Artikel

Executieve jurisdictie: het (grote) obstakel in grensoverschrijdende opsporingsonderzoeken naar (gebruikers van) cryptoaanbieders?

Mr. L.W. Verbeek en mr. T. Beekhuis*

1. Introductie

'Het grootste rechercheonderzoek ooit', zo duidde Andy Kraag, hoofd van de Dienst Landelijke Recherche, in juli 2020 het opsporingsonderzoek naar (gebruikers van) het bedrijf *EncroChat*.[1] Dit bedrijf verkocht internationaal cryptotelefoons: toestellen waarmee – door middel van een op de toestellen aanwezige applicatie – versleutelde berichten en beeldmateriaal konden worden verstuurd en ontvangen.[2] Door deze versleuteling (oftewel encryptie) worden leesbare data omgevormd in een wiskundig algoritme. De data zijn daardoor niet inzichtelijk voor derden.[3]

Tijdens het opsporingsonderzoek naar EncroChat – in Nederland bekend onder de naam '26Lemont' – hebben de Nederlandse (en Franse) opsporingsautoriteiten het voor elkaar gekregen om *live* mee te lezen met berichten van duizenden vermoedelijk overwegend criminele EncroChat-gebruikers, terwijl deze gebruikers zich vanwege de op de telefoons aanwezige encryptie onbespied waanden.[4] Operatie 26Lemont resulteerde in een enorme berg aan belastende informatie, waarover de eerdergenoemde Kraag het volgende stelde: 'Meestal krijgen we een zaak waarbij we bewijs moeten zoeken. Nu hadden we het bewijs, maar moesten we vol aan de bak om uit te zoeken hoe de zaak zat. Waar die criminelen zaten, wie het waren.'[5] De operatie vormt dan ook een *gamechanger* op het gebied van strafrechtelijke opsporing. Door de inzet van de expertise van data-analisten en cyberspecialisten hebben de autoriteiten op een andere wijze opgespoord dan traditioneel het geval is en hebben zij beter zicht gekregen op de onderwereld.[6] Alleen al in Nederland had de operatie op 2 juli 2020 reeds geleid tot 'de arrestatie van meer dan 100 verdachten, de inbeslagneming van verdovende middelen (meer dan 8.000 kilo cocaïne en 1.200 kilo crystal meth), de ontmanteling van 19 synthetische drugslaboratoria, de inbeslagneming van tientallen (automatische) vuurwapens, dure horloges en 25 auto's, waaronder voertuigen met verborgen compartimenten, en bijna EUR 20 miljoen aan contant geld.'[7] Gezien deze 'beslaglijst' lijkt

* Mr. L.W. Verbeek is medewerker bij het wetenschappelijk bureau van de Hoge Raad der Nederlanden. Deze bijdrage is geschreven op persoonlijke titel. Mr. T. Beekhuis is verbonden als promovenda aan het Willem Pompe Instituut voor Strafrechtswetenschappen en het Utrecht Centre for Accountability and Liability Law (Ucall) van de Universiteit Utrecht. De auteurs danken prof. dr. J.J. Oerlemans voor zijn waardevolle commentaar op een eerdere versie van deze bijdrage.

1 A. Mees & R. Andringa, 'Grootste recherche-onderzoek EncroChat: 'Als een spannende film'', *NOS* 2 juli 2020.

2 Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.2.

3 *Kamerstukken II* 2015/16, 34372, nr. 3, p. 7.

4 P. Vugts, 'De miljoenen berichten uit versleutelingsapp EncroChat: een blauwdruk van de onderwereld', *AD* 11 juli 2020.

5 Vugts 11 juli 2020.

6 Vugts 11 juli 2020.

7 www.eurojust.europa.eu/sites/default/files/2020-07/2020-07-02_joint-Eurojust-Europol-press-release_NL.pdf, laatst geraadpleegd op 14 december 2021.

doi: 10.5553/TBSenH/229567002022008002005

operatie 26Lemont een groot succes: de internationaal opererende onderwereld is veelal een onontgonnen terrein voor opsporingsautoriteiten, maar door operatie 26Lemont hebben de opsporingsautoriteiten een inkijkje gekregen in deze onderwereld en door hun handhavend optreden zijn verschillende internationaal opererende criminele organisaties veel mankracht en middelen verloren.

Wereldwijd worden landen in toenemende mate geraakt door georganiseerde misdaadgroepen die niet alleen alomtegenwoordig zijn, maar ook een groot aanpassingsvermogen hebben.[8] Zij gebruiken geavanceerde technologieën voor hun criminele activiteiten.[9] Versleuteling van communicatie speelt hierbij steeds vaker een (cruciale) rol[10] en vormt een grote uitdaging voor de opsporingsautoriteiten.[11] Immers, naast het feit dat de inhoud van de berichtgeving door encryptie voor derden wordt verborgen, is het veelal onduidelijk welke gebruiker achter de berichtgeving zit en waar ter wereld de gegevens staan opgeslagen. Bovendien kan een gebruiker zijn fysieke locatie via het internet eenvoudig versluieren. Het onderzoek naar deze misdaadgroepen is daarnaast complex omdat strafbare feiten steeds vaker een grensoverschrijdende dimensie krijgen aangezien de samenleving tegenwoordig sterk internationaal georiënteerd is.[12] Uit de memorie van toelichting behorende bij de Wijziging van het Wetboek van Strafvordering en enkele andere wetten met het oog op het moderniseren van de regeling van internationale samenwerking in strafzaken (herziening regeling internationale samenwerking in strafzaken) blijkt bijvoorbeeld dat in vrijwel alle opsporingsonderzoeken naar zware en georganiseerde criminaliteit ook opsporingsactiviteiten (moeten) worden verricht in het buitenland.[13] Omdat het voor autoriteiten niet zonder meer mogelijk is om buiten de eigen landsgrenzen op te sporen, is in geval van grensoverschrijdende criminaliteit de hulp van buitenlandse autoriteiten noodzakelijk. Efficiënte internationale en/of Europese samenwerking is daartoe essentieel.[14]

Operatie 26Lemont betreft slechts een voorbeeld van dergelijke internationale samenwerking. De afgelopen jaren werd al vaker een door criminelen gebruikt communicatienetwerk ontmaskerd. Zo werden door de Nederlandse autoriteiten door middel van rechtshulpverzoeken aan Canada en Costa Rica geautomatiseerde netwerken van aanbieders van respectievelijk *Ennetcom*[15] (2016) en *PGPSafe*[16] (2017) ontsleuteld waardoor zeer belastende berichten konden worden ontcijferd en verkregen zij met behulp van de Britse autoriteiten toegang tot de applicatie *IronChat* (2017)[17]. Drie jaar later onderschepten de Nederlandse autoriteiten, in samenwerking met Belgische autoriteiten, één miljard berichten van 's werelds grootste aanbieder van cryptotelefoons, *SKY ECC*.[18] Ook hebben zij waarschijnlijk een sleutelrol gespeeld in de in 2021 door Europol onthulde politieoperatie *AN0M/Operation Trojan Shield*[19] waaraan meer dan zestien landen samenwerkten. Wereldwijd hebben de operaties inmiddels tot tientallen opsporingsonderzoeken en strafzaken geleid.[20] De verwachting is dat dit aantal enkel zal toenemen, nu nog niet alle data zijn geanalyseerd. In het nieuws verschijnen hierover regelmatig berichten.[21]

Kortom, voornoemde politieoperaties doen vermoeden dat het verzamelen, ontsleutelen en analyseren van digitale berichtgeving *het* wapen is in de strijd tegen de georganiseerde misdaad; zodra de encryptie is gekraakt, hebben de opsporingsautoriteiten goud in handen.[22]

Alhoewel opsporingsautoriteiten door internationale samenwerking en de inzet van grensoverschrijdende opsporingsbevoegdheden inderdaad een belangrijke troef in handen hebben om de georganiseerde misdaad een halt toe te roepen, hebben deze internationale politieoperaties ook een keerzijde. Zij kunnen opsporingsauto-

8 www.eurojust.europa.eu/sites/default/files/2020-07/2020-07-02_joint-Eurojust-Europol-press-release_NL.pdf, laatst geraadpleegd op 14 december 2021.
9 www.eurojust.europa.eu/sites/default/files/2020-07/2020-07-02_joint-Eurojust-Europol-press-release_NL.pdf, laatst geraadpleegd op 14 december 2021.
10 www.eurojust.europa.eu/sites/default/files/2020-07/2020-07-02_joint-Eurojust-Europol-press-release_NL.pdf, laatst geraadpleegd op 14 december 2021.
11 *Kamerstukken II* 2015/16, 34372, nr. 3, p. 7.
12 *Kamerstukken II* 2015/16, 34493, nr. 3, p. 4.
13 *Kamerstukken II* 2015/16, 34493, nr. 3, p. 4.
14 *Kamerstukken II* 2015/16, 34493, nr. 3, p. 4.
15 P. Vugts, 'Miljoenen berichten ontcijferd over liquidaties', *Het Parool* 30 januari 2019. De oprichters van Ennetcom zijn in Nederland inmiddels veroordeeld. Zie Rb. Rotterdam 21 september 2021, ECLI:NL:RBROT:2021:9085, 9086 & 9087.
16 Vugts 30 januari 2019.
17 'Doorbraak in onderscheppen van cryptocommunicatie', *OM* 6 november 2018, www.om.nl/actueel/nieuws/2018/11/06/doorbraak-in-onderscheppen-van-cryptocommunicatie, laatst geraadpleegd op 2 februari 2022; J.J. Oerlemans 2021, 'Meer duidelijkheid over IronChat-operatie', www.jjoerlemans.com/2021/12/30/meer-duidelijkheid-over-ironchat-operatie/, laatst geraadpleegd op 2 februari 2022.
18 W. Laumans, 'Justitie hoopt op bewijs uit Sky-Hack in moordzaak Derk Wiersum', *Het Parool* 23 april 2021; 'Nieuwe klap voor georganiseerde misdaad', Politie.nl 9 maart 2021.
19 www.europol.europa.eu/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication, laatst geraadpleegd op 13 december 2021. Zie hierover ook C.M. Taylor Parkins-Ozephius, I.N. De Wit, D.A.G. van Toor & T. Beekhuis, 'De politie als winkelier van smartphones met 'versleutelde' communicatiemiddelen: de inzet van de opsporingshandelingen getoetst aan het legaliteitsbeginsel', *TBS&H* 2021, p. 322-333.
20 R. Andringa, 'Al tientallen strafzaken na EncroChat-hack en het einde is nog niet inzicht', *NOS* 18 december 2020; P. Vugts & W. Laumans, '49 arrestaties in Nederland dankzij internationale afluisteroperatie, 800 arrestaties wereldwijd', *Het Parool* 8 juni 2021; W. Thijssen, 'Politie kraakt criminele communicatiedienst: 'Hele onderwereld op een presenteerblaadje'', *Volkskrant* 9 maart 2021. Enkele voorbeelden van Nederlandse strafzaken zijn: het lopende liquidatieproces 'Marengo', de veroordeling voor wapenbezit en voorbereiding van moord in de strafzaak '26Koper', en de strafzaak tegen verdachten van 'martelkamers' in Noord-Brabant als gevolg van het internationaal rechercheonderzoek '26Lemont'.
21 Andringa 18 december 2020; Driessen & Meeus 9 maart 2021; 'Politie ontdekt crystal meth ter waarde van 1 miljoen in Wormer', *Het Parool* 28 juli 2021; Y. Tieleman, 'Politie en justitie kraken chatdienst gebruikt door criminelen: miljoenen berichten live meegelezen', *AD* 2 juli 2020.
22 C. Driessen & J. Meeus, 'Encryptie is niet meer weg te denken uit het criminele milieu', *NRC* 9 maart 2021.

