Mr. dr. J.J. Oerlemans
is onderzoeker bij eLaw, het Centrum voor Recht en Digitale Technologie van de Universiteit Leiden.

49. De Wet computercriminaliteit III: meer handhaving op internet

Met de Wet computercriminaliteit III wordt beoogd de opsporing en vervolging van cybercrime te versterken. De hackbevoegdheid en het take down-bevel bieden echter ook vergaande handhavingsmogelijkheden. In dit artikel wordt een overzicht gegeven van de voorstellen uit de Wet computercriminaliteit III en worden de twee nieuwe bevoegdheden uitgelicht.

1. Inleiding

De Wet computercriminaliteit III geeft meer mogelijkheden aan de politie en het Openbaar Ministerie om cybercrime te bestrijden.[1] De wijzigingen aan het materiële strafrecht maken de vervolging voor enkele veelvoorkomende vormen van cybercrime eenvoudiger en de introductie van de 'hackbevoegdheid' en het 'takedown-bevel' in het Wetboek van Strafvordering biedt nieuwe instrumenten voor de bestrijding van cybercrime.

In dit artikel worden eerst de wijzigingen voor het materiële strafrecht door de Wet computercriminaliteit III in vogelvlucht besproken. Daarna worden de belangrijkste wijzigingen voor het formele strafrecht behandeld. Daarbij wordt een kritische noot geplaatst bij de voorgestelde regeling voor een takedown-bevel en de hackbevoegdheid en wordt kort ingegaan op de mogelijkheid de hackbevoegdheid over onze landsgrenzen in te zetten.

2. Materieel strafrecht

De Wet computercriminaliteit III staat in de literatuur het meest bekend om de voorgestelde hackbevoegdheid (zie paragraaf 3.2) en (het later vervallen) decryptiebevel.[2] Toch brengt het wetsvoorstel ook een aantal belangrijke wijzigingen met zich voor het materiële strafrecht. De nieuwe strafbaarstellingen voor het publiceren van niet-openbare gegevens, heling van gegevens en online handelsfraude beogen groeiende vormen van cybercrime in Nederland tegen te gaan. Daarnaast maakt de voorgestelde wijziging bij de delicten grooming en ontucht een nieuw opsporingsmiddel mogelijk in de vorm van de zogenaamde lokpuber. Deze wijzigingen hebben tevens tot doel webcamseks met minderjarigen tegen te gaan. De voorstellen worden hierna achtereenvolgens kort besproken.

2.1 Publiceren van niet-openbare gegevens

In de Wet computercriminaliteit III wordt in artikel 138c Sr voorgesteld het opzettelijk en wederrechtelijk overnemen van niet-openbare gegevens uit een geautomatiseerd werk straf-

1 De wet Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit wordt in dit artikel afgekort als: Wet computercriminaliteit III. Ten tijde van het schrijven van dit artikel (augustus 2017) is het wetsvoorstel nog in behandeling bij de Eerste Kamer.

2 Zie o.a. B.J. Koops, 'Tijd voor computercriminaliteit III', *NJB* 2010/85, p. 2461-2466; M.E. Koning, 'Van teugelloos "terughacken" naar "digitale toegang op afstand"', *Privacy & Informatie* 2011, afl. 2, p. 46-52; N.J.M. Kwakman & M.E. Buwalda, 'Het ontwerp wetsvoorstel Computercriminaliteit III', *Ars Aequi* 2014, p. 9-18; P.J.D.J. Muijen, 'Wet computercriminaliteit III. To boldly go where no man has gone before', Privacy & Informatie 2016, p. 104-110; J.R.J. Aink, 'Het wetsvoorstel Computercriminaliteit III. Een high tech inhaalslag?', *TPWS* 2016/46 en R.L.D. Pool & B.H.M. Custers, 'The police hack back. Legitimacy, necessity and privacy implications of the next step in fighting cybercrime', *European Journal of Crime, criminal law and criminal justice* 2017, p. 123-144.

baar te stellen. Hierbij kan worden gedacht aan het kopiëren van gegevens uit een bedrijfsnetwerk door een werknemer op bijvoorbeeld een USB-stick. Hierbij moet uiteraard wel het opzet en de wederrechtelijkheid worden bewezen. In de memorie van toelichting staat dat hier 'als het ware sprake is van "verduistering" van gegevens'.[3] Strafbaarstelling op grond van artikel 321 Sr is niet mogelijk, omdat gegevens binnen het strafrecht in principe niet als goed worden beschouwd.[4]

De voorgestelde strafbaarstelling is deels het gevolg van Kamervragen naar aanleiding van de Manon Thomas-zaak uit 2010.[5] In deze zaak werden naaktfoto's van de voormalig presentatrice overgenomen en via internet openbaar gemaakt. Vermoedelijk zijn deze foto's van een gedeelde map uit het lokale wifi-netwerk bij haar thuis weggehaald en was het lastig de dader te vervolgen voor computervredebreuk.[6] Bij computervredebreuk (art. 138ab Sr) is vereist dat een computer wordt *binnengedrongen*. Dit vereiste valt weg bij de strafbaarstelling van artikel 138c Sr, waardoor vervolging voor de bovenomschreven gedraging mogelijk wordt.[7]

Echter, als gevolg van het voorstel wordt de drempel voor het vervolgen voor het overnemen van niet-openbare gegevens van een computer misschien wel érg laag. Koops vraagt zich bijvoorbeeld af wat nu de noodzaak precies is van de strafbaarstelling.[8] Een andere zorg is dat klokkenluiders in het algemeen belang straks niet meer niet-openbare gegevens willen kopiëren om misstanden aan de kaak te stellen. Deze kritiek is opgepakt. In de toelichting op het wetsvoorstel wordt opgemerkt dat het voorhanden hebben of openbaren van niet-openbare gegevens niet wederrechtelijk is indien hogere belangen een dergelijke inbreuk kunnen rechtvaardigen en het handelen proportioneel en subsidiair is.[9]

2.2 Heling van gegevens

Gegevens worden in het strafrecht in principe niet als goed beschouwd. Het traditionele artikel voor heling stelt kort gezegd het verwerven, voorhanden hebben of overdragen van een goed strafbaar, voor zover de verdachte ten tijde van deze handelingen op de hoogte was dat het goed uit misdrijf is verkregen. Lid 2 van artikel 416 Sr (opzetheling) stelt het opzettelijk uit winstbejag voorhanden hebben of overdragen van een uit misdrijf verkregen goed strafbaar. Het voorgestelde artikel 139g Sr stelt op zijn beurt het verwerven of voorhanden hebben van niet-openbare *gegevens* strafbaar. Dit zijn gegevens die bijvoorbeeld uit een datalek of computervredebreuk zijn verkregen.[10] Ook het ter beschikking stellen, aan een ander bekendmaken, of uit winstbejag voorhanden hebben van niet-openbare gegevens, is in het artikel strafbaar gesteld. Voor beide handelingen geldt dat de verdachte ten tijde van deze handelingen moet vermoeden dat deze door misdrijf zijn verkregen. De politie en het Openbaar Ministerie hebben behoefte aan de strafbaarstelling, omdat het voorheen lastig is gebleken succesvol vervolging in te stellen voor het online beschikbaar stellen van gestolen persoonsgegevens of creditcardgegevens.[11]

Internetoplichting is een veelvoorkomende vorm van cybercrime. Bij Landelijk Meldpunt Internetoplichting (LMIO) van de politie zijn in 2015 meer dan 35.000 aangiftes van internetoplichting binnengekomen.

