eLaw
Working Paper Series

No 2018/004 - ELAW– 24 April 2019

Nieuwe online opsporingsbevoegdheden en het recht op privacy

Een analyse van de Wet computercriminaliteit III

Bart Custers

Universiteit Leiden
eLaw

Nieuwe online opsporingsbevoegdheden en het recht op privacy

Een analyse van de Wet computercriminaliteit III

Bart Custers*

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

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

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

doi: 10.5553/JV/016758502018044005008

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

Achtergrond van de Wetten computercriminaliteit

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

Wet computercriminaliteit I (1993)

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

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

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

doi: 10.5553/JV/016758502018044005008

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

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

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

doi: 10.5553/JV/016758502018044005008

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

Wet computercriminaliteit II (2006)

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

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

doi: 10.5553/JV/016758502018044005008

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

Wet computercriminaliteit III (2018)

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

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

doi: 10.5553/JV/016758502018044005008

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

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

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

15 MvT, p. 7-15.

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

doi: 10.5553/JV/016758502018044005008

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

Inhoud van de Wet computercriminaliteit III

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

doi: 10.5553/JV/016758502018044005008

Strafrechtelijke onderdelen

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

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

doi: 10.5553/JV/016758502018044005008

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

Strafprocesrechtelijke onderdelen

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

doi: 10.5553/JV/016758502018044005008

kracht en wordt als eerste, vrijwillige stap gebruikt. Pas als aanbieders niet meewerken of niet zijn aangesloten bij deze gedragscode, wordt de tweede, verplichtende stap ingezet.

Hoe bepaald materiaal ontoegankelijk moet worden gemaakt, laat de nieuwe wet in het midden. Volgens de memorie van toelichting kan dit via hardware (ontoegankelijk maken van ingangen van computers, afsluiten van servers) of via software (internetfilters, gegevens versleutelen/wissen) en moet per geval worden bekeken welke maatregel het meest effectief is, rekening houdend met proportionaliteit en subsidiariteit.

Met behulp van het NTD-bevel kunnen *botnets* beter worden bestreden. Dit zijn netwerken van computers die zijn besmet met malware (kwaadaardige software) waarvan cybercriminelen op afstand misbruik kunnen maken. Voorbeelden zijn onder meer het gebruik van botnets voor bitcoin mining, het versturen van grote hoeveelheden spam, het verzamelen van bedrijfsgeheimen en andere vertrouwelijke informatie, het uitvoeren van DDoS-aanvallen[18] en het verspreiden van banking malware en ransomware.

De hackbevoegdheid, opgenomen in een nieuw artikel 126nba Sv, houdt in dat opsporingsambtenaren onder bepaalde omstandigheden mogen binnendringen in computers en netwerken, al dan niet met een technisch hulpmiddel. Na inzet van deze bevoegdheid kunnen vervolgens andere opsporingsbevoegdheden worden ingezet, zoals het vastleggen van gegevens, het uitvoeren van (stelselmatige) observatie, het direct afluisteren en het ontoegankelijk maken van gegevens (Oerlemans 2017b).

Het gebruik van technische hulpmiddelen betreft doorgaans software die wordt beschreven als *spyware* (in deze context ook wel *policeware* genoemd) en heeft functionaliteiten zoals het op afstand aanzetten van camera's, microfoons en GPS, het vastleggen van toetsaanslagen (zogeheten *keyloggers*), het maken van *screenshots* en het doorzoeken van bestanden op de betreffende computers.

