Cyberspace, the cloud, and cross-border criminal investigation

The limits and possibilities of international law

Bert-Jaap Koops
Morag Goodwin

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

December 2014

Colophon

Authors
prof.dr. Bert-Jaap Koops
dr. Morag Goodwin

Publisher
Tilburg University
TILT – Tilburg Institute for Law, Technology, and Society
and CTLD – Center for Transboundary Legal Development
P.O. Box 90153
5000 LE Tilburg
The Netherlands

Commissioned by
WODC, Ministry of Security & Justice
Turfmarkt 147
2511 DP The Hague
The Netherlands

© 2014 WODC, Ministry of Security & Justice. All rights reserved.

Date
December 2014

Table of Contents

Abbreviations ... 6
Summary ... 7

1. Introduction ... 14
1.1. Background ... 14
1.2. Research aim and questions ... 15
1.3. Limitations ... 15
1.4. Methods ... 16
1.5. Outline of the report ... 16
1.6. Acknowledgements ... 16

2. Background ... 17
2.1. Cyber-investigation: a primer for international law experts ... 17
2.2. International law: a primer for cyber-investigation experts ... 18
2.2.1. The nature and purpose of international law ... 18
2.2.2. International law challenges for cyber-investigation ... 20
2.3. Cloud computing ... 21
2.3.1. What is the cloud? ... 21
2.3.2. Cloud computing compounding challenges for cyber-investigation ... 22
2.4. Classic approach to cross-border criminal investigation ... 24
2.4.1. Forms of cooperation ... 24
2.4.2. Slowness and other limitations of mutual legal assistance ... 26
2.5. Summary ... 27

3. Conceptual Framework ... 29
3.1. Introduction: the importance of frames, metaphors, and a common conceptual ground 29
3.2. Conceptualising space, place, and cyberspace ... 30
3.3. Framing the international law perspective ... 31
3.3.1. Place, territory and jurisdiction in international law: from space to place and back again ... 31
3.3.2. Conceptualising sovereignty in a globalising world ... 35
3.3.3. The human rights obligations of states ... 37
3.3.4. Summary of the international law framing of cross-border cloud investigations ... 39
3.4. Framing the law-enforcement perspective ... 40
3.4.1. What do the main problems for criminal investigation consist of? ... 40
3.4.2. The role of the ‘I don’t know where the data are’ argument ... 42
3.4.2.1. Spoenle’s ‘loss of location’ ... 42
3.4.2.2. Geo-location technologies and cyberspace jurisdiction ... 43
3.4.2.3. The locatability of data in the cloud ... 44

3.4.3. The role of human rights ... 45
3.4.4. Summary of the law-enforcement framing of cross-border cloud investigations ... 47
3.5. Conceptualising transborder access to data ... 48
3.5.1. What does a transborder search amount to, technically? ... 48
3.5.2. What does a transborder search amount to, metaphorically? ... 50
3.6. Conclusion ... 51

4. Analysis ... 53
4.1. Current framework, practices, and discussions on cross-border access to data ... 53
4.1.1. The legal framework for transborder access to data ... 53
4.1.2. The practice of transborder searches ... 55
4.1.3. The debate about transborder searches ... 56
4.1.4. Directly contacting foreign providers ... 58
4.2. Possibilities under international law–the strict interpretation ... 61
4.2.1. International law as it is ... 61
4.2.2. What exceptions are allowed to states under international law? ... 62
4.2.3. An exception allowed under article 32(b) Cybercrime Convention: lawfully obtained credentials? ... 63
4.2.4. Interim conclusion ... 64
4.3. Possibilities under international law—broadening the perspective ... 65
4.3.1. Introduction ... 65
4.3.2. The common heritage of mankind ... 67
4.3.3. High seas and flag jurisdiction ... 68
4.3.4. Piracy as an analogy for (certain types of) cybercrime ... 69
4.3.5. The right to acquire remote sensing imagery and the principle of 'Open Skies' ... 71
4.3.6. The common concern of mankind ... 72
4.3.7. Developing a plausible account ... 73
4.4. Conclusion ... 76

5. Ways forward ... 78
5.1. Actions at the international level ... 79
5.1.1. United Nations ... 79
5.1.1.1. UN General Assembly ... 79
5.1.1.2. Commission on Crime Prevention and Criminal Justice ... 80
5.1.1.3. The ITU and the Internet Governance Forum ... 82
5.1.2. Actions in the context of the Cybercrime Convention ... 83
5.1.3. Other international action ... 84

5.2. Actions at the national level 84
5.2.1. Regulating cross-border searches 84
5.2.1.1. The proposal 85
5.2.1.2. Assessment of the proposal 86
5.2.2. Seeing things in a broader perspective 87
5.3. Conclusion 88

Appendices
1. Workshop 19 December 2013 93
2. Advisory committee 96
3. About the authors 97

Bibliography 98

Abbreviations

CCPCJ	Commission on Crime Prevention and Criminal Justice
CoE	Council of Europe
COPUOS	United Nations General Assembly's Committee on Peaceful Use of Outer Space
DCCP	Dutch Code of Criminal Procedure [Wetboek van Strafvordering]
ECHR	European Convention on Human Rights and Fundamental Freedoms
EU	European Union
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IaaS	infrastructure as a service
ICCPR	International Covenant on Civil and Political Rights
ICJ	International Court of Justice
ITU	International Telecommunications Union
LEA	Law Enforcement Agency
MLA	mutual legal assistance
MLAT	mutual legal assistance treaty
MR	mutual recognition
NGO	non-governmental organisation
OED	Oxford English Dictionary
OJ	Official Journal
PaaS	platform as a service
POP3	Post Office Protocol version 3
SaaS	software as a service
SMTP	Simple Mail Transfer Protocol
TOR	The Onion Router
WODC	Wetenschappelijk Onderzoeks- en Documentatiecentrum

Summary

Background, research question, and methods

With the rise of cloud computing (using scalable computing resources as a service via the Internet), computer data are increasingly stored remotely—'in the cloud'—instead of on users' devices. Due to the distributed, dynamic, and redundant nature of cloud storage, a particular file can often be stored in multiple places simultaneously, while it may not be stored in any single place in its entirety. For speed-optimisation reasons, data may be stored in the server park closest to the user's normal location. Cloud computing can involve multiple providers in different layered constellations and data can be encrypted. The cloud thus has significant implications for criminal investigation, particularly in cases where digital evidence is sought. Local search and seizure by the police will yield less and less evidence as users use cloud services such as webmail and remote data storage. This reinforces existing challenges of cyber-investigation, which not only requires swift evidence-gathering due to the vulnerability of data loss, but also powers to gain access to data remotely.

One particular challenge in cyber-investigation is that such remote evidence-gathering powers will quickly extend beyond national borders. Under the rules of international law, states must then resort to traditional procedures of mutual legal assistance. This is, broadly speaking, a challenging process in cyber-investigations. In addition to organisational limitations, such as lack of capacity or priority-setting, and some legal limitations, such as double criminality, mutual assistance procedures are viewed by those conducting on-line investigations as cumbersome or ineffective for seeking digital evidence. Despite efforts to streamline and facilitate mutual legal assistance in cyber-investigation, the procedures remain inadequate in situations in which there is a need for expeditious data gathering, or where (cyber)criminals move data around with high frequency, and also where the location of the data cannot, or only through time-consuming efforts, be identified, which may often be the case in cloud computing situations.

Where mutual legal assistance procedures do not work sufficiently, the question arises whether and under what conditions cross-border investigations are allowed, which is relevant not only for cybercrimes but for all crimes where perpetrators communicate via email or smartphone apps or use cloud storage services. Although a number of efforts have been aimed at trying to move forward in the field of cross-border cyber-investigation, these efforts have not yet resulted in any tangible improvement. A key reason for this is that territorially-based national sovereignty forms the basis of the international order and as a result, international law is strict in prohibiting investigative activities on foreign territory without the consent of the state concerned. The situation is thus one of stalemate: cyber-investigation officials wish to move forward in cross-border investigation but cannot do so because of the current limitations of international law and because the specific challenges of cyber-investigation have so far not induced states to create new international rules in this area that put strict interpretations of sovereignty aside.

It is against this background of a 21st-century cloud computing paradigm meeting with 20th-century-based procedures for mutual legal assistance in criminal matters that the central problem of this study takes shape. This report aims to advance the debate on cross-border cyber-investigation by combining the fields of cyber-investigation and international law. The central question addressed in this study is what limits and what possibilities exist within international law for cross-border cyber-investigations by law enforcement authorities. The focus is on cloud storage services, but the analysis applies more generally to Internet investigations, in particular in the form of remote searches and the contacting of foreign service providers to request data. In particular, the report focuses on questions of the legality of cross-border access to data under international law in terms of the core principles of territorial integrity and non-interference in domestic affairs rather than on questions of human rights.

The research for this report is based on desk research of international and supranational law and policy and academic literature in the fields of cyber-investigation and of international law, and on an international expert meeting with twenty experts in criminal law, cybercrime, Internet, and international law.

Conceptual framework

The fact that the problem of cross-border cyber-investigation as such has been recognised – at least by practitioners in the field – for a considerable length of time but that existing approaches are not able to really address the issue should give us pause for thought. It will not be easy to offer solutions. It is our contention that before discussing possible directions for addressing the problems identified, it is first necessary to uncover more of the underlying roots of the problem, and to combine—at a deeper level than has so far occurred—core elements and insights of both cyber-investigation and international law. Therefore, this report pays particular attention to developing a conceptual framework that can be used as a basis for further inquiry and discussion.

An important part of a conceptual framework is to analyse the metaphors used to describe phenomena, since metaphors play an important role in shaping our understanding of problems and possible solutions. If we look at the language used to describe actions in cyberspace, it becomes clear that 'cyberspace' is conceived by most states as a 'place', i.e., an area conceived in physical terms, rather than a 'space', i.e., a (possibly abstract) area sufficient for some purpose. Conceiving cyberspace as 'place' has important consequences, notably that it is subject to territorial jurisdiction.

Territory remains the key organisational principle of international law, despite declarations by some commentators in the years surrounding the Millennium of the end of sovereignty. While the uniform pattern of an international order comprised of almost 200 states has given away to a more fluid formation in which thousands of actors crowd the world stage and some of whom mount sovereignty-type claims to ultimate ordering power, international law remains fairly immune to such developments. What these shifts are doing, however, is helping us think of the state as more than its territorial extension. In place of territorial thinking, there is more attention to questions of jurisdiction i.e. the ability of a state to 'speak' the law, to enforce its law and the obligations that arise from it. This is most visible in the field of human rights, where extra-territorial jurisdiction for human rights obligations is now well accepted. At the same time, more powerful states or groups of states are using this new fluidity to assert their jurisdiction beyond their territorial borders – otherwise known as the 'effects doctrine' – primarily in areas of economic policy. What we are not seeing, however, is an extension of the jurisdiction *to enforce*, i.e., the ability of a state to enforce a claim within the territory of another state. Extraterritorial activities of state A on state B's territory without B's consent to enforce a claim of A based on material jurisdiction breaches the territorial integrity of state B and remains a serious violation of international law.

Examining cyberspace from a criminal investigation perspective, however, highlights the dubiousness of viewing cyberspace as 'place'. As cyber-investigation often involves a need for the expeditious securing of data for criminal-investigation purposes, many practitioners as well as cyber-investigation scholars frame the problem as a need to move beyond classic mutual legal assistance so as to enable law-enforcement authorities to exercise some form of 'self-help' through cross-border access to data. This can involve a cross-border search (an extension of a physical search or a separate remote online search, which may or may not be limited to lawfully accessible computers) or concern directly contacting a foreign provider (with a voluntary request or a compulsory order). Some of these modes of cross-border access are provided for in the Cybercrime Convention, but with significant limitations; the potentially most effective ones—a non-consensual cross-border search or a direct (compulsory) order to foreign service providers—are currently not permitted. One of the most pertinent questions raised by cloud computing and cyberspace for law enforcement is whether such more invasive forms of cross-border access to data should be allowed, and if so under what conditions. The question gains urgency through the fact that the foreign state may lack a substantive connection with the crime, its victims, or suspects, and thus lack an incentive to assist in the criminal investigation. In addition, it is also necessary to consider those situations in which the location of the remote data is not known or is insufficiently determinable.

Although determining the location of cloud-stored data is not as difficult as some authors have suggested, the cloud does compound the locatability problem of data even further, not only through its feature of moving data around but also through complications such as layered services and, possibly, floating cloud centres. This effectively means a 'loss of location', not in the ontological sense but in the epistemological sense: it is becoming very difficult to know where cloud-based data are stored. To avoid the suggestion that the data do not *have* a location (with

the connotation that they vaguely float somewhere in outer (cyber)space), however, it is important to speak of a 'loss of knowledge of location' rather than a 'loss of location'.

Finally, it is important not to allow language to obscure the nature of what a cross-border search entails. Although it is customary to speak of 'visiting' a server and 'looking around' in a mailbox, computer users do not really visit computers or actually look into mailboxes. The 'travel' metaphor is misleading, at least in our context: speaking of a police officer 'going to' a remote server tends to trigger a frame associated with police officers entering the territory of a foreign state, and the physical presence of officials of one state within the territory of another is a major factor in the international-law assessment of the legality of extraterritorial state activities. Since cross-border computer searches do not involve the physical presence of persons, we should attempt to avoid metaphors associated with this frame. We suggest instead that a search is best characterised as the sending and receiving of messages, which comes closer to the actual technical form in which remote searches occur: a client computer sends a message to a server computer with a certain request, and the server interprets and acts upon this request in the way it was programmed to do. The legal qualification of a cross-border search—its lawfulness—could thus be investigated in the frame of whether law enforcement agencies are allowed to send requests to entities on foreign territory.

International law—the strict interpretation

In the strict—and still dominant—interpretation of international law, any evidence-gathering activity in a foreign state, including the making of a mere phone call, can be considered a breach of state sovereignty. Accessing data that is, or later turns out to be, stored on a server located in the territory of another state, without the prior consent of that state, constitutes a breach of the territorial integrity of that state and thus a wrongful act. The fact that the searching state may have difficulty in determining the location of data at the moment of access does not preclude or mitigate the wrongfulness of the action, nor does the consent of the user or that of the provider. Exceptions such as self-defence, force majeure, and distress are not applicable in this context; only the latter might potentially apply in extreme circumstances, but not in the regular pursuit of normal criminal investigations. The only real possibility under existing international law for precluding wrongfulness is where the state affected has given prior consent, either for a specific search upon a specific request, or in a generic form for certain types of searches under certain conditions; Article 32(b) of the Cybercrime Convention, which allows cross-border access to data with consent of the user or provider, if both countries are parties to the Convention, is an example of the latter.

Article 32(b) can also be interpreted as including the possibility of cross-border searches with lawfully obtained credentials (i.e., the login name and password for remote accounts, if lawfully provided by the suspect or service provider, or found, for example, on a post-it note on the suspect's desk during a lawful search), if the law enforcement agency from state A knows that the data are in state B and B has ratified the Convention. However, this interpretation of the Cybercrime Convention has yet to be agreed among the state parties to the Cybercrime Convention and thus cannot be considered a legitimate interpretation of the provision yet. Although the reading we suggest here does provide one way of opening the discussion about cross-border access to data, it should be pointed out that it provides only a limited exception to the general status of cross-border access to data under international law: it applies only to states that are party to the Cybercrime Convention; it applies only if the law enforcement agency knows, or has good reason to believe, that the data are stored on the territory of another signatory state; and it applies only to the form of access to data with lawfully obtained credentials, and not to other forms of cross-border searches. Therefore, the possibilities within existing international law for cross-border access to data without the consent (ex ante or ex post) of the affected state are, in the strict interpretation of international law, rather limited.