In het voorgestelde artikel 139g, tweede lid, Sr is tevens expliciet gemaakt dat degene niet strafbaar is die te goeder trouw heeft kunnen aannemen dat het algemeen belang het helen van gegevens vereiste.[12] Bij de beslissing voor het

3 *Kamerstukken II* 2015/16, 34372, 3, p. 64.
4 Een uitzondering daarop is ontwikkeld in het *RuneScape*-arrest. Hierin is – kort gezegd – het concept ontwikkeld dat gegevens die uniek zijn en waarde in het economisch verkeer hebben tóch als goed kunnen worden beschouwd (HR 31 januari 2012, ECLI:NL:HR:2012:BQ9251). Zie ook HR 31 januari 2012, ECLI:NL:HR:2012:BQ6575 (*Belminuten*-arrest).
5 *Kamerstukken II* 2015/16, 34372, 3, p. 62-63.
6 Zie Rb. Noord-Nederland 18 december 2013, ECLI:NL:RBNNE:2013:8036, r.o. 2.10 (tussenuitspraak).
7 *Kamerstukken II* 2015/16, 34372, 3, p. 64.
8 Zie conceptverslag van een deskundigenbijeenkomst over 'Privacy in het kader van de wetsvoorstellen Vastleggen en bewaren kentekengegevens door politie (33542) en Computercriminaliteit III (34272)', p. 32.
9 *Kamerstukken II* 2015/16, 34372, 3, p. 66. Hierbij kan een vergelijking worden gemaakt met de omgang met 'ethisch hacken'. Als het algemeen belang groot genoeg is, hebben rechtbanken in Nederland aangenomen dat computervredebreuk niet wederrechtelijk is, onder de voorwaarden dat het handelen proportioneel is (door bijv. niet meteen buitgemaakte gegevens in zijn geheel online ter beschikking te stellen) en subsidiair is (door bijv. eerst contact te zoeken met de eigenaar van de computer of het netwerk en een reactie af te wachten voor de media in te lichten). Zie Rb. Oost-Brabant 15 februari 2013, ECLI:NL:RBOBR:2013:BZ1157 en Rb. Den Haag 17 december 2014, ECLI:NL:RBDHA:2014:15611.
10 In 2009 had de wetgever al aan de Tweede Kamer toegezegd heling strafbaar te stellen (*Kamerstukken II* 2008/09, 28684, 232, p. 4). Voor het helen van gegevens staat maximaal één jaar gevangenisstraf of een geldboete van de vierde categorie.
11 Zie ook *Kamerstukken II* 2015/16, 34372, 3, p. 81.
12 De suggesties van Bert-Jaap Koops in zijn artikel in het *Nederlands Juristenblad* (Koops, *a.w.*, p. 2463-2465) bij een eerdere versie van het wetsvoorstel zijn daarbij overgenomen.

vervolgen van het helen van niet-openbare gegevens, moet de officier van justitie voortaan expliciet rekening houden met conflicterende belangen: aan de ene kan het recht op een vrije nieuwsgaring en aan de andere kant het recht op bescherming van gegevens.[13]

2.3 Online handelsfraude

Internetoplichting is een veelvoorkomende vorm van cybercrime. Bij Landelijk Meldpunt Internetoplichting (LMIO) van de politie zijn in 2015 meer dan 35.000 aangiftes van internetoplichting binnengekomen. Daaruit bleek dat de gedupeerden gemiddeld voor € 200,= werden opgelicht.[14] In 2016 werden vijfhonderd verdachten geïdentificeerd.[15]

In de Wet computercriminaliteit III wordt voorgesteld artikel 326d Sr in te voeren. Met deze bepaling moet het eenvoudiger worden tegen online handelsfraude, ook wel 'Marktplaatsoplichting' genoemd, op te treden. Het aanbieden van goederen of diensten via internet, zonder de intentie om te leveren, is namelijk niet zonder meer strafbaar als oplichting in de zin van artikel 326 Sr. Daarvoor is namelijk ook het aannemen van een valse naam of hoedanigheid en listige kunstgrepen of een samenweefsel van verdichtsels vereist.[16] De enkele omstandigheid dat iemand in strijd met de waarheid zich voordoet als bonafide verkoper en in staat is en voornemens is om te leveren, maar dit vervolgens niet doet, levert nog geen oplichting in de zin artikel 326 Sr op.[17] Daarvoor is méér nodig, zoals het opzettelijk foute namen en e-mailadressen hanteren om de mogelijkheden tot verhaal te bemoeilijken.[18]

Voor het voorgestelde delict in artikel 326d Sr moet bewezen worden dat een beroep of gewoonte wordt gemaakt van het te koop aanbieden van een goed of het aanbieden van een dienst. Met het onderdeel 'gebruikmaking van een communicatiedienst' wordt specifiek het aanbod van de verkoop via internet (inclusief e-mail) tot uitdrukking gebracht.[19] Een eenmalig geval van online handelsfraude is op basis van dit artikel niet strafbaar. Dat komt in de strafbaarstelling tot uitdrukking bij het element dat er een *gewoonte* moet worden gemaakt van het delict. Hiervan kan sprake zijn wanneer gedurende een korte tijd een groot aantal afzonderlijke transacties via een website of meerdere websites plaatsvinden, zonder de intentie het aangeboden goed of dienst te leveren. Een conflict over niet-levering is in de eerste plaats wanprestatie dat via het civiele recht moet worden opgelost. Private partijen hebben een actieve rol bij de bestrijding van fraude via hun platform, hetgeen begrijpelijk is omdat een verlies van consumentenvertrouwen hun verdienmodel aantast. Slechts daar waar het echt noodzakelijk is zal het Openbaar Ministerie optreden.[20] Daarbij kan gebruik worden gemaakt van gebundelde aangiften van private partijen, zoals Marktplaats.nl.

2.4 De lokpuber

De 'lokpuber' is een woord dat in zwang is geraakt door een Leidse zedenzaak, waarbij een opsporingsambtenaar zich voordeed als een puber in een chatkanaal tijdens een opsporingsonderzoek naar grooming.[21] Het delict grooming kan worden omschreven als het voorstellen tot een ontmoeting met een persoon van minder dan zestien jaar met het oogmerk ontuchtige handelingen te plegen door gebruikmaking van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst (art. 248e Sr). Het oogmerk van de dader moet gericht zijn op het plegen van ontuchtige handelingen of het vervaardigen van kinderpornografie.[22] In de onderhavige zaak was de verdachte niet strafbaar, omdat niet werd voldaan aan de delictsomschrijving.[23] In de huidige redactie van het artikel moet immers een voorstel tot een ontmoeting worden gedaan met *een persoon van minder dan zestien jaar,*

13 *Kamerstukken II* 2015/16, 34372, 3, p. 66-67. Daarbij wordt verwezen naar HR 26 maart 2013, ECLI:NL:HR:2013:BY3752.

14 Zie Politie.nl, 'Internetoplichter schuift naar social media', 27 mei 2016, www.politie.nl/nieuws/2016/mei/26/internetoplichter-schuift-naar-social-media.html (laatst geraadpleegd 15 augustus 2017).

15 Politie.nl, 'Politie zet in op voorkomen internetoplichting', 29 mei 2017, www.politie.nl/nieuws/2017/mei/29/politie-zet-in-op-voorkomen-internetoplichting.html (laatst geraadpleegd 15 augustus 2017).

16 Zie ook HR 11 november 2014, ECLI:NL:HR:2014:3144, NJ 2014/518 en HR 20 december 2016, ECLI:NL:HR:2016:2889, *NJ* 2017/157, *Ars Aequi* 2017, p. 528-534, m.nt. J.M. ten Voorde.

