# 20 Strafrechtelijke aspecten van cybercriminaliteit en digitale opsporing

*Jan-Jaap Oerlemans en Dave van Toor*

## 1 Inleiding

Op ten minste twee manieren hebben technologische ontwikkelingen invloed op het nationale strafrecht en strafprocesrecht. Ten eerste bieden nieuwe technologische ontwikkelingen nieuwe mogelijkheden voor misdadigers om strafbare feiten te plegen. Ten tweede zorgen technologische ontwikkelingen voor zowel problemen als kansen voor opsporingsdiensten. Zo is het opsporen van bepaalde delicten lastiger geworden, doordat gegevens eenvoudig in het buitenland kunnen worden opgeslagen en de opsporende autoriteiten in beginsel geen jurisdictie hebben buiten hun territorium. Daar staat tegenover dat de autoriteiten hun eigen technische mogelijkheden en vaardigheden kunnen inzetten om bewijs te verzamelen, bijvoorbeeld door computers van verdachten te hacken.

In dit hoofdstuk staan deze ontwikkelingen centraal en wordt aandacht besteed aan cybercriminaliteit (materieel strafrecht) en digitale opsporing (strafprocesrecht). Wij bespreken de belangrijkste strafbaarstellingen en opsporingsbevoegdheden die worden gebruikt in opsporingsonderzoeken naar cybercriminaliteit. De lezer verkrijgt hierdoor brede en actuele kennis over het onderwerp.

Het eerste deel over het materiële strafrecht behandelt de strafbaarstellingen met betrekking tot 'cybercriminaliteit in enge zin'. Dat is criminaliteit waarbij computers en netwerken het doelwit zijn. De strafbaarstellingen voor computervredebreuk, kwaadaardige software en 'denial-of-service aanvallen' (dos-aanvallen) komen daarbij aan bod.

In het tweede deel staat het strafprocesrecht centraal en wordt de inzet van opsporingsbevoegdheden in cybercrimezaken besproken. In opsporingsonderzoeken naar cybercriminaliteit in enge zin zijn digitale sporen, zoals een IP-adres of nickname, vaak de enige sporen die beschikbaar zijn. Het opsporingsproces ziet er daardoor anders uit dan opsporingsonderzoeken naar traditionele criminaliteit met een fysieke plaatsdelict. In deze bespreking van het toepasselijke formele strafrecht wordt daarom de nadruk gelegd op de (bijzondere) opsporingsbevoegdhe-

den die gebruikt worden in opsporingsonderzoeken naar cybercriminaliteit in enge zin.

## 2 Het materiële strafrecht: Cybercriminaliteit in enge zin

De opkomst van computers en het internet hebben geleid tot nieuwe vormen van criminaliteit. Criminaliteit waarbij computers en netwerken het doelwit zijn, wordt 'cybercriminaliteit in enge zin' genoemd, en betreft strafbare feiten die voor de 'technologische revolutie' niet bestonden. Hierbij kan worden gedacht aan de strafbaarstellingen voor computervredebreuk, kwaadaardige software en *denial-of-service aanvallen* (dos-aanvallen). In deze paragraaf zetten wij kort de wetsgeschiedenis uiteen, als aanloop naar de bespreking van de belangrijkste strafbepalingen.[1]

### *2.1 Wetsgeschiedenis*

#### *2.1.1 Wet computercriminaliteit I*

Nederland was er tamelijk vroeg bij met onderzoek of de Nederlandse wetgeving moest worden aangepast ter bestrijding van computercriminaliteit. Op 13 november 1985 werd door de minister van Justitie de 'Commissie computercriminaliteit' (commissie-Franken) ingesteld. In april 1987 verscheen haar rapport 'Informatietechniek en Strafrecht'.[2] De Wet computercriminaliteit I, die in 1993 in werking trad, verwerkt een groot deel van de aanbevelingen uit het rapport.[3] Wetswijzigingen werden door de commissie-Franken en de wetgever noodzakelijk geacht, vanwege de beoogde strafrechtelijke bescherming van ICT met betrekking tot de beschikbaarheid van middelen, integriteit van systemen en daarin vervatte gegevens, en exclusiviteit van middelen en gegevens.[4] De strafbare gedragingen zelf waarvoor vervolging kan worden ingezet lieten overigens nog enkele jaren op zich wachten.[5]

De beschikbaarheid van middelen heeft betrekking op de opslag, verwerking en overdracht van gegevens en op die gegevens zelf (waaronder programmatuur). De afhankelijkheid van die middelen is in onze samenleving zo groot geworden dat het belang om die middelen en gegevens te gebruiken evenredig groot is. Met de integriteit van systemen en daarin vervatte gegevens wordt bedoeld dat de gegevens en programma's correct en volledig moeten zijn. Stel dat kwaadaardige software wordt geïnstalleerd op een computer, dan wordt de integriteit van een systeem aangetast. Als verkeerde gegevens worden ingevoerd, gegevens worden

1. Zie uitgebreid: Koops & Oerlemans 2019a, p. 29-116. Par. 2 is deels op dit hoofdstuk gebaseerd.
2. Rapport commissie-Franken 1987.
3. Wet van 23 december 1992 tot wijziging van het Wetboek van Strafrecht en van het Wetboek van Strafvordering in verband met devoortschrijdende toepassing vaninformatietechniek (Wet computercriminaliteit), *Stb.* 1993, 33.
4. Rapport commissie-Franken 1987, p. 21-24.
5. Zie ook Kaspersen 1993, p. 134.

gemanipuleerd of ondeugdelijke apparatuur wordt gebruikt, dan kan dat verstrekkende gevolgen hebben. Het belang van exclusiviteit van gegevens en middelen ten slotte heeft ermee te maken dat men niet wenst dat onbevoegden kennisnemen van als geheim of vertrouwelijk gekenmerkte gegevens of gebruikmaken van de apparatuur waarmee deze gegevens zijn opgeslagen.[6]

Om recht te doen aan de bescherming van de integriteit, vertrouwelijkheid en exclusiviteit van gegevens op computers zelf is met de Wet computercriminaliteit I het delict computervredebreuk (art. 138a (oud) Sr) aan het Wetboek van Strafrecht toegevoegd, analoog aan huisvredebreuk (art. 138 Sr) (zie verder paragraaf 2.1 en 2.2.1). Ook kreeg het Wetboek van Strafrecht een definitie van gegevens (art. 80quinqies Sr) en geautomatiseerde werken (art. 80sexies Sr).

Het vertrekpunt van de commissie-Franken was dat computergegevens als zelfstandig object van strafbare handelingen dienden te worden aangemerkt. Computergegevens zijn doorgaans niet hetzelfde als het strafrechtelijke vermogensobject 'goed'.[7] Gegevens zijn in beginsel het product van geestelijke arbeid, terwijl goederen (evenals elektriciteit) het product zijn van fysieke arbeid. Dit heeft tot gevolg dat na een delict als zaakbeschadiging (art. 350 Sr) een strafbepaling is toegevoegd over de 'gegevensaantasting' (art. 350a Sr). Art. 350 Sr verbiedt immers het vernielen, beschadigen en dergelijke van een goed dat aan een ander toebehoort. Met art. 350a Sr heeft de wetgever besloten gegevens dezelfde bescherming te bieden als goederen. In het eerste lid van art. 350a Sr wordt het opzettelijk en wederrechtelijk veranderen, wissen, onbruikbaar of ontoegankelijk maken van gegevens strafbaar gesteld, alsmede het daaraan toevoegen van andere gegevens. Daarmee is ook de installatie van kwaadaardige software strafbaar gesteld. In het derde lid is de verspreiding van kwaadaardige software strafbaar gesteld (zie verder paragraaf 2.2.3).

### *2.1.2 Wet computercriminaliteit II*

Hiermee was de ontwikkeling van het materiële strafrecht betreffende cybercriminaliteit (natuurlijk) nog niet afgerond. Op 8 juli 1999 werd het wetsvoorstel Computercriminaliteit II bij de Tweede Kamer ingediend.[8] De inwerkingtreding van de Wet computercriminaliteit II volgde pas op 1 september 2006.[9] In de tussentijd was veel tijd nodig voor een ingrijpende wijziging van het wetsvoorstel, onder andere

6. Zie ook uitgebreider Kaspersen & Koops 2019.
7. In het *Runescape*-arrest (HR 31 januari 2012, ECLI:NL:HR:2012:BQ9251, *NJ* 2012/536, m.nt. N. Keijzer) heeft de Hoge Raad hier voor het eerst een uitzondering gemaakt. Gegevens die uniek zijn en op geld waardeerbaar zijn, kunnen als goed worden gekwalificeerd.
8. *Kamerstukken II* 1998/99, 26671, nr. 1-3. Zie voor een bespreking Koops & Schellekens 1999, p. 1764-1772.
9. Besluit van 4 juli 2006 tot vaststelling van het tijdstip van inwerkingtreding van de Wet van 1 juni 2006, houdende wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II) (Stb. 300), *Stb.* 2006, 301.

om de onderdelen van het Cybercrimeverdrag te implementeren. Het Cybercrimeverdrag van de Raad van Europa harmoniseert computermisdrijven voor verdragsstaten, stelt lidstaten verplicht wetgeving te creëren voor het vorderen van gegevens bij aanbieder van elektronische communicatiediensten (zie paragraaf 3.3.1), en stelt een 24/7 contactpunt verplicht voor het ontvangen van rechtshulpverzoeken.[10] Een belangrijke materieelrechtelijke verandering vond plaats met de strafbaarstelling van denial-of-service (dos)-aanvallen en de vervaardiging, verspreiding en het bezit van virtuele kinderpornografie.

#### *2.1.3 Wet computercriminaliteit III*

Al snel na de inwerkingtreding van de Wet computercriminaliteit II werd het Wetsvoorstel versterking bestrijding computercriminaliteit in consultatie gegeven (2010). Tegelijkertijd begonnen in deze tijd discussies op te spelen over de invoering van een hackbevoegdheid en de invoering van een decryptiebevel. Deze onderwerpen werden opgepakt en leidden tot de publicatie van het conceptwetsvoorstel Computercriminaliteit III in april 2013. Uiteindelijk trad de Wet computercriminaliteit III op 1 maart 2019 in werking.[11]

De Wet computercriminaliteit III introduceerde naast de hackbevoegdheid (zie paragraaf 3.3.3) ook enkele nieuwe strafbepalingen over de heling van gegevens, het overnemen van niet-openbare gegevens, een nieuwe strafbaarstelling voor online handelsfraude, virtuele ontucht en *grooming*.[12]

### *2.2 Strafbaarstellingen*

Zoals uit de hierboven gegeven korte introductie over de Nederlandse wetten computercriminaliteit duidelijk wordt, is het materiële strafrecht door de laatste decennia heen regelmatig aangepast om nieuwe cybergedragingen strafbaar te stellen. Hieronder worden de belangrijkste nieuwe strafbaarstellingen van cybercriminaliteit in enge zin besproken, te weten *hacken*, ethisch *hacken*, *malware* en ddos-aanvallen.

