Cyberspace, de cloud, en grensoverschrijdende opsporing

De grenzen en mogelijkheden van internationaal recht

Samenvatting

Bert-Jaap Koops
Morag Goodwin

Tilburg University
TILT – Tilburg Institute for Law, Technology, and Society
CTLD – Center for Transboundary Legal Development
Postbus 90153
5000 LE Tilburg
<e.j.koops@uvt.nl>
<m.e.a.goodwin@uvt.nl>

december 2014

Cyberspace, de cloud, en grensoverschrijdende opsporing: de grenzen en mogelijkheden van internationaal recht

Samenvatting

Achtergrond, onderzoeksvraag en methode

Door de opkomst van cloud computing (het gebruik van schaalbare computercapaciteit als Internetdienst) worden computergegevens steeds vaker opgeslagen 'in de cloud' in plaats van op apparaten van gebruikers. Een bepaald bestand kan hierdoor gelijktijdig op meerdere plaatsen worden opgeslagen, terwijl het niet op één bepaalde plaats in zijn geheel hoeft te zijn opgeslagen. Uit snelheidsoverwegingen zullen data vaak opgeslagen worden in het serverpark dat het dichtst bij de locatie van de gebruiker ligt. Er kunnen meerdere aanbieders in gelaagde constructies betrokken zijn bij cloud computing. Ook kunnen data versleuteld zijn. De cloud heeft daarom significante gevolgen voor strafrechtelijke opsporingsonderzoeken, met name wanneer naar digitaal bewijs wordt gezocht. Lokale doorzoeking en inbeslagneming door de politie zal steeds minder bewijs opleveren door het gebruik van clouddiensten zoals webmail en dataopslag-op-afstand. Dit versterkt de al bestaande uitdagingen van cyberopsporing, zoals de noodzaak van snelle bewijsvergaring vanwege de kwetsbaarheid voor dataverlies en de vraag of bevoegdheden toereikend zijn om op afstand toegang te krijgen tot data.

Een specifieke uitdaging bij cyberopsporing wordt gevormd door het feit een onderzoek zich snel uitstrekt tot buiten de landsgrenzen. Staten zullen dan terug moeten vallen op de traditionele procedures voor wederzijdse rechtshulp in strafzaken, wat over het algemeen een lastig proces is in cyberopsporing. Naast de organisatorische (capaciteitsproblemen, prioriteitstelling) en juridische (dubbele strafbaarheid) beperkingen, beschouwen de uitvoerders van cyberopsporing de rechtshulpprocedures als omslachtig en ineffectief voor digitale bewijsvergaring. Ondanks de inspanningen die zijn verricht om wederzijdse rechtshulp in cyberopsporingszaken te vergemakkelijken, blijven de procedures ontoereikend in situaties waarbij snelle datavergaring essentieel is of in situaties waarbij (cyber)criminelen data veelvuldig verplaatsen. De procedures bieden ook geen soelaas wanneer de locatie van de data niet, of alleen door middel van tijdrovende inspanningen, kan worden vastgesteld; dat kan vaak het geval zijn bij cloud computing.

Waar de gangbare procedures voor wederzijdse rechtshulp ontoereikend zijn, dringt de vraag zich op of, en onder welke omstandigheden, grensoverschrijdende opsporing toegestaan is. Dit is niet alleen een relevante vraag voor computercriminaliteit, maar voor alle misdaden waarbij daders communiceren via email of smartphone-apps of gebruik maken van cloud-opslagdiensten. Ondanks de nodige pogingen om grensoverschrijdende cyberopsporing te vergemakkelijken, zijn er op dit vlak nog weinig zichtbare resultaten geboekt. Een belangrijke oorzaak daarvan is het feit dat op territorium gebaseerde nationale soevereiniteit de basis vormt voor internationaal recht, waardoor het internationaal recht onderzoeksactiviteiten op buitenlands grondgebied strikt verbiedt als er geen toestemming is van de buitenlandse staat. Er is daarom sprake van een impasse: cyberopspoorders willen op een of andere manier grensoverschrijdend kunnen opsporen maar kunnen dit niet door de huidige interpretatie van internationaal recht, en de uitdagingen van cyberopsporing hebben staten er vooralsnog niet toe bewogen om nieuwe regels te creëren die de strikte interpretatie van soevereiniteit loslaten.