17 Het bij herhaling schuldig maken aan het kopen van goederen of diensten zonder te leveren kan overigens ook het delict flessentrekkerij opleveren (art. 326a Sr).

18 Zie HR 11 november 2014, ECLI:NL:HR:2014:3144, NJ 2014/518. Toch bleef er naar aanleiding van dit '*Marktplaats*-arrest' enige onduidelijkheid bestaan over de aard van de oplichtingsmiddelen en de onderlinge samenhang van die middelen. In het overzichtsarrest over oplichting van HR 20 december 2016, ECLI:NL:HR:2016:2889, *NJ* 2017/157, m.nt. N. Keijzer, heeft de Hoge Raad getracht deze onduidelijkheid weg te nemen. Zie voor een bespreking van het arrest «JIN» 2017, afl. 1, M.L.C.C. de Bruijn-Lückers en *Ars Aequi* 2017, p. 528-534, m.nt. J.M. ten Voorde en *Nieuwsbrief Strafrecht* 2017/7, m.nt. D.J. van Leeuwen.

19 *Kamerstukken II* 2015/16, 34372, 3, p. 92.

20 *Kamerstukken II* 2015/16, 34372, 3, p. 75.

21 Zie o.a. S.F.J. Smeets, 'De "lokpuber": een mislukt experiment', *Strafblad* 2013, p. 336-338; F.P. Ölçer, 'De lokmethode bij de opsporing van grooming', *Computerrecht* 2014/3; en het artikel in dit nummer van *Strafblad* van C. Grijsen, B.J. Polman & A. de Lange, 'De uitbreiding van de strafbaarstelling van grooming met de inzet van de lokpuber tot doel. Het voorstel tot wijziging van artikel 248e Sr als een wolf in schaapskleren'.

22 *Kamerstukken II* 2008/09, 31810, 3, p. 9. Zie ook Hof Arnhem 15 september 2011, ECLI:NL:GHARN:2011:BT1553.

23 Rb. 's-Gravenhage 14 september 2012, ECLI:NL:RBSGR:2012:BX8497 en Hof Den Haag 25 juni 2013, ECLI:NL:GHDHA:2013:2302, *NJ* 2014/123.

terwijl de opsporingsambtenaar ouder was dan zestien jaar. Met de Wet computercriminaliteit III wordt de inzet van de lokpuber mogelijk gemaakt door artikel 248e Sr te wijzigen door de woorden *'of schijnbaar is betrokken'* toe te voegen.[24] In dat geval is niet langer vereist dat daadwerkelijk met een persoon van minder dan zestien jaar wordt gecommuniceerd. Uit een WODC-onderzoek naar de mogelijke herziening van zedendelicten blijkt dat de opsporing behoefte heeft aan de mogelijkheid een lokpuber in te zetten. De reden is dat de aard van het delict grooming met zich brengt dat bewijsmateriaal moet worden vergaard voor het op heterdaad betrappen van grooming tijdens de online communicatie of via logbestanden op in beslag genomen computers achteraf.[25] Met gebruik van een lokpuber is het mogelijk op heterdaad te betrappen tijdens de online communicatie.

Het voorstel brengt echter ook met zich dat van een *virtuele* minderjarige gebruik kan worden gemaakt als lokpuber.[26] Verschillende auteurs en de NVvR waarschuwen in dat kader voor het risico van burgeropsporing van grooming.[27] De staatssecretaris keurt dit in de memorie van toelichting niet expliciet af en stelt dat 'het belang van de bescherming van kinderen tegen gedrag op het internet om kinderen te verleiden tot seksuele gedragingen (...) mijns inziens het zwaarste weegt' en het OM een 'prudent vervolgingsbeleid hanteert'.[28] De politie en het OM moeten bij de inzet van de lokpuber als opsporingsmethode terughoudend en passief te werk gaan om niet in strijd te zijn met het uitlokkingsverbod, afgeleid uit het recht op een eerlijk proces zoals bedoeld in artikel 6 EVRM.[29]

2.5 Webcamseks

Webcamseks tussen twee volwassen is in Nederland niet strafbaar. Tegen webcamseks tussen een volwassene en minderjarige wil de wetgever echter in bepaalde omstandigheden beter kunnen optreden. Volgens de wetgever komt het steeds vaker voor dat groomers, waaronder loverboys, meisjes proberen te verleiden om zich voor de webcam uit te kleden en seksuele handelingen te verrichten. Het beeldmateriaal wordt vervolgens gebruikt om het slachtoffer onder druk te zetten om steeds opnieuw voor de camera te komen of verdergaande seksuele handelingen te verrichten.[30] Deze vorm van afpersing wordt ook wel *'sextortion'* genoemd.[31]

Artikel 248a Sr (ontucht) biedt al een grondslag voor het vervolgen van de meerderjarige indien deze een minderjarige door giften, misbruik van overwicht of misleiding beweegt tot het plegen van ontuchtige handelingen.[32] Met de Wet computercriminaliteit III wordt artikel 248a Sr gewijzigd om het seksueel benaderen van kinderen door volwassen via internet beter strafbaar te stellen.[33] Met de wijziging wordt ook de verleiding van een minderjarige, *of iemand die zich voordoet* als een minderjarige, tot ontucht strafbaar. Uit bewijsmiddelen zal voor het vereiste opzet moeten blijken dat er interactie is geweest tussen verdachte en de (zich als zodanig voordoende) minderjarige voor het plegen van ontucht. Met betrekking tot deze bewijsmiddelen kan gedacht worden aan het zich naakt voor de webcam tonen of het verrichten van ontuchtige handelingen voor de camera.[34]

24 Zie ook *Kamerstukken II* 2015/16, 34372, 3, p. 4 en 70-71. Zie uitgebreid K. Lindenberg, 'De lokpuber verstopt zich in het materiële recht. Over het aanpassen van zedendelicten door Computercriminaliteit III en hoe dit meer is dan het lijkt', *Ars Aequi* 2016/12, p. 942-950.

25 K. Lindenberg & A.A. van Dijk, *Herziening van de zedendelicten? Een analyse van Titel XIV, Tweede Boek, Wetboek van Strafrecht met het oog op samenhang, complexiteit en normstelling*, Den Haag: WODC, p. 397.

26 Zoals door private partijen ook is gedaan met het virtuele meisje 'Sweetie' om de problematiek rondom webcamseks met minderjarigen aan te tonen. Zie uitgebreid over juridische aspecten met betrekking tot 'Sweetie' B.W. Schermer et al., *Legal aspects of Sweetie 2.0*, Leiden/Tilburg: Center for Law and Digital Technologies (eLaw)/TILT 2016.

27 Zie Lindenberg, a.w., p. 950 en Ölçer, a.w., p. 15. Zie ook *Kamerstukken II* 2015/16, 34372, 3, p. 71.

28 *Kamerstukken II* 2015/16, 34372, 3, p. 71.

29 Zie uitgebreid Ölçer, a.w., p. 16-18, onder verwijzing naar EHRM november 2010, nr. 18757/06, «EHRC» 2011/9, m.nt. Ölçer (*Bannikova/Rusland*). Ölçer, a.w. en J.J. Oerlemans, *Investigating cybercrime* (diss. Leiden), Amsterdam: Amsterdam University Press 2017, p. 239-241 geven aan dat betrokkenheid van de rechter-commissaris bij inzet van de opsporingsmethode wenselijk is. De opsporingsmethode wordt vermoedelijk gebaseerd op de bijzondere bevoegdheid van stelselmatige informatie-inwinning (art. 126j Sv), waarvoor slechts een bevel van een officier van justitie is vereist.