#### *2.2.1 Hacken*

Hacken is de Engelse benaming voor het delict 'computervredebreuk'. Computervredebreuk betreft het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk en is strafbaar gesteld in art. 138ab Sr. Van binnendringen is *in ieder geval* sprake als men daarbij enige beveiliging doorbreekt of zich de toegang

10. Zie uitgebreid Oerlemans 2021.
11. Besluit van 12 februari 2019 tot vaststelling van het tijdstip van inwerkingtreding van de Wet computercriminaliteit III (Stb. 2018, 322), *Stb*. 2019, 67. De Wijzigingswet zelf is te vinden in: Wet van 27 juni 2018 tot 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 (computercriminaliteit III), *Stb*. 2018, 322.
12. Zie uitgebreid: Oerlemans 2017, p. 350-359.

verwerft door een technische ingreep, met behulp van valse signalen of een valse sleutel dan wel door het aannemen van een valse hoedanigheid. De maximale strafbedreiging is door de implementatie van de richtlijn Aanvallen op informatiesystemen in 2015 verhoogd tot twee jaar gevangenisstraf of een geldboete van de vierde categorie.[13]

De term 'geautomatiseerd werk' is het strafrechtelijke begrip voor een 'computer'. De definitie in art. 80sexies Sr is verbreed in de Wet computercriminaliteit III, zodat ook apparaten die onderdeel uitmaken van een netwerk, zoals een slimme lamp, als geautomatiseerd werk kwalificeren en het doelwit kunnen zijn van computerdelicten.[14]

Als na een 'hack' gegevens worden overgenomen, is sprake van een strafverzwarende omstandigheid (art. 138ab lid 2 Sr). Ook het gebruikmaken van reeds gehackte computers kan tot een strafverzwaring leiden (art. 138ab lid 3 Sr).

Met de implementatie van de Wet computercriminaliteit III in maart 2019 is ook het opzettelijk en wederrechtelijk overnemen van niet-openbare opgeslagen gegevens in een computer strafbaar gesteld. Het verschil met computervredebreuk is dat het bestanddeel 'binnendringen' is weggevallen.[15] De strafbaarstelling is kennelijk geïnspireerd door de Manon Thomas-zaak uit 2007. Vermoedelijk zijn naaktfoto's van een gedeelde map uit het lokale WiFi-netwerk bij haar thuis door een gast gekopieerd en verder verspreid, waarbij het lastig was de dader te vervolgen voor computervredebreuk.[16]

### *2.2.2 Ethisch hacken*

Met 'ethisch hacken' (ook wel 'white hat hacking' genoemd) wordt veelal het hacken met een 'nobel doel' aangeduid, namelijk het vergroten van de veiligheid van informatiesystemen in den brede. Het onderliggende idee is dat door het in brede kring openbaar maken van kwetsbaarheden sneller oplossingen voor beveiligingsproblemen worden gevonden en dit de informatieveiligheid ten goede komt. Een ethisch hacker maakt geen misbruik van de kwetsbaarheid die hij vindt in de beveiliging van een informatiesysteem, maar maakt deze openbaar op een manier dat de kwetsbaarheid kan worden opgelost voordat er misbruik van kan worden gemaakt.[17]

Als er geen sprake is van toestemming tot het binnendringen van het geautomatiseerde werk, dan kan sprake zijn van computervredebreuk en kan het Openbaar Ministerie (OM) overgaan tot vervolging. Mede om dit te voorkomen zijn richtlijnen opgesteld die hackers stimuleren om wel binnen de juridische ruimte te

13. Wet van 22 april 2015 tot implementatie van de richtlijn 2013/40/EU van het Europees Parlement en de Raad over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad (*PbEU* L 218/8), *Stb.* 2015, 165.
14. Zie *Kamerstukken II* 2015/16, 34372, nr. 3, p. 86.
15. *Kamerstukken II* 2015/16, 34372, nr. 3, p. 64.
16. Zie ook Oerlemans 2010, p. 148-152.
17. Zie Falot & Schermer 2016, p. 94-100. Zie ook Van 't Hof 2016.

blijven manoeuvreren. Dit wordt de 'Coordinated Vulnerabilty Disclosure'-richtlijn genoemd.

Het doel van de richtlijn is om bij te dragen aan de veiligheid van ICT-systemen door kennis over kwetsbaarheden door ethische hackers te laten delen met de eigenaren van ICT-systemen, zodat deze de kwetsbaarheden kunnen verhelpen, voordat deze actief worden misbruikt door derden. In de richtlijn staat omschreven dat de organisatie en melder kunnen overeenkomen geen aangifte te doen (van in de eerste plaats computervredebreuk), zolang de melder binnen de randvoorwaarden van het beleid van het bedrijf of instelling opereert. Het OM heeft daarnaast bepaald dat het in zijn beslissing meeweegt of het Coordinated Vulnerability Disclosure-beleid is nagekomen, bij het al dan niet instellen van strafrechtelijk onderzoek (in het kader van het opportuniteitsbeginsel).

Een eventuele vervolging betekent echter nog niet dat de ethisch hacker wordt veroordeeld. De ethisch hacker kan een beroep doen op de rechtvaardigingsgrond 'ontbreken van de materiële wederrechtelijkheid'. Komt het toch tot vervolging en doet de verdachte een beroep op het ethisch hacken voor het algemeen belang, dan zal de rechtbank beoordelen of de gedraging *proportioneel* is geweest (is niet vaker computervredebreuk gepleegd en zijn niet meer gegevens overgenomen dan nodig is om het doel te bereiken) en *subsidiair* is (waren er minder vergaande manieren voorhanden om hetzelfde doel te bereiken).[18]

### *2.2.3 Malware*

De term 'malware' is een samentrekking van 'malicious software', oftewel 'kwaadaardige software'. Het is een verzamelterm voor alle typen kwaadaardige software, zoals virussen, wormen en Trojaanse paarden. Een virus verwijst naar kwaadaardige software die computersystemen infecteert. Kenmerkend is dat het (in tegenstelling tot een worm) een handeling vereist van de computergebruikers, zoals het openen van een bijlage in een e-mail met de malware. Een bekend voorbeeld van een virus was het 'Anna Kournikova'-virus (vernoemd naar een voormalige Russische toptennisster). Uiteindelijk bleek een man in Sneek het virus via zogeheten nieuwsgroepen te verspreiden.[19] Hij werd hiervoor veroordeeld in een van de eerste (en weinige) veroordelingen voor malware in Nederland.[20]

Gijzelsoftware, of 'ransomware', staat sinds een aantal jaren op 'nummer 1' als populairste type malware onder cybercriminelen. Bij deze vorm van malware worden bestanden op afstand versleuteld. Het slachtoffer moet losgeld betalen om de bestanden te ontsleutelen en op die manier weer toegang te krijgen tot de systemen. In januari 2020 is bijvoorbeeld het gelduitwisselingskantoor Travelex slacht-

18. Zie bijvoorbeeld Rb. Den Haag 30 augustus 2018, ECLI:NL:RBDHA:2018:10451.
19. Zie 'Memories of the Anna Kournikova worm', Naked Security – Sophos, 11 februari 2011.
20. Zie Rb. Leeuwarden 27 september 2001, ECLI:NL:RBLEE:2001:AD3861 en HR 28 september 2004, ECLI:NL:HR:2004:AO7009, *NJ* 2004/642. Het virus was geüpload in de nieuwsgroep 'alt.binaries.anna-kournikova'.

offer geworden van de Sodinokibi-ransomware. De cybercriminelen versleutelden de gegevens van computers van het bedrijf en exfiltreerden ondertussen 5 gigabyte aan gevoelige gegevens, waaronder BSN-nummers (of het equivalent daarvan in het buitenland), geboortedatums van mensen en betaalinformatie. Deze gegevens werden gebruikt om het bedrijf onder druk te zetten. Travelex betaalde 2,3 miljoen dollar aan losgeld om de gegevens weer te ontsleutelen. Het 'succes' van ransomware valt te verklaren door het feit dat personen en organisaties al snel bereid zijn te betalen voor gegevens die niet meer toegankelijk zijn. Het kan gaan om kinderfoto's of vakantiefoto's van particulieren, maar ook om de financiële administratie van een multinational. Steeds vaker worden grote organisaties aangevallen, waarbij cybercriminelen in één keer veel geld verdienen.[21]

Het opzettelijk en wederrechtelijk ontoegankelijk maken van gegevens op een computer met behulp van ransomware valt onder de delictsomschrijving van art. 350a lid 1 Sr. De verspreiding van ransomware en ander malware is strafbaar op grond van art. 350a lid 3 Sr. Ook kan onder omstandigheden het delict dwang (art. 284 Sr), afpersing (art. 317 Sr) of oplichting (art. 326 Sr) ten laste worden gelegd.[22] In de CoinVault-ransomwarezaak, vooralsnog de enige veroordeling in Nederland voor ransomware, stelde de rechtbank het ontoegankelijk maken van bestanden gelijk aan het begrip geweld als bedoeld in art. 317 Sr, gelet op lid 2 van dat artikel.[23] Het delict afpersing in art. 317 lid 2 Sr is met de Wet computercriminaliteit II aangepast, zodat ook duidelijk is dat de afpersing kan bestaan uit het ontoegankelijk maken van gegevens.

Sinds mei 2015 is door de EU-richtlijn over aanvallen op informatiesystemen[24] ook art. 138b Sr gewijzigd, waardoor strafverzwarende omstandigheden zijn geformuleerd bij het plegen van delicten als dos-aanvallen, computervredebreuk en het gebruik van *malware*. Indien een (d)dos-aanval wordt gepleegd met 'een aanzienlijk aantal geautomatiseerde werken die getroffen zijn door het gebruik van een technisch middel' of met oogmerk zichzelf of een ander te bevoordelen, staat daar maximaal vier jaar gevangenisstraf op (art. 138b lid 2).[25] Hiervan kan sprake zijn als hackers gebruikmaken van een botnet, een netwerk van geïnfecteerde computers met malware die door een derde worden aangestuurd. Botnets worden vaak gebruikt om ddos-aanvallen mogelijk te maken (paragraaf 2.2.4). Als de aanval 'aanzienlijke schade' met zich meebrengt of is gericht op een 'vitale infrastructuur',

21. Zie het Europol 'internet Organised Crime Threat Assessment' (iOCTA) 2020. Zie bijvoorbeeld ook 'Vleesverwerker JBS betaalde 9 miljoen euro losgeld na grootschalige cyberaanval', *de Volkskrant* 10 juni 2021.
22. Zie ook de Richtlijn voor strafvordering cybercrime, *Stcrt*. 2018, 3271. Bij ransomware zal echter niet altijd sprake zijn van een 'listige kunstgreep' teneinde wederrechtelijk financieel voordeel te verkrijgen.
23. Rb. Rotterdam 26 juli 2018, ECLI:NL:RBROT:2018:6153.
24. Richtlijn 2013/40/EU van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ.
25. In dat geval is in technische zin overigens sprake van een *distributed* denial-of-service aanval (ddos-aanval).

is tevens een strafverzwaring van toepassing (art. 138b lid 3 Sr). De memorie van toelichting definieert niet helder wat 'ernstige schade' inhoudt, maar het ligt voor de hand dat een besmetting van duizenden computers met ransomware daaronder valt.[26] Hier was bijvoorbeeld sprake van bij de aanval met NotPetya-malware, die tot gevolg had dat de Tweede Maasvlakte een week lang niet kon worden gebruikt.[27] Van 'cyberterrorisme' is tot dusver geen sprake geweest in Nederland, maar ook voor die omstandigheid biedt art. 138b Sr een strafverzwaring (zie lid 4 en 5).