Tegen deze achtergrond van een 21e-eeuws cloud computing-paradigma dat aanloopt tegen 20e-eeuwse procedures voor wederzijdse rechtshulp in strafzaken ontvouwt zich het probleem dat centraal staat in dit onderzoek. Dit rapport beoogt het debat over grensoverschrijdende cyberopsporing een stap verder te brengen door een brug te slaan tussen de gebieden van cyberopsporing en internationaal recht. De onderzoeksvraag is welke grenzen en mogelijkheden er bestaan in het internationaal recht voor grensoverschrijdend cyberonderzoek door opsporingsinstanties. De nadruk ligt daarbij op cloud-opslagdiensten, maar de analyse is ook van

toepassing op cyberopsporing in bredere zin, meer specifiek op doorzoekingen op afstand en het opvragen van data bij buitenlandse dienstaanbieders. Deze studie onderzoekt de rechtmatigheid binnen het internationaal recht van grensoverschrijdende toegang tot data vooral vanuit de kernbeginselen van territoriale integriteit en het verbod op inmenging in binnenlandse aangelegenheden en niet zozeer vanuit de mensenrechtelijke aspecten van cyberopsporing.

Het onderzoek voor dit rapport is gebaseerd op een literatuurstudie van internationaal en supranationaal recht, beleidsdocumenten en wetenschappelijke literatuur op het gebied van cyberopsporing en internationaal recht, en op een internationale expertbijeenkomst met twintig experts op het gebied van strafrecht, cybercrime, Internet, en internationaal recht.

Conceptueel kader

De problemen waar grensoverschrijdende cyberopsporing mee te maken krijgt zijn al lange tijd bekend en onderkend. Desondanks is er nog geen oplossing gevonden om deze problemen aan te pakken. Volgens ons is het noodzakelijk om eerst nader in te gaan op de oorzaken van de problemen en het – diepgravender dan tot op heden is gebeurd – combineren van kernelementen en inzichten uit cyberopsporing en internationaal recht, voordat gekeken kan worden naar de aanpak van de problemen in de toekomst. Dit rapport besteedt daarom expliciet aandacht aan het ontwikkelen van een conceptueel kader dat als basis kan dienen voor nader onderzoek en discussie.

Een belangrijk onderdeel van een conceptueel kader is de analyse van metaforen die worden gebruik om fenomenen te beschrijven. Metaforen spelen immers een belangrijke rol in ons begrip van problemen en mogelijke oplossingen. Wanneer we kijken hoe over gedragingen in cyberspace wordt gesproken, dan blijkt dat ‘cyberspace’ door de meeste staten eerder wordt opgevat als een ‘plaats’, oftewel een gebied in de fysieke zin van het woord, dan als een ‘ruimte’, oftewel een meer abstract gebied dat een bepaald doel dient. De opvatting van cyberspace als ‘plaats’ heeft belangrijke gevolgen voor hoe ertegen aan wordt gekeken, waarbij het vanwege de fysieke connotatie voor de hand lijkt te liggen dat het onder territoriale jurisdictie valt.

Grondgebied blijft het kernelement waarop internationaal recht is gebaseerd, ondanks argumenten die rond de millenniumwisseling werden geuit dat staatssoevereiniteit voorbij zou zijn. Terwijl de internationale orde van bijna 200 staten langzamerhand plaats heeft gemaakt voor duizenden actoren op het wereldtoneel, waarvan sommigen soevereiniteits-achtige aanspraken doen gelden, blijft het internationaal recht toch relatief immuun voor deze ontwikkelingen. De veranderingen op het wereldtoneel hebben er echter wel voor gezorgd dat het begrip van de staat is uitgebreid; de staat is meer dan alleen grondgebied. Er wordt meer aandacht besteed aan vragen omtrent jurisdictie, dat wil zeggen de mogelijkheden van een staat om recht te spreken en te handhaven. Dit komt duidelijk naar voren komt op het gebied van mensenrechten in internationaal recht, waar de extraterritoriale jurisdictie voor mensenrechtenverplichtingen nu breed geaccepteerd is. Aan de andere kant gebruiken machtige staten (en groepen staten) dit nieuwe vloeibare begrip van soevereiniteit ook om jurisdictie buiten de landsgrenzen op te eisen, gebaseerd op de leer van het gevolg, met name op economisch terrein. We zien echter niet dat tegelijkertijd ook de jurisdictie om te handhaven wordt uitgebreid, dat wil zeggen de bevoegdheid van een staat om een juridische aanspraak binnen het territorium van een andere staat af te dwingen. Extraterritoriale activiteiten van staat A op het territorium van staat B, zonder de toestemming van B, om een aanspraak van A gebaseerd op materiële jurisdictie af te dwingen, is een schending van de territoriale integriteit van staat B en blijft een ernstige schending van het internationaal recht.