30 *Kamerstukken II* 2015/16, 34372, 3, p. 68. Zie ook S. van der Hof, 'Wraakporno op internet. Een verkenning van de (on)mogelijkheden voor een strafrechtelijke aanpak', *Ars Aequi* 2016, afl. 1, p. 57.

31 Noemenswaardig is dat in de jurisprudentie deze gedragingen ook wel tot (poging tot) (online) aanranding (art. 246 Sr) worden gekwalificeerd. Zie bijv. Rb. Dordrecht 20 oktober 2005, ECLI:NL:RBDOR:2005:AU4724; Rb. Gelderland 31 mei 2016, ECLI:NL:RBGEL:2016:3037; Hof Arnhem-Leeuwarden 8 december 2015, ECLI:NL:GHARL:2015:9221, UDH:IR/13054, m.nt. T. van der Linden-Smit en K. Kroeks-de Raaij en Rb. Amsterdam 16 maart 2017, ECLI:NL:RBAMS:2017:1627, *Computerrecht* 2017/103, m.nt. J.J. Oerlemans (*Aydin C.*). Aanranding kan in deze omstandigheid ook op afstand plaatsvinden. Slachtoffers hebben vaak niet de mogelijkheid te verhinderen dat de dader de afbeeldingen verspreidt. Voor het slachtoffer is het daarom onvermijdbaar dat het dreigement (het verspreiden van de foto/video) wordt uitgevoerd, als zij niet toegeven aan de dader. In dat geval is er sprake van (poging tot) aanranding op afstand.

32 Zie bijv. Rb. Haarlem 24 december 2004, ECLI:NL:RBHAA:2004:AR8212 en Rb. Zutphen 1 maart 2006, ECLI:NL:RBZUT:2006:AV3246. In art. 248 Sr zijn strafverzwarende omstandigheden geformuleerd, zoals het bezit, verspreiding en vervaardiging van kinderpornografie, ontucht en aanranding.

33 *Kamerstukken II* 2015/16, 34372, 3, p. 67.

34 *Kamerstukken II* 2015/16, 34372, 3, p. 90.

3. Formeel strafrecht

De belangrijkste wijzigingen voor het formele strafrecht die de Wet computercriminaliteit III met zich brengt, betreffen het takedown-bevel en de hackbevoegdheid. Daarnaast is het bijzonder dat de hackbevoegdheid onder omstandigheden over de grens kan worden ingezet. Deze drie onderdelen uit het wetsvoorstel worden in deze paragraaf kritisch belicht.

3.1 Takedown-bevel

'Notice and takedown' staat voor een procedure waarbij een partij in kennis wordt gesteld (de *notice*) van onmiskenbaar onrechtmatig of strafbaar materiaal op een online platform met verzoek dit materiaal te verwijderen (de *takedown*). In Nederland bestaat al sinds 2008 een notice and takedown-gedragscode, waarbij openbare telecommunicatiedienstaanbieders die internetdiensten leveren op verzoek van eenieder onmiskenbaar strafbaar of onrechtmatig materiaal op basis van vrijwilligheid verwijderen.[35] Ook opsporingsambtenaren kunnen een verzoek doen op basis van de gedragscode. De gedragscode is in de praktijk effectief.

Het ontbreekt de politie en het Openbaar Ministerie echter aan een deugdelijke grondslag voor het *verplicht* verwijderen van strafbaar materiaal.[36] Het voorgestelde artikel 125p Sv moet voorzien in de bevoegdheid strafbare inhoud van het internet te doen verwijderen. Een officier van justitie kan dit bevel aan een aanbieder van een communicatiedienst afgeven binnen een opsporingsonderzoek naar de meer ernstige misdrijven, zoals omschreven in artikel 67 Sv, nadat een machtiging van een rechter-commissaris is verkregen.
In het conceptwetsvoorstel uit 2010 ontbrak het vereiste van een machtiging van de rechter-commissaris en de beperking tot het afgeven van het bevel bij de meer ernstige misdrijven. Deze twee waarborgen zijn terecht noodzakelijk gebleken, gezien de ernstige inmenging met het recht op vrijheid van meningsuiting (en de toegang tot informatie als onderdeel daarvan) als gevolg van de toepassing van een takedown-bevel.[37]

Het bevel wordt pas ingezet als de aanbieder van de elektronische communicatiedienst geen opvolging geeft aan de vrijwillige NTD-gedragscode of niet bij deze code is aangesloten.[38] Indien niet wordt voldaan aan het bevel, kan vervolging worden ingesteld voor het niet voldoen aan een bevoegd gegeven ambtelijk bevel (184 Sr) of voor het deelnemen of medeplegen aan het gronddelict.[39] Als de officier van justitie en de betrokkene het niet met elkaar eens zijn, staat de beklagregeling in artikel 552a Sv open.[40]

3.1.1 Trapsgewijze toepassing

Een onderbelicht aspect van het takedown-bevel zijn de potentiële gevolgen van het bevel. In het uiterste geval kan een ontoegankelijkheidsmakingsbevel worden opgelegd aan een internet access provider, onder andere door een blokkade op het niveau van een IP-adres.[41] Dit is te beschrijven als een internetfilter. Internetfilters staan op gespannen voet met de vrijheid van meningsuiting; meer specifiek met betrekking tot het recht op toegang tot informatie.[42] Meer principieel bedreigen internetfilters ook het idee dat via internet in principe alles genetwerkt en toegankelijk moet zijn. Voor sommige mensen is het een schrikbeeld dat per staat een nationaal gefilterd internet – het 'splinternet' – wordt ontwikkeld. Voor het zo ver is, moet voor de praktijk echter volkomen helder zijn dat in het kader van proportionaliteits- en subsidiariteitstoets het in de rede ligt het takedown-bevel trapsgewijs in te zetten, waarbij eerst de notice and takedown-gedragscode wordt uitgevoerd.
Eerst moet daarbij de plaatser van het betwiste materiaal worden aangesproken het materiaal te verwijderen. Indien deze daar niet aan voldoet of niet aanspreekbaar is, kunnen de autoriteiten naar de websitehouder stappen. Als de websitehouder tevens weigert mee te werken aan het verwijderen van het strafbare materiaal, kunnen de autoriteiten zich tot de hosting provider wenden. Een hosting provider kan, als dat mogelijk is, de website van een server ontoegankelijk maken.

35 Zie de Gedragscode Notice-and-Take-Down, oktober 2008, www.rijksoverheid.nl/documenten/rapporten/2008/10/09/gedragscode-notice-and-take-down (laatst geraadpleegd 15 augustus 2017). Zie voor een uitgebreide analyse van de gedragscode in verhouding met de oude regeling M.H.M. Schellekens, B.J. Koops & W.G. Teepe, *Wat niet weg is, is gezien. Een analyse van art. 54a Sr in het licht van een Notice-and-Take-Down-regime*, Tilburg: TILT 2007.

36 Zie ook *Kamerstukken II* 2015/16, 34372, 3, p. 57. De bestaande grondslag in art. 54a Sr is niet deugdelijk vanwege van de formulering van het artikel en de vreemde plek in het Wetboek van Strafrecht in plaats van het Wetboek van Strafvordering. Verschillende rechters hebben een takedown-bevel op basis van art. 54a Sr dan ook niet geldig verklaard.

37 Zie ook J.J. Oerlemans, 'Het conceptwetsvoorstel versterking bestrijding computercriminaliteit nader bezien', *Tijdschrift voor Internetrecht* 2010, p. 148-152 en C. Kuş & J.M. ten Voorde, 'Het bevel Notice and Take Down in het wetsvoorstel Computercriminaliteit III en de vrijheid van meningsuiting op het internet', *Strafblad* 2014, p. 141-149.