#### *2.2.4 Ddos-aanvallen*

Bij een ddos-aanval bezoeken vele computers tegelijk een andere computer, zoals een server van een website, waarna deze webserver overbelast raakt en een website niet meer bereikbaar is. Ddos-aanvallen zijn strafbaar gesteld in art. 138b Sr met de implementatie van de Wet computercriminaliteit II in 2006. In heldere bewoordingen stelt het artikel strafbaar: 'het opzettelijk en wederrechtelijk toegang tot of het gebruik van een computer belemmeren door daaraan gegevens toe te zenden'. Op deze gedraging staat een maximale gevangenisstraf van twee jaar, maar de hierboven besproken omstandigheden voor strafverzwaring in art. 138b Sr zijn natuurlijk ook van toepassing.[28] Als de ddos-aanval specifiek een 'stoornis in een telecommunicatienetwerk of in de uitvoering van een telecommunicatiedienst' veroorzaakt, is ook art. 350c Sr van toepassing.

Een ddos-aanval op websites zoals die van de Belastingdienst of banken of overheid.nl is bovendien strafbaar als een aanval op een 'dienst van algemene nutte', waar een maximale gevangenisstraf op staat van zes jaar.[29] Met de zelfstandige strafbaarstelling wordt duidelijk gemaakt dat de integriteit en beschikbaarheid van gegevens op computers of het computersysteem van met name kritische systemen van groot maatschappelijk belang zijn.

### *2.3 Tussenconclusie: strafbaarstellingen*

Het eerste deel van dit hoofdstuk over het materiële strafrecht laat zien dat Nederland er al vroeg bij was met de strafbaarstellingen van cybercriminaliteit in enge zin. Een trend is zichtbaar waarbij van 1990-2000 het strafrecht up-to-date was, maar de boeven bij wijze van spreken nog moesten komen. Van 2000-2010 kwamen

26. Zie uitgebreid Rb. Rotterdam 26 juli 2018, ECLI:NL:RBROT:2018:6153, *Computerrecht* 2018/210, m.nt. J.J. Oerlemans (*CoinVault*-zaak).
27. T. Kreling & H. Modderkolk, 'Gijzelingssoftware legt al drie dagen een Rotterdamse haven plat – De schade in beeld', *de Volkskrant* 30 juni 2017. Lees ook A. Greenberg, 'The Untold Story of *NotPetya*, the Most Devastating Cyberattack in History', *Wired* 22 augustus 2018.
28. Zie bijvoorbeeld Rb. Den Haag 7 maart 2019, ECLI:NL:RBDHA:2019:2116, *Computerrecht* 2019/93, m.nt. J.J. Oerlemans (*Mirai*-zaak).
29. Art. 161sexies Sr. Zie bijvoorbeeld Rb. Den Haag 14 maart 2005, ECLI:NL:RBSGR:2005:AT0249 en Rb. Zeeland-West-Brabant 2 september 2014, ECLI:NL:RBZWB:2014:6659.

de boeven er en werd vaker vervolgd voor delicten als computervredebreuk en de verspreiding en installatie van kwaadaardige software. De strafbaarstelling van ddos-aanvallen was ook een belangrijke stap. In de jaren 2010-2020 had met name de Europese wetgever aandacht voor de (soms ernstige) schadelijke effecten van cybercriminaliteit. De strafbaarstellingen zijn daarop aangepast en er zijn enkele strafverzwaringen ingevoerd.

## 3 Strafprocesrecht: digitale opsporing

Het opsporingsproces naar cybercriminaliteit in enge zin ziet er anders uit dan het klassieke opsporingsproces in de fysieke wereld. Ooggetuigen, DNA-materiaal of video-opnames zijn meestal niet beschikbaar. In plaats daarvan zijn opsporingsinstanties veel meer afhankelijk van de beschikbaarheid van gegevens bij internetproviders die kunnen worden gevorderd en digitaal forensisch onderzoek op de computers van het slachtoffer en de dader.[30]

In dit deel ligt de nadruk op de (bijzondere) opsporingsbevoegdheden die worden gebruikt in opsporingsonderzoeken naar cybercriminaliteit in enge zin. Na een korte introductie over de hoofdregels voor digitale opsporing en een korte uiteenzetting over het jurisdictieprobleem, worden de regels voor de inzet van opsporingsmethoden besproken aan de hand van een IP-adres als digitaal spoor en een 'online handle' (zoals een 'nickname' (pseudoniem) die cybercriminelen doorgaans op internet gebruiken).

### *3.1 'Wat offline geldt, geldt ook online'*

De regels in het Wetboek van Strafvordering veranderen niet opeens als opsporingsmethoden in een digitale context worden ingezet. Hoewel de regels vaak zijn geschreven voor de fysieke wereld, geeft de Nederlandse wetgever regelmatig aan dat (bijzondere) opsporingsbevoegdheden ook op internet kunnen toegepast. Sinds halverwege de jaren negentig geldt al het adagium: 'wat offline geldt, geldt ook online'.[31] Om deze reden is hetzelfde juridische kader van toepassing bij de inzet van bevoegdheden in een online context, ongeacht of het cyberdelicten of andere delicten betreft.

Dit uitgangspunt werkt in principe goed. Zoals zal blijken, vinden (bijzondere) opsporingsbevoegdheden in toenemende mate hun toepassing in een digitale context. In de loop der jaren zijn er soms wijzigingen aan het Wetboek van Strafvordering noodzakelijk geweest om nieuwe bevoegdheden mogelijk te maken of het digitale opsporingsproces te faciliteren. De meest recente grote verandering betreft de introductie van de hackbevoegdheid in art. 126nba Sv op 1 maart 2019 met de

30. Zie uitgebreid: Koops & Oerlemans 2019b, p. 117-208. Par. 3 is deels op dit hoofdstuk gebaseerd.
31. Zie *Kamerstukken II* 1997/98, 25880, nr. 1, p. 1 (nota Wetgeving elektronische snelweg).

inwerkingtreding van de Wet computercriminaliteit III. Zoals in paragraaf 3.3.3 uitvoerig wordt uitgelegd is de bijzondere opsporingsbevoegdheid speciaal geïntroduceerd om de politie en het OM extra mogelijkheden te geven digitaal bewijs in strafzaken te verzamelen.

### *3.2 Met lege handen: Jurisdictieproblemen in de opsporing*

Ondanks het duidelijke adagium is het niet zo eenvoudig om een juridisch kader op cyberopsporing los te laten. Voordat de (bijzondere) opsporingsbevoegdheden op hoofdlijnen worden besproken, is het van belang zich te realiseren dat in relatief veel gevallen opsporingsinstanties met lege handen komen te staan in cybercrimezaken. Dat komt vanwege de territoriale beperking van de handhavingsjurisdictie, oftewel de jurisdictie van de staat om overheidsmacht uit te oefenen in opsporingsonderzoeken naar – in dit geval – cybercriminaliteit.[32]

Hoe een staat zijn opsporing reguleert en (organisatorisch) inricht, valt onder de soevereiniteit van een staat. Opsporing is een exclusieve taak van een staat. Dit vormt de achtergrond waarom het niet is toegestaan om in het buitenland opsporingshandelingen te verrichten.[33] Handhavingsjurisdictie is met andere woorden territoriaal beperkt.[34] Zo geldt dat Nederlandse agenten een kopstuk van een criminele organisatie niet zelf in Dubai kunnen aanhouden. Voor cyberopsporing levert deze beperking grotere problemen op: bij fysieke delicten die in Nederland worden gepleegd, kan ten minste de plaats delict worden onderzocht. Bij cybercriminaliteit is het niet altijd duidelijk waar het delict is gepleegd en waar de plegers zich ophouden.

Op het hierboven genoemde principe van territorialiteit van handhavingsjurisdictie gelden twee uitzonderingen, namelijk (1) dat opsporing op buitenlands territorium mag plaatsvinden met toestemming van de betrokken staat of (2) als voor de grensoverschrijdende inzet een verdragsbasis bestaat. Via het klassieke systeem van rechtshulp kunnen staten elkaar formeel verzoeken bewijs te vergaren. Een staat kan verzoeken dat de buitenlandse lokale opsporingsinstanties de opsporingshandeling uitvoeren, maar kan ook verzoeken de opsporingshandeling in het buitenland zelf uit te voeren (wat veel minder vaak voorkomt). Deze afspraken kunnen telkens eenmalig zijn (een ad-hocverzoek) of structureel in verdragen worden vastgelegd.

Het kernprobleem is echter dat het systeem van rechtshulp in cyberonderzoeken niet altijd werkt of te traag is.[35] Als een staat niet bereid is om mee te werken

32. Zie uitgebreid Oerlemans 2019, p. 209-232.
33. Zie uitgebreid Schmitt 2017.
34. Dit principe uit het internationaal recht is bevestigd in de belangrijke zaak *SS Lotus* (*Frankijk/Turkije*) (1927), *PCIJ Reports*, Series A, nr. 10, p. 18-19.
35. *Kamerstukken II* 2015/16, 34372, nr. 3, p. 49. Zie ook Koops & Goodwin 2014.

aan een rechtshulpverzoek om bewijs te verzamelen, kunnen opsporingsinstanties van de onderzoekende staat simpelweg met lege handen komen te staan.

Anno 2022 onderhandelen vertegenwoordigers van staten nog druk over internationale wetgeving om bepaalde vormen van digitale opsporing eenvoudiger te maken. Daarbij ligt de nadruk op het verzamelen van bewijs bij internetdienstverleners door het vorderen van gegevens (zie paragraaf 3.3.1). Hiermee wordt het bewijs bij een andere dan de verdachte verzameld, omdat de derde bewijs van en over de verdachte heeft moeten opslaan, bijvoorbeeld op grond van de EU-Dataretentierichtlijn.

Het is belangrijk om zich te realiseren dat het doorgaans lang duurt voordat (andere) internationale afspraken kunnen worden gemaakt. Zo wordt al meer dan tien jaar gesproken over een tweede protocol bij het Cybercrimeverdrag om het unilateraal (direct) vorderen van gegevens bij buitenlandse internetdienstverleners mogelijk te maken. Ook zijn er initiatieven op EU-niveau en van de Verenigde Staten van Amerika die digitaal bewijs verzamelen eenvoudiger moeten maken door het mogelijk te maken direct bepaalde gegevens te vorderen van internetdienstverleners.

Thans heeft Nederland hierover nog geen nieuwe afspraken gemaakt die het unilateraal vorderen van gegevens bij internetdienstverleners op basis van een rechtshulpverdrag mogelijk maken, laat staan dat er verdragen in de maak zijn over de grensoverschrijdende toepassing van andere bijzondere opsporingsbevoegdheden, zoals *undercover* bevoegdheden en de hackbevoegdheid.

Ondanks de bovengenoemde territoriale beperking vindt in de praktijk natuurlijk digitale opsporing naar cybercriminaliteit plaats. In de volgende paragraaf wordt nader aandacht besteed aan de bevoegdheden die de autoriteiten kunnen inzetten (die grotendeels dus zijn gebaseerd op al bestaande wettelijke grondslagen).