Wanneer we cyberspace echter vanuit een opsporingsperspectief bekijken, dan blijkt de opvatting van cyberspace als ‘plaats’ in de zin van een territorium twijfelachtig. Cyberonderzoek vergt vaak zeer snel ingrijpen om data voor het strafrechtelijke onderzoek veilig te stellen. Praktijkdeskundigen en cyberopsporingswetenschappers stellen dat hier een probleem speelt omdat verder dan de bestaande kaders voor wederzijdse rechtshulp moet worden gekeken en opsporingsautoriteiten speelruimte moeten krijgen voor enige vorm van ‘zelfhulp’ door middel van grensoverschrijdende toegang tot data. Dit kan onder meer betekenen dat zij een grensoverschrijdende doorzoeking verrichten (als verlengstuk van een plaatselijke doorzoeking of een zelfstandige doorzoeking op

afstand, al dan niet beperkt tot rechtmatig toegankelijke computers) of door direct contact op te nemen met buitenlandse aanbieders (met een vrijwillig verzoek of een bevel). Sommige van deze mogelijkheden worden geregeld door het Cybercrime-Verdrag, zij het met aanzienlijke beperkingen; de potentieel effectiefste maatregelen – een grensoverschrijdende doorzoeking zonder toestemming of een direct bevel aan buitenlandse dienstaanbieders – zijn niet toegestaan. Een van de prangendste vragen die zich opdringt door de opkomst van cloud computing is of ingrijpendere vormen van grensoverschrijdende toegang tot data zouden moeten worden toegestaan, en zo ja, onder welke voorwaarden. Het feit dat een buitenlandse staat waar data liggen opgeslagen geen of slechts een marginale connectie kan hebben met de misdaad, de slachtoffers, of de daders, speelt hierbij ook een rol: de staat heeft dan zelf geen motief om samen te werken bij het strafrechtelijke onderzoek. Bovendien kunnen zich situaties voordoen waarin de locatie van de data niet of onvoldoende bekend is.

Het bepalen van de locatie van in de cloud opgeslagen data is niet zo moeilijk als sommige auteurs ons willen doen geloven, maar de cloud zorgt wel voor extra moeilijkheden bij het lokaliseren van data. Dit komt niet alleen doordat data snel en vaak verplaatst kunnen worden, maar ook door meerlagige diensten met verschillende aanbieders en straks wellicht ook door (op zee) drijvende cloudcentra. Dit zorgt in de praktijk voor een ‘verlies van locatie’, niet in ontologische maar in epistemologische zin: het is lastig te achterhalen waar data in de cloud zijn opgeslagen. Dit betekent echter niet dat data geen locatie *hebben* (met de connotatie dat zij vaag rondzweven in cyberspace), alleen dat de locatie *onbekend* is. Het is daarom belangrijk om te spreken van een ‘verlies van kennis van locatie’ in plaats van een ‘verlies van locatie’.

Tot slot is het belangrijk om bedacht te zijn op de metaforen waarin we spreken over grensoverschrijdend onderzoek, die verkeerde connotaties kunnen oproepen. Zo spreekt men vaak over het ‘bezoeken’ van een server en het ‘rondkijken’ in een elektronische postbus, terwijl de gebruikers feitelijk niet onderweg zijn of in een computer kijken. De ‘reis’-metafoor is misleidend in onze context: spreken over politie die naar een server op afstand ‘gaat’ roept een beeld op van agenten die fysiek het territorium van een buitenlandse betreden. De fysieke aanwezigheid van ambtenaren speelt een grote rol in de beoordeling van de rechtmatigheid van extraterritoriale staatsactiviteiten in het internationaal recht. Omdat er bij grensoverschrijdende computeronderzoeken geen sprake is van fysieke aanwezigheid van personen, kan men beter metaforen uit dit ‘reis’-kader vermijden. Volgen ons kan een cyberonderzoek beter worden gekarakteriseerd als het zenden en ontvangen van berichten. Dit staat dichter bij wat er daadwerkelijk gebeurt: een *client*-computer zendt een bericht aan een server met een bepaald verzoek, waarna de server het bericht interpreteert en vervolgstappen onderneemt op basis van zijn programmering. De juridische kwalificatie van een grensoverschrijdend onderzoek – de rechtmatigheid – kan dan onderzocht worden binnen het kader van de vraag of opsporingsautoriteiten bevoegd zijn om verzoeken te richten aan entiteiten op buitenlands grondgebied.