riteiten namelijk voor complexe juridische vraagstukken stellen, in het bijzonder wanneer de autoriteiten willen opsporen (lees: rechtsmacht willen uitoefenen) buiten de territoriale grenzen van het eigen grondgebied. Rechtsmacht, ook wel 'jurisdictie' genoemd, omvat 'de bevoegdheid van staten om wetten te maken, toe te passen en uit te voeren met betrekking tot het gedrag van personen, binnen de grenzen van het internationale recht'.[23] Jurisdictie wordt onderverdeeld in wetgevende (de bevoegdheid tot het stellen van regels in wetgeving en jurisprudentie)[24] en uitvoerende (of executieve) jurisdictie (de bevoegdheid om nakoming van wetten te verzekeren; hieronder valt ook het vergaren van bewijsmateriaal door opsporingsdiensten)[25].

Executieve jurisdictie wordt gezien als het grootste obstakel bij grensoverschrijdende opsporingsonderzoeken.[26] Staten zijn bij het uitoefenen van executieve jurisdictie immers – vanwege het territorialiteitsbeginsel –[27] gebonden aan het eigen territorium, terwijl het onderzoek naar de georganiseerde misdaad een internationaal karakter kent. Het probleem dat hieruit voortvloeit, namelijk dat opsporingsautoriteiten op achterstand kunnen worden gezet wanneer criminaliteit grensoverschrijdend wordt,[28] is dan ook geen illusoir probleem.

Bezien tegen deze achtergrond rijst de vraag op welke wijze opsporingsautoriteiten het grensoverschrijdend opsporingsonderzoek naar (gebruikers van) cryptoaanbieders kunnen uitvoeren. Indien blijkt dat de thans bestaande onderzoeksmogelijkheden – gelet op hetgeen hiervoor is overwogen omtrent executieve jurisdictie – onvoldoende zijn om dit opsporingsonderzoek zo efficient mogelijk te (doen) verrichten, dan dringt de vraag zich op hoe opsporingsautoriteiten dit opsporingsonderzoek zouden kunnen uitvoeren zodat dergelijke criminaliteit eenvoudiger een halt kan worden toegeroepen. Wij beperken ons in deze bijdrage tot het grensoverschrijdende opsporingsonderzoek naar (gebruikers van) cryptoaanbieders dat plaatsvindt binnen de grenzen van de Europese Unie (hierna: EU). In de EU zijn verschillende mogelijkheden ontwikkeld om grensoverschrijdend op te sporen. Twee van deze mogelijkheden, zijnde het rechtshulpverzoek en het oprichten van een *Joint Investigation Team* (hierna: JIT), staan in deze bijdrage centraal. We gaan ervan uit dat Nederland de verzoekende staat is.

De opbouw van deze bijdrage is als volgt. In paragraaf 2 gaan wij in op het verzoeken van rechtshulp aan een EU-lidstaat. In paragraaf 3 lichten wij toe hoe een JIT uitkomst kan bieden in een grensoverschrijdend opsporingsonderzoek naar (gebruikers van) cryptoaanbieders. Aangezien tijdens de EncroChat-operatie een JIT is ingesteld, wordt in deze paragraaf tevens aandacht besteed aan de rol die het JIT bij deze operatie heeft gespeeld. In paragraaf 4 besluiten wij onze bijdrage met enkele afrondende beschouwingen.[29]

2. Executieve jurisdictie en het rechtshulpverzoek

Zoals eerder is opgemerkt, is executieve jurisdictie tijdens het grensoverschrijdend opsporingsonderzoek naar (gebruikers van) cryptoaanbieders problematisch vanwege het territorialiteitsbeginsel. Dit beginsel houdt in dat staten bij het uitoefenen van executieve rechtsmacht zijn gebonden aan het eigen territorium.[30] Dit vloeit onder meer voort uit een door het Internationaal Gerechtshof (destijds *the Permanent Court of International Justice*) (hierna: PCIJ) – reeds in 1927 – gewezen arrest, *Lotus* t. *Turkije*.[31] In dat arrest overwoog het PCIJ met betrekking tot het kunnen uitvoeren van rechtsmacht buiten de grenzen van het eigen territorium:

> '(..) *the first and foremost restriction imposed by international law upon a State is that-failing the existence of a permissive rule to the contrary-it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention*.'[32]

Aan deze territoriale begrenzing ligt het soevereiniteitsbeginsel ten grondslag: dit beginsel begrenst de macht van de overheid (de soeverein) tot het gebied waarover zij macht mag uitoefenen.[33] Het territorialiteitsbeginsel voorkomt dat staten door middel van grensoverschrijdende opsporing inbreuk maken op de

23 J.J. Oerlemans, 'Cybercriminaliteit en opsporing', in: W. van der Wagen, J.J. Oerlemans & M. Weulen Kranenbarg (red.), *Basisboek Cybercriminaliteit. Een criminologisch overzicht van studie en praktijk*, Den Haag: Boom criminologie 2020, p. 210; J.J. Oerlemans, 'Jurisdictie en grensoverschrijdende digitale opsporing', in: B.J. Koops & J.J. Oerlemans, *Strafrecht en ICT; Monografieën recht en informatietechnologie*, Den Haag: SDU Uitgevers 2018, p. 210. Soms wordt ook een driedeling gehanteerd, waarin ook rechtsprekende rechtsmacht als apart onderdeel wordt genoemd. Zie bijv. R. van Elst 2015, 'Rechtsmacht', in: E. van Sliedregt & R. van Elst (red,), Handboek Internationaal strafrecht. Internationaal en Europees strafrecht vanuit Nederlands perspectief, Deventer: Wolters Kluwer 2015, p. 76. In de gehanteerde tweedeling wordt rechtsprekende rechtsmacht als onderdeel gezien van de wetgevende rechtsmacht.

24 Van Elst 2015, p. 76.

25 Oerlemans 2018, p. 213.

26 Oerlemans 2020, p. 233.

27 W. Geelhoed & J.W. Ouwerkerk, 'De betekenis van territorialiteit in Europese strafrechtelijke handhaving', *Strafblad* 2019/4, p. 13-20.

28 Voor een uitgebreidere toelichting op dit probleem verwijzen wij naar par. 2.4.

29 De inhoudelijke bewerking van deze bijdrage is afgesloten op 9 februari 2022. Na deze datum ter beschikking gekomen informatie is door ons niet verwerkt en valt buiten het bestek van deze bijdrage.

30 Geelhoed & Ouwerkerk, *Strafblad* 2019/4, p. 13-20.

31 PCIJ, "S.S. Lotus" (Frankrijk t. Turkije), 1927, PCIJ Series A, No. 10.

32 PCIJ, "S.S. Lotus" (Frankrijk t. Turkije), 1927, PCIJ Series A, No. 10, p. 18-19.

33 Volgens Hirsch Ballin is het soevereiniteitsbeginsel 'het belangrijkste beginsel dat ten grondslag ligt aan het internationale recht en de relaties tussen staten'. Zie M. Hirsch Ballin, 'De rol van grenzen bij opsporing: grenzeloze inzet van opsporingsbevoegdheden', *Ars Aequi* 2018, p. 462.

doi: 10.5553/TBSenH/229567002022008002005

soevereiniteit van een andere staat.[34] Opsporing is immers een exclusieve taak van een staat en buitenlandse autoriteiten mogen zich hierin dan ook (behoudens uitzonderingen) niet mengen.[35] Bovendien zorgt het beginsel ervoor dat staten aan individuen die zich op haar grondgebied bevinden bescherming kunnen bieden tegen het optreden van een andere soevereine staat.[36] Zij heeft dus ook een rechtsbeschermende functie.

Alhoewel het territorialiteitsbeginsel de macht van de autoriteiten om opsporingsactiviteiten te verrichten buiten het eigen grondgebied beperkt,[37] is dit beginsel niet absoluut. Een aangezochte (ook wel uitvoerende) staat kan een verzoekende (of uitvaardigende) staat[38] toestemming verlenen om onderzoekshandelingen te verrichten op het grondgebied van de aangezochte staat. Een rechtshulpverzoek vormt daarbij het uitgangspunt.[39] Het is een staat dus niet toegestaan om op eigen houtje (unilateraal) grensoverschrijdend te opereren. Rechtshulp strekt ertoe de samenwerking tussen staten te vergemakkelijken en te stroomlijnen bij bewijsvergaring op het grondgebied van een andere staat.[40]

Een aangezochte staat kan op verschillende manieren rechtshulp verlenen: (1) de aangezochte staat verleent de autoriteiten van de verzoekende staat toestemming om fysiek op te sporen op het grondgebied van de aangezochte staat; (2) de aangezochte staat verricht zelf de opsporingshandelingen op het eigen grondgebied waarna de gevraagde informatie of gegevens worden gevorderd, verkregen en geleverd aan de verzoekende staat; en (3) de verzoekende staat zet (digitale) opsporingsbevoegdheden in vanaf haar eigen grondgebied ten aanzien van personen of gegevens die zich bevinden op het grondgebied van de aangezochte staat.[41] In het kader van het grensoverschrijdende onderzoek naar (gebruikers van) cryptoaanbieders liggen de tweede en derde opsporingsvorm het meest voor de hand.