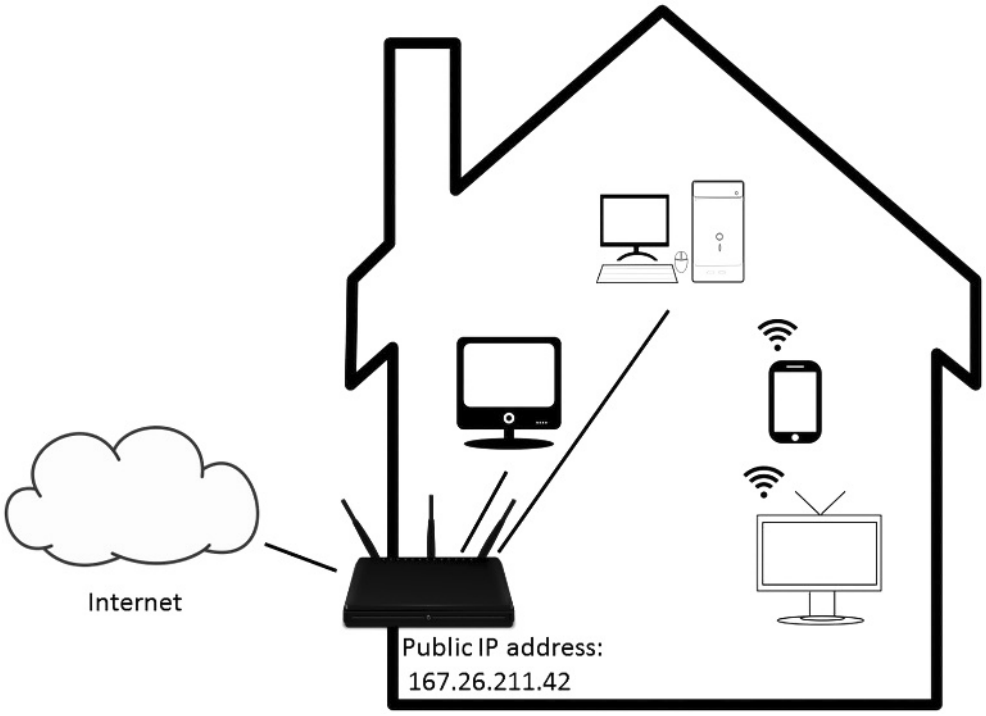
### *3.3 Het opsporingsproces met een IP-adres als digitaal spoor*

Een belangrijke methode voor de autoriteiten is het onderzoek naar een IP-adres, dat te vergelijken is met de registratie van een woning in de gemeentelijke basisadministratie. Een IP-adres is een set van cijfers die een computer binnen een netwerk identificeert, zoals 84.80.247.141 (bij IPv4) of 2001:0db8:85a3:0000:0000:8a2e:0370:7334 (bij IPv6). Als een persoon thuis is en gebruikmaakt van WiFi of een vaste internetverbinding, dan verloopt de internetverbinding via een modem dat door een 'internet access provider' wordt geleverd. Het modem krijgt dan een IP-adres door de internet access provider toegewezen.[36] Als een persoon via bijvoorbeeld zijn PC verbinding maakt met de webserver van een website, dan kan het IP-

36. Een router distribueert het internetverkeer naar de verbonden apparaten. Al die apparaten krijgen ook een IP-adres toegewezen.

adres van het modem worden gelogd. Deze situatie is in het onderstaande figuur gevisualiseerd.

**Figuur 1 Eenvoudige weergave van een internetverbinding in een woning**[37]




Een IP-adres kan een belangrijk digitaal spoor zijn in opsporingsonderzoeken naar cybercriminaliteit. Om dat duidelijk te maken bespreken we een kort scenario. Stelt u zich eens voor: na een internationale politieoperatie (gecoördineerd door Euro-

37. Dit figuur is afkomstig uit Oerlemans 2017, p. 29.

pol) ontvangt een Nederlands zedenteam van Europol een heleboel IP-adressen.[38] De IP-adressen zijn volgens Europol afkomstig van een forum waarop kinderpornografie werd uitgewisseld. In dat geval moeten opsporingsambtenaren de IP-adressen linken aan verdachten in Nederland om op deze manier Nederlandse verdachten te identificeren. Hoe gaat dat in zijn werk?[39]

**Stap 1**
Met een zoekopdracht in de zogenoemde 'Whois-database' kan worden nagegaan welke internet access provider het IP-adres heeft uitgegeven. Als het IP-adres toebehoort aan een Nederlandse internetprovider, dan is de kans aanwezig dat de verdachte in Nederland woonachtig is.

**Stap 2**
In Nederland kunnen opsporingsambtenaren de gegevens van de abonneehouder (degene die doorgaans betaalt voor de internetverbinding) bij de internetdienstverlener vorderen. Het betreffen dan naam- en adresgegevens. Het betreft mogelijk het adres waar een verdachte woonachtig is.

**Stap 3**
Door middel van een doorzoeking in een woning, waarvoor een vordering van een officier van justitie en een machtiging van een rechter-commissaris noodzakelijk zijn, kan binnen de woning van de verdachte bewijs over het misdrijf worden verzameld. Opsporingsambtenaren gaan dan op zoek naar gegevensdragers die mogelijk zijn gebruikt om kinderporno op te slaan en te verspreiden. Deze apparaten worden in beslag genomen.

38. Zie bijvoorbeeld Rb. Zwolle-Lelystad 1 juni 2010, ECLI:NL:RBZLY:2010:BM9626*:* 'Op 12 november 2007 ontving (naam), werkzaam als senior specialist expertise, in dienst van het Korps Landelijke Politiediensten, team bestrijding kinderpornografie, een rapport van Europol met betrekking tot een zaak van de Oostenrijkse politie over kinderpornografie op het internet. Uit het rapport bleek dat de Oostenrijkse politie een melding had ontvangen van de beheerder van een tweetal websites welke volgens de beheerder zouden worden misbruikt om kinderpornografisch beeldmateriaal te verspreiden. De beheerder van deze website heeft vervolgens 9737 afbeeldingen en download logfiles aan de Oostenrijkse politie overgedragen. Uit deze logfiles bleek dat tussen 29 augustus 2007 en 31 augustus 2007 110.031 keren een download van een bepaalde afbeelding had plaatsgevonden door 12.920 unieke IP-adressen. Vervolgens zijn de bijbehorende afbeeldingen, welke op een cd-rom waren bijgevoegd, door voornoemde (naam) bekeken. (naam) zag diverse afbeeldingen welke te classificeren waren als kinderpornografie zoals bedoeld in artikel 240b van het Wetboek van Strafrecht. Uit de logfiles bleek dat in 134 gevallen een IP-adres was gebruikt dat toegewezen is aan een Nederlandse provider.'
39. Zie ook Oerlemans 2020, p. 195-258.

**Stap 4**
Opsporingsambtenaren gaan op zoek naar kinderpornografisch materiaal of ander bewijs van het misdrijf (zoals verstuurde berichten of nicknames) op de inbeslaggenomen gegevensdragers en aangelegen netwerken.

**Stap 5**
Het is gebruikelijk om getuigenverklaringen af te nemen van de bewoners van het pand en mogelijk wordt een verdachte gearresteerd. De verdachte wordt vervolgens verhoord.

In bovenstaand scenario is de kans groot dat de verdachte wordt geïdentificeerd en bewijs kan worden geleverd dat het de verdachte was die vanachter zijn PC kinderpornografie via het forum heeft uitgewisseld of in bezit heeft gehad.

Het is belangrijk zich te realiseren dat bovenstaand scenario het ideale scenario is vanuit opsporingsperspectief. In de praktijk maken cybercriminelen vaak gebruik van anonimiseringstechnieken om hun IP-adres te verbergen. De bespreking van deze anonimiseringstechnieken valt buiten de reikwijdte van dit hoofdstuk.[40] Met de bespreking van het opsporingsproces hebben wij getracht duidelijk te maken dat het vorderen van gegevens en de doorzoeking van een woning ter inbeslagneming van relevante computers waar de verdachte mogelijk gebruik van heeft gemaakt, belangrijke opsporingsmethoden zijn, terwijl de basis van de inzet van die bevoegdheden kan worden gevonden in het onderzoek naar het IP-adres en het feitelijke adres van een verdachte. Vanwege het belang van het vorderen van gegevens en het in beslag nemen van gegevensdragers worden deze twee bevoegdheden hieronder nader toegelicht.

### *3.3.1 Vorderen van gegevens*

Nederland kent door de Wet vorderen gegevens[41] en de Wet vorderen telecommunicatiegegevens[42] een uitgebreid stelsel voor het vorderen van gegevens in het kader van een opsporingsonderzoek naar criminaliteit, zoals cybercriminaliteit in enge zin. Verschillende typen gegevens worden met verschillende bevoegdheden gevorderd. Afhankelijk van de zwaarte van de privacyinmenging zijn daar verschillende voorwaarden aan verbonden. Bij de bespreking van de bevoegdheden

40. Zie uitgebreider Oerlemans 2020. Zie ook Van der Vorst e.a. 2019.
41. Wet van 18 maart 2004 tot wijziging van het Wetboek van Strafvordering en andere wetten in verband met de aanpassing van de bevoegdheden tot het vorderen van gegevens terzake van telecommunicatie (vorderen gegevens telecommunicatie), *Stb.* 2004, 105.
42. Wet van 18 maart 2004 tot wijziging van het Wetboek van Strafvordering in verband met de regeling van bevoegdheden tot het vorderen van gegevens van instellingen in de financiële sector, mede ter uitvoering van het op 16 oktober 2001 te Luxemburg tot stand gekomen Protocol bij de Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen de Lid-Staten van de Europese Unie, door de Raad vastgesteld overeenkomstig artikel 34 van het Verdrag betreffende de Europese Unie (vorderen gegevens financiële sector), *Stb.* 2004, 109.

voor het vorderen van gegevens moet in het achterhoofd worden gehouden dat men bij alle vorderingen *altijd* moet nagaan of de vordering proportioneel (wordt er niet meer gevraagd dan noodzakelijk?) en subsidiair is (zijn er minder ingrijpende alternatieven om de benodigde informatie te verkrijgen beschikbaar?).[43]

**Gebruikersgegevens**
Gebruikersgegevens zijn identificerende gegevens over personen die van een bepaalde dienst gebruikmaken. Voor de context waar wij het over hebben, is het van belang dat dit de naam- en adresgegevens kunnen zijn van de abonneehouder die voor het internetabonnement betaalt. Dit kan de verdachte zelf zijn, maar ook een verdachte die bijvoorbeeld nog woonachtig is bij zijn ouders. Opsporingsambtenaren kunnen het bevel afgeven tot vordering van gebruikersgegevens in opsporingsonderzoeken naar elk misdrijf.[44]

**Verkeersgegevens**
Verkeersgegevens zijn gegevens over communicatie die niet de inhoud van het verkeer (zoals een verstuurd e-mailbericht of privébericht) betreffen. In opsporingsonderzoeken worden verkeersgegevens veelvuldig gevorderd om na te gaan met wie de verdachte heeft gebeld (om daarmee zijn sociale omgeving in kaart te brengen) en om de locatie van de verdachte of andere personen in een opsporingsonderzoek vast te stellen.

In het Besluit vorderen telecommunicatiegegevens is te vinden dat het gegevens betreft over (1) de tijd, (2) de duur, (3) de gebruikte apparatuur, (4) de afgenomen diensten en (5) de locatie van het netwerkaansluitpunt bij een communicatie of van de geografische positie van de randapparatuur van een gebruiker.[45]

Verkeersgegevens kunnen op grond van art. 126n Sv of art. 126nd Sv worden gevorderd, op bevel van officier van justitie en in opsporingsonderzoeken naar misdrijven zoals omschreven in art. 67 lid 1 Sv.[46] Hieronder vallen ook alle genoemde computermisdrijven in paragraaf 2.