International law—broadening the perspective and developing new agreements

While the strict legal interpretation is that cross-border data searches without the affected state's consent breach the obligations that all states owe one another to respect state sovereignty, a less doctrinal approach to international law views behaviour by a state as more or less justifiable depending upon the strength of the arguments made. There are several more or less plausible arguments that can be made on the basis of existing legal regimes that could advance an

alternative legal account of how states could better relate to one another within the space of the cloud and cyberspace to achieve shared aims.

Where states have sufficient interest in doing so, they are capable of developing legal regimes that put aside claims based on territorial sovereignty, although such regimes are rare. However, the legal framework applicable to outer space, and to satellite imaging in particular, suggests that where technology makes assertions of territorial sovereignty untenable (for instance, to fit the functioning of satellites to exact national territorial borders) and where states perceive a shared interest in an alternative framing (for example, benefitting from shared satellite imagery), a principle such as open skies can develop. This principle comprises the right of a sensing state to collect and distribute satellite imaging without regard to the wishes of the sensed state, as well as an obligation upon sensing states to make the imaging available to the sensed state on a non-discriminatory basis and on reasonable cost terms. Similarly, where the nature of a space, such as the oceans or the wildness of Antarctica, limits states' ability to make that space into place, capable of being subjected to territorial claims, states will create a regime that recognises that limitation and co-operate to ensure that such 'space' does not become a space outside the law, i.e., a space ungoverned and ruled by 'outlaws'.

The first possibility of moving forward in international law is to make efforts to change the status quo. The urgency of the need to do something about the increasing challenges of cyber-investigation, not least through the development of the cloud, is increasingly acknowledged. Cybercrime is high on the agenda of international policy-making institutions, which opens up pathways for the discussion of new instruments in which states may agree to allow certain forms of cross-border access to data. Such instruments might be developed within the United Nations (e.g., the Commission on Crime Prevention and Criminal Justice), but the momentum for moving forward in developing a new legal instrument seems rather to lay with the Council of Europe in the context of the Cybercrime Convention, in which a protocol on cross-border access to data is currently being discussed.

In developing a new instrument, there is a necessary trade-off between substance and process: the less ambitious a proposal is in scope and substance, the easier it will be to persuade more states to agree. An instrument is also more likely to be successful if concerns are adequately addressed about over-reaching powers and about the possibility of a lack of transparency. Strong safeguards should be built in, both relating to individuals in the context of data protection and human rights, and in relation to concerns about sovereignty infringements. It will be necessary to reassure particularly those smaller or less powerful states who are likely to view cross-border data searches by states of the global North as threatening and as something from which they do not benefit. Therefore, in addition to clear limitations on the scope and content of data searches, attention should also be paid to benefit-sharing.

Another pathway that may be possible within the Cybercrime Convention is to re-interpret Article 32(b) as including the possibility of cross-border searches with lawfully obtained credentials, if the law enforcement agency from state A knows that the data are in a signatory state B. This interpretation needs to be agreed among the state parties of the Cybercrime Convention before it can be accepted as a legitimate interpretation, but this could be done by agreeing on a Guidance Note, which may be easier than negotiating a new instrument that requires ratification to come into force. This pathway provides a relatively limited exception to the general status of cross-border access to data under international law and thus does not preclude other possibilities for creating cross-border access to data.

Advancing a plausible alternative account of international law by early adopter countries

Given the changing landscape of the Internet and the rise of cloud computing, which compounds the already existing challenges to cyber-investigation, states need to invest serious efforts in developing some form of agreement on cross-border cyber-investigation. Such agreement will not be easy or expeditious, regardless of whether it concerns a treaty or a Protocol, within the UN or the Council of Europe. It simply concerns too complex and too sensitive an issue for the necessary level of consensus to be reached within the short term.

This increases, then, the plausibility of a second possibility for moving forward. This is that one or a few countries take the initiative and develop a certain practice of cross-border cyber-investigation, while simultaneously advancing a plausible theoretical account of why they

consider this practice compatible with international law. Such countries could be considered early adopters of an emerging practice that will take time to be accepted by the wider international community. While the strict legal interpretation remains that cross-border data searches are unlawful, a non-doctrinal approach to international law sees behaviour as being more or less lawful depending upon the strength of the arguments that one makes. There are several more or less plausible arguments that can be made on the basis of existing legal regimes that could advance an alternative legal account of how states could better relate to one another within the space of the cloud to achieve shared aims. Legal regimes such as those for outer space, the high seas, combating piracy, port state jurisdiction, and satellite imaging (with its principle of open skies) can provide inspiration as well as arguments to draw from in developing an alternative account of cyberspace or the cloud in which some form of unilateral action within that space is plausibly acceptable.

To gather plausibility momentum, one or two states—better still, a group of states—need to forge ahead in developing an alternative legal account. These states could start suggesting a new principle of 'open cyberspace' in the context of cross-border access to data, similar to the principle of open skies in the context of remote sensing. Belgian law provides one step in that direction, but it seems to lack a well-developed theoretical account that is promulgated internationally, and a current Dutch proposal for cross-border searches another. The latter is, however, implausible in its current form, as it does not limit itself to what can be considered the minimum intrusion necessary in cross-border cyber-investigations. The account can be improved by limiting the scope (e.g., only accessing but not deleting data; only for investigations into (almost) universally penalised serious crimes, such as child pornography), including more safeguards (e.g., notification to states where possible), and better substantiation (e.g., connecting cross-border access to data more explicitly and in more detail to existing legal regimes for non-standard spaces). Another important aspect of a plausible account is to explain what the state considers to be a reasonable effort to ascertain the location of data. Some threshold must be proposed for the level of efforts that can be expected of law enforcement authorities, both in technical and in legal terms, before they can claim that the location of data is unknowable. States should attempt to make explicit what is good practice by identifying the necessary technical and operational measures for various situations of cross-border searches. It should be borne in mind that any breach of territorial integrity without prior consent of the searched state constitutes an international wrong, even where the law enforcement authorities acted in good faith and assumed that the data were located in their own territory or reasoned that they could not determine the location with sufficient likelihood. Therefore, any threshold of the effort that can be expected of law enforcement authorities to determine the location of data must be high in order to be plausible.

Where early adopters advance an alternative legal account for criminal investigation in cyberspace, it is crucial that they act openly in accordance with that account. The more forums in which an alternative account of the sovereignty question is presented and discussed—such as the Octopus conferences of the Council of Europe, the CCPCJ Congress, the Internet Governance Forum, and international Cyberspace Conferences—the more credence it may gain, even where it is not formally adopted. The more states that can be persuaded to similarly adopt the alternative account, the stronger the legal argument will become.

Further, other states are more likely to be reassured where early adopters are open about their actions and allow their actions to be overseen by an independent body. A mechanism could be developed, similarly to the role of the UN Secretary-General as a repository of all information on satellites' trajectories within the open skies framework, by which early adopters are required to make public the nature and scope of searches that they conduct, i.e., a precise and detailed account of the types of searches that their legislation allows and of the safeguards that limit the scope and intrusion of these searches. Moreover, it would also help credibility and transparency if certain basic details of particular cross-border actions (such as date and time of access, type of crime under investigation, type and amount of data accessed, and some identifying information of the servers accessed) were deposited with an independent body and accessible in some form to states.

While moving forward by developing a plausible account for the lawfulness of unilateral cross-border searches, early adopter states should be aware of certain risks involved in this process. First, where a state acts in a unilateral manner to access data stored in the cloud, other states will

act in a similar manner, and the state forging ahead would be estopped from protesting about such behaviour or from claiming an infringement of their territorial integrity where the data was located on their territory. Moreover, once a state starts down this path, it cannot easily reverse its position if the strategy later turns out to negatively affect its interests in certain circumstances. Therefore, any state pursuing such a strategy should think hard about how the alternative legal account proposed could be used in ways that harm their interests or those of its citizens. Second, there may be unintended consequences in other areas: any claims made in relation to cross-border access to data are likely to influence the development of rules in other areas fields related to cyberspace (e.g., trade, national security). Arguments about universal jurisdiction or about an 'open cyberspace' principle may not suit the interests of the original proposing state where they resurface in other areas. Third, any state that takes a unilateral stance may find that other states become less co-operative than they might usually expect, whether in relation to matters of cross-border policing or more broadly. In short, states aiming to move forward in cross-border cyber-investigations and proposing measures for unilateral actions should carefully consider the broader, possibly negative, consequences and weigh these against the benefits of unilateral cross-border access to data.

Conclusion

The analysis in this report leads to the conclusion that there are strict limits within international law for cross-border cyber-investigations. The dominant interpretation of international law implies that accessing data that are, or later turn out to be, stored on a server located in the territory of another state without the prior consent of that state constitutes a breach of the territorial integrity of that state and thus a wrongful act. The wrongfulness is not mitigated by the fact that the searching state may have difficulty in determining the location of data, nor by the consent of the user or the provider to access the data. The only possibility for lawful cross-border cyber-investigation is where the affected state has given prior consent, either on an ad-hoc basis or via a treaty that provides for certain types of searches under certain conditions. The latter is the case with Article 32(b) of the Cybercrime Convention, which allows cross-border access to data with consent of the user or provider, if both the states concerned are parties to the Convention.

Overall, international law therefore presents considerably larger limits than possibilities for cross-border cyber-investigations. This is problematic, since law enforcement is facing a serious challenge in gathering evidence as more and more data move to the cloud or are otherwise processed in cyberspace remotely from the traditional locus of criminal investigations. Negotiating the limits of international law and creating new possibilities will require much effort, patience, and care. As we have emphasised in this report, breaking through the current stalemate requires substantial preliminary work to create a shared basis of common understanding.

This preliminary work should comprise at least three types of efforts. First, the challenges of cyber-investigations, in particular the need for expeditious cross-border access to data in the cloud era, need to be formally recognised at the international level. It is not sufficient that law enforcement officers publicly voice the problems they are facing—these problems need to be acknowledged by state representatives in international fora before they can be recognised as challenges to be dealt with in international law. Second, the problems need to be conceptualised carefully and explicitly. Stakeholders should be aware of the effect of metaphors employed in debates, and care should be taken to use the most appropriate metaphors. Framing cyberspace as 'space' (a more abstract area) rather than as 'place' (a physical area) can make a difference in terms of thinking about solutions, as does conceiving of cross-border searches as the sending and receiving of messages rather than as 'going to' a server. The fact that the location of data is hard to identify in cloud-computing contexts should be conceptualised as a loss of knowledge of location rather than a loss of location itself. And defining legal authority in terms of effective control rather than controlling territory within national boundaries may also help to understand jurisdiction in relation to 'space' instead of uniquely connected to 'place'. Third, both the community of cyber-investigation and the community of international law must become acquainted with and familiarise themselves with the other community's language, concepts, and assumptions at a much deeper level than is currently the case. In our research, we were struck by the relative lack of understanding amongst cyber-investigation experts of the basic principles of and developments within international law, as well as by the relative lack of understanding on the part of international law experts of the basic principles of and developments within cyber-

investigation. Bringing these communities together is not only a matter of bridging theory (international law) and practice (cyber-investigation), but also of bringing together people who can develop a shared understanding of the problem and the framework within which the problem needs to be addressed. Only then can an account be developed of cross-border cyber-investigations that is plausible both in technical and in international law terms.

When preliminary work along these lines is undertaken, states can take steps forward to address the challenge of cross-border cyber-investigation in a two-prong approach. The focus of short-term efforts could be towards creating and enhancing the legitimacy of narrowly defined, transparently conducted, and strongly safeguarded unilateral actions of early adopters who advance an alternative account of sovereignty in cyberspace. At the same time, longer-term efforts can be undertaken that seek to create binding law at the international level in the form of an international or widely shared multilateral legal instrument allowing narrowly defined and strongly safeguarded forms of cross-border cyber-investigations. Neither will be an easy pathway to successfully solving the problems that cyber-investigation is facing in the cloud era, but both are necessary to embark upon if law enforcement is to move along in the 21st century.

1. Introduction

> 'By art is created that great Leviathan, called a commonwealth or state, which is but an artificial man… and in which, the sovereignty is an artificial soul.' (Thomas Hobbes)

1.1. Background

One of the consequences of the rise of cloud computing—which in simple terms refers to using scalable computing resources as a service via the Internet—is that computer data are increasingly stored remotely ('in the cloud') instead of on users' devices. This has significant implications for criminal investigation, particularly in cases where digital evidence is sought. Local search and seizure by the police will yield less and less evidence as users use cloud services such as webmail and remote data storage. This reinforces existing challenges of cyber-investigation, which not only has to deal with swift evidence-gathering due to the vulnerability of data loss, but also has to find ways of remotely getting access to data, such as remote online searches or production orders directed at service providers.

One particular challenge in cyber-investigation is that such remote evidence-gathering powers may well extend beyond national borders. Extraterritorial investigation is, in principle, not allowed unless international agreements among states provide for unilateral cross-border investigation powers. So far, international instruments dealing with cyber-investigation, such as the Convention on Cybercrime,[1] do not allow the use of cross-border investigative powers without consent (where the computer system is not intentionally open access). Therefore, remote access to computer data through remote cross-border searches or directly ordering foreign service providers to produce data are currently not allowed, and states must resort to traditional procedures of mutual legal assistance, which tend to be relatively slow and not well-suited to securing digital evidence.

Although this has been the case ever since computer networks existed, the rise of cloud computing makes the question of cross-border investigation more significant than in those earlier days of cyber-investigation. The extent to which users no longer store data on hardware in their possession (and thus likely to be located within the same jurisdiction) but in the cloud has created a major problem for law-enforcement agencies (LEAs) in the investigation of a wide range of crimes; this problem is not limited to cybercrime – those crimes that are facilitated either in nature or scope by the internet – but also traditional crimes that are located solely within one jurisdiction but where criminals communicate via email or smartphone apps. Although many debates have taken place aimed at trying to move forward in the field of cross-border cyber-investigation, no visible results have been achieved so far. A key reason for this is that international law tends to be strict in prohibiting investigative activities on foreign territory without the consent of the state concerned, due to the importance of territorially-based national sovereignty. The situation is thus one of stalemate: cyber-investigation officials would like to move forward in cross-border investigation but run into stop signs based on current interpretations of international law, while international law—although in considerable flux through developments in polycentric governance—does not provide scope for cross-border criminal investigation, because the specific challenges of cyber-investigation have so far not induced states to move beyond strict interpretations of sovereignty.

[1] Convention on Cybercrime, CETS 185, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185 (hereafter also: Cybercrime Convention). This Council of Europe convention is open for ratification by non-European states. It entered into force in 2004. As of December 2014, 44 states have ratified the convention, including the United States, Australia, Japan, the Dominican Republic, Mauritius, and Panama. CoE member states that have not ratified the convention include Greece, Ireland, Poland, Russia, and Sweden.
All URLs referred to in this report have been last accessed 1 December 2014.

1.2. Research aim and questions

Against the background of a possible stalemate between the increasing needs of cross-border cyber-investigation, particularly in, although not limited to, cloud computing environments, and the traditional interpretation of territory-based national sovereignty, the Research and Documentation Centre (WODC) of the Netherlands Ministry of Security and Justice has commissioned the authors to research the challenges of cyberspace and cloud computing for criminal investigation from the perspective of international law. This report is the result of that research and aims to advance the debate on cross-border cyber-investigation by combining the fields of cyber-investigation law and international law. Our aim is to determine not only the limitations and boundaries but also the possibilities that international law may afford for cross-border cyber-investigation. The central question we aim to answer is:

> What limits and what possibilities exist within international law for cross-border cyber-investigations?