Internationaal recht – de strikte interpretatie

In de strikte – en dominante – interpretatie van het internationaal recht kan iedere bewijs vergarende activiteit in een buitenlandse staat—zelfs een enkel telefoongesprek—als inbreuk op de soevereiniteit worden beschouwd. Het verkrijgen van toegang tot data opgeslagen op een server op het territorium van een andere staat, zonder toestemming van die staat, leidt tot een inbreuk op de territoriale integriteit en daarmee tot een onrechtmatige daad. Het feit dat de onderzoekende staat op het moment van toegangsverschaffing misschien moeilijk de locatie van de data kon bepalen, doet daar niets aan af. Ook toestemming door de gebruiker of de aanbieder van de data heft de onrechtmatigheid onder internationaal recht niet op. Eventuele uitsluitingsgronden als zelfverdediging, overmacht en noodweer zijn niet van toepassing; alleen noodweer zou toepasselijk kunnen zijn in enkele extreme gevallen, maar niet in de reguliere uitoefening van strafrechtelijk onderzoek. De enige uitzondering die in deze situatie van toepassing kan zijn is wanneer de buitenlandse staat voorafgaande toestemming heeft verleend. Dit kan toestemming zijn voor een specifiek onderzoek naar aanleiding van een concreet verzoek, of meer algemeen voor bepaalde

typen onderzoek onder speciale voorwaarden. Een voorbeeld van het laatste is artikel 32(b) van het Cybercrime-Verdrag, dat bepaalt dat grensoverschrijdende toegang tot data met toestemming van de gebruiker of de aanbieder is toegestaan als beide staten zijn aangesloten bij het Cybercrime-Verdrag.

Artikel 32(b) kan ook zo geïnterpreteerd worden grensoverschrijdend onderzoek met rechtmatig verkregen toegangsgegevens[1] mogelijk is in het geval dat de opsporingsdienst van staat A weet dat de data zich in staat B bevinden en staat B aangesloten is bij het verdrag. Deze interpretatie moet echter nog aanvaard worden door de lidstaten van het Cybercrime-Verdrag voordat zij als legitiem kan worden beschouwd. Deze lezing van het verdrag biedt weliswaar een opening in de discussie over grensoverschrijdende opsporingstoegang tot data, maar het gaat wel om een beperkte mogelijkheid: het heeft alleen betrekking op staten die partij zijn bij het Cybercrime-Verdrag; het is alleen van toepassing wanneer de opsporingsdienst weet, of goede redenen heeft om aan te nemen, dat de data zich op het territorium van een andere verdragsstaat bevinden; en het is alleen van toepassing wanneer de toegang tot de data geschiedt via rechtmatig verkregen toegangsgegevens, en niet bij andere manieren van grensoverschrijdende toegang. Uiteindelijk zijn daarom de mogelijkheden binnen het bestaande internationaalrechtelijke kader voor grensoverschrijdend cyberonderzoek zonder toestemming van de buitenlandse staat erg beperkt, binnen de strikte interpretatie van het internationaal recht.

Internationaal recht – een breder perspectief richting nieuwe afspraken

Terwijl de strikte interpretatie van internationaal recht luidt dat grensoverschrijdende doorzoekingen zonder toestemming van de buitenlandse staat een inbreuk vormen op de verplichtingen tussen staten om elkaars soevereiniteit te respecteren, kan men ook een minder doctrinaire lezing van het internationaal recht hanteren: een handeling van staten wordt dan als meer of minder toelaatbaar beschouwd afhankelijk van de argumenten die de staat voor die handeling aandraagt. Er zijn verschillende plausibele argumenten te hanteren die een alternatieve manier van omgang tussen staten met betrekking tot de cloud en cyberspace kunnen rechtvaardigen.

Staten kunnen juridische regimes ontwikkelen die klassieke soevereiniteitsargumenten terzijde schuiven wanneer zij daar voldoende belang bij hebben. Dergelijke regimes zijn schaars, maar het juridische raamwerk dat is ontwikkeld voor de (kosmische) ruimte, en met name voor satellietbeelden, geeft aan dat er wel degelijk nieuwe principes kunnen ontstaan wanneer technologie het vasthouden aan territoriale soevereiniteit onhoudbaar maakt (bijvoorbeeld om de signalen van satellieten te beperken tot exacte landsgrenzen) en waar staten een gemeenschappelijk gemeenschappelijk belang hebben bij een alternatief kader (bijvoorbeeld door foto's van satellieten te delen). Het binnen dat kader ontwikkelde 'open skies'-beginsel houdt in dat iedere staat die via satellieten waarnemingen doet van een andere staat, dit kan doen zonder de toestemming van die staat. Daarbij bestaat er de verplichting om beelden tegen een redelijke prijs beschikbaar te stellen aan de waargenomen staat. Eenzelfde ontwikkeling is zichtbaar met betrekking tot andere ruimten waar het karakter van de ruimte, zoals oceanen of de wildernis van Antarctica, het moeilijk maakt voor staten om die ruimte als 'plaats' (onderworpen aan territoriale aanspraken) te behandelen. In zulke gevallen ontwikkelt men nieuwe juridische regimes die deze beperkingen onderkennen en waarbij staten samenwerken om te voorkomen dat deze 'ruimte' tot een ongereguleerde ruimte verwordt die door bandieten wordt bevolkt.