38 *Kamerstukken II* 2015/16, 34372, 3, p. 57.

39 Zie ook *Kamerstukken II* 2016/17, 34372, 6, p. 109.

40 *Kamerstukken II* 2015/16, 34372, 3, p. 59. Tegen de beschikking op het beklag staat voor zowel de klager als de officier van justitie beroep in cassatie open.

41 Zie *Kamerstukken II* 2015/16, 34372, 3, p. 96.

42 Zie bijv. EHRM 1 december 2015, nrs. 48226/10 en 14027/11 (*Cengiz e.a./Turkije*).

Het volledig offline halen van een server ligt minder voor de hand, omdat honderden websites tegelijk zich op één server kunnen bevinden en de toegankelijkheidsmaking daardoor mogelijk niet meer proportioneel is. Als laatste stap kan een filterverplichting bij een internet access provider worden opgelegd. Dit is wellicht het beste voor te stellen als het bevel van de civiele rechter (in eerste instantie) aan de providers Ziggo en XS4ALL om de domeinnamen en IP-adressen van The Pirate Bay te blokkeren in 2012.[43] Door de filter is voor abonnees van deze providers de website niet meer via hun normale internetverbinding bereikbaar.[44]

3.1.2 Naar een internetfilter en zwarte lijsten?

Mijns inziens zet de mogelijkheid van een ontoegankelijkheidsmaking op het niveau van een IP-adres bij een internet access provider de deur open voor internetblokkades. In het nader verslag wordt al aangegeven dat het bevel ook kan worden ingezet om jihadistische propaganda tegen te gaan.[45] De vraag dringt zich op of dit uiteindelijk leidt tot een Nederlandse zwarte lijst van strafbare websites en online forums. De blokkering van websites wordt problematisch(er) als via – op zichzelf legale – websites een zeer kleine hoeveelheid illegaal materiaal wordt verspreid en de gehele website offline wordt gehaald en wanneer het onduidelijk is of de beschikbaarstelling van het materiaal daadwerkelijk strafbaar is.[46] Met de vereiste machtiging van een rechter-commissaris in de laatste versie van het wetsvoorstel kan in ieder geval een zorgvuldiger afweging worden gemaakt. Ook wordt met de beperking tot de meer ernstige misdrijven voorkomen dat voor lichte overtredingen de verstrekkende maatregel kan worden opgelegd.

3.1.3 Toezicht achteraf

Zoals in paragraaf 3.1 is aangegeven, hebben de betrokkenen die met een takedown-bevel te maken krijgen de mogelijkheid beklag te doen en de strafbaarheid van het materiaal te betwisten. Het is echter kostbaar met een gedegen vertegenwoordiging een klachtschrift in te dienen en verdediging te voeren. Mijn verwachting is dat veel betrokken bedrijven al snel tot de conclusie komen dat medewerking aan een takedown-bevel vanuit economisch perspectief het meest aantrekkelijk is. De bedoeling is dat het takedown-bevel vooral als *voorlopige maatregel* werkt en de zittingsrechter het laatste woord heeft.[47] Als het materiaal offline wordt gehaald, is het echter de vraag of vervolging voor een strafbaar feit nog wordt doorgezet. Als de verdachten zich in het buitenland bevinden, is dat nog minder waarschijnlijk.

De mijns inziens geringe kans dat gebruik wordt gemaakt van de klachtregeling of toets bij de zittingsrechter sterkt mij in de overtuiging dat meer *toezicht achteraf* noodzakelijk is. Met de Wet computercriminaliteit III wordt voor toezicht op de hackbevoegdheid een taak gecreëerd voor de Inspectie Veiligheid en Justitie.[48] Dit toezicht is echter niet gericht op de rechtmatigheid het takedown-bevel, terwijl deze bevoegdheid mogelijk wel grote gevolgen heeft. Toezicht door een onafhankelijke commissie op de rechtmatigheid van de inzet van de bevoegdheid heeft daarom mijn voorkeur.

De belangrijkste wijzigingen voor het formele strafrecht die de Wet computercriminaliteit III met zich brengt, betreffen het takedown-bevel en de hackbevoegdheid.

3.2 De hackbevoegdheid

De hackbevoegdheid wordt in de Wet computercriminaliteit III voorgesteld in artikel 126nba Sv. De bevoegdheid wordt geregeld als een bijzondere opsporingsbevoegdheid die heimelijk kan worden toegepast. Zoals ik eerder heb uiteengezet kan de hackbevoegdheid worden omschreven als een 'paraplubevoegdheid'.[49] Na het op afstand binnendringen in een geautomatiseerd netwerk kunnen andere opsporingsmethoden worden ingezet, zoals het vastleggen van gegevens, het uitvoeren van (stelselmatige) observatie, het direct afluisteren

43 Zie Rb. 's-Gravenhage 11 januari 2012, ECLI:NL:RBSGR:2012:BV0549. In hoger beroep oordeelde het Hof Den Haag (28 januari 2014, ECLI:NL:GHDHA:2014:88) dat de internetblokkade geen stand mocht houden, omdat het eenvoudig te omzeilen was en daarmee niet effectief zou zijn. De Hoge Raad stelde prejudiciële vragen over de vermeende auteursrechtschending van The Pirate Bay (HR 13 november 2015, ECLI:NL:HR:2015:3307). Het Hof van Justitie maakte zeer recentelijk duidelijk dat de The Pirate Bay met haar handelen inbreuk maakt op het auteursrecht van de rechthebbenden (HvJ EU 14 juni 2017, zaak C-610/15, ECLI:EU:C:2017:456 (*Stichting Brein/Ziggo BV & XS4ALL Internet BV*)).

44 Internetgebruikers kunnen echter ook eenvoudig omzeilingsmaatregelen nemen, zoals het gebruik van een *'virtual private network'* (VPN)-verbinding.

45 *Kamerstukken II* 2016/17, 34372, 6, p. 8.

46 Zie ook Schellekens, Koops & Teepe, *a.w.*, p. 13-14. Op p. 22 van de MvT op het Wetsvoorstel versterking bestrijding computercriminaliteit uit 2010, wordt terecht opgemerkt dat het niet altijd duidelijk is of het aangeboden materiaal via internet strafbaar is.

47 *Kamerstukken II* 2015/16, 34372, 3, p. 59.

48 Zie verder par. 3.2.4.

49 Zie J.J. Oerlemans, 'Hacken als opsporingsbevoegdheid', *DD* 2011/62, p. 888-908.

en het ontoegankelijk maken van gegevens.[50] De software die daarvoor kan worden gebruikt, biedt een breed scala aan functionaliteiten, zoals het vastleggen van toetsaanslagen, het maken van screenshots, het aanzetten van een microfoon of camera of het aanzetten van de GPS-functionaliteit.[51] In het geval de software wordt ingezet om in de bestanden in de computers van een verdachte te kijken en heimelijk beeld- en geluidsopnamen te maken, kan de bijzondere opsporingsbevoegdheid worden omschreven als een combinatie van een inkijkoperatie, een heimelijke doorzoeking en afluisteren in één. Vanwege de ernstige privacyinmenging die de bijzondere bevoegdheid met zich brengt, zijn strikte waarborgen noodzakelijk.

Deze strikte waarborgen zijn ook aanwezig in het voorgestelde artikel 126nba Sv. De hackbevoegdheid mag alleen worden ingezet in opsporingsonderzoeken naar strafbare feiten zoals bedoeld in artikel 67 Sv die de rechtsorde ernstig schaden en in het geval het opsporingsonderzoek dat dringend vordert.[52] Een officier van justitie mag het bevel afgeven voor de inzet van de bevoegdheid, nadat een machtiging van de rechter-commissaris is verkregen. Bovendien moet de Centrale Toetsingscommissie van het Openbaar Ministerie worden geraadpleegd over de inzet van de bevoegdheid.