We will address this question by answering the following sub-questions:

1. What is cloud computing, and how does this challenge cyber-investigation in the classic paradigm of mutual legal assistance?
2. How can the problem best be conceptualised? In particular:
    a. how can the international law perspective on cross-border cyber-investigation be conceptualised?
    b. How can the law-enforcement perspective on cross-border cyber-investigation be conceptualised?
    c. How can cross-border access to data be conceptualised?
3. What are the boundaries and possibilities of cross-border cyber-investigation? In particular:
    a. what are current laws and practices in cross-border cyber-investigation?
    b. What is allowed under the current international law framework?
    c. Which doctrines may help in interpreting grey areas?
    d. Which consequences attach to moving beyond current boundaries of international law?
4. What are useful ways forward in addressing the challenges of cross-border cyber-investigation?

1.3. Limitations

Cloud computing is an umbrella term for various kinds of remote computer services: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) (see section 2.3 for an explanation of the cloud). In this report, we limit ourselves to one type of usage of cloud computing, namely for remote data storage (which will usually be relevant in SaaS contexts, although investigative remote access to data can theoretically also be applied with PaaS or IaaS).

Cross-border cyber-investigations can take many forms; we will focus particularly on two types of cross-border access to data: remote searches (where state A searches data stored in state B through an Internet connection, with or without consent and with or without circumventing security measures) and contacting foreign service providers to request data (on a voluntary or obligatory basis). This report limits itself to the actions of LEAs; it does not consider the actions of other state agencies, such as intelligence or security services, in collecting and analysing data from the Internet. This report begins from the standpoint that these state actors have a strong interest in abiding by the rules of international law.

The perspective of international law primarily focuses on questions of the legality of cross-border access to data under international law in terms of the core principles of territorial integrity and non-interference in domestic affairs, rather than on questions of human rights. While this report indicates the ways in which human rights obligations are likely to be engaged by cross-border data searches, it does not deal with specific human rights in any depth. Where some of the suggestions for possible solutions in this report may lead to more intrusive forms of cross-border access to data, we recommend a further study focusing on the human rights implications, including issues of data privacy and secrecy of communications, of such action.

1.4. Methods

The research of this report is based on two methods. First, we have conducted desk research of international and supranational law and policy and academic literature in the fields of cybercrime/cyber-investigation and of international law. Second, we have organised an expert workshop, in which around twenty experts—both academics and practitioners—in the fields of criminal law, cybercrime, Internet, and international law discussed the issues of cross-border cloud-computing-related criminal investigation in a roundtable setting under Chatham House rules (see Appendices 0 and 0 for a list of participants and the discussion agenda). The results of the workshop have been used to fine-tune the research questions and focus of the research, and also as a source of specific findings, which we will reference in the footnotes as 'Expert workshop 19 December 2013'.

1.5. Outline of the report

The report follows the sub-questions identified above. Chapter 2 provides an introductory background, sketching the basics of cyber-investigation, international law, cloud computing, and the classic approach to cross-border cyber-investigation. Chapter 3 then provides an extensive conceptual background, which we think is a prerequisite for any attempt to solve the problems of cross-border cyber-investigation, since a common understanding of the ways in which cyber-experts and international law experts frame the issues is vital for moving beyond the current stalemate. The chapter describes the frames of the international law and the law-enforcement perspectives, and it discusses how the central notion of cross-border access to data is and could be conceptualised. Chapter 4 then provides the main analysis of the problem, sketching current practices and the existing legal frameworks, and assessing to what extent and under which conditions cross-border cyber-investigation can be considered lawful under international law. Chapter 5 provides insight into possible paths ahead, given the findings of the analysis. It sketches what could be done at the international and supranational level, and what—given the nature of this report as a contribution to Dutch policy-making—the Netherlands could do in its law and policy to foster international steps forward in this area.

1.6. Acknowledgements

We gratefully acknowledge the contribution that many people provided to assist our research. The experts participating in the workshop (see Appendix 1) have contributed to our understanding of the challenges and underlying problems we address in this research. We thank the members of the advisory committee (see Appendix 3) for their insightful and constructive comments on draft versions of the report. Jan-Jaap Oerlemans, Merel Koning, and Eleni Kosta provided welcome assistance in processing the workshop results. Jaap-Henk Hoepman, Rik Kaspersen, and Jan-Jaap Oerlemans offered helpful suggestions on particular aspects of the research. We also thank Anouk Sterks, Rosanne Franken, and Tomislav Chokrevski for research assistance and Femke Abousalama and Ghislaine van den Maagdenberg for practical assistance.

2. Background

2.1. Cyber-investigation: a primer for international law experts

The term 'cybercrime' is commonly used today instead of the term 'computer-related crime' that was more common in the 1980s and 1990s, indicating a shift in focus from computers to computer networks. The 'cyber' element—derived from the term 'cyberspace' (cf. *infra*, section 3.2)—refers to the fact that computer networks constitute a special type of environment, in which data can so easily and rapidly flow between all connected computers that they seem to reside in the fuzzy totality of the computer network rather than in specific computers (even though specific data at a specific point in time usually reside on a specific computer). The functionality of cyberspace, and one of the primary characteristics that make the Internet such an important development in society, is that it does not really matter on which specific computer data are located, as they can be retrieved almost instantaneously from any server within the network. This changes not only the character of the ways in which computers are used in society in general, but also how criminals can attack computers and data, as well as how law-enforcement authorities can find evidence.

Cyber-investigation, for the purposes of this report, refers to criminal investigation in relation to cyberspace, or more simply in relation to computer networks. Although one may be tempted to think that cyber-investigation is primarily relevant for investigating cybercrimes, this is not the case. In developed countries (and to some extent also in many developing countries), computers are ubiquitous and thoroughly ingrained in social life, particularly considering the fact that the term 'computer'—a device that 'pursuant to a program, performs automatic processing of data'[2]—not only covers traditional personal computers and laptops but also smartphones and many other types of data-processing devices, such as car navigation systems and sensor-equipped smart watches. Not only do people use computers or smartphones very frequently to create data (e.g., photos) and to communicate, but many activities also leave digital traces, such as browsing the web or travelling around with the smartphone in stand-by mode (generating location data that may be stored by telecommunications or app providers). These data can be relevant for criminal investigations, as digital documents and digital traces can reveal, for example, suspects' whereabouts, travels, contacts, behaviour patterns, and intentions. Consequently, any type of crime can involve evidence stored in a computer, and cyber-investigation is therefore potentially relevant for all criminal investigations.

Very generally speaking, classical criminal investigation involves two basic types of evidence-gathering: the police can ask people to provide evidence or go and search for evidence themselves. Both activities are backed up by coercive powers allowing the police to acquire information by force: production orders and search and seizure powers. In general, this is not different in cyber-investigation, where the police also have powers to give production orders (cf. art. 18 Cybercrime Convention) and to search and seize (cf. art. 19 Cybercrime Convention). The character of these powers is somewhat different, as the emphasis is less on physical evidence (such as objects or bodily material) and more on immaterial evidence, i.e., information or data. Computer-related production orders can therefore involve the production not only of goods (such as computers or data-storage devices) but also of data. Search and seizure can involve searching a house and seizing a hard disk found in the house, but also searching inside a computer and copying data. A key difference between seizing objects and 'seizing' (or rather, in the Cybercrime Convention's terminology, 'securing') data is that objects can only be in the possession of one person at one point in time and hence are removed from a suspect's power of disposal if seized, while data can be in possession of multiple people at the same time and can therefore remain at the suspect's disposal if secured by the police through copying. (Hence, if the police want to remove certain data, such as child pornography, out of the suspect's possession, they need to either seize the data *carrier* or make an additional effort, after copying the data, to 'render inaccessible or remove those computer data in the accessed computer system', in the

[2] Art. 1(a) Cybercrime Convention.

formulation of art. 19(3)(d) Cybercrime Convention.) And contrary to physical objects, which can only be seized when being directly present, data can be secured remotely through computer networks.

In addition to the classic production orders and search and seizure, there is a third type of evidence-gathering, in the form of special investigatory powers, such as covert camera surveillance, investigation of telecommunications, and undercover operations. These differ from search and seizure in two primary ways: they are usually covert (whereas a search is generally known to the suspect) and they usually take place over a certain, possibly long, period (whereas search and seizure is generally a one-off activity). All kinds of special investigation powers can be conducted in physical space (and in the case of telecommunications, in the analogue context of traditional telephony), but they are also well-suited to be applied in cyberspace. The modalities and scope of special investigatory powers differ significantly across countries, and they are infrequently regulated at an international level, with the exception of telecommunications investigations, which are to some extent harmonised through the Cybercrime Convention (articles 17, 20, and 21) and the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[3] (articles 17-21). Significantly, the Cybercrime Convention stipulates that parties to the convention should enable the use of their investigation powers for all criminal offences which were committed through computers and to collect electronic evidence of a criminal offence (in other words, search and seizure and production orders should apply, in principle, to any type of offence), but parties can choose to allow interception of communications and collection of traffic data[4] for a more limited set of crimes (article 14). This underlines the lack of harmonisation of special investigation powers, which may affect the possibilities for mutual legal assistance (cf. *infra*, section 2.4).

We have already mentioned the fact that physical objects and data are different animals, with data being multiple as well as movable and remotely accessible with the speed of light. This has several consequences for cyber-investigation being different from classical criminal investigation. Data are volatile: they can be moved thousands of miles with a few mouse clicks; they are also vulnerable, being easily changed or removed. To be sure, physical objects can also be moved and changed and removed, but this requires time and physical effort, making it less feasible for perpetrators to manipulate or hide evidence if they notice the police are about to conduct an investigation. With digital evidence, the risk of data being (re)moved or manipulated is much higher, making it often essential that cyber-investigations collect all possible evidence as soon as an investigation is started. If they notice, during a search of a computer in a house, that data are not stored locally but remotely, they will need to extend the investigation to the remote computer instantaneously, otherwise there is a high risk that the data will be moved or deleted (see article 19(2) Cybercrime Convention and *infra*, section 3.4.1). Time is of the essence in securing remotely stored, relevant data as evidence.

In a similar vein, tracing back a trail of evidence can be considerably more complex than in the physical world. Digital evidence can be moved back and forth around the world within seconds. Physical evidence can, of course, also be moved quickly, for example by car or plane, but this always requires some time, money, and effort, while digital evidence can be moved from a server in Germany via a server in Malaysia to a hidden server in Mexico within the space of minutes, at little cost and effort. This also underlines the need for almost instantaneous action by the police if they have good reason to believe certain evidence is stored in some place on the Internet.

2.2. International law: a primer for cyber-investigation experts

2.2.1. The nature and purpose of international law

International law is classically understood as regulating relations between states. It is a horizontal legal system woven from the reciprocal obligations that states owe each other. Although the remit of international law has been extended in the modern period to grant international legal personality to non-state actors, such as international and regional organisations and, to a more

[3] Council Act of 29 May 2000, 2000/C 197/01, *OJ* C 197/1, 12.7.2000.
[4] Traffic data are data about telecommunications use, such as who called whom when.

limited extent, individuals, states remain the primary actors within the international system. Only states are sovereign; all other international legal personality is derived from the will of states.[5]

All states are sovereign. Sovereignty in international law (sometimes known as 'external sovereignty') signifies independence from all other actors and denotes the right to exercise in regard to a defined physical space all the functions of a state. Sovereignty within international law is thus territorial sovereignty. The right of exclusive competence to regulate affairs within a defined territory is the basis of the doctrine of sovereign equality, which founds the sovereign right of all states – regardless of physical size, or military or economic might – to participate in international relations from a position of formal equality. All states are thus equal. Consequently, no state may interfere in the internal affairs of another state. This principle is codified and elaborated in the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States.[6] There are two keys aspects to non-interference as elaborated by the Declaration: the first is territorial integrity. The Declaration provides: 'States shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State.' A breach of territorial integrity – which occurs when a state enters the territory of another state without consent[7] – is thus equated with the use of force and may trigger the right to self-defence.[8] A breach of territorial integrity occurs even where no physical damage is done by an incursion; for example, where a police car of State A mistakenly crosses a border into State B and immediately retreats.

The second aspect of non-interference concerns the obligation not to interfere in any way in the domestic affairs of another state, whether or not such interference breaches territorial integrity. The Declaration provides: 'No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.' The principle of non-interference is a corollary of sovereignty and any breach constitutes a wrongful act.[9] The commission of a wrongful act has legal consequences, notably the obligations to cease the wrongful act and to make full reparation for the injury caused.[10]

As the primary actors of the international system, international law–classically understood–is the product of the will of states: states create international law by consenting to be bound. This principle was laid down by the Permanent Court of International Justice in the 1927 *Lotus* case. The Court stated: 'The rules of law binding upon States … emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims. Restrictions upon the independence of States cannot therefore be presumed.'[11] International law is thus a permissive system; anything that is not prohibited is therefore permitted and the general rule is that the consent of states cannot be

---

[5] For example, states create international organisations to serve their purposes and grant them legal personality to the extent that is necessary for them to fulfil their tasks; while liability for their actions may be independent of states, their competence to act is derivative. Likewise, actors such as NGOs are generally not understood as having international legal personality, except where it is specifically granted by states.

[6] Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, General Assembly Resolution 2625 (XXV) (1970), A/Res/25/2625. This Declaration is widely acknowledged to be a formulation of customary international law and, as such, is a binding source of international law.

[7] Determination of when actions are attributable to a state is governed by the law of state responsibility. See Article 4 of the 2001 Articles on State Responsibility, 53 UN GAOR Supp. (No. 10) at 43, U.N. Doc. A/56/83 (2001).

[8] The prohibition on the use of force is codified in Article 2(4) of the UN Charter and is a peremptory norm of international law. See, *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America)*; Merits, International Court of Justice (ICJ), 27 June 1986, available at: http://www.refworld.org/docid/4023a44d2.html. The right of self-defence is laid down in Article 51 of the UN Charter and the Caroline Doctrine.

[9] Circumstances in which a breach of an obligation owed does not constitute a wrongful act (circumstances precluding wrongfulness) are laid down in Part I, Chapter V of the 2001 Articles on State Responsibility. 53 UN GAOR Supp. (No. 10) at 43, U.N. Doc. A/56/83 (2001).