**Inhoudelijke gegevens**
De categorie 'inhoudelijke gegevens' betreft de inhoud van bij communicatieaanbieders opgeslagen berichten. De enigszins cryptische omschrijving hiervan in art. 126ng lid 1 Sv – 'gegevens die zijn opgeslagen in het geautomatiseerde werk

43. Zie daarover HvJ EU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, *EHRC* 2021/88, m.nt. D.A.G. van Toor (*Prokuratuur*).
44. Zie art. 126na Sv en 126nc Sv.
45. In art. 2 Besluit vorderen telecommunicatiegegevens zijn verkeersgegevens nader gespecifieerd die bij aanbieders van openbare aanbieders van telecommunicatienetwerken en -diensten kunnen worden gevorderd.
46. Deze bevoegdheid moet, na recente rechtspraak van het Hof van Justitie, worden aangepast: HvJ EU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, *EHRC* 2021/88, m.nt. D.A.G. van Toor (*Prokuratuur*).

van de aanbieder en niet voor deze bestemd of van deze afkomstig zijn' – ziet feitelijk op de inhoud van communicatie die onder het grondwettelijke telecommunicatiegeheim valt (want immers in de beschikkingsmacht van de transporteur van de communicatie).

Communicatie-inhoud betreft bijvoorbeeld opgeslagen e-mails bij online communicatieaanbieders. Deze moeten worden gevorderd op basis van art. 126ng lid 2 Sv.[47] Dit is slechts mogelijk op bevel van een officier van justitie, met machtiging van een rechter-commissaris, voor zover het belang van het onderzoek dit dringend vordert en bij de verdenking van misdrijven die een ernstige inbreuk op de rechtsorde opleveren. Bovendien mag alleen inhoud van communicatie worden gevorderd van de verdachte of met betrekking tot het strafbare feit. De ratio voor deze strenge voorwaarden voor toepassing van de bevoegdheid ligt met name in het recht op bescherming van vertrouwelijke communicatie.

### *3.3.2 Doorzoeking en inbeslagname van gegevensdragers*

Hierboven is de situatie beschreven dat over de verdachte informatie bij een derde – de communicatieaanbieder – wordt verzameld. Dit bedrijf heeft meestal een schat aan informatie opgeslagen van en over een verdachte. Opsporing via een derde is natuurlijk niet de enige wijze waarop de autoriteiten informatie over en van de verdachte kunnen vergaren. Ook het doorzoeken van de woning van de verdachte (of een andere ruimte die hij gebruikt) en het in beslag nemen van daar aangetroffen goederen, zoals elektronische gegevensdragers, draagt bij aan de opsporing van cybercriminaliteit. In deze paragraaf worden deze klassieke bevoegdheden besproken die veel worden ingezet in opsporingsonderzoeken naar cybercriminaliteit.

Op grond van het huidige wettelijke kader kan de rechter-commissaris bij elk strafbaar feit elke plaats doorzoeken ter inbeslagname (art. 110 Sv). 'Elke plaats' moet letterlijk worden opgevat: de rechter-commissaris heeft de bevoegdheid om onder andere de woning van de verdachte te doorzoeken (en op grond van art. 2 Algemene wet op het binnentreden (Awbi) heeft de rechter-commissaris geen binnentredingsmachtiging nodig), alsmede bedrijfsruimtes en kantoren van verschoningsgerechtigden. De officier van justitie komt, op basis van art. 97 Sv, een beperktere doorzoekingsbevoegdheid toe. Ten eerste zijn de gevallen waarin deze bevoegdheid mag worden ingezet beperkt: alleen in het geval van ontdekking op heterdaad of de gevallen van voorlopige hechtenis uit art. 67 lid 1 Sv is de officier van justitie bevoegd. Ten tweede is de officier van justitie alleen bevoegd woningen (waarvoor hij op basis van art. 2 Awbi ook geen binnentredingsmachtiging nodig heeft) en kantoren van verschoningsgerechtigden op basis van deze bepaling te doorzoeken.[48] Ten derde dient de rechter-commissaris een machtiging af te

47. *Kamerstukken II* 2003/04, 29441, nr. 3, p. 14.
48. Op basis van art. 96c Sv is de officier van justitie bevoegd andere plaatsen te doorzoeken.

geven voor de rechtmatige uitoefening van art. 97 Sv. Ten slotte kan de officier van justitie de eerdergenoemde plaatsen alleen doorzoeken bij dringende noodzakelijkheid en indien de inzet van art. 110 Sv door de rechter-commissaris niet kan worden afgewacht. Dit is bijvoorbeeld het geval als collusiegevaar bestaat: zeker in deze context bestaat het risico dat de verdachte, indien hij op enige wijze op de hoogte is van een aankomende doorzoeking, gegevens wist, onbruikbaar maakt of zelfs hele gegevensdragers vernietigt.

De hierboven besproken doorzoekingsbevoegdheid is een steundwangmiddel. Het uiteindelijke doel is de inbeslagname van daarvoor vatbare voorwerpen. Bij cyberopsporing gaat het dan vooral om elektronische gegevensdragers, maar ook documenten – waarin mogelijk informatie is te vinden over versleuteling of vergrendeling – kunnen natuurlijk in beslag worden genomen. Op basis van art. 104 Sv en art. 96 Sv is de rechter-commissaris respectievelijk de officier van justitie bevoegd voorwerpen in beslag te nemen die bij kunnen dragen aan de waarheidsvinding (art. 94 lid 1 Sv). De toepassingsvoorwaarden van art. 104 Sv en art. 96 Sv zijn gekoppeld aan art. 110 Sv respectievelijk art. 97 Sv. Dat betekent dat de rechter-commissaris te allen tijde daarvoor vatbare voorwerpen in beslag mag nemen en de officier van justitie dat alleen mag bij ontdekking op heterdaad of een geval van voorlopige hechtenis op grond van art. 67 lid 1 Sv. Met betrekking tot de inzet van deze doorzoekingsbevoegdheden en de inbeslagname is het nog belangrijk op te merken dat voorwerpen die deel uitmaken van het verschoningsrecht niet of verzegeld in beslag mogen/moeten worden genomen.

Indien een voorwerp in beslag is genomen, volgt uit de wettelijke grondslag voor de inbeslagname dat vervolgens ook de inhoud van het voorwerp mag worden geanalyseerd. Met andere woorden, de autoriteiten hebben geen expliciete wettelijke grondslag nodig voor nadere analyse van de inhoud van een in beslag genomen elektronische gegevensdrager. Volgens de Hoge Raad mag 'voor de waarheidsvinding onderzoek worden gedaan aan inbeslaggenomen voorwerpen ten einde gegevens voor het strafrechtelijk onderzoek ter beschikking te krijgen en in computers opgeslagen gegevens [zijn] daarvan niet (…) uitgezonderd'.[49] De Hoge Raad heeft voor het nadere onderzoek aan de smartphone in de zogeheten *Smartphone*-arresten wel een toetsingskader geschetst om handvatten te geven voor een rechtmatig onderzoek aan de smartphone.[50] Hierin legt de Hoge Raad bijvoorbeeld veel nadruk op de *hoeveelheid geraadpleegde gegevens* als bepalende factor voor nadere normering van het onderzoek aan in beslag genomen smartphones. Afhankelijk van de aard van de inbreuk is, hoewel de wet dat niet vereist, toch toestem-

49. HR 29 maart 1994, ECLI:NL:HR:1994:AD2076, *NJ* 1994/577, m.nt. T.M. Schalken, r.o. 9.3. Zie ook HR 4 april 2017, ECLI:NL:HR:2017:584, *NJ* 2017/229, m.nt. T. Kooijmans, r.o. 2.5-2.8.
50. HR 4 april 2017, ECLI:NL:HR:2017:580, *NJ* 2017/412, m.nt. B.F. Keulen; HR 4 april 2017, ECLI:NL:HR:2017:584, *NJ* 2017/229, m.nt. T. Kooijmans; HR 4 april 2017, ECLI:NL:HR:2017:588, *NbSr* 2017/172, m.nt. T. Urbanus; HR 4 april 2017, ECLI:NL:HR:2017:592, *NJ* 2017/230, m.nt. T. Kooijmans.

ming van de officier van justitie of een machtiging van de rechter-commissaris nodig.[51] De Hoge Raad erkent daarmee in zekere zin de bijzondere status van de smartphone in het huidige tijdperk. Ook voor het eventueel ontgrendelen van een in beslag genomen elektronische gegevensdrager bestaat (nog) geen wettelijke grondslag. De Hoge Raad heeft hiervoor aanvaard dat de inbeslagnamebevoegdheid mede omvat het verkrijgen van toegang tot de inhoud van het voorwerp wanneer de toegang tot de inhoud van het voorwerp is vergrendeld.[52] De verdachte verplichten de autoriteiten toegang tot de inhoud van een elektronische gegevensdrager (of andere voorwerpen) te verstrekken, is beperkt tot het ontsluiten van de inhoud door middel van een biometrisch kenmerk.[53] De verdachte kan niet worden gedwongen een wachtwoord uit te spreken, op te schrijven of in te toetsen: dat levert een schending van het nemo-teneturbeginsel op.

Naast deze klassieke mogelijkheden om bewijs voor cybercriminaliteit in beslag te nemen, geeft de wet de autoriteiten ook de bevoegdheid een plaats te doorzoeken ter vastlegging van gegevens die op deze plaats op een gegevensdrager zijn opgeslagen of vastgelegd (art. 125i Sv). De toepassing van dit artikel is in de wettekst van art. 125i Sv expliciet gekoppeld aan de uitvoering van de doorzoekingsbevoegdheden op grond van onder andere art. 110 Sv en art. 97 Sv. Omdat de voorwerpen waarop gegevens staan wel, maar gegevens zelf niet in beslag kunnen worden genomen, vond de wetgever het noodzakelijk art. 125i Sv in het leven te roepen. Een belangrijke uitbreiding van bevoegdheden vormt de koppeling van art. 125i Sv met art. 125j Sv. In die laatste bepaling is de netwerkzoeking opgenomen: bij de uitvoering van art. 125i Sv mogen de autoriteiten zich ook toegang verschaffen tot geautomatiseerde werken die verbonden zijn met bijvoorbeeld een computer op de plaats waar zij art. 125i Sv uitvoeren.[54] Deze bevoegdheid breidt de reikwijdte van onderzoek aan elektronische gegevensdragers enorm uit.[55] In de Innovatiewet wordt de netwerkzoeking verder uitgebreid. Niet langer is het noodzakelijk dat de autoriteiten een geautomatiseerd werk op locatie (art. 125i Sv) gebruiken. Het plan is ook om via in beslag genomen geautomatiseerde werken een netwerkzoeking uit te voeren.[56] Hierbij wordt met name gedacht aan de toe-

51. Zie hierover kritisch: Royer & Oerlemans, *Computerrecht* 2017/200, p. 277-284 en HR 9 februari 2021, ECLI:NL:HR:2021:202, *Computerrecht* 2021/63, m.nt. D.A.G. van Toor & T. Beekhuis.
52. HR 9 februari 2021, ECLI:NL:HR:2021:202, *Computerrecht* 2021/63, m.nt. D.A.G. van Toor & T. Beekhuis.
53. Van Toor 2017.
54. Zie voor een nadere bespreking over de toepassingsvoorwaarden: Postma 2020.
55. Zie hierover kritisch: Conings & Oerlemans 2013, p. 23-32.
56. De Raad voor de rechtspraak is over de rechtsbescherming kritisch: Raad voor de rechtspraak, Advies Wijziging van het Wetboek van Strafvordering ter bevordering van innovatie van verschillende onderwerpen in het kader van de modernisering van het Wetboek van Strafvordering (Innovatiewet Strafvordering).

gang tot bestanden in een cloud via een in beslag genomen smartphone.[57] Dit maakt dat met een 'simpele' inbeslagname van een smartphone een grote wereld aan informatie geopend wordt: na inbeslagname mag de verdachte namelijk worden gedwongen de autoriteiten toegang tot de inhoud van de elektronische gegevensdrager te verschaffen door middel van een biometrisch kenmerk, waarna de inhoud van de elektronische gegevensdrager mag worden geanalyseerd en de via de elektronische gegevensdragers toegankelijke geautomatiseerde werken op afstand mogen worden doorzocht.