3.2.1 Noodzaak van de hackbevoegdheid

De noodzaak van de bevoegdheid wordt mijns inziens voldoende duidelijk uitgelegd in de memorie van toelichting en het nader verslag van de behandeling van het wetsvoorstel.[53] In essentie wordt daar beschreven hoe cybercrimeonderzoeken de politie tot drie uitdagingen stelt. Ten eerste kan de identificatie en lokalisering van verdachten bijzonder lastig zijn, omdat verdachten gebruikmaken van verschillende wifi-netwerken en anonimiseringstechnieken.[54] In bepaalde omstandigheden wordt het daarmee onmogelijk voor de politie met de huidige bijzondere bevoegdheden bewijs te verzamelen en daarmee als het ware de verdachte achter het toetsenbord te plaatsen ten tijde van het misdrijf. Ten tweede is het duidelijk dat de toename in standaardversleuteling bestaande opsporingsmethoden minder effectief maakt. Deze versleuteling ziet zowel op de versleuteling van gegevens in opslag (bijvoorbeeld de versleuteling van harde schijven en computers zoals iPhones) als van gegevens in transport (zoals de versleuteling van netwerkverkeer van communicatie-apps of het netwerkverkeer naar websites).[55] Vooral de bevoegdheden van de telecommunicatietap en de inbeslagname en het doorzoeken van gegevensdragers worden minder effectief door versleuteling. Ten derde is jurisdictie een enorme uitdaging, omdat verdachten overal ter wereld via internet misdrijven in Nederland kunnen plegen en bewijs op computers verspreid over de hele wereld ligt opgeslagen. In de memorie van toelichting wordt in het bijzonder gewezen op het feit dat steeds meer mensen gebruikmaken van elektronische communicatiediensten die werken met *cloud computing*,[56] zoals de populaire webmaildiensten Outlook-mail en Gmail en online opslagdiensten als MegaUpload en Google Drive. Het is daarbij niet altijd duidelijk op welke computers de gegevens liggen opgeslagen. Vanuit een traditioneel jurisdictieconcept is dat een probleem, omdat niet meer helder is welke staat jurisdictie heeft over de gegevens en welk recht van toepassing is.[57] Ook zijn verdachten niet altijd redelijkerwijs te lokaliseren, omdat zij bijvoorbeeld steevast gebruikmaken van anonimiseringstechnieken en uitsluitend onder een schuilnaam op internet actief zijn. De verdachte kan zich potentieel overal ter wereld bevinden, zonder dat opsporingsautoriteiten de instrumenten hebben de verdachte te identificeren en te lokaliseren.

De hackbevoegdheid biedt op verschillende manieren een oplossing voor het anonimiteitsprobleem en versleutelpro-

50 Op deze wijze is art. 126nba lid 1 Sv ook opgebouwd. In het wetsartikel wordt zo veel mogelijk aangesloten bij bestaande opsporingsbevoegdheden.

51 *Kamerstukken II* 2015/16, 34372, 3, p. 19-25.

52 Bij het ontoegankelijk maken van gegevens op afstand en het aanzetten van een GPS-signaal op afstand mag de bevoegdheid alleen worden toegepast bij opsporingsonderzoeken naar misdrijven met een maximale gevangenisstraf van minimaal acht jaar of meer, dan wel voor misdrijven die bij algemene maatregel van bestuur zijn aangewezen. Deze misdrijven betreffen in ieder geval het gebruik van een botnet (strafbaar gesteld als een gekwalificeerde vorm van computervredebreuk), grooming en kinderpornografie (*Kamerstukken II* 2016/17, 34372, 6, p. 36).

53 Zie *Kamerstukken II* 2015/16, 34372, 3, p. 7-12 en *Kamerstukken II* 2016/17, 34372, 6, p. 14-22. Deze omschrijving sluit goed aan bij de resultaten van mijn eigen dissertatieonderzoek naar het opsporingsproces en de normering van opsporingsmethoden die worden gebruikt in cybercrimezaken. Zie Oerlemans, *a.w.* (2017).

54 In het kader van mijn dissertatieonderzoek heb ik het gebruik van *'virtual private networks'* en *'Tor'* geanalyseerd en ben ik nagegaan hoe deze anonimiseringstechnieken het opsporingsonderzoek naar cybercrime frustreren. Zie Oerlemans, *a.w.* (2017), p. 38-42. De beperkte omvang van dit artikel laat een bespreking van deze technieken niet toe.

55 Zie *Kamerstukken II* 2015/16, 34372, 3, p. 7-8. Zie ook uitgebreid Oerlemans, *a.w.* (2017), p. 45-52.

56 'Cloud computing' is een verzamelterm voor een techniek waarbij elektronische communicatieaanbieders via internet gegevensverwerkingsdiensten aanbieden in de vorm van opslag- en rekencapaciteit (definitie ontleend aan B.J. Koops et al., 'Misdaad en opsporing in de wolken. Knelpunten en kansen van cloud computing voor de Nederlandse opsporing', Den Haag/Tilburg: WODC/TILT 2012, p. 10).

57 Zie ook *Kamerstukken II* 2015/16, 34372, 3, p. 9 en *Kamerstukken II* 2016/17, 34372, 6, p. 15-16.

bleem in cybercrimezaken. In de memorie van toelichting van het wetsvoorstel worden enkele voorbeelden genoemd. Met gebruik van politiesoftware na inzet van de hackbevoegdheid kan de politie mogelijkerwijs het IP-adres en andere gegevens van een computer en een computergebruiker vastleggen, hetgeen kan bijdragen aan de identificatie en lokalisering van de verdachte.[58] Met de mogelijkheid op afstand software te plaatsen op een computer, kan de politie op afstand 'op de bron' aftappen door het gesprek via een microfoon of camerabeelden op te nemen en door te sturen naar een politieserver.[59] Ook kan versleuteling worden omzeild door op afstand bewijsmateriaal op een computer te identificeren en vast te leggen. Met de zogenoemde *keylog*-functionaliteit van deze politiesoftware kunnen bovendien inlognamen en wachtwoorden van computergebruikers worden vastgelegd, zodat deze later kunnen worden gebruikt voor toegang tot beveiligde gegevens.[60] De recente uitspraak in de *Aydin C.*-zaak, licht een tipje van de sluier op van de huidige toepassing van politiesoftware in Nederland.[61]

3.2.2 Over de grens?

Met het jurisdictieprobleem wordt op een bijzondere manier omgegaan door een vergaand standpunt in te nemen over het beginsel van de territoriale beperking van handhavingsjurisdictie. In principe mogen opsporingsmethoden niet over de territoriale grens worden toegepast, tenzij de betrokken staat hiervoor toestemming geeft of een verdragsbasis bestaat voor de extraterritoriale bewijsgaringsactiviteiten. Rechtshulpverdragen regelen onder welke voorwaarden (de meestal lokale) opsporingsautoriteiten op verzoek het bewijs verzamelen.