[10] The full legal consequences are laid down in Part II, Chapter I of the 2001 Articles on State Responsibility, *ibid.*

[11] *Lotus* case (1927), Judgement No. 9, *PCIJ*, Ser A, No. 10.

presumed. Moreover, international law is based upon the notion of reciprocity. Although modern international law does know obligations that continue to bind irrespective of the behaviour of other states – notably *ius cogens* norms (i.e., the prohibition on genocide or on torture) – the general principle is that a wrongful act by one state against another relieves the wronged state of the reciprocal obligation in relation to that state until the wrongful act ceases.[12]

The purpose of international law is to regulate the interaction of states. The prime function of international law in the modern era is to ensure peace.[13] It is for this reason that respect for sovereign equality and the principle of non-interference are accorded such centrality in general international law. These principles are contained in the secondary norms of international law that govern the interactions between states and the functioning of international law; examples of these areas of international law include the law of treaties, the rules on state responsibility and the laws of state and diplomatic immunity. However, international law not only governs the interaction between states but also regulates the co-operation of states to resolve shared international problems of an economic, social, cultural, or humanitarian character.[14] This has led to the rapid development and proliferation of areas of specialisation within international law, such as international environmental law, international human rights law, international economic law and international criminal law, to name a few. These areas of international law are not self-contained and are bound by the general rules of international law.[15] However, the principle of *lex specialis* determines that where two rules clash, it is the rule of the specialist system that has precedence; this stems from the express will of states (who have created the specialised regime). Thus, where the rules of international criminal law clash with older, general norms of international law, such as in relation to the norms of state immunity, it is, generally, the specialised rules that take precedence. The proliferation of specialised regimes within international law has led to the widely noted fear of fragmentation i.e. that the aims of specialised regimes begin to erode the general fabric of international law.[16]

International law, as the preceding paragraph suggests, is not static. As international law emerges from the will of states, states can act together to change international law. It also entails that the behaviour of states has the potential to change international law, particularly in a new or ill-defined area. Customary international law is created by the behaviour of states where they express their understanding to be bound by a rule i.e. not all behaviour changes international law but only that behaviour that is motivated by an understanding that the behaviour is either permitted or required by the law. Thus, where a state or group of states behave openly in a certain manner because they understand such behaviour to be permitted or obligated under international law, and, crucially, where no objections are registered from other states, the norms expressed by such behaviour will begin to be defined by it.

2.2.2. International law challenges for cyber-investigation

Territorial sovereignty is based upon the understanding that it is possible to determine the physical boundaries of a state. As Arbitrator Huber noted in the *Island of Palmas case*, '[t]erritorial sovereignty is, in general, a situation recognised and delimited in space, either by so-called natural frontiers as recognised by international law or by outward signs of delimitation that are undisputed, or else by legal engagements entered into between interested neighbours … or by acts of recognition by States within fixed boundaries.'[17] The idea that territory has determined boundaries does not of course entail that boundary disputes do not arise; indeed, most disputes

[12] The Permanent Court of International Justice confirmed the principle of *inadimplenti non est adimplendum* in a case between the Netherlands and Belgium concerning the course of the Meuse river: *Diversion of Water from the Meuse* [1937], PICJ, Series A/B, no. 70, 50. The rules on countermeasures are governed by the 2001 Articles on State Responsibility, 53 UN GAOR Supp. (No. 10) at 43, U.N. Doc. A/56/83 (2001), notably Article 49.
[13] See Article 1(1) of the UN Charter.
[14] See Article 1(4) of the UN Charter.
[15] See India etc versus US: 'shrimp-turtle', WTO case Nos. 58 (and 61). Ruling of Appellate Body adopted on 6 November 1998.
[16] E.g., B. Simma & D. Pulkowski, 'Of Planets and the Universe: Self-contained Regimes in International Law', *European Journal of International Law,* 17/483 (2006); M. Koskenniemi & Päivi Leino, 'Fragmentation of International Law? Postmodern Anxieties', *Leiden Journal of International Law,* 15/03 (2002), 553-79. For example, that the law of state immunity is interpreted through the lens of international human rights law, eroding the unity of international law as a system.
[17] *Island of Palmas (or Miangas)* Case (1928) 2 RIAA 829, 838-839.

within international law concern the precise delimitation of territorial boundaries, whether of land or at sea. However, the basic assumption is that it is possible to define the limits of a state's territorial realm. Moreover, while states are willing to acknowledge physical realms beyond the territorial reach of any state – most notably the high seas,[18] Antarctica, and Space and other celestial bodies[19] – states have not been willing to view cyberspace as a place beyond the reach of territorial sovereignty (see, *infra*, section 3.2.2). Rather, state behaviour in relation to cyberspace has seen states explicitly seek to assert their jurisdiction over activities in cyberspace.[20] The international legal context in relation to cloud computing is that cyberspace is not currently understood within international law as a separate legal space with specialised rules.[21]

The consequence is that data are viewed in international law through the lens of material objects – as a physical thing – that is necessarily located somewhere. International law is used to regulating objects that move across borders, such as maritime vessels or marine life, and it does so by locating the object legally by reference to its physical location.[22] Thus, once the location of data has been determined, territorial sovereignty tells us which state has jurisdiction over it. Any attempt to retrieve data from a server located within a state without that state's consent would then constitute a breach of territorial integrity and a violation of international law. There are some exceptions to this (see *infra*, section 4.1), but overall the lens of identifying a territory and the consequent exclusivity of state power over that territory remains the dominant international law perspective.

2.3. Cloud computing

2.3.1. What is the cloud?

In the last one to two decades, computing applications have increasingly used applications that are not on the user's computer but that are located somewhere with application services providers, which offer services via the Internet. Increasingly, these providers do not merely store data on a local server, but in a distributed way across several servers or server parks. At some point, this model was termed 'cloud computing', in which the term 'cloud' is based on the custom, in pictures of computing models, of using a cloud to graphically represent the network in which data processing takes place. Although the model of remote and distributed services is not new, the combination of characteristics of present-day cloud computing causes new challenges in many fields. The special combination of characteristics is captured in the US standardisation institute NIST's definition of cloud computing as

> a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[23]

In simpler terms, cloud computing can be described as 'a way of delivering computing resources as a utility service via a network, typically the Internet, scalable up and down according to user

[18] Convention on the Law of the Seas.
[19] 1967 Space Treaty.
[20] See section 3.3.1; cf. Jack L. Goldsmith, 'The Internet and the Abiding Significance of Territorial Sovereignty', *Indiana Journal of Global Legal Studies,* 5 (1998b), 475-91 and the cases described in section 4.1.2 *infra*.
[21] Although cyberwarfare is discussed extensively in the context of international law, this is typically done from the perspective of fitting cyberspace into the framework of existing international law, not in a separate, *sui generis* legal regime.
[22] A partial exception are civilian marine vessels on the high seas; here jurisdiction is determined by the place of vessel registration, more commonly denoted by the flag flown by the vessel ('flag jurisdiction'). It is a partial exception because flag jurisdiction is not absolute and its parameters are determined by the location of the vessel i.e. whether on the high seas, in territorial waters or in contiguous zones etc. The exceptions are laid down in the 1982 Law of the Sea Convention. See also R. C. F. Reuland, 'Interference with Non-National Ships on the High Seas: Peacetime Exceptions to the Exclusivity Rule of Flag-State Jurisdiction', *Vanderbilt ournal of Transnational Law,* 22/1161 (1989)
[23] Peter Mell and Timothy Grance, 'The NIST Definition of Cloud Computing' (Gaithersburg, MD: National Institute of Standards and Technology, 2011).

requirements'.[24] 'Typical' cloud computing examples are email services such as Gmail and Hotmail, data storage or sharing services such as DropBox and Megaupload, and application services such as Google Docs. Cloud computing is often distinguished in three forms: Infrastructure as a Service (IaaS) ('raw' computing resources, such as Rackspace or Google Compute Engine), Platform as a Service (PaaS) (platforms for developing and using software applications, such as Microsoft's Windows Azure and Amazon AWS), and Software as a Service (SaaS) (offering software as a remote service for end users, such as webmail services or word-processing software apps).[25] A subcategory of the latter is 'storage as a service', in which users 'can manage data storage, organization, and retrieval from any location over the Internet, for example Dropbox or Rackspace's Cloud Files'.[26] For the purposes of our study, we are particularly interested in SaaS applications, and more particularly in remote storage services, since these are of primary concern for criminal investigations of data.[27]

Data can be stored in the cloud in different ways. For efficiency purposes, a certain set of data can be distributed (in pieces) among various computers, and automatically relocated depending on the supply and demand of storage space in the cloud at a certain point in time. Thus, a 'data set may be dispersed in fragments (…) among servers or other storage equipment, to be reunited and delivered to a user logging in with the correct credentials.'[28] This occurs particularly with databases, but may also happen with other types of data.[29] For information security reasons, data will often be stored redundantly, in multiple copies, so that if one server (or server park) malfunctions, data can still be retrieved. For example, 'Google and Microsoft maintain two replicas of each data set, typically in different data centres'.[30]

The distributed, dynamic, and redundant nature of cloud storage makes it difficult to say 'where' a certain file 'is' when it is stored in the cloud: it can often be in multiple places simultaneously, while it may not be in any single place in its entirety. Although this could well imply that, with cloud providers having server parks in various places and countries, data might be stored anywhere, the unlocatability of cloud data needs to be qualified in two ways. First, users can increasingly indicate a preference or requirement of a certain region in which their data should be stored (for example, 'in Europe').[31] Second, data storage depends not only on the fluctuating storage capacity in the provider's server parks, but also on the time it takes to reassemble a file and facilitate user access to the file; as longer distance does affect retrieval time, despite the Internet's lightning-speed data transfer capability, at least one copy of the data or data set will often be stored in the server park that is closest, or at least relatively close, to the user's normal location.[32]

2.3.2. Cloud computing compounding challenges for cyber-investigation

Obviously, when data are no longer stored on the user's device but in the cloud, investigating user devices to collect data for criminal investigation purposes will be less useful. It will not be completely useless, as traces of cloud activity may remain in the user's computer, for example in temporary files or in the form of passwords stored in the computer's short-term memory. In searches, the police will therefore have to be more aware of the importance of searching and

[24] W. Kuan Hon and Christopher Millard, 'Cloud Technologies and Services', in Christopher Millard (ed.), *Cloud Computing Law* (Oxford: Oxford University Press, 2013a), 3-17 at 3.
[25] See ibid., at 4.
[26] Ibid.
[27] The cloud poses some other relevant challenges for criminal investigations, such as distributed denial-of-service attacks and sending malware (see for an overview Bert-Jaap Koops et al., 'Misdaad en opsporing in de wolken. Knelpunten en kansen van cloud computing voor de Nederlandse opsporing' (Tilburg / Den Haag: TILT / WODC, 2012),), which may involve having to investigate remote computers in potentially unknown locations, but since this is more specific and relatively less frequent than investigating remotely stored data—which can occur in any type of crime—we will leave aside these other situations.
[28] Kuan Hon and Millard, 'Cloud Technologies and Services', at 9 (footnotes omitted).
[29] Ibid.
[30] Ibid., at 10.
[31] Ibid. The authors observe, however, that it is not clear whether providers in fact do restrict the storage to the indicated region, and that it is difficult for users and auditors to check compliance with a regional storage preference.
[32] Expert workshop 19 December 2013; Joseph J. Schwerha Iv, 'Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers"' (Strasbourg: Council of Europe, 2010), at 9.

seizing computers while they are active (i.e., turned on and with a power supply), in order to secure the computer's temporary memory and activated network connections, including connections with cloud services.

The combination of mobile devices (laptops, smartphones) and cloud computing implies that the police can rely less on search and seizure powers, which challenges criminal investigation practices that are today still often focused on searching particular places, such as the suspect's home or car.[33] Classic searches and classic wire interceptions will gradually be forced to make room for network searches, Internet interceptions, and production orders to cloud providers.[34] This is a considerable challenge, as it requires technical expertise and know-how, which is currently often limited to relatively small and specialised cyber-investigation units within the police. Moreover, the law may not be well adapted to these forms of investigation.[35] For example, in cloud contexts, it is not always clear whether a provider should be qualified—in European terms—as an electronic communications provider (simply put, a classic telecom provider) or as a provider of information society services (simply put, a hosting provider), which have differing legal regimes.[36] It may also be difficult to distinguish between stored data and data in transit, which is another distinction made in many legal systems.[37]

At the same time, the migration of data from suspects' hard disks to the cloud also presents something of an opportunity, as it enables the police to covertly investigate a much wider range of data, without a physical search of computers alerting the suspects that they are being investigated. This allows preliminary investigations to continue for a longer period, which can have tactical advantages in certain cases. However, this opportunity can only be exploited if legal and organisational challenges of cloud investigation are addressed, including impediments of Internet interception and of location-focused investigation practices.

Cyber-investigation challenges of cloud data are compounded by certain other factors. For example, cloud computing can involve multiple providers, in different layered constellations; a SaaS provider can, for example, use the infrastructure of a IaaS provider, or even use the platform of a PaaS provider which in turn relies on a IaaS service.[38] Dropbox, for example, is a SaaS provider that uses Amazon's infrastructure service;[39] in such layered constructions, it may be more difficult to determine the scope of the different providers' rights and capacities to access customer-uploaded data, or at least to determine the possible or likely place of the server(s) on which data are stored. Another factor is that data can be encrypted, by the cloud provider or the user, or by both. Encryption is used by several providers to protect data when stored in the cloud, and it will depend on the constellation whether the provider has access to the decryption key; many storage services seem designed at least to give providers 'backdoors' so that they can access user data for maintenance or support purposes.[40] When users encrypt data stored in the cloud themselves, however, data can only be retrieved via the user's decryption key (or by cracking, if the users do not use sophisticated cryptography or strong passwords). A third factor is that cloud-retrieved data may present evidence problems in court. Standards and procedures for gathering evidence from the cloud remain embryonic and have not yet been tested in legal practice. Technically, it is not easy to prove that a document downloaded from the cloud is the

[33] It should be noted that users may keep back-up copies of data they store in the cloud, so that cloud usage does not simply mean that classic searches become meaningless. According to Kuan Hon and Millard (Kuan Hon and Millard, 'Cloud Technologies and Services', at 25), 'users often back up their cloud data, whether to internal servers or to other cloud services', but this claim is based on corporate and institutional users rather than on individual users (ibid., at 74, 83).

[34] Note that the distributed and dynamic mode of storage in the cloud do not necessarily hamper these investigation powers, since a network search would retrieve the data from the cloud in the same way that the user does; Internet interception (near the user, or possibly near the provider) intercepts the documents as a whole as they move into or out of the cloud, and providers executing production orders are also likely to retrieve documents from the cloud in their entirety in the way that users would do.

[35] See, for example, G. Odinot et al., 'Het gebruik van de telefoon- en internettap in de opsporing' (Meppel: Boom Lemma, 2012), for some challenges in the Dutch legal framework for Internet interceptions.

[36] Ian Walden, 'Law Enforcement Access to Data in Clouds', in Christopher Millard (ed.), *Cloud Computing Law* (Oxford: Oxford University Press, 2013), 285-310 at 303.

[37] Koops et al., 'Misdaad en opsporing in de wolken', at 44-45.

[38] Kuan Hon and Millard, 'Cloud Technologies and Services', at 15-16.

[39] Ibid., at 15.

[40] Ibid., at 20-21.

same as the document that was uploaded into it, because of the distributed and automated dynamic storage, and files retrieved via the provider present evidence problems as the forensic procedures followed by cloud providers to obtain a document may not meet the forensic standard for not altering in any way the (meta)data provided to law enforcement.[41] Legally, the standards for admissible or reliable evidence differ from state to state, and particularly the rule of thumb that the (evidence) law applies of the state where data are stored ('lex situs') is problematic in the cloud context.[42]

The most serious overall challenge of cloud computing to criminal investigation may well, however, be the cross-border nature of cloud services. The most prevalent methods to collect digital evidence (searches, production orders, intercepting data) have limited effect with data that are stored in, or exchanged through, the cloud, given that criminal investigation is generally restricted to national territorial boundaries. Traditionally, in cases where data are or may be stored in another state, law enforcement will have to rely on mutual legal assistance or other forms of international cooperation, which we will discuss in the next section.

2.4. Classic approach to cross-border criminal investigation

2.4.1. Forms of cooperation

The main rule in criminal investigation is that for any enforcement action beyond the exercise of the territorial principle, the express consent of affected states is required. As the PCIJ remarked in the Lotus case, '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.'[43] States can therefore only exercise criminal investigation outside their borders if there is a basis in a treaty or custom, or with the permission of the affected state.