Een eerste optie om een stap verder te komen in het internationaal recht is de status quo te veranderen. De urgentie om iets te doen aan de uitdagingen voor cyberopsporing, niet in het minst door de ontwikkeling van de cloud, wordt steeds breder erkend. Cybercriminaliteit staat hoog op de internationale beleidsagenda, wat mogelijkheden biedt om nieuwe instrumenten te bespreken waarin staten afspraken maken over grensoverschrijdende toegang tot data. Deze instrumenten kunnen

[1] Rechtmatig verkregen toegangsgegevens zijn de login-naam en het wachtwoord tot een computer of dienst; deze kunnen rechtmatig door de verdachte of dienstaanbieder zijn afgegeven, maar ook bijvoorbeeld gevonden zijn op een memobriefje op het bureau van de verdachte tijdens een rechtmatige huiszoeking.

ontwikkeld worden binnen de VN (bijvoorbeeld de Commission on Crime Prevention and Criminal Justice, CCPCJ). Momenteel lijkt het momentum echter eerder te liggen bij de Raad van Europa, waar in de context van het Cybercrime-Verdrag momenteel een aanvullend Protocol omtrent grensoverschrijdende toegang tot data wordt bediscussieerd.

Bij het ontwikkelen van een instrument zal men een afweging moeten maken tussen de inhoud en het proces: hoe minder ambitieus een voorstel is voor wat betreft de inhoud en reikwijdte, des te kansrijker is het proces van acceptatie door staten. Ook zal een instrument succesvoller zijn wanneer het de zorgen serieus neemt van sommige staten over excessieve bevoegdheden en gebrek aan transparantie van andere staten in hun internationale activiteiten. Het systeem moet sterke waarborgen bevatten, zowel tegen inbreuken op individuele rechten als bescherming van persoonsgegevens en privacy, als tegen inbreuken op de soevereiniteit. Met name ook moeten kleinere en minder machtige staten gerustgesteld worden, die vermoedelijk het grensoverschrijdend doorzoeken van data door ontwikkelde landen en machtige staten als bedreigend zullen ervaren. Daarom moet er niet alleen oog zijn voor het beperken van de reikwijdte van cyberopsporing, maar ook voor het eerlijk delen in de opbrengsten van een dergelijk instrument.

Een andere manier om vooruitgang te boeken in dit domein is door artikel 32(b) van het Cybercrime-Verdrag te herinterpreteren, in de zin dat staten ook grensoverschrijdend onderzoek mogen verrichten met rechtmatig verkregen toegangsgegevens, wanneer de opsporingsdienst van staat A weet dat de data zich in verdragsstaat B bevinden. Zoals gezegd vergt deze interpretatie instemming van de partijen bij het verdrag, maar dit kan worden bereikt via een ‘Guidance Note’ bij artikel 32, wat eenvoudiger is dan een nieuw instrument uit te onderhandelen dat door staten moet worden geratificeerd. Dit leidt slechts tot een relatief beperkte uitzondering en sluit daarom het zoeken naar andere mogelijkheden voor grensoverschrijdend cyberonderzoek niet uit.

Een aannemelijk verhaal binnen het internationaal recht door vooroplopers

Door het snel veranderende Internetlandschap en de opkomst van de cloud worden de bestaande uitdagingen van cyberopsporing extra op scherp gezet. Staten zullen daarom hun best moeten doen om enige overeenstemming te bereiken over grensoverschrijdend cyberonderzoek. Die overeenstemming zal niet makkelijk of snel bereikt kunnen worden, of het nu gaat om een verdrag of een protocol, binnen de VN of de Raad van Europa. Het is simpelweg een te complexe en delicate kwestie om op korte termijn overeenstemming te bereiken.

Een tweede optie voor een stap vooruit op dit gebied is daarom dat één of enkele landen het voortouw nemen; zij kunnen een praktijk van grensoverschrijdend cyberonderzoek ontwikkelen en tegelijkertijd een aannemelijke theorie naar voren brengen waarom zij vinden dat deze praktijk binnen het internationaal recht past. Deze landen kunnen dan worden beschouwd als de vooroplopers van een opkomende praktijk die meer tijd zal vergen om geaccepteerd te worden door de bredere internationale gemeenschap.