### *3.3.3 Hackbevoegdheid*

Mocht de toegang tot gegevens op een hierboven beschreven manier niet mogelijk zijn, dan kunnen de autoriteiten ook toegang door middel van hacken verkrijgen. Hacken als opsporingsbevoegdheid is een paraplubegrip, waarbij het kenmerkend is dat opsporingsambtenaren heimelijk en op afstand toegang verschaffen tot een geautomatiseerd werk. Vaak zal de inzet plaatsvinden met behulp van een technisch hulpmiddel (zoals een Trojaans paard of andere software), waarmee vervolgens tal van handelingen mogelijk zijn, zoals het bekijken en kopiëren van gegevens, het heimelijk aanzetten van de microfoon of camera en het ontoegankelijk maken van gegevens.

De voorbereidingen voor het invoeren van een 'hackbevoegdheid' voor de politie en justitie zijn terug te voeren tot 2009. In een Kamerbrief uit 2009 gaf de toenmalige minister van Justitie aan dat het opsporen van cybercriminaliteit door anonimiseringstechnieken en encryptie 'extreem gecompliceerd' is geworden.[58] Om met deze problematiek om te gaan is met de Wet computercriminaliteit III een nieuwe opsporingsbevoegdheid ingevoerd om hacken door de politie en justitie mogelijk te maken.[59] De hackbevoegdheid – officieel het 'toegang verschaffen op afstand tot een geautomatiseerd werk' genoemd – is nu geregeld in art. 126nba Sv.

Door toepassing van hacken als opsporingsmethode is de mogelijkheid gecreëerd rechtstreeks toegang te verschaffen tot de computer waarvan een verdachte gebruikmaakt. Ook is het mogelijk met behulp van een programma (een 'technisch hulpmiddel'), het echte IP-adres van de gebruiker en andere identificerende gegevens naar opsporingsdiensten toe te sturen.[60] De anonimiseringsmaatregelen of -technieken die de verdachte heeft genomen, zijn in die gevallen nutteloos, omdat de politie op de bron direct kan meekijken. Toch moet men zich realiseren dat het niet altijd mogelijk zal zijn de computer waarvan een verdachte gebruik-

57. Memorie van toelichting bij Wijziging van het Wetboek van Strafvordering ter bevordering van innovatie vanverschillende onderwerpen in het kader van de modernisering van het Wetboek van Strafvordering (Innovatiewet Strafvordering), p. 28.
58. Zie *Kamerstukken II* 2008/09, 28684, nr. 232, p. 2-3.
59. In de praktijk had de politie al enige malen computers gehackt voordat de bijzondere bevoegdheid werd ingevoerd op basis van art. 125i Sv jo. art. 94 Sv (zie voor een overzicht: Oerlemans 2017, p. 258-261).
60. *Kamerstukken II* 2015/16, 34372, nr. 3, p. 20.

maakt te hacken. Het is onder andere afhankelijk van het type apparaat en de beveiligingsmaatregelen die een verdachte heeft genomen of het haalbaar is de computer van de verdachte op afstand binnen te dringen.

De hackbevoegdheid draagt ook bij aan het omzeilen van het versleutelprobleem in opsporingsonderzoeken. Voordat versleuteling van netwerkverkeer (met communicatie) of opgeslagen gegevens in werking treedt, kan de politie met de inzet van de hackbevoegdheid gegevens veiligstellen door deze te kopiëren. Met de zogenoemde keylogfunctionaliteit van politiesoftware kunnen bovendien inlognamen en wachtwoorden van computergebruikers worden vastgelegd, zodat deze later kunnen worden gebruikt voor toegang tot beveiligde gegevens.[61]

Ten slotte is de hackbevoegdheid nadrukkelijk ook geïntroduceerd om met het probleem van 'cloud computing' in opsporingsonderzoeken om te gaan.[62] Met de inzet van de hackbevoegdheid kunnen opsporingsambtenaren – voor zover aan alle voorwaarden van de voorgestelde bevoegdheid wordt voldaan – webmailaccounts of accounts die worden gebruikt voor online opslagdiensten hacken om een 'online doorzoeking' van het account uit te voeren. Daarbij moet wel worden opgemerkt dat zich hierbij mogelijk problemen met betrekking tot de territoriale soevereiniteit van andere staten kunnen voordoen.[63] Hoewel de toelichting op de hackbevoegdheid naar deze toepassing verwijst, wordt in de toekomst mogelijk de regeling van de netwerkzoeking aangepast, zodat na de inbeslagname van het apparaat van de verdachte op afstand aanliggende accounts kunnen worden doorzocht (zie paragraaf 3.3.3).

De hackbevoegdheid in art. 126nba Sv is gelaagd opgebouwd. In het eerste deel staat dat opsporingsambtenaren zich op afstand toegang verschaffen tot een geautomatiseerd werk. Daarbij mogen opsporingsambtenaren de volgende vijf opsporingshandelingen inzetten:

1. het vaststellen van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;
2. het onderscheppen van communicatie, zoals bedoeld in art. 126l Sv of 126m Sv;
3. het stelselmatig observeren van gedrag van een persoon met een technisch hulpmiddel, zoals bedoeld in art. 126g Sv;
4. het vastleggen van gegevens die in een computer zijn opgeslagen of tijdens de uitvoering worden opgeslagen; en
5. de ontoegankelijkheidsmaking van gegevens, als bedoeld in (het nieuwe) art. 126cc lid 5 Sv.[64]

61. Zie, in enigszins andere bewoordingen, *Kamerstukken II* 2015/16, 34372, nr. 3, p. 21.
62. Zie ook *Kamerstukken II* 2015/16, 34372, nr. 3, p. 11-12.
63. Zie in dit kader ook de Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex artikel 126nba Sv, *Stcrt.* 2019, 10277.
64. Zie ook uitgebreid *Kamerstukken II* 2015/16, 34372, nr. 3, p. 21-31.

De officier van justitie en rechter-commissaris (lid 4), evenals de Centrale Toetsingscommissie, zullen elk een afweging maken of inzet van de bevoegdheid proportioneel en subsidiair is, mede in het licht van de omstandigheden van het geval.

### *3.4 Het opsporingsproces op basis van een 'online handle'*

In paragraaf 3.3 is het digitale opsporingsproces beschreven vanuit het idee van het (IP-)adres als uitgangspunt voor de opsporing in cybercrimezaken. Als de autoriteiten echter geen IP-adres van de verdachte te weten komen, maar wel andere informatie over hem vergaren, kan het opsporingsonderzoek anders worden ingestoken. Cybercriminelen gebruiken veelal een nickname, bijvoorbeeld een pseudoniem in een chatkanaal, op een online discussieforum of een handelsplatform. Net als een andere 'online handles', zoals een e-mailadres, zijn dat belangrijke – en soms de enig beschikbare – digitale sporen in cybercrimezaken.[65]

#### *3.4.1 Openbronnenonderzoek*

Het verzamelen van gegevens uit open bronnen, inclusief gegevens op het internet, is in de meeste opsporingsonderzoeken de standaard geworden.[66] Dat is ook niet verwonderlijk, gezien de hoeveelheid en diversiteit aan persoonlijke informatie die over delicten en verdachten of personen in de nabijheid van de verdachte te vinden is. Open bronnen zijn gegevens die voor eenieder toegankelijk zijn. Het gaat daarbij ook om gegevens die na registratie beschikbaar zijn, zolang er geen restrictie geldt voor de groep personen die zich kan registreren. Daarbij kan worden gedacht aan het bekijken en vergaren van gegevens van online discussieforums en socialemediadiensten, ook als daarvoor registratie is vereist.

In de Wet computercriminaliteit II werd expliciet gemaakt dat opsporingsambtenaren (1) 'op internet kunnen rondkijken', (2) de gevonden informatie kunnen downloaden van verschillende bronnen op internet en (3) deze informatie kunnen opslaan in hun politiesysteem, alles op basis van art. 3 Politiewet 2012.[67] De opsporingsactiviteit is in dat geval onderdeel van de taakstelling van de politie om bewijs te verzamelen in opsporingsonderzoeken en vormde volgens de wetgever destijds een beperkte inbreuk op de persoonlijke levenssfeer van mensen.[68] De toepassing van de opsporingsmethode vergt dan geen bevel van een officier van justitie en de opsporingsmethode kan worden toegepast in opsporingsonderzoeken naar elk type strafbaar feit.

65. Zie uitgebreid Oerlemans 2017, p. 30-36. Dit proces wordt mooi in 'beeld' gebracht in de podcast *Hunting Warhead*, waar 'Warhead' de nickname van de nog onbekende verdachte is. Ook andere onderwerpen, zoals jurisdictie, komen in deze podcast aan bod.
66. Zie bijvoorbeeld Lensink & Janssen, 'Plaats delict: social media', *Vrij Nederland* 18 april 2014.
67. Zie *Kamerstukken II* 1998/99, 26671, nr. 3, p. 35-36.
68. Zie *Kamerstukken II* 1998/99, 26671, nr. 3, p. 35.

Toch kan openbronnenonderzoek onder omstandigheden een ernstige inbreuk op de persoonlijke levenssfeer van de verdachte opleveren. In de huidige systematiek voor de normering van opsporingsmethoden is dan de inzet van een bijzondere opsporingsbevoegdheid vereist. In de praktijk wordt dan ook wel de bijzondere bevoegdheid van 'stelselmatige informatie-inwinning' toegepast.[69] Er is sprake van stelselmatigheid als een 'min of meer volledig beeld van bepaalde aspecten van iemands privéleven wordt verkregen'.[70] Om dat vast te stellen zijn de volgende factoren in de Wet bijzondere opsporingsbevoegdheden (Wet BOB) geformuleerd: duur, plaats, intensiteit, frequentie en het gebruik van een technisch hulpmiddel.[71] Het is ook mogelijk stelselmatig (passief) gedrag van mensen op sociale media te volgen of waar te nemen.[72] Net als observatie in de fysieke wereld, moet in dat geval de bijzondere opsporingsbevoegdheid van stelselmatige observatie worden ingezet.[73]

De wetgever is ook van mening dat de stelselmatige vastlegging van persoonsgegevens, ook al zijn de gegevens mogelijk vrijwillig beschikbaar gesteld, een meer dan geringe inmenging met de rechten en vrijheden van de betrokkene vormt en dat toepassing van een bijzondere bevoegdheid noodzakelijk is.[74] De voorgestelde bijzondere opsporingsbevoegdheid in art. 2.8.8 Sv in de ambtelijke versie van het conceptwetsvoorstel van de modernisering van het Wetboek van Strafvordering, hoeft pas te worden ingezet als het verzamelen van de gegevens 'stelstelmatig' wordt. Voor de inzet van de bevoegdheid is een voorafgaand bevel van de officier van justitie vereist, waarbij de bevoegdheid voor ten hoogste drie maanden kan worden toegepast, met de mogelijkheid tot verlenging.