In the past decades, states have agreed to accept various forms of mutual assistance, co-operation, and cross-border investigation in a number of legal instruments and practices.[44] This is not only due to the increasingly cross-border or global character of criminal activities, but also because extraterritorial investigation is considered by several states to be a 'first line of defence' to combat crime.[45] The types of cross-border investigation include the following:

A. mutual legal assistance (MLA), usually based on a mutual legal assistance treaty (MLAT), in which state A (the requesting state) asks state B (the requested state) to perform some investigative action, such as search and seizure, a production order, hearing a witness, or freezing a bank account;
B. mutual supranational data sharing, often in an institutionalised setting, including:
    a. multinational databases, such as the Schengen Information System;
    b. exchange or matching of national databases, such as DNA databases under the Prüm treaty;
    c. establishing bodies to facilitate information exchange between countries, such as Interpol, Europol, and Eurojust;

[41] Ian Walden, 'Law Enforcement Access to Data in Clouds', ibid., 285-310 at 288; Koops et al., 'Misdaad en opsporing in de wolken', at 50-52.
[42] Dominik Birk, Dennis Heinson, and Christoph Wegener, 'Virtuelle Spurensuche. Digitale Forensik in Cloud-Umgebungen', *Datenschutz und Datensicherheit,* /5 (2011), 329-32 at 331.
[43] PCIJ, *Lotus* (1927), Judgment No. 9, PCIJ, Ser A, No. 10, at 18-19.
[44] For overviews, see J.D. Mcclean, *International co-operation in civil and criminal matters* (3rd edn.; Oxford, U.K.: Oxford University Press, 2012) at 160-244; Saskia Hufnagel, '(In)security crossing borders: a comparison of police cooperation within Australia and the European Union', in Saskia Hufnagel, Clive Harfield, and Simon Bronitt (eds.), *Cross-border law enforcement: regional law enforcement cooperation - European, Australian and Asia Pacific perspectives* (Abingdon, Oxon; New York, NY: Routledge, 2012), 177-208; Marco Gercke, 'Understanding cybercrime: phenomena, challenges and legal response' (Geneva: ITU, 2012), at 267-80.
[45] Cyrille Fijnaut, 'The globalisation of police and judicial cooperation: drivers, substance and organisational arrangements, political complications', in Saskia Hufnagel, Clive Harfield, and Simon Bronitt (eds.), *Cross-border law enforcement: regional law enforcement cooperation - European, Australian and Asia Pacific perspectives* (Abingdon, Oxon; New York, NY: Routledge, 2012), 1-15 at 4, 6.

   d. (not institutionalised) spontaneous information exchange, where state B acquires information that it thinks may be relevant to state A;

C. extraterritorial investigation, in which officials from state A perform or assist in investigative activities in state B; these include:
   a. short-term extraterritorial investigation activities, such as cross-border hot pursuit;
   b. longer-term extraterritorial investigation activities, without assistance (but with implicit or explicit permission) of the foreign state, such as intercepting mobile communications or infiltration;
   c. police or judicial liaison officers working at a foreign embassy;

D. joint supranational investigations, such as EU Joint Investigation Teams or joint UN police missions to train or establish a police force in post-conflict regions.

Within these forms of international co-operation, it is traditional to apply limiting conditions so as to ensure that investigative activities in state B conducted by or on behalf of state A will comply with state B's laws, norms, and traditions.[46] This is demanded by the sovereignty of state B and the jurisdiction that flows therefrom to regulate what happens on its territory. However, within the European Union, there is a trend towards applying the national conditions in cross-border investigations less strictly. As a polity in which states should mutually trust each other sufficiently not to question each other's procedures, the EU has advanced the principle of mutual recognition (MR) as a cornerstone of judicial cooperation in criminal matters.[47] As a result, EU member states are obligated to assist other member states in criminal matters by complying with arrest warrants, evidence warrants, confiscation orders, and certain other orders, without full scrutiny of compliance with their own legislation.[48] In particular, the requirement of double criminality has been abolished for a list of specified offences, so that states cannot refuse assistance on the ground that the offence is not criminalised in their own legal system, except for offences that are not included in the 'mutual recognition' list.

Beyond the exception of a list of specified offences within the EU, cooperation without autonomous, full-scale scrutiny of compliance with the law of the requested state seems to exist only in local cross-border contexts in which there is a high level of mutual trust and strong connections among practitioners, such as among Scandinavian countries[49] and in the Meuse-Rhine Euroregion (encompassing regions of Germany, Belgium, and the Netherlands).[50] In such local contexts of border regions, the authorities are more likely to appreciate the seriousness of transnational crime in the same way, to have a common interest in cooperating, and to be concerned with maintaining public order and security in their immediate surroundings – three key factors that Fijnaut mentions as affecting countries' willingness to cooperate. With these factors pointing in the direction of more cooperation, the 'partial surrender of sovereignty rights in order to facilitate the exercise of powers beyond individual jurisdiction and onto a foreign territory' is likely to be more acceptable.[51]

---

[46] See, e.g., P.J.P. Tak, 'Bottlenecks in International Police and Judicial Cooperations in the EU', *European Journal of Crime, Criminal Law and Criminal Justice,* 8/4 (2000), 343-60 at 344 (arguing that 'the international investigating officer can never exercise powers exceeding those of the national investigating officer in the state in question').

[47] European Council 15-16 October 1999, *Conclusions of the Presidency*, SN 200/1/99 REV 1 ('Tampere conclusions'); Programme of measures to implement the principle of mutual recognition of decisions in criminal matters, 2001/C 12/02, *OJ* C 12/10, 15.1.2001.

[48] Framework Decisions 2002/584/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA and 2008/947/JHA as amended by Framework Decision 2009/299/JHA. See http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/ for an overview.

[49] Fijnaut, 'The globalisation of police and judicial cooperation: drivers, substance and organisational arrangements, political complications', at 10; Maren Eline Kleiven, 'Nordic police cooperation', ibid., 63-71.

[50] Saskia Hufnagel, '(In)security crossing borders: a comparison of police cooperation within Australia and the European Union', ibid., 177-208 at 182-84.

[51] Ibid., at 191.

2.4.2. Slowness and other limitations of mutual legal assistance

With the exception of successful local and smaller-scale forms of cross-border cooperation, cooperation in criminal matters is 'an extremely complicated process in many respects'.[52] Challenges can be found both within the national context and in the international context. At the national level, the success of mutual legal assistance depends on whether the police and judiciary are sufficiently well-equipped, in terms of internal organisation, capacity, and priority-setting, to honour MLAT requests. Also the distribution of responsibilities is not always clear.[53]

At the international level, there are major differences as to views on the seriousness of various types of crime. This is only partly addressed by international treaties on specific crimes, such as drugs, organised crime, or cybercrime, which harmonise or approximate the criminalisation of these specific crimes for those states that have ratified the treaties. Even among states that have ratified crime-specific treaties, there can be substantial differences in maximum penalties; for example, hacking a computer by breaking security measures is punishable with up to one year imprisonment in the Czech Republic, with up to four years' imprisonment in the Netherlands, and with two to seven years' imprisonment in Romania,[54] thus showing significantly different views on the seriousness of this crime despite the fact that all three states have ratified the Cybercrime Convention. The result is a patchwork of piecemeal and partial harmonisation that does not amount to a substantial degree of consensus on the seriousness of crimes in general. Moreover, legal systems do not always allow the use of investigation powers required to obtain evidence solely for mutual legal assistance; for example, the United States, Canada, and Australia are reported not to allow wiretapping at the request of a foreign state.[55] Moreover, countries differ significantly in the relationship between the police and the judiciary, and in the culture of these institutions, which can hamper the execution of MLAT requests. And then there are also some countries that do not participate in the international MLAT agreements.[56]

While MLAT requests, despite these challenges, function up to some point in traditional criminal cases, they are generally considered cumbersome or ineffective in cases where digital evidence is sought, as illustrated by the following comments from cybercrime experts:

> 'The traditional mechanisms of international cooperation, including letters rogatory, mutual assistance and other formalities with roots in the 19th century and earlier, are ill-suited to an era in which offences can be, and are, committed from across the world in real time.'[57]

> 'Historically, MLA procedures have been notoriously complex, slow, and bureaucratic, which is particularly unsuitable for cloud-based investigations.'[58]

To address the need for speed within the system of international cooperation in cyber-evidence matters, some measures have been taken, most notably in the Council of Europe's Cybercrime Convention.[59] A 24/7 network of national contact points has been established (or consolidated where contacts existed) so that countries seeking assistance from other countries can find out the right procedures and addresses for MLAT requests on a twenty-four hour, seven-day-a-week basis (art. 35). Moreover, countries should have a low-threshold investigative power to order expedited preservation of stored computer data, which ensures that data are 'frozen' for a period of up to 90 days, pending which a formal MLAT request can be sent and executed (art. 16). Some providers may voluntarily store the data for a longer period; Microsoft, Yahoo!, and Google, for

---

[52] Cyrille Fijnaut, 'The globalisation of police and judicial cooperation: drivers, substance and organisational arrangements, political complications', ibid., 1-15 at 13.
[53] Ibid., at 10-11.
[54] Art. 230 Czech Criminal Code; art. 138ab Dutch Criminal Code; art. 360(3) Romanian Criminal Code.
[55] Shannon Cuthbertson, 'Mutual assistance in criminal matters: cyberworld realities', in Saskia Hufnagel, Clive Harfield, and Simon Bronitt (eds.), *Cross-border law enforcement: regional law enforcement cooperation - European, Australian and Asia Pacific perspectives* (Abingdon, Oxon; New York, NY: Routledge, 2012), 127-42 at 133, 34.
[56] Cyrille Fijnaut, 'The globalisation of police and judicial cooperation: drivers, substance and organisational arrangements, political complications', ibid., 1-15 at 11-13.
[57] Kim-Kwang Raymond Choo et al., *Future directions in technology-enabled crime: 2007-09* (Research and public policy series; Canberra: Australian Institute of Criminology, 2007) at 72.
[58] Walden, 'Law Enforcement Access to Data in Clouds', at 297. See also Gercke, 'Understanding cybercrime', at 77-78.
[59] Convention on Cybercrime, CETS 185.

example, are said to preserve certain data for 180 days pending the receipt of a formal MLAT request.[60] In addition, the Convention requires countries to allow expedited preservation and partial disclosure of traffic data (i.e., the metadata of communications, which indicate the communication's origin, destination, route, time, date, size, duration, or type of underlying service) (art. 17). This facilitates that the path through which a communication was transmitted can be relatively easily reconstructed, allowing a member state seeking evidence to identify the (likely or apparent) origin of a communication in order to be able to address an MLAT request.

Despite such efforts to streamline and facilitate mutual legal assistance in cases where digital evidence is needed, procedures are still often felt to be inadequate in all or most situations in which there is a need for expeditious data gathering.[61] 'In a general sense, it can be said that it has become extremely complicated to trace a criminal and his activities in the internet.'[62] If transmissions need to be traced back to their origin (for example, to know where a cyber-attack originated from, or from which computer illegal content was uploaded), the procedure of expedited preservation and partial disclosure of traffic data—even if less time-consuming than classic MLAT requests—still costs time, and 'time is the decisive factor in safeguarding volatile data, in particular if the exact location of the server in question is not known or can only be identified through time-consuming efforts, that will come too late.'[63] For example, in order to know which foreign state should (expeditedly) enact the preservation, investigation measures may be needed that require authorisation or other time-consuming procedures, thus re-introducing the problem that the expedited preservation measure was intended to overcome.[64] Moreover, perpetrators of crime can relatively easily use services in countries that are not party to the main mutual-assistance treaties and that do not generally co-operate with foreign law enforcement requests, so that they can easily break the chain that would allow the police to trace back activities to the origin.

Preservation orders are also of limited value in cases where (cyber)criminals move from one IP address to another and use (possibly very short-term) temporary storage facilities, which seems—although not precisely documented—to be experienced more and more in practice.[65] The cloud further compounds the already existing challenges of locatability of data, in light of the dynamic storage model (see also section 3.4.2 *infra*), and thus of the efficacy of MLAT requests that rely on asking the authorities of the state in which data are stored to retrieve the data.

2.5. Summary

Cloud computing is a model in which providers offer flexible, demand-driven computing resources to users as a service via the Internet. In this report, we are particularly interested in remote email services such as Gmail and Hotmail, and remote data storage or sharing services such as DropBox or Google Docs. Due to the distributed, dynamic, and redundant nature of cloud storage, a particular file can often be stored in multiple places simultaneously, while it may not be stored in any single place in its entirety. For speed-optimisation reasons, however, data may be stored in the server park closest to the user's normal location.

The cloud compounds existing challenges for cyber-investigation. Classic searches and classic wire interceptions will gradually have to make room for network searches, Internet interceptions, and production orders to cloud providers, to which legal systems may not always be well adapted. Moreover, cloud computing can involve multiple providers in different layered

[60] Cuthbertson, 'Mutual assistance in criminal matters: cyberworld realities', at 134.
[61] Expert workshop 19 December 2013.
[62] H. W. K. Kaspersen, 'Cybercrime and Internet jurisdiction. Discussion paper (draft)' (Strasbourg: Council of Europe Project on Cybercrime, 2009), at 28.
[63] Ibid.
[64] 'If an investigation officer wants to preserve data by going directly to law enforcement in the repository state, how would a typical officer proceed in my example? I suspect that you would be forced to contact Google directly in order to find the jurisdiction containing the actual data. However, some commentators may consider that contact to be a search. So the lowly law enforcement officer may be forced to do a kind of transborder investigation, or search, in order to find out even in what jurisdiction the data actually resides.' Schwerha Iv, 'Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers"', at 9.
[65] Kaspersen, 'Cybercrime and Internet jurisdiction. Discussion paper (draft)', at 29.

constellations and data can be encrypted, which makes it more difficult to acquire the sought-after data. Legal rules for (digital) evidence can also present difficulties to cloud-based data, such as the rule of thumb that the (evidence) law applies of the state in which data are stored.

Since cloud services are offered and used in a global context, criminal investigation of cloud-stored data will usually have a cross-border character. In the classic paradigm, law enforcement has to rely on mutual legal assistance or other forms of international cooperation, such as limited forms of (treaty-based or consensual) extraterritorial investigation or joint supranational investigation teams. To some extent, mutual legal assistance is easier in relatively homogeneous polities such as the European Union (which moves towards a principle of mutual recognition) or in local cross-border contexts in which there is a high level of mutual trust and strong connections exist among practitioners, but generally speaking, it is a challenging process. In addition to organisational limitations such as lack of capacity or priority-setting and some legal limitations, such as double criminality or a lack of specific powers to execute a foreign state's request, procedures are generally considered cumbersome or ineffective particularly in cases where digital evidence is sought. Despite some efforts to streamline and facilitate mutual legal assistance in cyber-investigation, through 24/7 networks and expedited preservation of data, MLAT procedures can be inadequate in situations with a need for expeditious data gathering, or where (cyber)criminals move data around with high frequency, and also where the location of the data can be identified only through time-consuming efforts, which may well be the case in cloud computing situations.