Wanneer Nederland een andere staat om rechtshulp verzoekt, dient dit verzoek een juridische basis te hebben op grond van internationaal gewoonterecht of een verdrag waarop de opsporing kan worden gebaseerd.[42] Nederland is partij bij verschillende rechtshulpverdragen.[43] Op basis van deze verdragen hebben Nederlandse opsporingsautoriteiten onder de daarin genoemde voorwaarden de mogelijkheid om op te treden buiten het eigen grondgebied. In Europees verband is het Europees Onderzoeksbevel (hierna: EOB) wat betreft grensoverschrijdende opsporing het meest relevant.[44]

Het EOB (zijnde een rechtshulpverzoek) kan worden uitgevaardigd door een EU-lidstaat zodat in een andere lidstaat bewijsmateriaal wordt verzameld of bewijs wordt opgevraagd dat in die staat reeds voorhanden is: de zogeheten 'kleine rechtshulp' verloopt tussen de EU-lidstaten vrijwel altijd op basis van het EOB.[45] Een EOB is gebaseerd op het beginsel van wederzijdse erkenning: in principe moet een lidstaat binnen specifiek in de EOB-richtlijn vastgelegde termijnen[46] aan een EOB gehoor geven, tenzij specifieke weigeringsgronden (zoals wanneer het uitvoeren van een EOB in strijd is met het *ne bis in idem*-beginsel)[47] zich voordoen.[48] De verzoekende staat geeft in het EOB onder meer aan welke opsporingshandeling in en/of door de aangezochte staat dient te worden verricht.[49] Wanneer de gevraagde onderzoekshandeling niet bestaat in het recht van de aangezochte staat of wanneer de gevraagde handeling niet kan worden uitgevoerd in een vergelijkbare nationale zaak, wordt de aangezochte staat in beginsel geacht een soortgelijke handeling te verrichten.[50] Na afloop worden de resultaten van het uitgevoerde EOB zo spoedig mogelijk aan de verzoekende staat ter beschikking gesteld.[51] Indien het voor de aangezochte staat niet mogelijk is om uitvoering te geven aan het EOB (omdat geen soortgelijke handeling kan worden verricht) dient zij de verzoekende staat hiervan in kennis te stellen.[52] Een voorbeeld van een politieoperatie waarin de Nederland-

34 Oerlemans 2018, p. 227; *Kamerstukken II* 2015/16, 34372, nr. 3, p. 45. Zie ook C. Ryngaert, *Unilateral Jurisdiction and Global Values*, Den Haag: Eleven International Publishing 2015, p. 23 e.v.

35 Vgl. Oerlemans 2018, p 214.

36 B. J. Koops, C. Conings & F. Verbruggen, *Zoeken in computers naar Nederlands en Belgisch recht. Welke plaats hebben 'digitale plaatsen' in de systematiek van opsporingsbevoegdheden? (Preadviezen voor de Nederlands-Vlaamse Vereniging voor Strafrecht)*, Oisterwijk: Wolf Legal Publishers 2016, p. 141.

37 Hirsch Ballin, *AA* 2018, p. 463.

38 Omwille van de leesbaarheid spreken wij hierna van aangezochte en verzoekende staten.

39 Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv, par. 1.2.

40 Hirsch Ballin, *AA* 2018, p. 463.

41 Hirsch Ballin, *AA* 2018, p. 463-464.

42 Oerlemans 2020, p. 234.

43 Bijvoorbeeld het Europees Verdrag aangaande de wederzijdse rechtshulp in strafzaken (1959), de Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie (2000) en het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (2001) (Cybercrimeverdrag). Dit laatste verdrag vormt een aanvulling op de reeds bestaande toepasselijke multilaterale of bilaterale verdragen of regelingen tussen partijen.

44 Richtlijn 2014/41/EU van het Europees Parlement en de Raad van 3 april 2014 betreffende het Europees onderzoeksbevel in strafzaken (hierna: EOB-richtlijn). In Nederland is deze richtlijn geïmplementeerd in titel 4 van Boek 5 Sv. De EOB-richtlijn vervangt namelijk de vergelijkbare bepalingen die in bepaalde andere verdragen waren opgenomen, zoals die in het Europees Verdrag aangaande de wederzijdse rechtshulp in strafzaken (1959). Zie art. 34 en 35 EOB-richtlijn.

45 Art. 1 lid 1 EOB-richtlijn; Verrest, *T&C Strafvordering*, commentaar op titel 4 Sv, aant. 2. Art. 5.4.1 lid 1 Sv: het EOB kan niet worden gezonden aan Denemarken of Ierland. Zie ook Preambule, par. 6 EOB-richtlijn. Zie voor uitzonderingen: Verrest, *T&C Strafvordering*, commentaar op titel 4 Sv, aant. 1. Voor zover het EOB niet voorziet in samenwerking, moet worden teruggevallen op andere internationale instrumenten. Het EOB geldt dus niet voor in par. 3 te bespreken gemeenschappelijke onderzoeksteams (behoudens met betrekking tot het bepaalde in art. 13 lid 8 Overeenkomst, door de Raad vastgesteld overeenkomstig artikel 34 van het Verdrag betreffende de Europese Unie, betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie (hierna EU Rechtshulpovereenkomst). Zie art. 3 EOB-richtlijn.

46 Art. 12 EOB-richtlijn.

47 Art. 11 EOB-richtlijn en art. 5.4.4. Sv.

48 Art. 9 EOB-richtlijn.

49 Zie art. 5 lid 1 onder e jo. lid 3 jo. bijlage A EOB-richtlijn.

50 Art. 10 lid 1 EOB-richtlijn. Zie over de voorwaarden en uitzonderingen art. 10 en 11 EOB-richtlijn.

51 Art. 13 EOB-richtlijn.

52 Art. 10 lid 5 EOB-richtlijn.

se autoriteiten een EOB hebben uitgevaardigd, is het onderzoek naar de versleutelde chatapplicatie IronChat. Op basis van het EOB verkregen Nederlandse opsporingsautoriteiten van de Britse autoriteiten een kopie van de inhoud van de server – die was gelokaliseerd in het Verenigd Koninkrijk – waarvan IronChat gebruik maakte.[53] In 2017 slaagden de autoriteiten erin de applicatie te ontsleutelen.[54]

Zoals gezegd geeft de verzoekende staat aan welke opsporingshandeling in en/of door de aangezochte staat dient te worden verricht. In het kader van het onderzoek naar (gebruikers van) cryptoaanbieders springt de hackbevoegdheid (geregeld in de artt. 126nba, 126uba en 126zpa Sv) daarbij het meest in het oog. Deze bevoegdheid wordt uitgewerkt in de Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex artikel 126nba Sv (hierna: de Aanwijzing).[55] Op grond van deze Aanwijzing hebben opsporingsautoriteiten de mogelijkheid om op afstand en heimelijk een geautomatiseerd werk (hierna: server) binnen te dringen met het oog op het verrichten van bepaalde onderzoekshandelingen. Wanneer de autoriteiten een server willen hacken die zich buiten de territoriale grenzen van de eigen staat bevindt, verzoeken zij de aangezochte staat om rechtshulp. De aangezochte staat kan vervolgens rechtshulp verlenen op een van de eerder in deze paragraaf beschreven drie manieren.

Alhoewel het thans bestaande rechtshulpkader voor de Nederlandse autoriteiten mogelijkheden biedt om op buitenlands grondgebied op te treden, brengt het kader in geval van grensoverschrijdende opsporingsonderzoeken naar (gebruikers van) cryptoaanbieders de nodige complexiteit met zich. Het is immers (op voorhand) niet altijd vast te stellen waar in de EU de te hacken server zich bevindt en aan welke staat of staten om rechtshulp moet worden verzocht. In feite kunnen zich gedurende het onderzoek naar (gebruikers van) cryptoaanbieders drie scenario's voordoen: (1) voorafgaand aan de inzet van (digitale) opsporingsbevoegdheden is de locatie – zijnde een locatie buiten Nederland – bekend; (2) in eerste instantie is de locatie niet bekend, maar gedurende het opsporingsonderzoek wordt bekend waar de gegevens staan opgeslagen; en (3) de locatie van de server blijft onbekend. In de volgende subparagrafen lichten wij ieder scenario kort toe.

2.1 Scenario 1-gevallen: de locatie van de gegevens is bekend

In scenario 1-gevallen wordt voorafgaand aan de inzet van opsporingsbevoegdheden door de Nederlandse autoriteiten (zijnde de officier van justitie) om rechtshulp verzocht aan een andere staat.[56] De aangezochte staat wordt gevraagd de gegevens te vorderen en/of (zelfstandig) veilig te stellen op basis van de daarvoor in de aangezochte staat geldende wettelijke grondslagen.[57] De officier van justitie kan de autoriteiten van de aangezochte staat ook toestemming vragen om de gegevens zelf veilig te mogen stellen.[58] In de aanvraag vermeldt de officier van justitie de locatie van de gegevens.[59] Alhoewel voorafgaande toestemming (in mondelinge of schriftelijke vorm) het uitgangspunt vormt, zijn blijkens de Aanwijzing uitzonderingen mogelijk, bijvoorbeeld wanneer de reactie van de aangezochte staat op het rechtshulpverzoek niet kan worden afgewacht of wanneer er geen reactie te verwachten is. De opsporingsautoriteiten kunnen dan besluiten zonder voorafgaande toestemming op te treden. Van de autoriteiten wordt verlangd dat zij hierbij een zorgvuldige afweging maken tussen het belang van het onderzoek en de mogelijke inbreuk op de soevereiniteit van de andere staat.[60] In deze afweging spelen meerdere factoren een rol waaronder: de ernst of onmiddellijkheid van de gevolgen van de aanval of dreiging, aard en ernst van het strafbare feit, vluchtigheid van de gegevens of de informatie die wordt gezocht, mate van betrokkenheid van de Nederlandse rechtsorde, aard van de te verrichten opsporingshandelingen en de risico's van het geautomatiseerde netwerk (waaronder verstaan technische risico's of inschatting van de mogelijke gevaren voor derden).[61]

2.2 Scenario 2-gevallen: de locatie van de gegevens wordt bekend

Wanneer op voorhand onbekend is waar de gegevens staan opgeslagen, is niet duidelijk aan welke staat om rechtshulp moet worden verzocht. Voorafgaande toestemming is dan niet mogelijk. Ook in deze gevallen dient te worden afgewogen of de inzet van opsporingsbevoegdheden die effect sorteren buiten het eigen grondgebied desondanks toelaatbaar wordt geacht.[62] In deze afweging wordt rekening gehouden met de onder scenario 1 besproken factoren. Indien de uitkomst van

53 J.J. Oerlemans 2021, 'Meer duidelijkheid over IronChat-operatie', www.jjoerlemans.com/2021/12/30/meer-duidelijkheid-over-ironchat-operatie/, laatst geraadpleegd op 2 februari 2022. In 2020 is er enige rechtspraak gepubliceerd waarin het verloop van de IronChat-operatie wordt toegelicht, zie bijv. Rb. Overijssel 23 april 2020, ECLI:NL:RBOV:2020:1563; ECLI:NL:RBOV:2020:1587; ECLI:NL:RBOV:2020:1592.

54 'Doorbraak in onderscheppen van cryptocommunicatie', *OM* 6 november 2018, www.om.nl/actueel/nieuws/2018/11/06/doorbraak-in-onderscheppen-van-cryptocommunicatie, laatst geraadpleegd op 2 februari 2022.

55 *Kamerstukken II* 2015/16, 34372, nr. 3, p. 49; *Kamerstukken II* 2015/16, 34493, nr. 3, p. 8. Blijkens de Aanwijzing voorziet art. 539a Sv in de bevoegdheid van opsporingsautoriteiten om ook buiten het eigen grondgebied op te treden.

56 Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv, par. 1.3.

57 Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv, par. 1.3.

58 Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv, par. 1.3.

59 Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv, par. 1.3.