Binnen de huidige strikte interpretatie van internationaal recht blijft grensoverschrijdend cyberonderzoek onrechtmatig, maar een niet-doctrinaire benadering van internationaal recht beoordeelt de rechtmatigheid van statelijke handelingen naar de kracht van de daarbij gehanteerde argumenten. Er zijn verschillende meer of minder plausibele argumenten af te leiden uit bestaande juridische regimes, die een alternatieve verklaring kunnen bieden hoe staten beter met elkaar kunnen omgaan binnen de ruimte van de cloud en cyberspace om een gemeenschappelijk doel te bereiken. Juridische regimes zoals die voor de (kosmische) ruimte, oceanen, bestrijding van piraterij, jurisdictie van havenstaten, en het maken van satellietbeelden (met het ‘open skies’-principe) kunnen inspiratie en argumenten bieden voor een alternatief verhaal over cyberspace en de cloud waarin het voldoende aannemelijk is dat bepaalde vormen van unilaterale acties binnen die ruimte aanvaardbaar zijn.

Om de aannemelijkheid te vergroten, zouden een of twee staten – of liever nog een groep van staten – het voortouw moeten nemen in het ontwikkelen van een alternatieve uitleg van de huidige juridische kaders. Deze staten zouden een principe van een ‘open cyberspace’ kunnen introduceren in de context van grensoverschrijdende toegang tot data, vergelijkbaar met het beginsel van ‘open skies’ in de context van afstandswaarneming (*remote sensing*) via satellieten. Belgisch recht doet

wat dat betreft al een stap in deze richting, maar lijkt daarbij vooralsnog geen goed ontwikkelde theoretische onderbouwing te geven die internationaal uitgedragen wordt. Ook in Nederland wordt momenteel een regeling van grensoverschrijdend onderzoek voorbereid, maar dit is in de huidige vorm weinig aannemelijk omdat het aanzienlijk verder gaat dan het absoluut noodzakelijke voor grensoverschrijdend onderzoek. Het voorstel kan verbeterd worden door de reikwijdte te versmallen (bijvoorbeeld alleen toegang tot data maar niet het verwijderen daarvan; alleen voor onderzoeken naar (bijna) universeel strafbaar gestelde ernstige misdaden zoals kinderpornografie), meer waarborgen in te bouwen (bijvoorbeeld het notificeren van staten waar mogelijk), en een betere onderbouwing te geven (bijvoorbeeld het explicieter en gedetailleerder koppelen van grensoverschrijdende toegang tot data aan bestaande juridische regimes voor andere atypische ruimten). Een ander belangrijk aspect van een aannemelijk verhaal is de uitleg van wat de staat beschouwt als redelijke inspanning om de locatie van data te achterhalen. Er moeten bepaalde minimumeisen worden geformuleerd voor de inspanningen die opsporingsautoriteiten geacht worden te verrichten, zowel in technische als in juridische zin, voordat zij kunnen stellen dat de locatie van de data niet te achterhalen is. Staten moeten duidelijk maken wat zij als een goede praktijk beschouwen, door vast te stellen welke technische en operationele maatregelen nodig zijn voor verschillende vormen grensoverschrijdend onderzoek. Hierbij dient eens te meer benadrukt te worden dat elke inbreuk op de territoriale integriteit van een staat zonder voorafgaande toestemming een internationale onrechtmatige daad oplevert, zelfs wanneer de opsporingsinstantie te goeder trouw handelt en ervan uitgaat dat de data zich op eigen grondgebied bevonden of dat de locatie niet met voldoende zekerheid was vast te stellen. In dat licht moeten de minimumeisen voor de inspanningen van opsporingsautoriteiten voor locatiebepaling hoog zijn, willen ze aannemelijk geacht kunnen worden.

Het is cruciaal dat de vooroplopers die een aannemelijk alternatief verhaal voorstaan van het internationaal recht betreffende cyberopsporing open en transparant opereren. Het alternatief zal meer voet aan de grond krijgen wanneer het in verschillende fora wordt gepresenteerd en besproken, ook als het daar niet formeel wordt aangenomen. Voorbeelden van dergelijke fora zijn de Octopus-conferenties van de Raad van Europa, het CCPCJ-congres, het Internet Governance Forum, en de internationale cyberspace-conferenties. Hoe meer staten naar aanleiding hiervan overgehaald kunnen worden om ook dit alternatieve verhaal te omarmen, des te sterker zal het juridische argument worden.

