digitale infiltratie is onzes inziens een onderzoek van deze aard en daarom stellen we in dit artikel een aantal extra waarborgen voor. Zo is het allereerst wenselijk een machtiging van de R-C als voorwaarde op te nemen, ook het EHRM acht toezicht door een onafhankelijke rechter het meest geschikte middel bij undercover infiltratieoperaties. Op deze manier wordt het afgeven van een bevel tot digitaal infiltreren voorzien van een daaraan voorafgegane rechterlijke toetsing. Daarnaast kan de R-C voorafgaand aan het aanwenden van de bevoegdheid het voorgestelde onderzoek onderwerpen aan een strenge proportionaliteits- en subsidiariteitstoets, waarbij de woorden 'indien het onderzoek dit dringend vordert' eng moeten worden uitgelegd. Het is naar onze mening niet nodig de infiltratieoperatie lang te laten voortduren, omdat, indien het eenmaal is gelukt te infiltreren in de *dark market,* het leggen van contact met en verkrijgen van informatie over de organisatie niet veel tijd nodig heeft. Zoals is gebleken uit de beschrijving van operatie Bayonet wordt immers bij digitale infiltratieoperaties door de politie toegang verkregen tot de gehele *market*, waardoor de politie in één keer toegang heeft tot veel informatie. Daarom zou de bevoegdheid tot digitale infiltratie aan een wettelijke termijn moeten worden gebonden. Deze termijn kan indien dit nodig wordt geacht worden verlengd, maar alleen nadat een nieuwe machtiging door de rechter-commissaris is afgegeven.

De bevoegdheid tot in(ternet)filtratie roept dus om meer waarborgen dan de klassieke infiltratiebevoegdheid. We hopen dat deze roep om waarborgen wordt gehoord, zodat een volgende digitale infiltratieoperatie met recht een succes op alle fronten kan worden genoemd.

46. *Kamerstukken II* 1998/99, 26671, 3, p. 36-37.

doi: 10.5553/TBSenH/229567002020006005004