60 Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv, par. 2.1.

61 *Kamerstukken II* 2015/16, 34372, nr. 3, p. 48; Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv, par. 2.4.

62 Volledigheidshalve merken wij op dat vanwege het feit dat de locatie niet bekend is, de server ook in Nederland kan staan. Mocht dat gedurende het onderzoek zo blijken te zijn, dan moet de inzet van de hackbevoegdheid conform Nederlands recht worden uitgevoerd. Deze situatie laten wij verder buiten beschouwing.

doi: 10.5553/TBSenH/229567002022008002005

deze afweging rechtvaardigt dat onderzoekshandelingen worden ingezet zonder voorafgaande toestemming van het land waar de gegevens feitelijk staan opgeslagen, maakt de officier van justitie aan de rechter-commissaris kenbaar wat eventueel bekend is over de locatie van de gegevens.[63] Indien de server gedurende het onderzoek toch wordt gelokaliseerd, wordt zo snel mogelijk alsnog om toestemming gevraagd aan het desbetreffende land.[64] Daarbij wordt verantwoording afgelegd over de tot dan toe uitgevoerde onderzoekshandelingen.[65] In afwachting van een reactie op dit verzoek hebben autoriteiten de mogelijkheid om de opsporing te staken of de bevoegdheden te voltooien.

2.3 Scenario 3-gevallen: de locatie is en blijft onbekend

Indien onduidelijk is en blijft waar de server zich bevindt, zijn de autoriteiten verplicht te beoordelen of de server alsnog met 'redelijke inspanning' kan worden gelokaliseerd. Hierbij komt betekenis toe aan de concrete omstandigheden van het geval. In de Aanwijzing staat hieromtrent het volgende: 'Bij een redelijke inspanning staan de tijd en moeite voor het vaststellen van een specifieke geografische locatie in een reële verhouding tot de noodzakelijkheid van onverwijld optreden, de tijdsdruk en de doorlooptijd van het onderzoek.'[66] Indien na redelijke inspanning geen locatie wordt vastgesteld, ontbreken concrete handvatten voor het vragen van internationale rechtshulp. Ook in dat geval geldt dat – na een zorgvuldige afweging tussen het belang van het onderzoek en de soevereiniteit van de onbekende staat waarin de gegevens feitelijk staan opgeslagen – kan worden bepaald dat de inzet van de onderzoekshandelingen desondanks gerechtvaardigd is. De autoriteiten gaan er dan vanuit dat de gegevens op Nederlands grondgebied staan opgeslagen, zodat de Nederlandse rechtsregels worden toegepast.[67]

2.4 Tussenconclusie

Op basis van de hiervoor besproken scenario's kan de conclusie worden getrokken dat rechtshulp in het grensoverschrijdend onderzoek naar (gebruikers van) cryptoaanbieders het uitgangspunt vormt. Tegelijkertijd blijkt dat rechtshulp niet steeds uitkomst kan bieden. Bij het thans bestaande rechtshulpkader kunnen daarnaast nog enkele kritische kanttekeningen worden geplaatst.

Allereerst is inmiddels door meerdere auteurs onderschreven dat rechtshulpverzoeken met de nodige beperkingen kampen.[68] Zo verloopt het verkrijgen van toestemming vaak onnodig traag.[69] Alhoewel rechtshulp in de vorm van het EOB al meer is gestroomlijnd en er afspraken zijn gemaakt over de termijn waarbinnen aan het verzoek om rechtshulp gehoor moet worden gegeven, kan ook het EOB vertragend werken.[70]

Ten tweede wordt het systeem door autoriteiten veelal als complex ervaren.[71] Complexiteit speelt met name een rol wanneer meerdere staten bevoegd zijn om rechtsmacht uit te oefenen. Alhoewel staten in onderling overleg kunnen bepalen wat de meest geschikte manier is om het concrete geval aan te pakken, heeft iedere staat zijn eigen, mogelijk met andere staten conflicterende belangen. Bovendien is het maar de vraag of, en zo ja in hoeverre, aan alle afzonderlijke belangen kan worden tegemoetgekomen. Met de wetenschap dat het systeem van rechtshulp tijdrovend, complex en niet altijd efficiënt is, ligt het gevaar van unilaterale opsporing op de loer: staten hoeven dan niet om toestemming te vragen en opsporingshandelingen kunnen sneller worden ingezet.[72]

Een derde kanttekening is dat in de praktijk valt te bezien hoe wordt omgegaan met situaties waarin (achteraf) om toestemming wordt gevraagd (scenario 2-gevallen). Mogelijk is het bewijs dan al effectief vergaard.[73] Volgens Oerlemans ontbreekt voor de verzoekende staat de noodzaak alsnog een verzoek te doen als het bewijs toch al is vergaard. Tegelijkertijd bestaat ook voor de aangezochte staat weinig urgentie om het verzoek snel te behandelen aangezien de verzamelde gegevens niet meer verloren kunnen gaan.[74] Daarnaast bestaat altijd het risico dat het verzoek door de aangezochte staat wordt afgewezen. Het is de vraag of de vergaarde gegevens dan nog voor het bewijs mogen worden gebruikt in een strafrechtelijke procedure.[75] Enerzijds zou dit risico drempelverhogend kunnen werken: autoriteiten van de verzoekende staat besluiten om ingezette bevoegdheden – in afwachting van een reactie op het verzoek – niet te voltooien. Anderzijds kan dit risico ertoe leiden dat voor autoriteiten een duidelijke prikkel ontbreekt om de staat waarin de server is gevestigd überhaupt om toestemming te vragen.[76]

63 Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv, par. 2.1.
64 Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv, par. 1.5.
65 *Kamerstukken II* 2015/16, 34372, nr. 3, p. 48.
66 Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv, par. 2.2.
67 Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv, par. 1.4.
68 B.J. Koops & M. Goodwin, *Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law*, (WODC) TILT: 2014, p. 41; Hirsch Ballin, *AA* 2018, p. 462; Oerlemans 2018, p. 220; Oerlemans 2020, p. 235.
69 *Kamerstukken II* 2015/16, 34372, nr. 3, p. 45; Hirsch Ballin, *AA* 2018, p. 462; Oerlemans 2018, p. 220.
70 Zie M.J. Dubelaar, M.I. Federova & R.M. te Molder, 'De vergaring en het gebruik van digitale gegevens in een strafvorderlijke context', in: P.T.J. Wolters e.a. (red.), *Digitalisering en conflictoplossing (O&R nr. 130)*, Deventer: Wolters Kluwer 2021, p. 66.
71 Oerlemans 2020, p. 235; *Kamerstukken II* 2015/16, 34 372, 3, p. 9; Hirsch Ballin, *AA* 2018, p. 462; J. Kleijssen & P. Perri, 'Cybercrime, Evidence and Territoriality: Issues and Options', in: M. Kuijer & W. Werner, *Netherlands Yearbook of International Law. The Changing Nature of Territoriality in International Law*, New York: Springer 2017, p. 162.
72 Oerlemans 2020, p. 235.
73 Oerlemans 2018, p. 227-228.
74 Oerlemans 2018, p. 228.
75 Oerlemans 2018, p. 228.
76 Oerlemans 2018, p. 228.

Tot slot verdient opmerking dat het huidige systeem de mogelijkheid openlaat dat opsporingsautoriteiten zich tijdens het onderzoek verschuilen achter het argument dat de locatie van de gegevens, na redelijke inspanning, niet met voldoende zekerheid kon worden achterhaald (scenario 3-gevallen), waardoor de mogelijkheid wordt gecreëerd om naar Nederlands recht op te treden.[77] In dat geval kunnen de belangen van de staat waarin de gegevens feitelijk staan opgeslagen met voeten worden getreden.

3. Gemeenschappelijke onderzoeksteams

Zoals al in paragraaf 1 is opgemerkt, kan in geval van grensoverschrijdende opsporing ook een gemeenschappelijk onderzoeksteam, een JIT, worden opgericht. Dergelijke teams moeten grensoverschrijdende samenwerking in strafzaken vergemakkelijken.[78] In deze paragraaf besteden wij aandacht aan JIT-overeenkomsten.[79] Het onderzoek naar EncroChat – waarbij Frankrijk en Nederland een JIT-overeenkomst sloten – dient daarbij als voorbeeld.[80]

3.1 Wettelijk kader

De Europeesrechtelijke basis voor een JIT kan onder meer worden gevonden in de EU Rechtshulpovereenkomst.[81] De bevoegde autoriteiten[82] van twee of meer lidstaten kunnen voor een bepaald doel en een beperkte periode een JIT instellen om in één of meer van de betrokken staten een strafrechtelijk onderzoek uit te voeren.[83] In artikel 13 EU Rechtshulpovereenkomst staat een niet-limitatieve opsomming[84] van situaties waarin een JIT kan worden opgericht, namelijk als: (1) 'het onderzoek van een lidstaat naar strafbare feiten moeilijke en veeleisende opsporingen vergt die ook andere lidstaten betreffen' en (2) 'verscheidene lidstaten onderzoeken uitvoeren naar strafbare feiten die wegens de omstandigheden van de zaak een gecoördineerd en gezamenlijk optreden in de betrokken lidstaten vergen'.[85] In de regel wordt een JIT dus ingesteld in geval van complexe, grensoverschrijdende onderzoeken.[86] In het verzoek tot instelling van een JIT moet – naast de voorwaarden die gelden voor een rechtshulpverzoek –[87] ook worden ingegaan op de beoogde samenstelling van het team.[88] Het team wordt gevestigd in de lidstaat waar het onderzoek 'naar verwachting' zal worden verricht.[89] Dit betreft, volgens de Nederlandse minister van Justitie (thans: Justitie & Veiligheid), het land waarin het 'zwaartepunt' van het onderzoek ligt.[90] Het JIT wordt geleid door een vertegenwoordiger van de aan het onderzoek deelnemende bevoegde autoriteit van de lidstaat waarin het team actief is.[91] Het team moet zijn werkzaamheden verrichten conform het nationale recht van het land waarin het actief is.[92] De teamleden verrichten hun taken onder leiding van de teamleider, maar moeten wel de vereisten die hun eigen autoriteiten hebben

77 Oerlemans 2018, p. 228.

78 C. Rijken, 'Joint Investigation Teams: Een nieuw instrument voor de grensoverschrijdende samenwerking in strafzaken. Een evaluatie van de eerste Nederlandse ervaringen met een JIT', *DD* 2007/4.

79 Het verdient overigens opmerking dat een JIT niet enkel wordt opgericht ten behoeve van het onderzoek naar (gebruikers van) cryptoaanbieders. Een JIT kan ook worden opgericht ten behoeve van de opsporing van andere vormen van grensoverschrijdende criminaliteit.

80 Met ondersteuning van Eurojust en Europol, zie www.eurojust.europa.eu/sites/default/files/2020-07/2020-07-02_joint-Eurojust-Europol-press-release_NL.pdf, laatst geraadpleegd op 8 december 2021. Ook in het onderzoek naar Sky-ECC is een JIT opgericht, zie www.jjoerlemans.com/2021/12/20/iets-meer-duidelijkheid-over-sky-ecc-operatie/, laatst geraadpleegd op 24 januari 2022.