It is against this background of cloud computing (involving a paradigm that makes the 'location' of data less relevant than in traditional data-processing models) meeting with 19th or 20th-century-based procedures for mutual legal assistance in criminal matters (involving a paradigm that first and foremost relies on the territory-based sovereignty of authorities to conduct criminal investigations on their territory) that the central problem of this study takes shape. Although the problem of cross-border cyber-investigation is not new, it has gained new momentum and significance with the advent of cloud computing. But the facts that the problem of cross-border cyber-investigation as such has been recognised for a long time,[66] and that existing approaches have apparently not worked so far to really address the issue, should give us pause. Solutions will not be easy to find. It is our contention that before we can discuss future directions to address the problem, we need to uncover more of the underlying roots of the problem, and to combine—at a deeper level than has so far occurred—core elements and insights of both cyber-investigation and international law. This is what we aim to do in the next chapter.

[66] E.g., *A Paper for the 12th Council of Europe Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime*, Strasbourg, 15-18 November 1976, p. 225-229, at which a number of categories of computer crime were introduced; also, European Committee on Crime Problems, *Computer-related crime: Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems* (Strasbourg 1990), p. 86-89 (discussing the problem but considering, on p. 88, 'that the time is not ripe for putting forward [a proposal to regulate cross-border "direct penetration"] both for reasons of principle and also because of practical considerations').

3. Conceptual Framework

3.1. Introduction: the importance of frames, metaphors, and a common conceptual ground[67]

The discussion on cross-border cyber-investigation is riddled with metaphors, even if the participants in the debate do not often realise this. For example, police officers investigating in 'cyberspace' 'go to' a server and 'download' data—these are all metaphors. A metaphor is, in the definition of the Oxford English Dictionary, 'a figure of speech in which a word or phrase is applied to an object or action to which it is not literally applicable'.[68] Although that could sound as if metaphor were a linguistic exception to plain speech, metaphors are actually the rule rather than the exception in language. For example, in the previous sentence, 'sound' and 'plain' are metaphors, while the first sentence of this paragraph uses three significant metaphors: a 'discussion' is a metaphor, since it refers to a broad set of literature, conferences, and policy documents that does not literally constitute a discussion between people in a (usually physically) delineated setting aimed at resolving an issue;[69] people who contribute to the 'discussion' are not literally 'participants in the debate' but people contributing statements in a more unstructured sense than occurs in a debate; and to say that the debate is 'riddled' with metaphors subtly suggests not only that metaphors abound but also that they pose riddles in the communication, i.e., intellectual challenges that the participants need to solve if they want to understand what is being said, while the negative connotation of 'being riddled' also expresses that this situation is considered undesirable. Moreover, metaphor is pervasive not only in our language but also in our thought and action.[70] Lakoff and Johnson argue that our conceptual system is 'fundamentally metaphorical in nature' and that this 'plays a central role in defining our everyday realities'.[71]

Since metaphors play a role in defining reality by influencing the way we perceive it, applying different metaphors implies offering different perspectives on the world. Using a metaphor means offering a window on the world – a frame – which structures the way we look and which defines what we see (and what we do not see). In this sense, metaphors are 'symptoms of a particular kind of seeing-as, the 'meta-pherein' of 'carrying over' of frames or perspectives from one domain of experience to another'.[72] This process of transferring meaning, which Donald Schön has called 'generative metaphor',[73] occurs when people – intentionally or unintentionally – use language associated with one domain and apply it to another domain, thus framing the perspective from which that other domain is being perceived. The associations can be more or less explicitly present, depending partly on whether a metaphor is strikingly fresh or long-established and on how forcibly it illuminates the object being described. However, even if associations are less prominently present for the audience, they can influence perception by privileging certain connotations over other connotations. Therefore, a frame constituted through generative metaphors can easily lead to 'a sort of cognitive myopia wherein some aspects of a situation are unwittingly (or not) emphasized at the expense of other, possibly equally important aspects.'[74]

Schön has shown that for this reason, framing and metaphors play an important role in defining problems in public policy.[75] And since the problem definition has significant implications for the way in which a problem can or will be solved, metaphors play a key role in public policy:

---

[67] This section partly draws on B.J. Koops, 'The role of framing and metaphor in the therapy versus enhancement argument', in Federica Lucivero and Anton Vedder (eds.), *Beyond Therapy v. Enhancement. Multidisciplinary analyses of a heated debate* (Pisa: Pisa University Press, 2013), 35-68.
[68] Oxford English Dictionary online, http://www.oxforddictionaries.com/definition/english/metaphor.
[69] In its original sense, a discussion refers to an 'Examination, investigation, esp. so as to allow a judgement to be made', *Oxford English Dictionary*, http://www.oed.com/.
[70] George Lakoff and Mark Johnson, *Metaphors We Live By* (Chicago, London: University of Chicago Press, 1980 (2003)) at 3.
[71] Ibid.
[72] Donald A. Schön, 'Generative metaphor: A perspective on problem-setting in social policy', in Andrew Ortony (ed.), *Metaphor and Thought* (2nd edn.; Cambridge, etc.: Cambridge University Press, 1993), 137-63 at 137.
[73] Ibid.
[74] Andrew Ortony, 'Metaphor, language, and thought', ibid., 1-16 at 5.
[75] Donald A. Schön, 'Generative metaphor: A perspective on problem-setting in social policy', ibid., 137-63.

> 'When we examine the problem-setting stories told by the analysts and practitioners of social policy, it becomes apparent that the framing of problems often depends upon metaphors underlying the stories which generate problem setting and set the directions of problem solving.'[76]

Schön gives the example of social services, which are often portrayed as being problematic because of 'fragmentation'. This metaphor suggests that the problem with social services, like with a broken vase, is the shattering of a prior integration. The obvious solution to this is co-ordination. However, the obviousness of this solution crucially depends on whether the diagnosis of 'fragmentation' makes sense. Does the problem really have to do with a previously existing co-operation among services which no longer work well together? Other metaphors to frame the problem could trigger other associations and lead to different solutions than co-ordination.[77]

The crucial importance of metaphors and frames became apparent at the workshop we organised in the context of this study, which confronted the perspectives of cyber-investigation with those of international law. A significant part of the discussion turned out to go into conceptual issues. In particular, the notions of 'place' and 'space' apparently caused confusion to participants with different backgrounds and frames of mind. Also, the conceptualisation of cross-border searches seemed unimportant to the cyber-investigation experts, who considered that you simply 'do a cross-border search' in a server that is (probably or possibly) located abroad, but turned out to be of vital relevance to international law experts, for whom it was important to tease out what such a 'search' actually consists of in terms of actions on foreign territory. Therefore, if cyber-investigation and international law perspectives are to be combined, it is vital to first identify a common ground (note the use of a territorial metaphor here, which is unintended but hard to avoid). Therefore, in this chapter we describe the frames and analyse the metaphors in which international law and law-enforcement conceive of cloud investigations, in order to 'increase the rigor and precision of our analysis of social policy problems by examining the analogies and "disanalogies" between the familiar descriptions – embodied in metaphors (…) – and the actual problematic situations that confront us.'[78]

3.2. Conceptualising space, place, and cyberspace

As international law is pervaded by the notion of territory, it is important to start with two concepts related to this notion: 'space' and 'place'. Although the terms are sometimes used rather loosely as synonyms, for many people they raise somewhat different connotations. This can cause confusion, as we noticed at the workshop organised for this research: some workshop participants used the term 'space' in the more literal sense of denoting a certain physical territory and 'place' in a more abstract sense of a metaphorical location, i.e., a context where something occurs without necessarily being tied to some physical territory; and other participants use the terms the other way around.

The Oxford English Dictionary (OED) defines space (in the sense relevant for this report) generally as 'area or extension', and more particularly as 'superficial extent or area; also, extent in three dimensions' (i.e., a more literal relationship with territory) or 'extent or area sufficient for some purpose; room' (i.e., a more metaphorical relationship with territory). In the latter meaning, 'space' is often used in an abstract sense, illustrated in the OED by the sentence 'Crime that leaves no space for penitence!'[79] The OED describes 'place' (in the sense relevant for this report) generally as 'a material space', and more particularly as 'space; extension in two (or three) directions; "room", 'a particular part of space, of definite situation', or 'the portion of space actually occupied by a person or thing; locality'.[80] Both terms can thus be used literally to denote some physical area, but 'space' can also be used in a more abstract sense as an 'area[81] sufficient for some purpose'. We think it useful in this light to restrict the use of 'place' to the more literal meaning and to use 'space' where (also) the more metaphorical meaning is intended.

[76] Ibid., at 138.
[77] Ibid., at 138-39.
[78] Ibid., at 139.
[79] *The Shorter Oxford English Dictionary*, Oxford: Oxford UP, 1973, 'Space (II)'.
[80] Ibid., 'Place (II)'.
[81] 'Area' can be read literally as a particular extent of the earth's surface but also metaphorically as 'scope, range, extent', see ibid., 'Area'.

The difference is particularly important in the conceptualisation of cyberspace. As Dan Hunter has argued, '[t]he cognitive metaphor of CYBERSPACE AS PLACE is central to our understanding of the abstract idea of the Internet in all its various forms.' Almost all Internet-related metaphors, such as frontier, superhighway, and gatekeepers, assume a kind of 'abstract physical space that may be navigated'. As a result, we cannot but think of the Internet in terms of spatial characteristics – cyber*space* – and frame it as a 'place'.[82] Note the use of 'place' here: the frame of a spatial metaphor, even if people use the metaphors only to refer to a very abstract sense of 'space', triggers the literal connotations of place as 'material space'.

There are broadly speaking two schools of thought to conceptualise this 'place' of cyberspace. One school conceives of cyberspace as a separate space, which functions differently than material space and should therefore also be treated differently. This vision is based on 'one simple principle: conceiving of Cyberspace as a distinct "place" for purposes of legal analysis by recognizing a legally significant border between Cyberspace and the "real world".'[83] The other school emphasises that cyberspace is no less real than the 'real world', as it is intimately connected to physical objects (cables, servers, computers of end-users) and real persons. Hence, it should be treated as part of the material space, including real-world regulation of material space.[84]

Although the academic debate between the so-called exceptionalists (the first school) and the non-exceptionalists (the second school) has not been resolved (and is not likely to be resolved, as both sides have forcible arguments to underpin their views), Internet regulation practice has largely sided with the non-exceptionalists. National governments pass laws and enforce these to regulate activities taking place in 'their' part of the Internet, finding ways to establish jurisdiction on the basis of cyberspace's connections with objects, persons, or data processing activities on their territory. Although this does not rule out a conceptualisation of cyberspace as a separately regulated space (with a special regime for 'online' situations next to the legal regime for 'offline' situations), it does come along with a conceptualisation of cyberspace as 'place' rather than 'space', i.e., a realm that is territorial (somewhere in three-dimensional space) in nature rather than a-territorial (an abstract realm).

Thus, although '[t]erritorial regulation faces pressure from a variety of modern factors (...) it remains the dominant method for regulating all transnational transactions in our interdependent world, including Internet transactions.'[85] Part of this development is due to the increasing possibilities to determine national borders in cyberspace,[86] through geo-location technologies,[87] which enable identifying the geographic (national) origin of an IP address.

3.3. Framing the international law perspective

3.3.1. Place, territory and jurisdiction in international law: from space to place and back again

There can be little doubt about the importance of place over human minds. Our attachment to a particular portion of the earth – *a* place, as opposed to just space – began as the need for physical and economic survival: we must all be located somewhere on the surface of the earth and our security can only be ensured if we can define this space as our place, erect borders and defend it. Such basic needs ensured that the foundation of political community is equated with the defining of physical borders, of determining an 'in' and an 'out'. For Arendt, the Greek polity was 'quite literally a wall, without which there might have been an agglomeration of houses, a town (…) but not a city, a political community.'[88]

[82] Dan Hunter, 'Cyberspace as Place and the Tragedy of the Digital Anticommons', *California Law Review,* 91/2 (2003), 439-519 at 515-16.
[83] David R. Johnson and David G. Post, 'Law and Borders – The Rise of Law in Cyberspace', *Stanford Law Review,* 48 (1996), 1367-402 at 1378.
[84] Jack L. Goldsmith, 'Against Cyberanarchy', *University of Chicago Law Review,* 65 (1998a), 1199-250.
[85] Goldsmith, 'The Internet and the Abiding Significance of Territorial Sovereignty', at 491.
[86] Michael A. Geist, 'Is There a There There? Toward Greater Certainty for Internet Jurisdiction', *Berkeley Technology Law Journal,* 16 (2001), 1345-406.
[87] See *infra*, section 3.4.2.
[88] Hannah Arendt, *The human condition* ([Chicago: University of Chicago Press, 1958), 63.

It remains difficult for us to imagine a political community that does not define its boundaries by physical borders. Within nationalism studies, territory is considered to be the one vital ingredient to a national claim; it does not need to be an exclusive claim to territory or even a currently plausible one (diasporic communities are included), but it must be there.[89] The idea that political community must be physically located and bounded became in the course of the Middle Ages fixed as the exclusive relationship between a single political entity and a defined territory.[90] The Europe of the medieval period had been a sprawling web of over-lapping and intersecting competences and authorities: city-states, bishoprics, noble fiefdoms, towns and guilds, all of which intersected and frequently clashed with the Kings and Emperors who claimed personal authority over a people and with the Church that claimed *imperium* over all of Christendom. What emerged to define the modern era was the co-joining of private and public authority – both *dominium* (ownership) and *imperium* (control) – in an exclusive relationship to a place; this relationship was termed territorial sovereignty.[91] It was this model of political community, developed within Europe, that was later imposed upon the rest of the world as 'natural' and 'God-given', and which justified the subjugation of other forms of community under colonialism. In sum, while the formation of political communities requires space to become place, in the modern period (generally understood as starting in the seventeenth century), place became territory.

The emergence of the state as the solely acceptable expression of political community is the foundation of international law and respect for the exclusive relationship between authority and place – otherwise known as territorial sovereignty – is the basis of the international legal order. So central is the notion of territory to international law, that it has almost become a purpose in itself. In the much-cited phrase of Arbitrator Huber in the *Island of Palmas* case: 'Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.'[92] Huber went on to note that international law had established this principle of exclusive competence of the State in regard to its own territory in such a way that it formed 'the point of departure in settling most questions that concern international relations'. A state is thus defined not by its political community but by its territory. In many respects, Huber's observation still holds: exclusive sovereignty over a defined territory remains the basic organising principle of international law and thus of the world order.[93] In classic international law, place (whether land, sea or air) is conceived through the lens of (exclusive) territoriality. As a consequence, international law places territorial integrity above any other claim, such as the self-determination claim of a people; crudely put, territory trumps people.[94]

The exclusive right of action within a defined territory is the basis of the doctrine of sovereign equality, which founds the sovereign right of all states – regardless of physical size, or military or economic might – to participate in international relations from a position of formal equality. Sovereign equality – 'the basic constitutional doctrine of the law of nations'[95] – is thus given most concrete expression as the principle that the territorial integrity and political independence of a

---

[89] See in this regard, M. Moore, *The Ethics of Nationalism* (Oxford: Oxford University Press, 2001) and M. Keating, *Plurinational Democracy. Stateless Nations in a Post-Sovereignty Era* (Oxford: Oxford University Press, 2001a) and M. Keating, ''Nations without States: The Accommodation of Nationalism in the New State Order'', in M. Keating & J. Mcgarry (ed.), *Minority Nationalism and the Changing International Order* (Oxford: Oxford University Press, 2001b) (Cf. Morag Goodwin, 'The Romani claim to non-territorial nationhood: taking legitimacy-based claims seriously in international law', (Florence, 2006), unpublished Ph.D. thesis, Florence).

[90] J. G. Ruggie, ''Territoriality and Beyond: Problematizing Modernity in International Relations', *International Organization,* 47/139 (1993); J. Zielonka, 'Enlargement and the Finality of European Integration', in Mény & Weiler Joerges (ed.), *What Kind of Consitution for What Kind of Polity: Responses to Joschka Fischer* (Florence: Robert Schuman Center, 2003).