Daarnaast zullen andere staten eerder gerustgesteld worden wanneer de vooroplopers open zijn over hun activiteiten en toestaan dat een onafhankelijk orgaan hierop toezicht houdt. Binnen het ‘open skies’-kader fungeert de secretaris-generaal van de VN als verzamelplaats voor alle informatie over satellietactiviteiten. Evenzo zou voor cyberopsporing een mechanisme kunnen worden ontwikkeld, waarbij vooroplopende staten verplicht zijn de aard en reikwijdte van hun onderzoeken publiek te maken; zij geven daarbij een precieze en gedetailleerde beschrijving van de typen onderzoek die wettelijk zijn toegestaan en van de waarborgen om de reikwijdte en ingrijpendheid van dergelijke onderzoeken te beperken. Het zou de geloofwaardigheid en transparantie van de alternatieve benadering ook ten goede komen wanneer bepaalde details van concrete grensoverschrijdende onderzoeken bij een onafhankelijk orgaan in bewaring zouden worden gegeven, die onder bepaalde voorwaarden voor andere staten toegankelijk zouden zijn. Hierbij kan gedacht worden aan details zoals de datum en tijd waarop toegang tot de data is verschaft, de misdaad die onderzocht wordt, typen en aantal data die zijn verkregen, en identificerende informatie over de servers waartoe toegang is verschaft.

Vooroplopende staten moeten wel bedacht zijn op de risico’s die gepaard gaan met argumenten om unilaterale grensoverschrijdende doorzoekingen te rechtvaardigen. Allereerst zullen andere staten op eenzelfde manier te werk gaan als de staat die unilateraal toegang verkrijgt tot data in de cloud, waardoor de vooruitstrevende staat niet langer kan protesteren tegen hetzelfde gedrag van andere staten met een beroep op de eigen territoriale integriteit. Bovendien kan de staat in een later stadium, als mocht blijken dat de aanpak haar belangen in sommige opzichten schaadt, niet makkelijk terugkomen op haar standpunt. Daarom zal elke staat die een voortrekkersrol op zich wil nemen voldoende aandacht moeten besteden aan het inventariseren van de manieren waarop de

belangen van de staat en haar burgers bij het gebruik van de alternatieve benadering benadeeld zouden kunnen worden. Ten tweede kan er sprake zijn van onbedoelde gevolgen op andere terreinen: elke aanspraak in relatie tot grensoverschrijdende toegang tot data zal vermoedelijk een reflexwerking hebben in de regulering van andere domeinen, zoals handel en nationale veiligheid. De argumenten voor universele jurisdictie of een open cyberspace zouden wel eens niet in het belang van de staat kunnen blijken als ze in de context van andere gebieden opduiken. Ten derde kunnen unilaterale handelingen van een staat leiden tot een lagere bereidheid bij andere staten om samen te werken, zowel op het gebied van grensoverschrijdende opsporing als in meer algemene zin. Kortom, staten die vooruitstrevend te werk willen gaan in grensoverschrijdende cyberopsporing en unilaterale acties voorstellen, moeten zorgvuldig overwegen wat de bredere en mogelijk negatieve gevolgen kunnen zijn van deze acties, en beoordelen of de voordelen van unilaterale grensoverschrijdende toegang tot data daartegen opwegen.

Conclusie

De analyse in dit rapport leidt tot de conclusie dat er strikte internationaalrechtelijke beperkingen bestaan voor grensoverschrijdende cyberopsporing. Volgens de dominante interpretatie van internationaal recht leidt toegang tot data die zijn opgeslagen op een buitenlandse server zonder toestemming van de desbetreffende staat tot een inbreuk op de territoriale integriteit van die staat, en daarmee tot een onrechtmatige daad. Dat de onderzoekende staat moeite heeft om de locatie van de data te bepalen of dat er toestemming is gegeven door een gebruiker of aanbieder, doet niets af aan de onrechtmatigheid van de actie. De enige manier om rechtmatig grensoverschrijdend cyberonderzoek te verrichten is om vooraf toestemming te krijgen van de buitenlandse staat. Deze toestemming kan op ad hoc-basis worden gegeven, maar ook zijn vastgelegd in een verdrag waarin bepaalde typen onderzoek onder bepaalde omstandigheden worden toegelaten. Een voorbeeld van dit laatste is artikel 32(b) van het Cybercrime-Verdrag, dat het mogelijk maakt zich grensoverschrijdende toegang te verschaffen tot data met toestemming van de gebruiker of de aanbieder. Beide landen moeten dan wel aangesloten zijn bij het verdrag.