81 De EU Rechtshulpovereenkomst is een aanvulling op o.a. het Europees Verdrag van 20 april 1959 aangaande de wederzijdse rechtshulp in strafzaken (zie art. 1 EU Rechtshulpovereenkomst). Omdat het lang duurde voordat de EU Rechtshulpovereenkomst door de verschillende EU-lidstaten werd geratificeerd, heeft de Raad op 13 juni 2002 het Kaderbesluit 2002/465/JBZ van de Raad inzake gemeenschappelijke onderzoeksteams (PB L 162 van 20.6.2002, blz. 1) vastgesteld, waaraan op 1 januari 2003 moest zijn voldaan. Het hierna besproken art. 13 EU Rechtshulpovereenkomst is vrijwel gelijkluidend aan art. 1 Kaderbesluit. Voor zover de bepalingen uit art. 13 EU Rechtshulpovereenkomst niet volledig duidelijk en/of onvoorwaardelijk zijn geformuleerd, zijn deze in Nederland geïmplementeerd in de art. 5.2.1 t/m 5.2.5 Sv. Zie Rijken, *DD* 2007/4.

82 Uit art. 5.2.1 lid 1 Sv blijkt dat dit in Nederland de officier van justitie is. De officier van justitie moet voor het instellen van een JIT wel intern toestemming krijgen. Zie Van Rookhuizen, *T&C Strafvordering*, commentaar op art. 5.2.1, aant. 3. Sinds januari 2021 bestaat er een interne instructie van het College van procureurs-generaal over de instelling van een JIT en de interne toestemmingsprocedure. Zie Van Rookhuizen, *T&C Strafvordering*, commentaar op art. 5.2.1, aant. e. Uit art. 5.2.1 lid 1 Sv blijkt dat de officier van justitie enkel bevoegd is een JIT op te richten op het moment dat hiervoor een verdragsbasis of een kaderbesluit van de Raad van de EU is.

83 Zie art. 13 lid 1 EU Rechtshulpovereenkomst. Deze periode kan in onderling overleg worden verlengd.

84 In art. 13 lid 1 EU Rechtshulpovereenkomst staat immers '(..) kan worden ingesteld in het bijzonder wanneer (..)'.

85 Art. 13 lid 1 EU Rechtshulpovereenkomst. In de praktijk worden dan ook (vanwege de niet-limitatieve opsomming) JIT-overeenkomsten gesloten voor opsporingsonderzoeken die niet corresponderen met deze twee vormen. Zie Meissen 2014, par. 16.4.

86 Vgl. Van Rookhuizen, *T&C Strafvordering*, commentaar op titel 2 Sv, aant. a. Dit neemt niet weg dat een JIT ook in kleine onderzoeken kan worden ingezet. Zie Handboek voor gemeenschappelijke onderzoeksteams 2011, p. 7-8. Dit handboek is te raadplegen via www.eumonitor.nl/9353000/1/j9vvik7m1c3gyxp/viu85h5n8fym, laatst geraadpleegd op 16 december 2021.

87 Als bedoeld in art. 14 Europees Rechtshulpverdrag en art. 37 Benelux-Verdrag. Aan de instelling van een JIT ligt dan ook een rechtshulpverzoek ten grondslag.

88 Art. 13 lid 2 EU Rechtshulpovereenkomst. Uit art. 13 lid 12 EU Rechtshulpovereenkomst blijkt dat onder voorwaarden ook derden kunnen deelnemen aan het JIT-team. Zie voor de Nederlandse regeling met betrekking tot de inhoud van de overeenkomst, art. 5.2.1 lid 3 Sv. Hieruit blijkt o.a. dat in de overeenkomst ook moet worden opgenomen welke opsporingsbevoegdheden de Nederlandse opsporingsambtenaren op het buitenlandse grondgebied mogen uitoefenen en vice versa. Zie voor het geval dat door het onderzoeksteam op Nederlands grondgebied opsporingsbevoegdheden worden uitgeoefend, art. 5.2.2. Sv. Art. 5.2.5 Sv bevat een regeling voor het rechtstreeks doorgeleiden van telecommunicatie.

89 Art. 13 lid 1 EU-rechtshulpovereenkomst.

90 *Kamerstukken II* 2001/02, 28350 (R 1720), 3, p. 6. Zo ook T.M. Schalken & M. Pronk, 'Over *joint investigation teams*, Europol en het toezicht op hun gezamenlijke acties, *DD* 2001/8, p. 833.

91 Art. 13 lid 2 sub a EU Rechtshulpovereenkomst. De autoriteiten van het land op wiens grondgebied het team werkzaam is moeten overigens ook de benodigde organisatorische maatregelen treffen zodat het team kan functioneren. Zie art. 13 lid 3 sub c EU Rechtshulpovereenkomst.

92 Art. 13 lid 3 sub b EU Rechtshulpovereenkomst. Zie ook Van Rookhuizen, *T&C Strafvordering*, commentaar op titel 2 Sv, aant. d. Zie ook art. 5.2.2 Sv.

doi: 10.5553/TBSenH/229567002022008002005

vastgelegd in de (schriftelijke)[93] JIT-overeenkomst, in acht nemen.[94] Gedetacheerde leden van het JIT – dit zijn de leden van het JIT afkomstig uit de andere lidstaat dan de lidstaat waarin het JIT optreedt –[95] mogen in beginsel[96] aanwezig zijn als in de lidstaat waarin wordt opgetreden onderzoekshandelingen worden verricht. Bovendien kunnen zij onder voorwaarden zelf onderzoekshandelingen verrichten in de lidstaat waarin het JIT opereert.[97] In de praktijk komt het voor dat de verschillende JIT-leden enkel in hun eigen lidstaat onderzoeksactiviteiten verrichten.[98] Voorts kunnen de gedetacheerde leden in hun eigen land opsporingshandelingen (laten) verrichten[99] ten behoeve van het JIT en kunnen zij gegevens die voorhanden zijn in hun eigen lidstaat ten behoeve van het gezamenlijke onderzoek met het team delen.[100] De gegevens die tijdens het onderzoek (rechtmatig) zijn verkregen mogen worden gedeeld onder de volgende voorwaarden:

> 'a. voor het doel waarvoor het team is ingesteld;
> b. behoudens voorafgaande toestemming van de lidstaat waar de informatie vandaan komt, voor het opsporen, onderzoeken en vervolgen van andere strafbare feiten. Die toestemming kan alleen worden geweigerd in gevallen waarin dergelijk gebruik strafrechtelijk onderzoek in de betrokken lidstaat in gevaar brengt of ten aanzien waarvan die lidstaat rechtshulp kan weigeren;
> c. ter voorkoming van een onmiddellijke en ernstige bedreiging van de openbare veiligheid, onverminderd het bepaalde onder b) indien vervolgens een strafrechtelijk onderzoek wordt geopend;
> d. voor andere doeleinden, voorzover dat tussen de lidstaten die het team hebben ingesteld is overeengekomen.'[101]

Een groot voordeel van een JIT is dat de JIT-partners gezamenlijk en gecoördineerd[102] onder leiding van een teamleider onderzoek kunnen verrichten naar (complexe) strafbare feiten die een grensoverschrijdend karakter hebben, zonder dat voor het toepassen van opsporingsbevoegdheden (zoals bijvoorbeeld de inzet van digitale opsporingsbevoegdheden, maar ook het aanhouden van verdachten en/of het horen van getuigen) steeds rechtshulpverzoeken moeten worden gedaan.[103] Ook kunnen de gedetacheerde JIT-leden onderzoekshandelingen verrichten op het territorium van de lidstaat waarin het JIT-team is ingesteld, mits zij daarvoor toestemming hebben gekregen van de betrokken lidstaten.[104] In de JIT-overeenkomst worden voorts afspraken gemaakt over het onderling delen van specialistische kennis, informatie en bewijsmateriaal en kan worden overeengekomen dat informatie of bewijsmateriaal, dat reeds voorafgaand aan het instellen van het JIT beschikbaar was over de partij waarop het gezamenlijke onderzoek zich richt, onderling wordt uitgewisseld.[105] Bovendien kunnen Europol en Eurojust het JIT ondersteunen.[106]

Belangrijk voor het doen slagen van een JIT is wel dat er voldoende onderling vertrouwen bestaat tussen de samenwerkende autoriteiten.[107] Een mogelijk nadeel is dat het voorbereiden van de overeenkomst veel tijd kan kosten als de JIT-leden weinig kennis hebben over de werking van een dergelijk team,[108] er hoge kosten verbonden kunnen zijn aan het onderzoek dat wordt uitgevoerd en dat de informatie-uitwisseling niet altijd goed verloopt indien de betrokken lidstaten uiteenlopende wet- en regelgeving hebben betreffende de openbaarmaking van gegevens.[109] Het kan hierdoor voorkomen dat de verzamelde informatie niet direct voor het bewijs kan worden gebruikt; dit is namelijk afhankelijk van nationale wet- en regelgeving.[110] In 2007 stelde Rijken naar aanleiding van zijn onderzoek naar de eerste ervaringen van Nederland met een JIT, dat het niet moet worden gezien als *de* oplossing voor alle problemen die spelen in de samenwerking in geval van grensoverschrijdende criminaliteit.[111]