[91] M. Loughlin, 'Ten Tenets of Sovereignty', in Walker (ed.), *Sovereignty in Transition* (Oxford: Hart Publishing, 2013).

[92] *Island of Palmas (or Miangas)* Case (1928) 2 RIAA 829.

[93] R. Y. Jennings, *The acquisition of territory in international law* (Manchester; New York: Manchester University Press ; Oceana Publications, 1963).

[94] See Malcolm N Shaw, 'Peoples, territorialism and boundaries', *Eur. J. Int'l L.,* 8 (1997), 478 for a comprehensive discussion. Of course, the reality is slightly more nuanced but certain very strict conditions would need to apply before the demands of a people might trump territorial integrity. See Declaration on Principles of International Law concerning Friendly Relations and Co-operation Among States, G.A. Res. 2625 (XXV) (1970).

[95] Ian Brownlie, *Principles of public international law* (Oxford: Clarendon Press, 1973), 280.

State are inviolable.[96] This inviolability holds even where territorial integrity is breached for the purposes of self-help or in response to action or inaction by another state; the ICJ held in the 1949 *Corfu Channel* case that the actions of the UK, in sweeping the Corfu Channel for mines, constituted an illegal use of force against the territorial integrity of Albania, even though Albania was held responsible by the Court for allowing the mines to be in an important maritime channel and even though those mines had caused the death of several British sailors and damage to a British warship. The Court dismissed the UK's argument that the main aim of the minesweeping operation had been one of 'gathering evidence'; an alternative argument of 'self-help' was also rejected in favour of a strict interpretation of territorial integrity.[97] Moreover, the obligation of a state to respect the territorial inviolability and non-interference of other states is not limited to material acts, such as actual territorial incursion, but protects sovereign dignity from both tangible and intangible wrongful acts of other states. In the 2002 *Arrest Warrant* case, the mere issuing of an arrest warrant by Belgium for the Foreign Minister of Congo for crimes against humanity was deemed by the International Court of Justice to be a breach of Congo's sovereign dignity.[98] What this means is that even non-coercive acts can breach the obligations that states owe one another: it is enough to claim adjudicative jurisdiction over events in another state to breach these principles, without necessarily seeking to enforce that jurisdiction.[99] That said, material actions are, generally speaking, more likely to constitute serious breaches of international law. It is important to note, though, that territorial integrity and non-interference protect states only from unwanted or unauthorised incursions into their sovereign space; a state can of course *consent* to such 'interference'. This then becomes co-operation.

Territory has attained its fundamental status under international law as an organisational principle. What this means is that international law grants rights to states, foremost territorial integrity and inviolability, because they demonstrate the capacity to govern and thus are capable of delivering on their international commitments (notably in regard to other states). Theoretical or historical title to territory is not sufficient to establish sovereignty; rather, the claim to sovereignty must be continuously and peacefully performed in order to be effective.[100] Territorial sovereignty is thus the effective control of a defined territory;[101] territory in relation to the state signifies both *dominium* (ownership) and *imperium* (control). Legitimacy to rule in the international order is therefore traditionally derived from the capacity to enforce one's will within a defined territory. Territorial sovereignty in international law thus denotes more than simply a defined geographical space; it refers rather to a 'relationship between people and space, as characterized by the existence of an effective governmental authority.'[102]

The territorial principle of jurisdiction is a corollary of territorial sovereignty.[103] Within the boundaries of its own territory, a state has exclusive right to adjudicative and enforcement jurisdiction, but its territory also represents the limit of those rights: these types of jurisdiction are confined to a state's territory.[104] Prescriptive jurisdiction concerns the question of to whom a state may extend its laws; this form of jurisdiction is not restricted by territory. As the Permanent Court

---

[96] Declaration on Principles of International Law concerning Friendly Relations and Co-operation Among States, G.A. Res. 2625 (XXV) (1970).

[97] *The Corfu Channel Case*, Merits, [1949] ICJ Reports 4.

[98] *Arrest Warrant* case (*Democratic Republic of the Congo v. Belgium)*, Judgement of 11 April 2000, ICJ Reports 2002.

[99] See, e.g., the hostile responses by states (even traditional allies) to the US Helms-Burton Act, which claims to regulate global trade with Cuba. J. Klabbers, *International Law* (Cambridge: Cambridge University Press, 2013), 96. Of course, the US also sought to enforce the Act in relation to property present within the US. The Helms-Burton Act is an example of the 'effects doctrine' described below.

[100] *Island of Palmas* case. Peacefully here means without the objection of another state. See also H. Spruyt, *The Sovereign State and Its Competitors* (Princeton: Princeton University Press, 1994).

[101] Article 1, Montevideo Convention. A 'portion of the globe' thus becomes territory by being subject to a sovereign claim.

[102] Malcolm N Shaw, 'Territory in International Law', *Netherlands Yearbook of International Law,* 13 (1982), 61-91, 75.

[103] Vaughan Lowe, 'Jurisdiction', in Malcolm D. Evans (ed.), *International Law* (2nd edn.; Oxford: Oxford University Press, 2006).

[104] As famously noted by the PCIJ in the *Lotus* case (1927), Judgement No. 9, *PCIJ*, Ser A, No. 10, 18-19. Adjudicative jurisdiction concerns the right of a state's courts to hear a case; enforcement jurisdiction concerns the ability of a state to enforce its laws.

of International Justice noted in the *Lotus* case, 'Far from laying down a general prohibition to the effect that states may not extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, [international law] leaves them in this respect a wide measure of discretion (…).'[105] Accepted grounds for jurisdiction to prescribe are the territorial principle[106] (including the controversial effects doctrine, whereby states seek to regulate acts that take place outside their territory but which have economic effects inside it[107]); the nationality principle (regulating how *nationals* behave); the protective principle (whereby acts by non-nationals outside a state's territory threaten the vital interests of that state, e.g. in relation to drug smuggling); the universal principle (whereby any state can assert jurisdiction over a heinous crime or where a serious crime is likely to go unpunished);[108] and, more recently although fairly strictly circumscribed, the passive personality principle, whereby states assert jurisdiction where their national is a victim.[109] The right of a state to regulate conduct on these grounds is limited by immunities and the obligation to respect the territorial integrity and political independence of other states. As Lowe notes, '[i]t should be clear that if in any case the exercise by one State of its jurisdiction threatens to subvert the laws that another State has enacted to regulate life in its borders, the boundaries of lawful jurisdiction have been over-stepped.'[110] In addition, it should be equally clear that jurisdiction to prescribe does not entail jurisdiction to adjudicate or to enforce; in particular, the jurisdiction to enforce (through exercising investigation powers) can never (lawfully) impinge upon the territorial integrity of another state.

As should be clear from the preceding paragraph, jurisdiction is a legal concept. It determines the boundaries of legal authority. Jurisdiction gives spatial scope to law. The boundaries of the spatial expanse of legal authority have traditionally, in the modern era, been territorial and remain so to a large extent, i.e., defined by place. This is why jurisdiction is largely seen as synonymous with territory. However, recent developments in the field of human right obligations have helped to remind us that legal space is not necessarily defined by place but by the extent to which law determines the legal relations between persons.[111] Put another way, jurisdiction is determined by the extent to which the sovereign exercises effective control. Where a state – for whatever reason – has effective control over an area (place) that is formally within the territory of another state, it will be held accountable for all actions that take place there, i.e., that place, while remaining the territory of State A, becomes part of the legal space of State B. For example, Article 1 of the European Convention of Human Rights (ECHR) states that '[t]he High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of [the] Convention'. In a series of cases, the European Court of Human Rights has thus held that the jurisdiction of contracting states is not limited to their territorial expanse; rather, they are accountable for violations of Convention rights that take place anywhere in the world, where such violations occur within their jurisdiction (legal space).[112] In *Al-Skeini and Others v the United*

---

[105] *Lotus* (1927), 19. According to Lowe, the best view on jurisdiction to prescribe is that there must be a clear connecting factor between the legislating state and the conduct that it seeks to regulate; Lowe, 'Jurisdiction'. 342.

[106] The territorial principle includes what is known as subjective territorial jurisdiction (a claim by states to jurisdiction in circumstances in which an incident is initiated inside its territory but is completed outside it e.g. Scotland's claim to jurisdiction in the Lockerbie case) and objective territorial jurisdiction (the claim in situations in which an incident was initiated in the territory of another state but completed in the territory of the claiming state).

[107] The effects doctrine, a form of objective territorial jurisdiction, has been used solely in relation to economic matters and is controversial because it impinges upon the territorial jurisdiction of other states and because the jurisdictional link is viewed as tenuous. US Anti-Trust legislation and EU competition rules are the best known examples of this. See Lowe, 'Jurisdiction'.

[108] Ibid. at 348, noting that piracy falls under the latter i.e. universal jurisdiction applies to piracy not because it is necessarily a particularly serious crime but because the rules in relation to the high seas would otherwise allow it to go unpunished.

[109] Controversial until very recently (see the Separate Opinion in the *Arrest Warrants* case), it now seems to be accepted that passive personality jurisdiction is tolerated by other states where it is used to prosecute terrorists.

[110] Lowe, 'Jurisdiction', at 358.

[111] S. Dorsett & S Mcveigh, *Jurisdiction* (Abingdon, Oxon; New York, NY: Routledge, 2012).

[112] See, for a range of circumstances in which the Court has found the Convention to apply extra-territorially, *Loizidou v. Turkey*, Judgement of the Grand Chamber of the European Court of Human Rights of 23 March 1995; *Ilaşcu and Others v. Republic of Moldova and Russia*, Judgment of the Grand Chamber of the European Court of Human Rights of 8 July 2004; *Öcalan v. Turkey*, Judgment of the Grand Chamber of the European Court of Human Rights of 12 May 2005; *Pad and Others v. Turkey*, admissibility decision of 28 June 2007; *Hirsi Jamaa*

Kingdom (2011),[113] the Grand Chamber of the European Court of Human Rights unanimously held that the United Kingdom had jurisdiction in respect of civilians killed in the British zone of occupation in Iraq. Thus, as a consequence of the UK exercising effective control over a place that was nonetheless far outside its own territory, the place became UK legal space for the period during which that control was exercised and the UK government was therefore accountable for abuses that took place there in the same way as if those abuses had taken place in Wolverhampton. Legal space is necessarily spatially defined, but it is not necessarily defined by place and thus by territory. Yet the extent to which the concept of territory holds sway over our legal imaginations is visible in the label giving to such a broader approach to jurisdiction: extra-territorial.

Jurisdiction, or 'the life of the law', remains spatially organised. It has become commonplace to suggest in the context of globalisation that law is being 'de-territorialised'.[114] What is meant is that the claim of exclusive authority or jurisdiction over a defined place that was such a key part of modernity – the territorial state – is being increasingly undermined. In its stead, a given space can host multiple claims to legal authority. The classic example is the European Union. Within any EU state, recognised claims to legal authority exist at the local, city, sub-national, national, European, international, and transnational levels, and all in relation to the same physical space or portion of the globe. What we are increasingly cognisant of as legal scholars is the fact of over-lapping jurisdictional claims with different spatial expansions and often in relation to different content; e.g., even in relation to a topic as mundane as product standardisation, there are a variety of bodies asserting authority to issue rules relating to products at various governmental and non-governmental levels (this is most frequently described as the shift from government to governance).

The increasing awareness of the complexity of legal authority in a globalising world should not be equated, however, with de-territorialisation, where de-territorialisation suggests that law does not require a spatial dimension. This would be to misunderstand what a legal order entails. As Lindahl has forcefully argued, every legal order requires a spatial dimension, i.e., a boundary both in time and space that defines the scope of collective action, and such a legal space must by definition be claimed as exclusive space.[115] Such (exclusive) space need not equate to a(n exclusive) place, however; thus it is possible to conceive of legal orders that overlap across a given geographical surface. That said, in the context of their relations with each other, states remain wedded to the notion of exclusive territoriality.[116] This is particularly so in the area of law and order, which has always been viewed as one of the most essential responsibilities of the sovereign state.[117]

3.3.2. Conceptualising sovereignty in a globalising world

As described in section 3.2.1., the modern era that ran from the sixteenth/ seventeenth century to the mid-twentieth century was defined by the combination of private (dominium) and public (imperium) ordering authority in a single person or institution: the sovereign. Internally, this sovereign claimed the monopoly of violence; externally, in relation to other sovereigns, sovereignty was independence, defined as the ability to exercise absolute authority within one's own borders to the exclusion of all others. However, during the course of the twentieth century, the state was widely perceived to be losing many of its traditional functions in a world in which

---

and Others v. Italy, Judgment of the Grand Chamber of the European Court of Human Rights of 23 February 2012.

[113] *Al-Skeini and Others v the United Kingdom* (55721/07) (2011) 53 E.H.R.R.18.

[114] E.g., J. A. Scholte, *Globalization: A Critical Introduction* (London: Macmillan, 2000); P. Dicken, *Global Shift: Transforming the World Economy* (3rd Edition edn.; London: Sage Publications, 1998); G. Mundlak, 'Deterritorializing Labour Law', *Law & Ethics of Human Rights,* 3 (2009), 189-222.

[115] H. Lindahl, *Fault Lines of Globalization. Legal Order and the Politics of A-Legality* (Oxford: Oxford University Press, 2013), at 101-105. See below section 3.2.3. on the necessity of legal systems making an absolute claim to ultimate ordering authority but the impossibility of ever achieving it.

[116] The European Union is a unique exception and it is this – the idea of ever closer integration – that makes the EU such a special/ threatening project (depending upon the particular viewpoint).

[117] Klabbers, *International Law* , 228.

non-state actors were becoming increasingly important. This led some commentators to proclaim the end of sovereignty, either as a normative ideal or a description of empirical reality.[118]

However, these proclamations of the end of sovereignty seem at best premature. How then should we understand sovereignty in an era in which the state can no longer (assuming it ever could) make good on the claim to absolute authority within its own borders? What the changes of the last 60-70 years make clear is the contingent nature of the form of sovereignty that defined the modern period: the combination of dominium and imperium that entailed exclusive rule over a defined territory. It does not mean that we can do away with sovereignty, where sovereignty is understood as the final act of decision-making. In the context of the EU constitutional debate, Neil Walker has developed a definition of sovereignty in which sovereignty is the claim to ultimate ordering power.[119] This is sovereignty as *imperium* detached from *dominium*. By detaching a claim to ultimate authority from territory, it becomes possible to make sense of the wide range of claims to authority that we see at the global level, and their varied nature. This does not mean that such a claim cannot be territorial, only that it is not necessarily so; *dominium* is thus not an inherent element of sovereignty but simply the form of one institutionalisation of it. Where a territorial sovereign's claim is defined by the territory, the claim of a different actor is likely to be functionally distinct; for example, the claim of FIFA to govern world football. This claim is defined by the subject – football – and not by a limited geographical expanse.

Of course, FIFA does not use the language of sovereignty to assert its authority. What the idea of sovereignty as claim to ultimate ordering power allows us to see is that it is the claim to authority that is central, not the language of sovereignty. The claim might be one of sovereignty, but it might well be couched in different terms, such as supremacy or authority. Walker has termed this phenomenon 'late sovereignty'.