### *3.4.2 Online undercoverbevoegdheden*

Een online handlekan ook aanleiding geven tot de inzet van vergaande heimelijke opsporingsbevoegdheden. Deze undercoveroperaties worden gekenmerkt door de *interactie* tussen individuen *onder dekmantel* met het doel bewijs te verzamelen in een opsporingsonderzoek.[75] De betrokken individuen die onderwerp zijn van het

69. Aldus Stol, Leukfeldt & Klap 2012, p. 25-39.
70. Bijv. HR 1 juli 2014, ECLI:NL:HR:2014:1563, *NJ* 2015/114, m.nt. P.H.P.H.M.C. van Kempen, r.o. 2.4.
71. *Kamerstukken II* 1996/97, 25403, nr. 3, p. 27. In de praktijk zijn deze factoren soms lastig te vertalen naar een internetcontext. De Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018 (commissie-Koops) heeft aanbevelingen gedaan om de toepassing van het criterium in de memorie van toelichting duidelijk te maken.
72. Zie ook Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, *Computerrecht* 2016/46, p. 113-124, m.nt. J.J. Oerlemans (*Context*-zaak).
73. Zie *Kamerstukken II* 1996/97, 25403, nr. 3, p. 26-27 en *Kamerstukken II* 1998/99, 26671, nr. 3, p. 36.
74. Memorie van toelichting bij de ambtelijke versie van het conceptwetsvoorstel modernisering van het Wetboek van Strafvordering (juli 2020), p. 49-50.
75. Vgl. Fijnaut & Marx 1995, p. 1-27; Kruisbergen & De Jong 2012, p. 50-67.

onderzoek, zijn niet op de hoogte van het doel van de interactie noch van de identiteit van de undercoveragenten.[76]

Voor de toepassing van deze bijzondere opsporingsbevoegdheden in een online context is het van belang dat in de wetsgeschiedenis is opgemerkt dat bijzondere opsporingsbevoegdheden, zoals infiltratie, onder gelijke voorwaarden in de digitale wereld kunnen worden toegepast.[77] Opsporingsambtenaren en burgers onder instructie van de politie en het OM kunnen – praktisch gezien – net zo anoniem en grensoverschrijdend te werk gaan als de betrokken verdachten in een opsporingsonderzoek. Daarbij kan worden gedacht aan de online interactie onder dekmantel met verdachten door het versturen van privéberichten via e-mail, sociale media en online fora. Het internet biedt daarom interessante mogelijkheden voor undercoveroperaties.[78]

Bij de Wet BOB zijn drie bijzondere opsporingsbevoegdheden met betrekking tot undercover opsporingsmethoden in het Wetboek van Strafvordering geïntroduceerd:

1. pseudokoop en pseudodienstverlening (art. 126i Sv);
2. stelselmatige informatie-inwinning (art. 126j Sv);
3. infiltratie (art. 126h Sv).

**Pseudokoop**

Het uitvoeren een pseudokoop op internet kan het best worden omschreven als de situatie waarbij een undercoveragent zich voordoet als potentiële koper van een illegaal via internet aangeboden goed of dienst. De online pseudokoop wordt in de praktijk vaak toegepast.[79] Daarbij kan bijvoorbeeld worden gedacht aan de aankoop van drugs op online handelsplaatsen, de aankoop van illegaal vuurwerk bij webwinkels en de aankoop van gestolen goederen van marktplaats.nl, in het kader van opsporingsonderzoeken.[80]

Bij de Wet computercriminaliteit II is art. 126i lid 1 onder b Sv aangepast, zodat duidelijk is dat ook gegevens gekocht kunnen worden in plaats van alleen goederen. Voor de toepassing van de pseudokoop of pseudodienstverlening is een bevel van een officier van justitie vereist; het mag alleen worden toegepast in opsporingsonderzoeken met betrekking tot misdrijven zoals omschreven in art. 67 lid 1 Sv.

76. Zie ook Joh 2009, p. 161.
77. Zie *Kamerstukken II* 1998/99, 26671, nr. 3, p. 36.
78. Zie ook uitgebreider Oerlemans 2018, p. 83-99.
79. Zie ook Kruisbergen & De Jong 2010, p. 216.
80. Zie Rb. Den Haag 10 juli 2008, ECLI:NL:RBSGR:2008:BD7012 (online pseudokoop van drugs), Rb. Roermond 4 maart 2009, ECLI:NL:RBROE:2009:BH4757 (online pseudokoop van gestolen goederen op marktplaats.nl), Rb. Zutphen 28 januari 2011, ECLI:NL:RBZUT:2011:BP2308 (online pseudokoop van illegale wapens), Rb. Oost-Brabant 6 mei 2013, ECLI:NL:RBOBR:2013:BZ9467 (online pseudokoop van illegaal vuurwerk) en Rb. Rotterdam 8 mei 2014, ECLI:NL:RBROT:2014:3504 (online pseudokoop van drugs op Silk Road). Zie ook het persbericht van het Landelijk Parket, 'Undercover onderzoek naar illegale marktplaatsen op internet' van 12 februari 2014.

**Stelselmatige informatie-inwinning**

De actieve interventie in het leven van de verdachte door de opsporingsambtenaar is kenmerkend voor de toepassing van stelselmatige informatie-inwinning als bijzondere opsporingsbevoegdheid. Dit gaat verder dan louter het observeren van gedrag van personen of zaken.[81] Slechts met de juiste kennis van internetsubculturen kunnen opsporingsambtenaren op een geloofwaardige manier op internet communiceren en relaties aangaan met mensen in het kader van een opsporingsonderzoek.[82] In de Wet BOB heeft de wetgever expliciet aangegeven dat deze bijzondere opsporingsbevoegdheid ook op internet mag worden toegepast.[83]

De juridische basis voor het online interacteren onder dekmantel met verdachten of derden is art. 3 Politiewet 2012 (voor zover het niet stelselmatig is) of art. 126j Sv (de bijzondere bevoegdheid voor stelselmatige informatie-inwinning). Voor de bijzondere opsporingsbevoegdheid is een bevel van een officier van justitie vereist. Art. 126j Sv kan worden ingezet bij de opsporing van elk misdrijf en voor een (telkens verlengbare) periode van drie maanden.

Het is van belang dat de betrokken undercoveragent niet verder gaat dan is afgesproken met zijn leidinggevenden in de undercoveroperatie en dat dit voldoende wordt gecontroleerd. Hier wordt onder andere in EHRM-jurisprudentie met betrekking tot het recht op een eerlijk proces in art. 6 EVRM op gewezen. Daarbij zij opgemerkt dat in Nederland geen machtiging van een rechter-commissaris is vereist, terwijl het EHRM deze wel voor het toezicht in undercoveroperaties prefereert.[84]

Jurisprudentie over de BOB-bevoegdheid van stelselmatige informatie-inwinning in een online context is zeer schaars. Slechts één zaak geeft antwoord op de bovengenoemde vraag wanneer sprake is van stelselmatigheid bij online interacties met de verdachten in een opsporingsonderzoek. In de zogenoemde *Context*-zaak hebben opsporingsambtenaren een fictief profiel opgesteld en zichzelf als vriend toegevoegd aan het profiel van de verdachte op Facebook. Daarnaast hebben ze deelgenomen aan een Facebookgroep waarvan werd gedacht dat de leden zich bezighielden met jihadistische activiteiten. Kort gezegd waren de rechters van mening dat al voor het aanmaken van een profiel de bevoegdheid tot stelselmatige informatie-inwinning moest worden ingezet. De opsporingsambtenaren hebben het bevel van de officier van justitie pas later verkregen en er was sprake van een

81. Zie *Kamerstukken II* 1996/97, 25403, nr. 3, p. 35.
82. Zie ook o.a. Siemerink 2000, p. 145.
83. Zie *Kamerstukken II* 1996/97, 25403, nr. 3, p. 34. Zie ook *Kamerstukken II* 1998/99, 26671, nr. 3, p. 37.
84. Zie bijvoorbeeld EHRM 24 juni 2008, ECLI:CE:ECHR:2008:0624JUD007435501 (*Milinienè/Litouwen*), EHRM 4 november 2010, ECLI:CE:ECHR:2010:1104JUD001875706, *NJB* 2011/176 (*Bannikova/Rusland*) en EHRM 23 oktober 2014, ECLI:CE:ECHR:2014:1023JUD005464809, *EHRC* 2015/1, m.nt. P. Ölçer (*Furcht/Duitsland*).

gebrekkige verbalisering van de opsporingshandelingen. De vormverzuimen leidden echter niet tot een sanctie, omdat ze werden gerelativeerd door de rechter.[85]

**Infiltratie**

Infiltratieoperaties onderscheiden zich door het kenmerk dat de undercoveragent (tot op zekere hoogte) strafbare feiten mag plegen om zijn dekmantel te behouden en het vertrouwen te winnen van leden van een criminele organisatie. Met andere woorden, in een infiltratieoperatie *participeren* opsporingsambtenaren in een criminele organisatie teneinde bewijsmateriaal over strafbare feiten te verzamelen en toegang te krijgen tot de hogere regionen van een criminele organisatie.[86] Het is daarbij mogelijk dat (geautoriseerde) strafbare feiten worden gepleegd.

Voor de inzet van infiltratie als bijzondere opsporingsbevoegdheid door een opsporingsambtenaar geldt het bepaalde in art. 126h Sv. Met een infiltratieoperatie mag alleen worden begonnen nadat een bevel is verkregen van een officier van justitie in opsporingsonderzoeken naar misdrijven zoals omschreven in art. 67 lid 1 Sv, met een ernstige inbreuk op de rechtsorde. Daarbij moet een machtiging van de rechter-commissaris worden verkregen. Als intern controlemechanisme moet ook de Centrale Toetsingscommissie van het OM advies geven over de inzet van infiltratieoperaties. Deze zware voorwaarden zijn aangewezen gelet op de indringendheid van deze opsporingsbevoegdheid en vooral het risico omtrent de integriteit van een opsporingsonderzoek.

De meest opzienbarende toepassing van de infiltratiebevoegdheid op het internet betreft de overname van het online handelsplatform Hansa ('operatie Bayonet' genoemd).[87] Van 20 juni tot 20 juli 2017 nam de Nederlandse politie de online drugsmarktplaats Hansa over. Daartoe werd de inhoud van de servers van de Hansa Market gekopieerd en overgeplaatst van Litouwen naar een datacentrum in Nederland. Als zijnde de 'administrators' van de markt runde de Nederlandse politie onder leiding van het OM en in samenwerking met buitenlandse opsporingsinstanties de drugsmarkt. Tijdens deze overname vonden in totaal meer dan 27.000 transacties plaats en werd een schat aan informatie verzameld, waaronder de informatie van 20.000 gebruikers en 10.000 thuisadressen. Deze gegevens zijn verstrekt aan Europol en van daaruit verder gedistribueerd naar opsporingsinstanties in andere landen. Ook de communicatie tussen het personeel en gebruikers van de darknet market en de financiële administratie is in kaart gebracht. Deze informatie kan belastende informatie opleveren voor verdere vervolging.