In de Wet computercriminaliteit III wordt voorgesteld dat de hackbevoegdheid ook over de territoriale grenzen mag worden ingezet, indien de verdachte of het bewijs redelijkerwijs niet is te lokaliseren. Daarbij moet worden gedacht aan het eerder aangehaalde voorbeeld van het gebruik van cloud computing of anonimiseringstechnieken. De opstellers van het wetsvoorstel willen voorkomen dat het internet een 'vrijplaats' voor criminaliteit vormt en de opsporingsautoriteiten met lege handen komen te staan.[62] Nadat de verdachte is gelokaliseerd of is gebleken dat bewijsverzamelingsactiviteiten op buitenlands grondgebied hebben plaatsgevonden, is het de bedoeling dat de betrokken staat hierover wordt genotificeerd. Als van tevoren duidelijk is dat de bevoegdheid over de territoriale grenzen mogelijk wordt ingezet, moet de officier van justitie dit in zijn bevel en de overwegingen daaromtrent meenemen, zodat een rechter-commissaris hier ook aan kan toetsen. Daarbij moet rekening worden gehouden met andere belangen, zoals de vereiste inspanning om de identiteit en locatie van een geautomatiseerd werk te achterhalen, de ernst van het strafbare feit, de mate van betrokkenheid van Nederlands slachtoffers en Nederlandse infrastructuur, de aard van de opsporingshandelingen en de risico's voor het geautomatiseerde werk.[63]

In de Verenigde Staten is in 2016 een gelijksoortige wijziging in de federale wetgeving aangebracht met betrekking tot de zogenaamde *Rule 41-warrant.*[64] Kort gezegd houdt deze wijziging in dat als de verdachte gebruikmaakt van een anonimiseringsdienst of botnet, een Amerikaanse rechter toestemming kan geven tot de doorzoeking via internet in de computers waarvan de verdachte gebruikmaakt; ook als deze computers zich buiten de regio van de rechter bevinden.[65] Andere staten zijn nog zeer terughoudend in het publiceren van formele wetgeving waarbij informatie wordt gegeven onder welke omstandigheden een 'extraterritoriale doorzoeking' mogelijk is.

In principe mogen opsporingsmethoden niet over de territoriale grens worden toegepast, tenzij de betrokken staat hiervoor toestemming geeft of een verdragsbasis bestaat voor de extraterritoriale bewijsgaringsactiviteiten.

58 Zie *Kamerstukken II* 2015/16, 34372, 3, p. 20.
59 *Kamerstukken II* 2015/16, 34372, 3, p. 10.
60 Zie, in enigszins andere bewoordingen, *Kamerstukken II* 2015/16, 34372, 3, p. 21.
61 Rb. Amsterdam 16 maart 2017, ECLI:NL:RBAMS:2017:1627, *Computerrecht* 2017/103, m.nt. J.J. Oerlemans (*Aydin C.*). In deze zaak werd de software fysiek op de computer geïnstalleerd en werden vervolgens toetsaanslagen en schermafbeeldingen gemaakt ter vaststelling van de strafbare gedragingen van de verdachte.
62 *Kamerstukken II* 2015/16, 34372, 3, p. 46.
63 *Kamerstukken II* 2015/16, 34372, 3, p. 48.
64 Zie bijv. persbericht van het Amerikaanse ministerie van Justitie van 20 juni 2016, 'Rule 41 changes ensure a judge may consider warrant for certain remote searches', www.justice.gov/archives/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches (laatst geraadpleegd 30 augustus 2017). De Amerikaanse senaat heeft het amendement niet tegengehouden; het Amerikaanse Hooggerechtshof heeft het inmiddels goedgekeurd.
65 De relevante tekst van het amendement luidt als volgt: *'a magistrate judge with authority in any district where activities related to a crime may have occurred, has the authority to issue a warrant to use remote access to search electronic storage and to seize or copy electronically stored information located within* ***or outside*** *that district'.*

Voor de mogelijkheid tot extraterritoriale bewijsgaring door een vorm van 'toegang op afstand' kan sympathie worden opgebracht. In sommige gevallen is de verdachte of het bewijs inderdaad niet meer te lokaliseren en bieden de huidige rechtshulpverdragen simpelweg te weinig mogelijkheden om effectief bewijs te verzamelen.[66] Uit verschillende hoeken wordt echter ook gewaarschuwd dat dit bijzondere standpunt van Nederland grote risico's met zich brengt. Andere staten kunnen zich bijvoorbeeld ook meer gerechtigd voelen

De hackbevoegdheid kan worden ingezet voor het binnendringen in álle geautomatiseerde werken.

onder omstandigheden unilaterale bewijsgaringsactiviteiten in Nederland te ondernemen, waarbij mogelijk Nederlandse ingezetenen of Nederlandse infrastructuur zijn betrokken. Het zelfstandig optreden door opsporingsinstanties van een andere staat kan leiden tot diplomatieke spanningen. Bovendien bedreigt een extraterritoriale bewijsgaring de rechtszekerheid van de betrokkenen, omdat buitenlandse opsporingsautoriteiten onder hun eigen lokale wetgeving een inbreuk maken op hun rechten en vrijheden.[67]

3.2.3 *Kritiek op de hackbevoegdheid*

De kritiek op de hackbevoegdheid en het parlementaire debat over het wetsvoorstel gingen vooral over de reikwijdte van de hackbevoegdheid en het gebruik van kwetsbaarheden. De hackbevoegdheid beperkt zich niet tot laptops, pc's en smartphones van verdachten in cybercrimezaken. De hackbevoegdheid kan worden ingezet voor het binnendringen in álle geautomatiseerde werken, waaronder objecten die vallen onder het *'internet of things'*, zoals slimme meters, lampen, pacemakers en slimme auto's. Terecht merkt staatssecretaris Dijkhoff in de nota naar aanleiding van het verslag op dat het niet voor de hand ligt dat de opsporingsautoriteiten een pacemaker of auto's willen hacken binnen een opsporingsonderzoek. Het hacken van deze apparaten brengt namelijk dusdanig grote risico's mee met betrekking tot de veiligheid van personen dat deze toepassing de proportionaliteitstoets niet zal doorstaan.[68]

Daarnaast werd beargumenteerd, onder andere door de digitale burgerrechtenorganisatie Bits of Freedom en in navolging van enkele parlementariërs, dat het hacken van apparaten met het gebruik van onbekende kwetsbaarheden (zogenaamde *zero days*) meer onveiligheid dan veiligheid biedt voor de maatschappij. De redenering is dat opsporingsautoriteiten een belang hebben bij het in stand houden van onbekende kwetsbaarheden in apparaten, waardoor apparaten onveilig blijven. Aangezien deze kwetsbaarheden niet bekend zijn bij de fabrikant van hardware of software, kan het beveiligingsprobleem niet worden opgelost. Deze onbekende kwetsbaarheden kunnen dus worden misbruikt door kwaadwillenden, totdat het beveiligingsprobleem wordt verholpen.[69] Uiteindelijk heeft deze discussie geleid tot het aangenomen amendement-Recourt/Telligen, waarbij een verplichting wordt geïntroduceerd onbekende kwetsbaarheden te melden die bij de politie bekend zijn geworden bij toepassing van de hackbevoegdheid.[70] Slechts bij een zwaarwegend opsporingsbelang kan, na accordering van het centraal aanspreekpunt bij het Landelijk Parket, worden besloten een rechter-commissaris toestemming te vragen de melding van de onbekende kwetsbaarheid uit te stellen.[71]

3.2.4 *Toezicht op de verstoringsmogelijkheid*

De toepassing van de hackbevoegdheid waarbij 'op afstand gegevens ontoegankelijk worden gemaakt' verdient mijns inziens speciale aandacht. In de memorie van toelichting wordt namelijk expliciet opgemerkt dat deze toepassing van de hackbevoegdheid ook mag worden ingezet voor 'verstoringsdoeleinden'.[72] Daarbij moet worden gedacht aan het onklaar maken van *'botnets'*, een netwerk van geïnfecteerde computers die op afstand door een derde worden aangestuurd. Ook wordt het voorbeeld genoemd van het ontoe-

66 Zie ook United Nations Office on Drugs and Crime, *Comprehensive study on cybercrime*, 2013, p. 214; B.J. Koops & M.E.A. Goodwin, 'Cyberspace, the cloud and cross-border criminal investigation. The limits and possibilities of international law', Den Haag/Tilburg: WODC/TILT 2014, p. 41.