Daarmee biedt het internationaal recht veel meer beperkingen dan mogelijkheden om cyberopsporing over de grens uit te voeren. Dat is problematisch, omdat opsporingsinstanties voor een grote uitdaging staan om bewijs te vergaren nu steeds meer data naar de cloud verhuizen of anderszins ergens in cyberspace worden verwerkt, ver van de lokale plaatsen van strafrechtelijk onderzoek. Het zal veel inspanning, geduld en zorg vergen om met de beperkingen van het internationaal recht om te gaan en nieuwe mogelijkheden te creëren. Zoals we in dit rapport hebben benadrukt, kan de huidige impasse alleen worden doorbroken als er eerst substantieel voorbereidend werk wordt verricht om een gemeenschappelijke basis met een gedeeld begrippen- en denkkader tot stand te brengen.

Dit voorbereidende werk omvat ten minste drie verschillende soorten inspanningen. Ten eerste is het zaak dat op internationaal niveau formeel wordt erkend dat cyberopsporing, in het bijzonder met betrekking tot de cloud, vraagt om snelle toegang tot data buiten de landsgrenzen. Het is niet voldoende dat individuele opsporingsambtenaren zich uitspreken over het feit dat ze tegen problemen oplopen; de problemen moeten worden erkend door staatsvertegenwoordigers in internationale fora, voordat deze als vraagstukken worden onderkend die binnen het internationaal recht moeten worden aangepakt. Ten tweede moeten de uitdagingen zorgvuldig en expliciet worden geconceptualiseerd. Men moet beducht zijn op de effecten van metaforen in debatten, en belanghebbenden zouden zorgvuldig moeten bekijken wat de meest toepasselijke metaforen zijn om te gebruiken. Het benaderen van cyberspace als een ‘ruimte’ (in abstracte zin) in plaats van een ‘plaats’ (als fysieke ruimte) kan al een verschil maken bij het zoeken naar oplossingen. Dit geldt ook voor het conceptualiseren van grensoverschrijdende doorzoekingen als het zenden en ontvangen van berichten in plaats van het ‘gaan’ naar een server. Het feit dat de locatie van data moeilijk te achterhalen is wanneer zij zich in de cloud bevinden, moet beschouwd worden als een verlies van kennis van locatie in plaats van een verlies van locatie als zodanig. En ook het conceptualiseren van juridische zeggenschap in termen van effectieve controle in plaats van controle over een nationaal afgegrensd territorium kan bijdragen aan het begrijpen van jurisdictie als zeggenschap over een

‘ruimte’ in plaats van een zeggenschap over uitsluitend ‘plaatsen’. Ten derde zullen de gemeenschappen van cyberopsporing internationaal recht dichter tot elkaar moeten komen, door zich te verdiepen in elkaars taal, concepten, en aannames, op een veel dieper niveau dan tot op heden het geval is. Tijdens dit onderzoek viel ons op hoezeer het bij de experts uit beide gemeenschappen vaak ontbreekt aan kennis over de basisprincipes en ontwikkelingen in het andere veld. Het samenbrengen van deze gemeenschappen is dan ook niet alleen een kwestie van bruggen slaan tussen theorie (internationaal recht) en praktijk (cyberopsporing); het gaat ook om mensen bij elkaar te brengen die samen een begrip kunnen ontwikkelen van het onderhavige probleem en van het kader waarbinnen dat probleem aangepakt moet worden. Alleen dan kan een verhaal over grensoverschrijdende cyberopsporing worden ontwikkeld dat aannemelijk is in zowel technische als internationaalrechtelijke zin.

Wanneer dit voorbereidende werk is gedaan, kunnen staten nadere stappen ondernemen. De aanpak moet tweeledig zijn. Op de korte termijn kan men zich richten op het verhogen van de legitimiteit van nauw afgebakende, transparant uitgevoerde, en met sterke waarborgen omklede unilaterale acties van enkele vooroplopende staten, die daarbij een aannemelijk alternatief verhaal voor het voetlicht brengen over soevereiniteit in cyberspace. Tegelijkertijd kan er op de langere termijn worden gestreefd naar het creëren van een internationaal bindend instrument. Dit kan worden gegoten in de vorm van een internationaal of breed onderschreven multilateraal juridisch instrument, waarin enkele nauw omschreven en met sterke waarborgen omklede vormen van grensoverschrijdende cyberopsporing worden toegestaan. De korte- noch de langetermijnaanpak zal eenvoudig zijn om de problemen voor cyberopsporing in het cloudtijdperk op te lossen. Beide zijn echter noodzakelijk, wil de rechtshandhaving meegaan in de 21^{e} eeuw.