85. Zie Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, *Computerrecht* 2016/46, m.nt. J.J. Oerlemans, r.o. 5.26-5.27 (*Context*-zaak).
86. Zie *Kamerstukken II* 1996/97, 25403, nr. 3, p. 28-29. Zie ook de brief van de minister van Veiligheid en Justitie van 8 oktober 2014 (nr. 571620) over het juridische verschil tussen 'informanten' en 'individuen die infiltreren binnen een opsporingsonderzoek'.
87. Zie o.a. A. Greenberg, 'Operation Bayonet: Inside the Sting That Hijacked an Entire Dark Web Drug Market', *Wired* 3 augustus 2018. Zie ook Van Wegberg & Verburgh 2018.

De gepubliceerde uitspraken naar aanleiding van deze operatie zijn op één hand te tellen; de operatie had ook een duidelijk verstoringselement om kopers en verkopers van drugs op internet te ontmoedigen (zie paragraaf 4). Op 3 juli 2019 veroordeelde de rechtbank Rotterdam een van de verkopers tot vijf jaar gevangenisstraf voor het witwassen van bitcoins voor in totaal meer dan € 800.000; ook had de verdachte samen met anderen meer dan 22.000 drugsbestellingen afgeleverd. De rechtbank legt in het vonnis uit dat geen sprake was van uitlokking. De rechtbank past daarbij de gebruikelijke toets toe of de verkopers en kopers door het onderzoeksteam door de overname niet tot andere strafbare feiten zijn gebracht dan die waarop hun opzet reeds was gericht. Met de geruisloze overname van Hansa Market heeft het onderzoeksteam de bestaande situatie in zoverre ongewijzigd voortgezet. Niet is gebleken dat verkopers (of kopers) door de overname, dan wel door het handelen van het onderzoeksteam, zijn gebracht tot het begaan van andere strafbare feiten dan waarop hun opzet reeds van tevoren was gericht. Het toelaten van nieuwe verkopers en het aanbieden van een korting bij personen bij wie al het opzet bestond om te handelen in verdovende middelen op deze specifieke en verborgen website, passen volgens de rechtbank eveneens in dit kader en kunnen dan ook niet worden gekwalificeerd als uitlokking.[88]

## 4 Van opsporing naar verstoring en weer terug

In het eerste deel van dit hoofdstuk is de beweging in de strafbaarstellingen van cybercriminaliteit beschreven. Net zoals het gebruik van computers en het internet aanleiding gaf en geeft tot aanpassing van het materiële strafrecht, is het strafprocesrecht op basis van dezelfde ontwikkelingen constant in beweging. In het tweede deel zijn de voornaamste opsporingshandelingen en -bevoegdheden beschreven. Die laten een beeld zien van steeds toenemende mogelijkheden, afhankelijk van de ontwikkeling van de techniek (denk aan het ontgrendelbevel bij in beslag genomen smartphones en de in de Innovatiewet voorgestelde netwerkzoeking naar bestanden in de cloud).

Aangezien de klassieke opsporing en vervolging van verdachten van cybercriminaliteit vaak complex zijn, komt er steeds meer aandacht voor andere strategieën om cybercriminaliteit te bestrijden. De Nederlandse politie heeft in samenwerking met het OM bij cybercriminaliteit een strategie van 'preventie, opsporing, vervolging, verstoring of een combinatie daarvan'.[89] Bij verstoring kan het bijvoorbeeld gaan om 'het criminele verdienmodel het meest effectief [te] kunnen verstoren', en dat kan noodzakelijk zijn als bijvoorbeeld de verdachten nog steeds uit beeld zijn maar hun methode wel invloed heeft op Nederlands grondgebied (via bijvoorbeeld *phishing*).

88. Rb. Rotterdam 3 juli 2019, ECLI:NL:RBROT:2019:5339, *Computerrecht* 2019/178, m.nt. J.J. Oerlemans (*Hansa Market*-zaak).
89. Zie o.a. de Kamerbrief over de integrale aanpak van cybercriminaliteit van 18 april 2018.

Uit digitale opsporingsoperaties uit de afgelopen jaren valt bijvoorbeeld op dat online handelsplatformen ontoegankelijk werden gemaakt. Dit zijn duidelijk verstorende activiteiten (waarbij natuurlijk ook bewijs wordt vergaard tegen een deel van de gebruikers). Voor de operaties worden 'opkomende criminele werkwijzen geanalyseerd, vaak in publiek-privaat verband, en wordt bezien welke slimme interventies kunnen worden ingezet om het criminelen zo lastig mogelijk te maken'.[90]

Daarbij worden soms grote hoeveelheden gegevens vergaard. Zo zijn via de Ennetcom server miljoenen berichten en via de EncroChat-hack zelfs tientallen miljoenen berichten vergaard (om nog maar te zwijgen over de 'oogst' van 'Operation Trojan Shield'/'Greenlight'). Dit doet ten minste vragen rijzen over de proportionaliteit van de inzet van digitale opsporingsbevoegdheden. Ook vragen met betrekking tot eventuele schending van het eerlijk procesrecht, en dan met name de 'disclosure', rijzen.[91] Dit betekent dat ook digitale opsporing de komende jaren volop in beweging zal zijn.

## Literatuur

C. Conings & J.J. Oerlemans, 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?', *Computerrecht* 2013/5, p. 23-32.
N. Falot & B.W. Schermer, 'De strafrechtelijke positie van de Nederlandse ethisch hacker', *Computerrecht* 2016/45, p. 94-100.
C.J.C.F. Fijnaut & G.T. Marx, 'The normalization of undercover policing in the West: Historical and contemporary perspectives', in: C.J.C.F. Fijnaut & G.T. Marx (red.), *Undercover: police surveillance in comparative perspective*, Den Haag: Kluwer Law International 1995, p. 1-27.
H. Franken, *Informatietechniek en Strafrecht*, Den Haag: WODC 1987.
M. Galic, 'De rechten van de verdediging in de context van omvangrijke datasets en geavanceerde zoekmachines in strafzaken: een suggestie voor uitbreiding', *Boom Strafblad* 2021, afl. 2, p. 41-49.
C. van 't Hof, *Helpende hackers. Verantwoorde onthullingen in het digitale polderlandschap*, Rotterdam: Tek Tok Uitgeverij 2016.
E.E. Joh, 'Breaking the Law to Enforce It: Undercover Police Participation in Crime', *Stanford Law Review* 2009, 61, p. 155-198.
H.W.K. Kaspersen, 'De Wet computercriminaliteit is er – nu de boeven nog', *Computerrecht* 1993/4, p. 134-145.
H.W.K. Kaspersen & B.J. Koops, 'Computercriminaliteit in historisch perspectief', in: B.J. Koops & J.J. Oerlemans (red.), *Strafrecht en ICT* (Monografieën recht en informatietechnologie), Den Haag: Sdu Uitgevers 2019, p. 15-28.
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.
B.J. Koops & J.J. Oerlemans, 'Materieel strafrecht en ICT', in: B.J. Koops & J.J. Oerlemans (red.), *Strafrecht en ICT* (Monografieën recht en informatietechnologie), Den Haag: Sdu Uitgevers 2019, p. 29-116.

90. Zie o.a. de Kamerbrief over de integrale aanpak van cybercriminaliteit van 18 april 2018 en de Kamerbrief over de aanpak van cybercriminaliteit van 12 juni 2019.
91. Schermer & Oerlemans 2020; Galic 2021.

B.J. Koops & J.J. Oerlemans, 'Formeel strafrecht en ICT', in: B.J. Koops & J.J. Oerlemans (red.), *Strafrecht en ICT* (Monografieën recht en informatietechnologie), Den Haag: Sdu Uitgevers 2019, p. 117-208.
B.J. Koops & M.H.M. Schellekens, 'Computercriminaliteit II: de boeven zijn er – nu de wet weer', *NJB* 1999, p. 1764-1772.
E.W. Kruisbergen & D. de Jong, 'Undercoveroperaties: een noodzakelijk kwaad? Heden, verleden en toekomst van een omstreden opsporingsmiddel', *JV* 2012, afl. 3, p. 50-67.
J.J. Oerlemans, 'Het conceptwetsvoorstel versterking bestrijding computercriminaliteit nader bezien', *Tijdschrift voor Internetrecht* 2010, afl. 5, p. 148-152.
J.J. Oerlemans, *Investigating Cybercrime* (diss. Leiden), Amsterdam: Amsterdam University Press 2017.
J.J. Oerlemans, 'De Wet computercriminaliteit III: meer handhaving op internet', *Strafblad* 2017/49, p. 350-359.
J.J. Oerlemans, ''Facebookvrienden worden met de verdachte': Over undercoverbevoegdheden op internet', *JV* 2018, afl. 5, p. 83-99.
J.J. Oerlemans, 'Jurisdictie en grensoverschrijdende digitale opsporing', in: B.J. Koops & J.J. Oerlemans (red.), *Strafrecht en ICT* (Monografieën recht en informatietechnologie), Den Haag: Sdu Uitgevers 2019, p. 209-232.
J.J. Oerlemans, 'Cybercriminaliteit en opsporing', in: W. van der Wagen, J.J. Oerlemans & M. Weulen Kranenbarg (red.), *Basisboek Cybercriminaliteit. Een criminologisch overzicht voor studie en praktijk*, Den Haag: Boom criminologie 2020, p. 195-258.
J.J. Oerlemans, 'Cybercrimeverdrag', in: J.W. Ouwerkerk & P.A.M. Verrest (red.), *Tekst & Commentaar Internationaal Strafrecht*, Deventer: Wolters Kluwer 2021.
A. Postma, 'Doorzoeking ter vastlegging van gegevens', in: *Handboek Strafzaken* (online, actueel tot 1 november 2020).
S. Royer & J.J. Oerlemans, 'Naar een nieuwe regeling voor beslag op gegevensdragers', *Computerrecht* 2017, afl. 5, p. 277-284.
D.A.G. van Toor, 'De vergrendelde smartphone als object van strafvorderlijk onderzoek', *Computerrecht* 2017, afl. 1, p. 3-11.
B.W. Schermer & J.J. Oerlemans, 'AI, strafrecht en het recht op een eerlijk proces', *Computerrecht* 2020, afl. 1, p. 14-21.
M.N. Schmitt (ed.), *Tallinn manual 2.0 on the international law applicable to cyber operations*, Cambridge: Cambridge University Press 2017.
L.A.R. Siemerink, 'Bob logt in: infiltratie en pseudokoop op internet', *Computerrecht* 2000, afl. 3, p. 141-147.
S.Ph. Stol, E.R. Leukfeldt & H. Klap, 'Cybercrime en politie', *JV* 2012, afl. 1, p. 25-39.
T. van der Vorst e.a., *Mogelijkheden voor identificatie op internet op basis van IP-adres*, Den Haag: WODC 2019.
R.S. van Wegberg & T. Verburgh, 'Lost in the dream? Measuring the effects of Operation Bayonet on vendors migrating to Dream Market', *Evolution of the Darknet Workshop at the Web Science Conference* (WebSci 18), Amsterdam 2018.