93 Art. 5.2.1 lid 2 Sv. Op de website van Eurojust staat een modelovereenkomst die staten kunnen gebruiken, zie www.eurojust.europa.eu/nl/model-agreement-setting-joint-investigation-team, laatst geraadpleegd op 7 december 2021.
94 art. 13 lid 2 sub b EU Rechtshulpovereenkomst.
95 Art. 13 lid 4 EU Rechtshulpovereenkomst.
96 Uit art. 13 lid 5 EU Rechtshulpovereenkomst blijkt dat de gedetacheerde leden het recht hebben om in een dergelijke situatie aanwezig te zijn, maar dat de onderzoeksleider kan beslissen – 'om bijzondere redenen en in overeenstemming met het recht van de lidstaat waar het team optreedt' – dat de gedetacheerde leden niet aanwezig mogen zijn.
97 Hiervoor dienen zowel de bevoegde autoriteiten van de lidstaat waarin het team optreedt als de bevoegde autoriteiten van de detacherende lidstaat toestemming te geven. Deze onderzoekshandelingen moeten dan wel worden verricht conform het recht van de lidstaat waarin het team optreedt. Zie art. 13 lid 6 EU Rechtshulpovereenkomst.
98 Meissen 2014, par. 6.2.
99 Art. 13 lid 7 EU Rechtshulpovereenkomst: in een dergelijke situatie worden de onderzoekshandelingen verricht 'onder de voorwaarden die van toepassing zouden zijn indien zij in het kader van een nationaal onderzoek werden gevraagd.' Het is derhalve niet nodig om een rechtshulpverzoek in te dienen. Zie Rijken, *DD* 2007/4.
100 Art. 13 lid 9 EU Rechtshulpovereenkomst. Dit dienen zij wel te doen met inachtneming van het nationale recht en binnen de grenzen van hun bevoegdheid.
101 Art. 13 lid 10 EU Rechtshulpovereenkomst: de gegevens mogen worden verstrekt als deze niet op een andere manier voor de autoriteiten beschikbaar zijn. Zie voor de Nederlandse regeling met betrekking tot het delen van gegevens, art. 5.2.4 Sv.
102 Er ontstaan derhalve geen parallelle onderzoeken. Vgl. Rijken, *DD* 2007/4.
103 Van Rookhuizen, *T&C Strafvordering*, commentaar op titel 2 Sv, aant. a.
104 Vgl. Rijken, *DD* 2007/4.
105 Zie bijv. art. 9 en 10 van de eerdergenoemde modelovereenkomst die beschikbaar is op de website van Eurojust. Vgl. art. 13 lid 9 en 10 EU-rechtshulpverdrag. Zie voor andere voordelen ook het Handboek voor gemeenschappelijke onderzoeksteams 2011, p. 3 en Sollie & Kop 2012, p. 9-10; W.J.B. ten Kate, Mensenhandel. Moderne slavernij (Praktijkwijzer Strafrecht nr. 5), Deventer: Wolters Kluwer 2018, p. 258-260.
106 Ten Kate 2018, p. 258-260.
107 Rijken, *DD* 2007/4, par. 5.4.1.
108 Ten Kate 2018, p. 260.
109 Rijken, *DD* 2007/4, par. 5,1, 5.4.2 en 6.
110 Vgl. Rijken, *DD* 2007/4, par. 2.2.3.
111 Rijken, *DD* 2007/4, par. 6.

doi: 10.5553/TBSenH/229567002022008002005

3.2 EncroChat[112]

Uit een gezamenlijk persbericht van Eurojust en Europol blijkt dat Nederland en Frankrijk in het kader van de EncroChat-operatie een JIT-overeenkomst hebben gesloten.[113] Het resultaat van het gezamenlijke onderzoek was dat miljoenen berichten, uitgewisseld tussen criminelen teneinde ernstige misdrijven te plegen, werden onderschept, gedeeld en vervolgens werden geanalyseerd.[114] Tot op heden bestaat nog steeds veel onduidelijkheid over (in ieder geval delen van) de EncroChat-operatie.[115] Onderstaande beschrijving van het onderzoek is gebaseerd op thans bekende informatie uit beschikbare rechtspraak en andere openbare bronnen.[116]

Het bedrijf EncroChat leverde telefoons met daarop een bepaald soort applicatie waardoor haar gebruikers versleutelde berichten en beeldmateriaal naar elkaar konden versturen en ontvangen.[117] De EncroChat-gebruikers konden alleen onderling communiceren.[118] Om gebruik te kunnen maken van de EncroChat-telefoons moesten de gebruikers een abonnement afsluiten bij het bedrijf.[119] De afgelopen jaren werden EncroChat-telefoons in verschillende strafrechtelijke onderzoeken aangetroffen waardoor bij de politie het beeld ontstond dat zij voornamelijk in het (georganiseerde) criminele milieu werden gebruikt.[120] Dit vormde in 2017 voor zowel de Franse (onder de naam 'Emma 95')[121] als de Nederlandse autoriteiten (onder de naam '26Lemont') aanleiding een onderzoek te starten naar het bedrijf.[122] Aangezien de EncroChat-telefoons ook in verschillende landen werden gebruikt, hebben politie en justitie in ieder geval begin 2020 meerdere keren interstatelijk overleg gehad over een mogelijk gecoördineerde onderzoeksaanpak.[123]

Nadat de server van EncroChat bleek te zijn gevestigd in de Franse plaats Roubaix, installeerden de Franse autoriteiten op 1 april 2020 een door henzelf ontwikkeld opnamemiddel op de server.[124] De installatie had als doel om alle inkomende en uitgaande communicatie door middel van de EncroChat-telefoontoestellen vast te leggen.[125] Het installatieproces bestond uit twee fases: (1) het inzetten van een hacktool op alle EncroChat-telefoons via een update vanaf de Franse server, waardoor alle op de telefoons aanwezige data (zoals locatiegegevens, opgeslagen chatberichten en IMEI-gegevens) konden worden verzameld. Vervolgens werden deze data naar de Franse autoriteiten verzonden; (2) het verzamelen van de op de EncroChat-telefoons aanwezige communicatie op het moment dat deze op een EncroChat-telefoon werden opgeslagen.[126] Het resultaat van deze installatie was dat de Franse autoriteiten vanaf 1 april 2020 EncroChat-data verzamelden en opsloegen op in Frankrijk gevestigde computersystemen. Gedurende de politieoperatie heeft het Franse onderzoeksteam de Nederlandse politie toegang gegeven tot de opgeslagen EncroChat-data.[127] Deze data werden steeds gekopieerd naar het onderzoeksnetwerk van de Nederlandse politie (waardoor de dataset 26Lemont ontstond).[128] Op 13 juni 2020 ontdekte EncroChat dat de communicatie-

112 Zie voor een beschrijving van de meest relevante EncroChat-jurisprudentie de bijdrage van B.W. Schermer & J.J. Oerlemans, 'De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie?' in dit themanummer van TBS&H.

113 De JIT-overeenkomst heeft dus geen betrekking op een strafrechtelijk onderzoek naar individuele Nederlandse gebruikers. De rechtbank Rotterdam is dan ook van oordeel dat de JIT-overeenkomst niet aan de verdediging hoeft te worden versterkt, omdat de verdediging daar geen verdedigingsbelang bij heeft. Zie Rb. Rotterdam 22 december 2020, ECLI:NL:RBROT:2020:11947, onder 'Beoordeling rechtbank'.

114 www.eurojust.europa.eu/sites/default/files/2020-07/2020-07-02_joint-Eurojust-Europol-press-release_NL.pdf, laatst geraadpleegd op 10 december 2021.

115 Het is de vraag in hoeverre de inhoud van de operatie volledig bekend zal worden. Immers, een deel van de informatie over deze operatie, namelijk de werking van de Franse interceptietool, is geclassificeerd als staatsgeheim. Zie bijv. www.nos.nl/artikel/2390840-rechtbank-rotterdam-vervangt-rechters-die-onbedoeld-franse-staatsgeheimen-inzagen, laatst geraadpleegd op 10 december 2021 en Rb. Rotterdam 25 juni, ECLI:NL:RBROT:2021:6113, r.o. 3.2.4.

116 Voor deze omschrijving is met name gebruikgemaakt van de uitspraak van de rechtbank Rotterdam van 25 juni 2021, ECLI:NL:RBROT:2021:6113, aangezien in deze uitspraak (veel) aandacht is besteed aan de wijze waarop de EncroChat-hack heeft plaatsgevonden en ook informatie bevat over deze operatie, die voorafgaand aan deze uitspraak nog niet bekend was.

117 Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.2. De verstuurde berichten werden na een vooraf ingestelde tijd (standaard stond de termijn op zeven dagen) verwijderd. Ook bevatte de telefoon een zogeheten '*panic-wipe*': de gebruiker van de telefoon kon de inhoud volledig wissen.

118 Voordat communicatie tussen de EncroChat-gebruikers onderling kon plaatsvinden, moesten de gebruikers elkaar toevoegen aan hun contactenlijsten. Een EncroChat-gebruiker diende zijn *username* naar een andere gebruiker te sturen waarbij hij de andere gebruiker verzocht om hem aan zijn contactenlijst toe te voegen. Het was dus niet mogelijk om 'zomaar' met een andere EncroChat-gebruiker te communiceren. Zie Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.2.

119 Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.2: een abonnement voor de duur van zes maanden kostte ongeveer € 1.500.-.

120 Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.3.

121 www.eurojust.europa.eu/sites/default/files/2020-07/2020-07-02_joint-Eurojust-Europol-press-release_NL.pdf, laatst geraadpleegd op 10 december 2021.

122 EncroChat werd verdacht van 'deelnemen aan een criminele organisatie, (gewoonte)witwassen en medeplichtigheid aan strafbare feiten die door klanten/gebruikers van EncroChat zijn gepleegd'. Zie Rb. Oost-Brabant 6 september 2021, ECLI:NL:RBOBR:2021:4723, onder IV. Dat in het onderzoek naar EncroChat ook onderzoek is gedaan naar de gebruikers van EncroChat is vanwege deze verdenkingen dan ook logisch. In het onderzoek naar de oprichters van Ennetcom – deze oprichters werden ook verdacht van o.a. witwassen en het deelnemen aan een criminele organisatie – werd immers ook onderzoek gedaan naar Ennetcom-gebruikers, omdat dit noodzakelijk was voor het kunnen bewijzen van de tegen Ennetcom bestaande verdenkingen. Zie Rb. Rotterdam 21 september 2021, ECLI:NL:RBROT:2021:9085, onder 'kern van het vonnis', r.o. 60.

123 Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.3.

124 Deze tool is ingezet op basis van art. 706-102-1 du Code de procédure pénale français. Zie www.eurojust.europa.eu/sites/default/files/Press/2020-07-02_EncroChat-investigation-in-France_FR.pdf, laatst geraadpleegd op 7 december 2021.

125 Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.3. Het is aldus een Frans opsporingsonderzoek, verricht onder de verantwoordelijkheid van de Franse justitiële vereisten. Zie r.o. 3.2.4.

126 Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.3.

127 Het gaat dan om de EncroChat-data die betrekking hebben op de Nederlandse gebruikers, zie Rb. Rotterdam 25 juni 2021 ECLI:NL:RBROT:2021:6113, r.o. 3.2.4: toegang werd verschaft via een beveiligde verbinding.