Het mag duidelijk zijn dat de inzet van de hackbevoegdheid een ernstige inbreuk op het recht op privacy met zich meebrengt (zie hieronder). Om die reden is de inzet van de hackbevoegdheid afgebakend en zijn extra waarborgen aangebracht. Zo is de inzet van de hackbe-

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

doi: 10.5553/JV/016758502018044005008

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

Legitimiteit en noodzakelijkheid

De Wet computercriminaliteit III biedt opsporingsdiensten vergaande bevoegdheden voor hacken en de inzet van spyware. De inzet van zulke bevoegdheden brengt inbreuken op het recht op privacy met zich mee. Volgens de Hoge Raad speelt bij het beoordelen van inbreuken op het recht op privacy artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) een fundamentele rol.[19] Het recht op privacy is niet absoluut: inbreuken kunnen gerechtvaardigd zijn, mits die inbreuken bij wet zijn voorzien, voor legitieme doeleinden zijn (legitimiteit) en noodzakelijk in een democratische samenleving (noodzakelijkheid). Hier wordt ingegaan op de criteria van legitimiteit en noodzakelijkheid van de hackbevoegdheid in relatie tot het recht op privacy. Voor een meer gedetailleerde analyse, zie Pool en Custers (2017).
Het legitimiteitscriterium vereist dat voor het gebruik van opsporingsbevoegdheden een duidelijke wettelijke basis aanwezig is. Het is om deze reden dat de Nederlandse overheid de hackbevoegdheid in de wet wil vastleggen. Hoewel deze bevoegdheid al in zekere mate bestond (Oerlemans 2017b), wordt met de nieuwe wet voorzien in een expliciete(re) wettelijke basis. Ook het beoogde doel van de Wet computercriminaliteit III is legitiem, namelijk het bestrijden van cybercrime, hetgeen in lijn is met de belangen van nationale veiligheid, openbare veiligheid en het voorkomen van strafbare feiten. Kortom, aan het legitimiteitscriterium wordt goed voldaan.
Het noodzakelijkheidscriterium ligt ingewikkelder. Hoe noodzakelijkheid moet worden afgewogen tegen privacyinbreuken is niet zonder

19 HR 9 januari 1987, NJ 1987/928.

doi: 10.5553/JV/016758502018044005008

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

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

doi: 10.5553/JV/016758502018044005008

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

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

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

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

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

doi: 10.5553/JV/016758502018044005008

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

Conclusie

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

doi: 10.5553/JV/016758502018044005008

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

doi: 10.5553/JV/016758502018044005008

Literatuur

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

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

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

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

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

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

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

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

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

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

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

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

doi: 10.5553/JV/016758502018044005008

Jacobs 2012
B.P.F. Jacobs, 'Policeware', *Nederlands Juristenblad* 2012, p. 2761-2764.

Kerr 2013
O. Kerr, 'Fascinating new case on legal standards for searching a remote computer with unknown location', 2013, http://volokh.com/2013/04/26/fascinating-new-case-on-legal-standards-for-searching-a-remote-computer-with-unknown-location/.

Kwakman & Buwalda 2014
N.J.M. Kwakman & M.E. Buwalda, 'Het ontwerp wetsvoorstel Computercriminaliteit III', *Ars Aequi* 2014, p. 9-18.

Lindenberg & Van Dijk 2016
K. Lindenberg & A.A. van Dijk, *Herziening van de zedendelicten?* Den Haag: WODC 2016.

Moitra 2003
S.D. Moitra, 'Developing policies for cybercrime', *European Journal of Crime, Criminal Law and Criminal Justice* (13) 2003, p. 435-464.

Muijen 2016
P.J.D.J. Muijen, 'Wet computercriminaliteit III. To boldly go where no man has gone before', *Privacy & Informatie* 2016, p. 104-110.

Odinot e.a. 2012
G. Odinot, D. de Jong, J.B.J. van der Leij, C.J. de Poot e.a., *Het gebruik van de telefoon- en internettap in de opspring*, Den Haag: Boom Lemma 2012.

Oerlemans 2017a
J.J. Oerlemans, 'De Wet computercriminaliteit III: meer handhaving op internet', *Strafblad* 2017, p. 350-359.

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

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

Ölçer 2014
F.P. Ölçer, 'De lokmethode bij de opsporing van grooming', *Computerrecht* 2014/3.

Van de Pol 2006
W. van de Pol, *Onder de tap. Afluisteren in Nederland*, Amsterdam: Uitgeverij Balans 2006.

doi: 10.5553/JV/016758502018044005008

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

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

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

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

doi: 10.5553/JV/016758502018044005008