67 Zie uitgebreid Oerlemans, *a.w.* (2017), p. 295-296 en 329-333.

68 Zie *Kamerstukken II* 2016/17, 34372, 6, p. 32 en 53.

69 Overigens wijzen andere cybersecuritydeskundigen erop dat in de meeste gevallen geen gebruik hoeft te worden gemaakt van onbekende kwetsbaarheden voor het hacken van apparaten. Daarnaast zijn onbekende kwetsbaarheden zeer kostbaar en slechts kort bruikbaar (totdat de kwetsbaarheid wordt ontdekt). Zie bijv. de bijdrage van de heer Prins aan de hoorzitting in de Tweede Kamer over de Wet computercriminaliteit III.

70 *Kamerstukken II* 2016/17, 30372, 14.

71 Zie art. 126ffa Sv. Zie ook *Kamerstukken I* 2016/17, 34372, D, p. 20-21. De staatssecretaris geeft aan dat de politie geen onbekende kwetsbaarheden zal inkopen, maar hij sluit niet uit dat van onbekende kwetsbaarheden gebruik wordt gemaakt door de software die de politie aanschaft om de hackbevoegdheid uit te voeren. In een tamelijk unieke brief van 23 november 2016 (*Kamerstukken II* 2016/17, 26643, 428) zetten de Staatssecretaris van Veiligheid en Justitie en de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie hun gezamenlijke standpunt uiteen over het omgaan met kwetsbaarheden. Binnen het beleid moet een expliciete afweging worden gemaakt omtrent het melden van onbekende kwetsbaarheden.

72 *Kamerstukken II* 2015/16, 34372, 3, p. 29.

gankelijk maken van kinderpornografie op het *'dark web'*, dat wil zeggen dat deel van het internet dat slechts toegankelijk is met anonimiseringssoftware en waarbij de IP-adressen van servers verborgen zijn. Mijn zorg bij toepassing van de verstoringsbevoegdheid, die tevens mogelijk extraterritoriale effecten met zich brengt, is het gebrek aan controle *achteraf*. Vooraf gelden strenge waarborgen, zoals de machtiging van een rechter-commissaris, het inwinnen van advies bij de Centrale Toetsingscommissie en de beperking tot zeer ernstige misdrijven. Maar achteraf zal een rechtmatigheidstoets vaak achterwege blijven.

Veel cybercrime wordt namelijk niet vervolgd, omdat het (digitale) spoor in het buitenland doodloopt of de verdachte in een staat woont die geen eigen onderdanen uitlevert. Het is zeer de vraag of de rechtmatigheid van een dergelijke verstoringsactie, die in het verleden al verschillende keren (al dan niet onder coördinatie van Europol) is uitgevoerd, tijdens een zitting door een rechter wordt getoetst.[73] Ook acht ik de kans gering dat de betrokkenen gebruikmaken van de klachtprocedure. Dit bezwaar is ook kort tijdens de parlementaire behandeling van het wetsvoorstel ter sprake gekomen.[74] Staatssecretaris Dijkhoff legt daarop uit dat de Inspectie Veiligheid en Justitie achteraf toezicht houdt op de inzet van de hackbevoegdheid.[75] Het toezicht ziet echter in de eerste plaats op het nakomen van de voorgeschreven procedures en niet op de rechtmatigheid van de toepassing van de bevoegdheid. Het gebrek op een rechtmatigheidstoets achteraf vind ik zorgelijk, omdat het onduidelijk is op welke schaal de Nederlandse opsporingsautoriteiten de bevoegdheid gaan toepassen en hoe ver zij hier precies in gaan. Een dergelijk verstrekkende toepassing van overheidsmacht moet afdoende worden gecontroleerd, óók in het digitale domein.

4. Conclusie

In dit artikel is een overzicht gegeven van de belangrijkste wijzigingen die het Wetsvoorstel computercriminaliteit III met zich brengt. De wetgever gaat in op zorgen die in de samenleving bestaan door vormen van cybercrime eerder strafbaar te stellen, zoals Marktplaatsoplichting en webcamseks met minderjarigen. Daartoe worden nieuwe strafbaarstellingen geïntroduceerd en enkele bestaande artikelen gewijzigd. Met de strafbaarstelling van het openbaren van niet-openbare gegevens en heling van gegevens kunnen opsporingsautoriteiten straks eenvoudiger voor bepaalde vormen van cybercrime vervolgen. Het mogelijk maken van de lokpuber door wijzigingen van het delict grooming is bijzonder te noemen. Opsporingsautoriteiten zullen in hun opstelling tijdens de toepassing van de opsporingsmethode zeer terughoudend moeten blijven om niet tot uitlokking over te gaan. Met de regeling van het takedown-bevel en de nieuwe vergaande hackbevoegdheid in het Wetboek van Strafvordering krijgen opsporingsautoriteiten in de ogen van het demissionaire kabinet de noodzakelijke instrumenten om cybercrime aan te pakken. De mogelijkheid de hackbevoegdheid unilateraal over de landsgrenzen toe te passen, is in internationaalrechtelijke zin zeer vooruitstrevend te noemen. Alles overziende leiden deze maatregelen tot meer handhaving op internet.

Het gebrek op een rechtmatigheidstoets achteraf vind ik zorgelijk, omdat het onduidelijk is op welke schaal de Nederlandse opsporingsautoriteiten de bevoegdheid gaan toepassen en hoe ver zij hier precies in gaan.

Het is lastig in te schatten op welke schaal de 'verstoringstoepassing' van de hackbevoegdheid wordt ingezet en informatie op internet via het takedown-bevel ontoegankelijk wordt gemaakt. Het is daarmee ook onzeker welke gevolgen het wetsvoorstel voor onze samenleving heeft. In het uiterste geval zijn er in Nederland over vijf jaar talrijke internetfilterverplichtingen van kracht met een internationaal opererende internetpolitie die kinderporno en botnets offline haalt, maar waarvan de activiteiten nauwelijks door een instantie achteraf op rechtmatigheid worden gecontroleerd. Strafrechtjuristen dragen daarom een belangrijke verantwoordelijkheid scherp te zijn op de praktijk die volgt op de wijzigingen naar aanleiding van het wetsvoorstel.

73 Zie bijv. de volgende persberichten (waarbij geen gearresteerde verdachten worden genoemd) 'Notorious botnets infecting 2 million computers disrupted', 5 december 2013, www.europol.europa.eu/content/notorious-botnet-infecting-2-million-computers-disrupted en 'Botnet taken down through international law enforcement cooperation', 25 februari 2015, www.europol.europa.eu/content/botnet-taken-down-through-international-law-enforcement-cooperation (laatst geraadpleegd 15 augustus 2017).

74 Zie ook de bijdrage van de heer Baardman, senior raadsheer van het Hof Den Haag en Coördinator van het Kenniscentrum Cybercrime van 10 februari 2016 aan een debat over de Wet computercriminaliteit in de Tweede Kamer en verschillende bijdragen voor de deskundigenbijeenkomst van het wetsvoorstel in de Eerste Kamer.

75 *Kamerstukken II* 2016/17, 34372, 6, p. 82-83.