128 Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.3: hierbij werd een bepaalde techniek gebruikt waardoor nieuwe EncroChat-data 'met een zo klein mogelijke vertraging' naar het onderzoeksnetwerk van de Nederlandse politie werd gekopieerd.

doi: 10.5553/TBSenH/229567002022008002005

dienst was gehackt. Zij adviseerde haar gebruikers de versleutelde telefoons weg te gooien, waarna de politieoperatie op 20 juni 2020 werd beëindigd.[129]

Over de juridische grondslag van de door de Franse aan de Nederlandse autoriteiten verstrekte EncroChat-data, kan het volgende worden opgemerkt. Uit een uitspraak van de rechtbank Amsterdam van 18 december 2020 blijkt dat de dataverstrekking op een tussen de Franse en Nederlandse autoriteiten gesloten JIT-overeenkomst was gebaseerd.[130] Deze overeenkomst zou zijn gesloten nadat de Franse autoriteiten, met toestemming van de Franse rechter, de eerdergenoemde EncroChat-hack reeds hadden uitgevoerd.[131] Uit een uitspraak van de rechtbank Oost-Brabant van 6 september 2021 blijkt onder meer dat is overeengekomen dat 'alle informatie en bewijsmiddelen die ten behoeve van het JIT worden vergaard, worden gevoegd in een gezamenlijk onderzoeksdossier'.[132]

Zoals eerder is opgemerkt, was EncroChat al sinds 2017 in beeld bij de Nederlandse politie. Bovendien was reeds bekend dat de EncroChat-telefoons ook in Nederland veelvuldig werden gebruikt binnen het criminele circuit. Er werd dan ook voorzien dat de Franse interceptie inbreuk zou maken op de persoonlijke levenssfeer van Nederlandse EncroChat-gebruikers. Om die reden heeft het Nederlandse Openbaar Ministerie (hierna: OM) een machtiging gevorderd bij de rechter-commissaris om de data die zouden worden verzameld van en over de Nederlandse gebruikers, te mogen analyseren en te gebruiken in bepaalde strafrechtelijke onderzoeken.[133] Deze machtiging betrof overigens een extra waarborg. Het Wetboek van Strafvordering verplicht hiertoe niet.[134] Het OM heeft bij de rechter-commissaris een lijst aangeleverd met daarop specifieke opsporingsonderzoeken waarin een EncroChat-telefoon was aangetroffen en waarnaar zij onderzoek wilde verrichten in de verzamelde EncroChat-data.[135] Vervolgens heeft de rechter-commissaris de machtiging (o.g.v. art. 126uba Sv) verleend en daarin voorwaarden gesteld aan het gebruik van de data (verzameld in het onderzoek 26Lemont) in andere – met name genoemde – strafrechtelijke onderzoeken.[136] Uit een uitspraak van de rechtbank Amsterdam van 14 september 2021 blijkt dat deze machtiging op 1 april 2020 door de rechter-commissaris is verleend.[137] Ook is na 1 april 2020 de eerdergenoemde lijst steeds aangevuld met nieuwe opsporingsonderzoeken en heeft de rechter-commissaris in die nieuwe gevallen het OM steeds toestemming gegeven om de dataset 26Lemont te onderzoeken ten behoeve van die nieuwe opsporingsonderzoeken.[138] Op het moment dat de rechter-commissaris toestemming had verleend aan het OM om de dataset 26Lemont te mogen gebruiken in een specifiek strafrechtelijk onderzoek naar een EncroChat-gebruiker, gaf de officier van justitie een bevel af op grond van artikel 126dd Sv, waardoor de data behorende tot het strafrechtelijk onderzoek naar EncroChat (zijnde de dataset 26Lemont) ook konden worden gedeeld om te kunnen worden gebruikt in een ander strafrechtelijk onderzoek.[139]

Tot slot, de EncroChat-operatie is door de rechter bestempeld als een enkel Franse aangelegenheid.[140] Zo overwoog de rechtbank Rotterdam op 21 juni 2021 dat van enige, laat staan doorslaggevende, bemoeienis van Nederlandse autoriteiten op individueel *gebruikers*niveau niet is gebleken.[141] Op het moment van installatie van de hack door de Franse autoriteiten was de locatie van de desbetreffende toestellen nog niet bekend en de hack heeft ook plaatsgevonden vóórdat de JIT-overeenkomst tot stand kwam. Pas nadat de locatiegegevens waren geanalyseerd, werd helder waar de toestellen zich feitelijk bevonden. Deze locatiegegevens, alsook de overige verzamelde data, zijn toen met Nederland gedeeld en hier verder geanalyseerd en verwerkt ten behoeve van strafrechtelijke onderzoeken naar individuele gebruikers.[142]

3.3 Analyse

Wanneer de locatie van de gegevens op voorhand bekend is, heeft een JIT-overeenkomst, in vergelijking met rechtshulp (par. 2), onzes inziens een aantal voordelen. Wij lichten dit toe. Omdat de EncroChat-operatie niet onder Nederlandse verantwoordelijkheid viel, hoefde Nederland de Franse autoriteiten in dit specifieke geval niet om rechtshulp te verzoeken. Van een onder Nederlandse verantwoordelijkheid uitgevoerd onderzoek zou bijvoorbeeld sprake zijn geweest wanneer Nederland Frankrijk had verzocht een hack uit te voeren ter verkrijging van data van in Nederland geïdentificeerde toestellen. In een dergelijk geval had Nederland Frankrijk op voorhand om toestemming moeten vragen aangezien de locatie van de server bekend was (scenario 1). Weliswaar kan van voorafgaande toestemming worden afgeweken

129 Zie voor de inhoud van dat bericht bijv. www.eurojust.europa.eu/sites/default/files/2020-07/2020-07-02_joint-Eurojust-Europol-press-release_NL.pdf, laatst geraadpleegd op 7 december 2021.
130 Rb. Amsterdam 18 december 2020, ECLI:NL:RBAMS:2020:6443, r.o. 6.2.
131 Rb. Amsterdam 18 december 2020, ECLI:NL:RBAMS:2020:6443, r.o. 5: volgens het OM liggen er dan ook geen Nederlandse strafrechtelijke onderzoeken ten grondslag aan de (inzet van de) Franse bevoegdheid.
132 Rb. Oost-Brabant 6 september 2021, ECLI:NL:RBOBR:2021:4723, onder IV. Een dergelijke overweging is volgens de rechtbank 'gebruikelijk'.
133 Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.3. Zo kon de rechter-commissaris toetsen aan de vereisten van proportionaliteit, subsidiariteit en het bestaan van een wettelijke grondslag. Zie Rb. Oost-Brabant 6 september 2021, ECLI:NL:RBOBR:2021:4723, onder IV.
134 Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.3.
135 Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.3.
136 Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.4. Uit deze uitspraak blijkt ook dat de rechtbank nader wil worden geïnformeerd over de afweging die de rechter-commissaris heeft gemaakt bij het afgeven van zijn machtiging. Zie r.o. 3.2.4.
137 Rb. Amsterdam 14 september 2021, ECLI:NL:RBAMS:2021:5460, onder 28.
138 Rb. Amsterdam 14 september 2021, ECLI:NL:RBAMS:2021:5460, onder 28: de rechter-commissaris heeft ook incidenteel zijn toestemming geweigerd.
139 Zie Rb. Oost-Brabant 6 september 2021, ECLI:NL:RBOBR:2021:4723, onder IV.
140 Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.4.
141 Rb. Rotterdam 25 juni 2021, ECLI:NL:RBROT:2021:6113, r.o. 3.2.4.
142 Rb. Noord-Holland, 23 juli 2021, ECLI:NL:RBNHO:2021:6213, r.o. 2.3.

wanneer een reactie van de aangezochte staat niet kan worden afgewacht, dan wel niet te verwachten is, maar als zonder toestemming wordt opgetreden schuilt daarin het gevaar dat inbreuk wordt gemaakt op de soevereiniteit van de aangezochte staat. In paragraaf 2 is al aangestipt dat rechtshulpverzoeken door autoriteiten in de regel als tijdrovend, complex en niet altijd efficiënt worden ervaren.

Kortom, in scenario 1-gevallen kan een JIT-overeenkomst voordeliger zijn dan een rechtshulpverzoek: (1) het onderzoek wordt gecoördineerd en onder verantwoordelijkheid van een teamleider uitgevoerd; (2) de overeenkomst voorkomt dat staten inbreuk maken op de soevereiniteit van de staat waarin de gegevens staan opgeslagen (in geval van een rechtshulpverzoek, de aangezochte staat); (3) in de JIT-overeenkomst kunnen staten afspraken maken over het onderling uitwisselen van informatie; en (4) het JIT kan verzoeken dat onderzoek wordt gedaan in het land van de gedetacheerde JIT-leden, zonder dat daartoe een rechtshulpverzoek is vereist.

Daartegenover staat dat een JIT-overeenkomst in scenario 3 en mogelijk ook in scenario 2-gevallen onzes inziens waarschijnlijk geen soelaas biedt. Wanneer onduidelijk blijft in welk land de gegevens staan opgeslagen (scenario 3) doet zich immers een soortgelijk probleem voor als bij rechtshulp. Een JIT vergt een gezamenlijk en gecoördineerd optreden in de betrokken lidstaten, maar hiervoor is wel noodzakelijk dat men weet wie de betrokken staten zijn. Ook wanneer de locatie van de gegevens pas gedurende het onderzoek bekend wordt (scenario 2), ligt het sluiten van een JIT-overeenkomst niet voor de hand. Kenmerkend voor een JIT is tenslotte dat staten, alvorens de overeenkomst wordt gesloten, in onderling overleg een strategie bepalen en besluiten gezamenlijk op te treden. Dit wordt belemmerd wanneer de locatie pas gedurende het opsporingsonderzoek komt vast te staan. Bovendien kan het zijn dat een JIT-overeenkomst niet langer van toegevoegde waarde is op het moment dat de data feitelijk al zijn vergaard.

4. Afrondende beschouwingen

Alhoewel het territorialiteitsbeginsel niet absoluut is, stelt het de opsporingsautoriteiten voor complexe vraagstukken wanneer zij grensoverschrijdend willen opsporen, zo ook wanneer zij grensoverschrijdend onderzoek verrichten naar (gebruikers van) cryptoaanbieders. In deze bijdrage hebben wij twee juridische mogelijkheden beschreven op basis waarvan aan dit grensoverschrijdend opsporingsonderzoek invulling kan worden gegeven. Zo kunnen de autoriteiten een aangezochte staat om rechtshulp verzoeken. Daarnaast kan internationaal worden samengewerkt op basis van een JIT-overeenkomst. In beide situaties stuiten de opsporingsautoriteiten echter op bezwaren, waardoor een effectieve grensoverschrijdende opsporing kan worden bemoeilijkt. De grensoverschrijdende opsporing naar (gebruikers van) cryptoaanbieders wordt met name belemmerd wanneer (op voorhand) onduidelijk is welke lidstaten bij dit opsporingsonderzoek moeten worden betrokken, omdat in die gevallen niet duidelijk is waar de server zich bevindt.

De gestage toename van grensoverschrijdende criminaliteit waarmee opsporingsautoriteiten tegenwoordig worden geconfronteerd en de technologie waarachter criminelen zich kunnen verschuilen, nopen onzes inziens tot een efficiëntere Europese onderzoeksaanpak. Deze opvatting lijkt breed te worden gedeeld.[143] De oplossing voor het probleem is helder, zo stelt Oerlemans: 'staten moeten afspraken maken over de wijze waarop grensoverschrijdende digitale opsporing mag plaatsvinden, ook wanneer deze opsporing extraterritoriale effecten heeft'.[144] Tegelijkertijd blijkt uit de praktijk dat consensus over de inhoud van deze afspraken niet eenvoudig is. Wij noemen een aantal mogelijke oorzaken.

In de eerste plaats zijn er tal van uiteenlopende culturele, historische en/of politieke redenen[145] die het maken van internationale afspraken kunnen belemmeren. Bovendien, zo schrijven Hirsch Ballin, Van Ginneken en Schrijver, hechten staten veel waarde aan het behoud van soevereiniteit en beleidsvrijheid.[146] Volgens Hirsch Ballin houden staten, waar het de soevereiniteit betreft, te star vast aan de territoriale begrenzing van bevoegdheden.[147] Geelhoed en Ouwerkerk betogen daarnaast dat de EU-lidstaten weinig bereidheid tonen om hun executieve jurisdictie te delen met andere EU-lidstaten of deze vorm van jurisdictie aan EU-agentschappen over te dragen.[148] Territorialiteit blijft daarmee een groot obstakel voor een effectieve opsporing van grensoverschrijdende criminaliteit.

Zoals in paragraaf 2 is opgemerkt, voorkomt het territorialiteitsbeginsel niet alleen dat inbreuk wordt gemaakt op de soevereiniteit van een staat, maar waarborgt het beginsel ook dat de grondrechten van individuen die zich op het grondgebied van deze staat bevinden, worden gewaarborgd.[149] Deze instrumentele en rechtsbeschermende functie van het territorialiteitsbeginsel zijn onlosmakelijk met elkaar verbonden. Hirsch Ballin vraagt zich af of met de thans gekozen benadering van het territorialiteitsbeginsel nog wel voldoende recht wordt gedaan aan haar rechtsbeschermende functie.[150] Bij een strafrechtelijk onderzoek moeten de rechten van

143 M. Hirsch Ballin, M. van Ginneken & N. Schrijver, *De grenzen voorbij. De actualiteit van territorialiteit en jurisdictie*, Deventer: Wolters Kluwer 2019, p. 9; Koops, Conings & Verbruggen 2016, p. 177-178, *Kamerstukken II* 2015/16, 34372, nr. 3; Oerlemans 2020, p. 240; Hirsch Ballin 2018, p. 465; M. Luchtman, *Transnationale rechtshandhaving - Over fundamentele rechten in de Europese strafrechtelijke samenwerking*, Den Haag: Boom juridisch 2017.
144 Oerlemans 2020, p. 240.
145 Hirsch Ballin, *AA* 2018, p. 465; Oerlemans 2020, p. 240.
146 Hirsch Ballin, Van Ginneken & Schrijver 2019, p. 9.
147 Hirsch Ballin, *AA* 2018, p. 465.
148 Geelhoed & Ouwerkerk, *Strafblad* 2019/4, p. 18.
149 Hirsch Ballin, *AA* 2018, p. 465.
150 Hirsch Ballin, *AA* 2018, p. 466.

doi: 10.5553/TBSenH/229567002022008002005

het onderzochte individu worden beschermd, maar tegelijkertijd wordt de controle op naleving van zijn rechten bemoeilijkt vanwege het internationale karakter. Indien sprake is van grensoverschrijdende opsporing wordt namelijk uitgegaan van het vertrouwensbeginsel en het beginsel van wederzijdse erkenning, waardoor erop wordt vertrouwd dat de aangezochte staat de opsporingsbevoegdheden heeft ingezet conform het eigen nationale recht en de mensenrechtenverdragen. Gelet op het vertrouwensbeginsel en het beginsel van wederzijdse erkenning is de controle op de naleving van buitenlandse opsporingshandelingen dan ook zeer beperkt.[151] Hirsch Ballin bepleit een benadering waarbij territorialiteit minder strikt wordt gehanteerd en het mensenrechtenperspectief naar de voorgrond wordt geschoven. Concreet houdt haar oplossing in dat de vervolgende staat ook de verantwoordelijkheid draagt voor de buiten haar grondgebied verrichte opsporingshandelingen en verantwoordelijk kan worden gehouden voor de bescherming van de rechten van het onderzochte individu.[152] De rechtsbescherming van een individu kan immers worden bemoeilijkt wanneer de verantwoordelijkheid voor deze bescherming telkens tussen staten verschuift.[153] Bovendien kan deze verschuivende verantwoordelijkheid '*forum shopping*' in de hand werken, doordat er door de autoriteiten voor wordt gekozen om opsporingsbevoegdheden daar in te zetten of de vervolging daar te laten plaatsvinden waar de meest gunstige (lees: de voor de autoriteiten meest efficiënte) wet- en regelgeving van toepassing is. Volgens Geelhoed en Ouwerkerk kan, vanwege allerlei Europese verplichtingen tot samenwerking, niet zozeer meer worden gesproken van gescheiden, soevereine rechtsruimtes. Veeleer is sprake van een gedeelde ruimte, 'een ruimte waarbinnen nationale autoriteiten nadrukkelijk op basis van gelijkwaardigheid opereren, maar niet volledig afhankelijk zijn van elkaars goedkeuring alvorens tot buiten-nationale handhaving kan worden overgegaan'.[154] In een dergelijke gedeelde Europese rechtsruimte bestaan gedeelde belangen, maar ook gedeelde verantwoordelijkheden die niet overeenstemmen met de thans geldende territorialiteitsgerichte benadering van rechtshandhaving.[155]

Zowel de opvatting van Hirsch Ballin als van Geelhoed en Ouwerkerk zet aan tot heroverweging van het geldende uitgangspunt van territorialiteit. Door het mensenrechtenperspectief voorop te zetten en de verantwoordelijkheid van staten om mensenrechten te beschermen niet strikt territoriaal te beperken, moet ervoor worden gezorgd dat de opsporing (alsook het toezicht en de controle daarop) efficiënter kan plaatsvinden.[156]

Echter, om Europese samenwerking daadwerkelijk succesvol te laten zijn, is onder meer een 'gemeenschappelijk normenkader' nodig.[157] Gelet op de hiervoor door ons genoemde redenen, is het vaststellen van zo'n gemeenschappelijk Europees normenkader geen eenvoudige opgave ook juist vanwege de verschillende belangen die in de nationale lidstaten spelen. Dit geldt eveneens voor het vooropplaatsen van het mensenrechtelijke perspectief. Wanneer de vervolgende staat – indien zij (digitaal) grensoverschrijdend heeft opgespoord – ook verantwoordelijk is voor het waarborgen van de rechten van de verdachte die zich niet op haar grondgebied bevindt (of wanneer de onderzochte server buiten het territorium van de vervolgende staat is gevestigd), wordt hiermee weliswaar getracht te waarborgen dat aan de bescherming van de rechten van de verdachte in de strafrechtelijke procedure wordt tegemoetgekomen, maar tegelijkertijd vragen wij ons af of het – gelet op de thans aanwezige verschillen in de nationale strafvorderlijke wet- en regelgeving in de EU-lidstaten – wel steeds haalbaar zal zijn om de rechten van de verdachte op het hoogste niveau te waarborgen. Ter illustratie: stel, in staat A gelden hogere eisen voor de mogelijkheid tot het hacken van een server dan in staat B. Hoe moet dan worden geoordeeld over de rechtmatigheid van de hack indien staat B de hack heeft uitgevoerd in staat A? Als staat B de hack conform de eigen wet- en regelgeving (en conform mensenrechtenverdragen) rechtmatig heeft uitgevoerd, is daarmee in dat geval de kous af of speelt de regelgeving van staat A nog een rol? Naar onze mening brengt het vooropplaatsen van het mensenrechtelijke perspectief theoretisch gezien een aantal voordelen met zich, maar zal dit de opsporingsautoriteiten – zonder dat binnen de EU sprake is van geharmoniseerde strafvorderlijke wet- en regelgeving – in de praktijk nog steeds voor complexe juridische vraagstukken blijven stellen. Wij betwijfelen of volledige harmonisatie van strafvorderlijke wet- en regelgeving in de praktijk haalbaar is.[158] Om harmonisatie te kunnen bewerkstelligen, is in ieder geval de Europese wetgever aan zet.

De toename van grensoverschrijdende georganiseerde criminaliteit onderschrijft de noodzaak van een verder gevorderd Europeesrechtelijk kader. Met name in de in paragraaf 2.2 en paragraaf 2.3 genoemde scenario 2- en 3-gevallen waarin (op voorhand) niet kan worden vastgesteld in welke staat de benodigde gegevens staan opgeslagen, schiet het huidige systeem van rechtshulp tekort. Indien autoriteiten in dergelijke situaties zonder

151 Hirsch Ballin, *AA* 2018, p. 466.
152 Hirsch Ballin, *AA* 2018, p. 466-467.
153 Hirsch Ballin. *AA* 2018, p. 465-466. Zie over het probleem van 'versnipperde rechtsbescherming' ook Luchtman 2017, p. 33-34.
154 Geelhoed & Ouwerkerk, *Strafblad* 2019/4, p. 19.
155 Geelhoed & Ouwerkerk, *Strafblad* 2019/4, p. 19. Zij wijzen er ook op dat het idee van een gedeelde rechtsruimte kan zorgen voor een verbeterde toegang tot de rechter en dat hiermee de problematiek van de verschillen in de nationale regels met betrekking tot bewijsgaring kan worden ondervangen.
156 Hirsch Ballin, *AA* 2018, p. 462.
157 Luchtman 2017, p. 41. Luchtman stelt overigens dat hiervoor niet alleen een gemeenschappelijk normenkader nodig is, maar bijvoorbeeld ook gemeenschappelijke instituties. Zie verder Luchtman 2017, p. 41 e.v.
158 Overigens kan het door ons geschetste probleem niet alleen door de EU-wetgever worden opgelost. Er is ook een rol weggelegd voor de (rechterlijke macht en de wetgever van de) individuele lidstaten. Zie Luchtman 2017, p. 50 en 52.

doi: 10.5553/TBSenH/229567002022008002005

toestemming opereren worden zij tenslotte geconfronteerd met de niet irreële mogelijkheid dat zij inbreuk maken op de soevereiniteit van een andere staat. Wanneer staten het territorialiteitsbeginsel strikt blijven interpreteren, zoals thans het geval lijkt te zijn, kan dit een effectieve grensoverschrijdende opsporing bemoeilijken en mogelijk op den duur zelfs ondermijnen. De huidige digitale, internationaal georiënteerde samenleving vraagt om een herziening van territorialiteit. Door het beginsel ruimer in te vullen wordt aansluiting gezocht bij het gegeven dat misdaad de landsgrenzen overschrijdt en dat steeds meer strafbare feiten digitaal worden beraamd en gepleegd.

Het resultaat van deze internationale afspraken zou moeten zijn dat autoriteiten, die hun bevoegdheden inzetten buiten het eigen territoir, voor het grensoverschrijdend onderzoek naar (gebruikers van) cryptoaanbieders volledig verantwoordelijk kunnen worden gehouden. Vervolgens moet dit ertoe leiden dat een betere rechtsbescherming kan worden geboden aan individuen indien buitenlands digitaal bewijs jegens hen wordt gebezigd in een Nederlandse strafrechtelijke procedure. Immers, wanneer sprake is van bestrijding van grensoverschrijdende criminaliteit moet de bescherming van fundamentele rechten volgen.[159]

159 Vgl. Luchtman 2017, p. 54.

doi: 10.5553/TBSenH/229567002022008002005