What the idea of sovereignty as a claim to ultimate ordering authority makes clear is the relational and contingent nature of sovereignty.[120] Yet while sovereignty can only ever be contingent, there is a totalising logic at its core. For a claim to be a sovereign-type claim, it must be absolute – a claim to be the ultimate decision-maker. Yet while the term 'sovereign' suggests that such a claim must be absolute, the term 'claim' reminds us that it is only ever aspirational. As sovereignty always depends upon how its claim is 'heard', both by those over whom the claim is made and by those external to it, it is not possible to make good on the absolute nature of the claim; even those who rule by violence are vulnerable to revolution.[121] Although an entity making a claim to ultimate ordering power cannot recognise any other such claim in its domain (whether geographical or functional), in practice different legal orders co-exist and even co-operate. The ECJ reference procedure is a good example of two legal orders, both claiming supremacy, co-operating to achieve common aims.[122] In the global era sovereignty thus becomes not a claim to independence – for what would that mean in a globally-interdependent world? – but a plausible and *reasonably effective* claim to autonomy of decision-making.[123]

In the context of cyberspace and of cross-border data searches, these discussions remain somewhat theoretical: there have been no attempts to make a claim of ultimate ordering authority

[118] The highpoint of these claims was the 1990s: from among a large literature, 'Theme Panel IV: The End of Sovereignty', 88th Annual meeting (1994), *ASIL Proceedings* 71; Christoph Schreuer, ''The Waning of the Sovereign State: Towards a New Paradigm for International Law'', *European Journal of International Law,* 4 (1993).

[119] Walker's definition in full is sovereignty as 'the discursive form in which a claim concerning the existence and character of a supreme ordering power for a particular polity is expressed, which supreme ordering power purports to establish and sustain the identity and status of the particularly polity *qua* polity and to provide a continuing source and vehicle of ultimate authority for the juridical order of that polity.' N. Walker, 'Late Sovereignty in the European Union', in Walker (ed.), *Sovereignty in Transition* (Oxford: Hart Publishing, 2003), 3.

[120] Even during the height of the modern era, the sovereign claim was never absolute and was contingent upon the acceptance of the claim by those over who it was made i.e. the people. Even Hobbes, author of *The Leviathan*, accepted that 'the power of the mighty hath no foundation but in the opinion and belief of the people.' (*Behemoth or the Long Parliament* (1682)).

[121] L. L. Fuller, *The Morality of Law: Revised Edition* (New Haven: Yale University Press, 1964).

[122] N. Walker, 'Flexibility within a metaconstitutional frame: reflections on the future of legal authority in Europe', in G. De Búrca & J. Scott (ed.), *Constitutional Change in the EU: From Uniformity to Flexibility* (Oxford: Hart Publishing, 2000).

[123] Walker, 'Late Sovereignty in the European Union', 10-12.

in relation to cyberspace by entities other than states acting on territorial impulses.[124] What the discussions do show is that the global era is one marked by pluralism, in which actors, among whom states, co-operate in functional networks of governance to solve common problems.[125] While states, or crucially public authority actors within the state structure, co-operate in the thousands of governance networks that now exist, we should not under-estimate the continuing importance of states as actors. We may now see sovereignty as the claim to ultimate ordering authority detached from territory, but a sovereign-type claim contains two elements: legitimacy and capacity. This is what makes the claim more or less plausible and effective. What the state as polity continues to do far better than any other actor that has emerged onto the global stage is to combine legitimacy and capacity: the ability to make good on its claims because it has the resources to do so and because its claims are viewed (largely) as legitimate. It is for this reason that any claim of the demise of the state is inaccurate and, arguably, undesirable; and it is why we accept the continuing and exclusive claim of the state to sovereignty, even though we now recognise it for the fiction that it is and always was.

3.3.3. The human rights obligations of states

3.3.3.1. The nature and status of human rights obligations

International human rights law is a sub-field of international law. This means that human rights at the international level are governed by the general rules of international law relating to state immunity, diplomatic immunity and, of course, state sovereignty. Human rights are thus universal as moral rights; but as legal rights their existence depends, with notable but limited exceptions, upon the consent of states to be bound by them.

At the international level, human rights are mainly contained in the corpus of human rights treaties drafted under the auspices of the UN and in the regional human rights treaties. The UN treaties include, among many others, the International Covenant on Civil and Political Rights (ICCPR); its sister treaty, the International Covenant on Social, Economic and Cultural Rights (ICESCR); the Convention Against Torture (CAT); the Convention on the Elimination of All Forms of Racial Discrimination (ICERD); and the Convention on the Rights of the Child. The European Convention on Human Rights is an example of a regional human rights treaty. All these human rights treaties are no different from any other treaty, despite the subject matter, and are thus governed by the international law on treaties; this means that in order to be binding, a state must have signed and ratified them and it entails that reservations can be made.[126]

Some human rights have attained the status of customary international law and even of *ius cogens*. While it is not possible to state with certainty what rights have attained what status, there is general agreement that most but not all of the Universal Declaration of Human Rights can be considered custom; and that the list of rights that have *ius cogens* status should be constructed narrowly. In practice, this means that only the prohibitions on torture, slavery, apartheid and (possibly) disappearances are understood to be peremptory norms.[127]

Thus whether a particular individual has certain human rights will depend upon the status of those rights; if the rights are not part of customary law but found only in treaty, it will depend upon whether the state in question has signed and ratified the relevant treaty.

It worth noting that under international law a state does not, strictly speaking, owe its human rights obligations to the individuals within its jurisdiction. Instead, as with any treaty, it owes those obligations to the other treaty parties. Thus, unless a treaty provides an institutional mechanism to which individuals can bring complaints and unless the state has agreed to allow a complaint mechanism, the individual has no legal recourse where a state fails to implement its obligations.

---

[124] An exception would be the claims of ICANN in relation to ordering domain names. See J. Von Bernstoff, 'Democratic Global Internet Regulation? Governance Networks, International Law and the Shadow of Hegemony', *European Law Journal,* 9/511 (2003).

[125] A-M. Slaughter, *A New World Order* (Princeton: Princeton University Press, 2004); see also K-H. Ladeur, *Public Governance in the Age of Globalization* (Aldershot: Ashgate Pub Ltd, 2004).

[126] Treaty law is codified by the 1969 Vienna Convention on the Law of Treaties. The lists of signatures, ratifications and details of the reservations entered by states can be viewed on the UN website dedicated to each treaty; and on the Council of Europe website for the European Convention on Human Rights.

[127] Olivier De Schutter, *International Human Rights Law: Cases, Materials, Commentary* (2nd edn.: Cambridge University Press, 2014).

A good example of this is the UK's refusal under the International Covenant on Civil and Political Rights to ratify the Optional Protocol to the Covenant that establishes an individual complaint mechanism. This entails that individuals within UK jurisdiction have no legal means for addressing violations of the Covenant.[128]

By and large it is correct to characterise human rights as vertical in nature; what this means is that an individual is a rights-bearer and it is the state that is the duty-bearer. We may have rights in relation to other individuals or groups in given circumstances (for example contractual rights), but we do not have *human* rights. Human rights are limited to the relationship between a state and an individual, or specially defined group of individuals, such as a minority.[129]

Human rights obligations are not limited to the negative requirement on states not to violate rights, e.g., not to kill. Rather, all rights contain both negative and positive obligations. While the state is not allowed to kill individuals within its jurisdiction (except in certain circumstances), it is also obligated to ensure an environment in which the right to life is protected. For example, by securing law and order or by adequate training of a police force (particularly in relation to weapons training or the detention of vulnerable individuals). This positive aspect of the right to life also requires that the state provide reasonable protection for individuals from others. Obviously a state cannot prevent all murders, but it must provide protection where a life is known to be in danger, and it must investigate where a murder has occurred. Failure to conduct an adequate investigation of a private murder will also violate a state's obligations under the right to life. The nature of human rights obligations are frequently characterised as the obligation to respect, protect and fulfil: respect entails not inferring with the enjoyment of rights; protect requires a state to protect individuals from the violation of rights by others; and fulfil entails the obligation to create an environment within which rights have meaning, i.e. to facilitate rights' enjoyment.[130]

3.3.3.2. Human rights and jurisdiction

Where a state has ratified a human rights treaty, or where the norm in question forms part of customary international law, this does not imply it is responsible for realising those rights throughout the world, for example in the context of the right to food. Individuals starving in South Sudan, for example, do not engage the human rights responsibility of a major grain producing state that decides to limit exports; indeed of any state but South Sudan. A state's human rights commitment is thus limited to but applies throughout its jurisdiction. In general, this entails that a state must protect, promote and ensure the enjoyment of those rights throughout its territory and regardless of whether the individual concerned is a national or not.

However, the extent of a state's accountability for human rights is not limited by its territory; it is, rather, determined by its jurisdiction which, as discussed in section 3.2.1 above, is not equivalent to its territorial borders.[131] This has been confirmed by a string of recent cases. While a state cannot be held accountable for all its actions that lead to human rights violations,[132] where it has effective control, even far outside its territory, it will be understood to have jurisdiction for the purposes of accountability for human rights violations. This is known as extra-territorial

[128] Unlike in the Netherlands, treaties are not directly enforceable in UK courts (the UK is a dualist system) and the ICCPR has not been incorporated into UK law. The state reporting system does, however, allow for NGO participation in the drafting of the state report; this does not provide redress for an individual, though.

[129] Minority rights are conceived under international law as rights of individual members of a minority group i.e. there are no binding collective rights in the human rights canon. See Article 27 ICCPR.

[130] For one of the earliest articulations of this triple obligation, see Committee on Economic, Social and Cultural Rights, General Comment 12, Right to adequate food (Twentieth session, 1999), U.N. Doc. E/C.12/1999/5 (1999).

[131] Note the distinction between human rights, applicable to all within a state's jurisdiction, including beyond its territorial borders, and US Constitutional rights, such as the 4th Amendment, which are applicable only to US citizens and those non-citizens that can demonstrate a sufficient connection to the political community of the US, i.e., not to non-citizens overseas. See the ruling by the US Supreme Court in *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990).

[132] See *Bankovic et al, v. Belgium et al*, Judgement of the Grand Chamber of the European Court of Human Rights, 12 December 2001; this case concerned the deaths of Serbian citizens in the NATO bombing of FRY in 1999. The Court held that jurisdiction could not be construed to mean any action of a state that impinged upon human rights.

jurisdiction.[133] While aerial bombing of the territory of another state does not entail jurisdiction in this sense, having boots on the ground sufficient to constitute effective control over a certain territory will.

In addition, jurisdiction can include within its meaning a situation in which a state does not have effective control but where its actions have led to an individual's rights being violated by another state. For example, in the leading case in the field, *Soering* v. *UK*,[134] the European Court of Human Rights held the UK accountable for the inhuman and degrading treatment suffered by Mr. Soering in detention in the US because he had been deported by the UK. In a more recent case, the Strasbourg Court ruled that Belgium was accountable for the inhuman and degrading living conditions of asylum seekers in Greece because it had deported those individuals to Greece in compliance with the Dublin Regulation under EU law,[135] even though it had not been aware of the deplorable living conditions to which it was deporting them.[136] Such extra-territorial jurisdiction is not only applicable to the core rights of the Convention – Article 2 (right to life) and Article 3 (torture, inhuman and degrading treatment) – but has also been applied by the Court to Article 8 (right to family life) in deportation cases and to Article 1 Protocol 1 (the right to property). There is no suggestion that the Court would not apply extra-territorial jurisdiction to other Convention rights were such cases to come before it.

What the notion of the extra-territorial application of human rights implies in the context of cross-border cloud investigations is that where states act outside their territorial borders, they *may* incur human rights liability for their actions. The willingness of a judicial body, such as the European Court of Human Rights, to hold a state accountable for interference with human rights will depend primarily upon the extent of the control exercised. The *Bankovic* case suggests that, at least within the European system, accountability is not influenced by the possibility of a human rights 'gap', i.e., that the failure to find a jurisdictional basis for the claims made in *Bankovic* left the applicants without any form of redress for the harm done did not persuade the Court to give them standing.[137] The nature of the right affected is also important in determining the standard to which a state will be held i.e. the extent of a state's margin of appreciation.[138]

3.3.4. Summary of the international law framing of cross-border cloud investigations

Territory remains the key organisational principle of international law, despite the declarations by some of the end of sovereignty. While the uniform pattern of an international order comprised of almost 200 states has given away to a more fluid formation in which thousands of actors crowd the world stage and some of whom mount sovereignty-type claims to ultimate ordering power, international law remains fairly immune to such claims. What these shifts are doing, however, is helping us think of the state as more than its territorial extension. In place of territorial thinking, there is more attention to questions of jurisdiction. This is visible in the field of human rights within international law. At the same time, more powerful states or groups of states are using this new fluidity to assert their jurisdiction beyond their territorial borders; otherwise known as the 'effects doctrine'. What we are not seeing, however, is an extension of the jurisdiction to enforce, i.e. the ability to enforce a claim within the territory of another state. This remains a step too far.

---

[133] M. Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles and Policy* (Oxford: Oxford University Press, 2011).

[134] *Soering v. UK*, Judgement of the European Court of Human Rights, 7 July 1989.

[135] Specifically, Article 10 § 1 of Regulation 343/2003/EC.

[136] *M.S.S. v. Belgium and Greece*, Judgement of the Grand Chamber of the European Court of Human Rights, 21 January 2011. Greece was also held to have violated the Convention under a more straightforward application of jurisdiction.

[137] By refusing to ascribe jurisdiction to the NATO states, the Strasbourg Court affectively left the complaints without remedy for the harm done them. *Bankovic*, *op. cit.* n. 132.

[138] Eva Brems and Janneke Gerards, *Shaping Rights in the ECHR* (Cambridge University Press, 2014); Andrew Legg, *The Margin of Appreciation in International Human Rights Law: Deference and Proportionality* (Oxford University Press, 2012).

3.4. Framing the law-enforcement perspective

3.4.1. What do the main problems for criminal investigation consist of?

As the discussion on cross-border cloud investigations seems to be at least partly induced by practitioners claiming to suffer from the limitations of (national) territory-based legal investigation frameworks in relation to the rise of cloud computing, it is important to identify what the main problems for law enforcement actually consist of, and how these are framed. As far as we can determine, however, the problem is perhaps still more theoretical than practical. At least, in a previous study that one of us conducted to map the problems of cloud computing for criminal justice,[139] remarkably few real-life cases turned up where cloud computing had substantially affected criminal investigation. A small-scale survey among experts in ten countries, in early 2012, revealed that experiences with cloud computing in investigation and prosecution practice seemed as yet scarce. The only exception were web services, in particular webmail, which had existed for a longer time and which regularly feature in criminal investigations. Only two significant court cases were mentioned, the Yahoo! case in Belgium and the Rackspace case in the UK (see *infra*, section 4.1.4), both concerning law-enforcement authorities directly contacting a foreign-based provider. Although cloud computing was generally expected, both by the international experts and the interviewees in the Netherlands, to create considerable challenges for investigation in the foreseeable future, there was thus a scarcity of actual cases that could illustrate the challenges of cloud computing for criminal investigation.[140]

This was in line with the earlier finding of Kaspersen that there is an impression that cross-border investigation is becoming more complicated (in general, not limited to cloud computing), but that he knows few ‘adequately documented cases that will demonstrate the seriousness of the problem for criminal investigations’. Hence, Kaspersen recommended to first empirically document that existing measures are inadequate and to analyse whether there is an actual need for transborder access to data, before policy decisions are taken.[141] In our workshop, law-enforcement practitioners articulated various problems they face in practice, but these were not particularly cloud-specific; this seems to corroborate the idea that cyber-investigation faces significant challenges in an international context, but that the notional additional impact of cloud computing compounding these challenges—with the noted exception of accessing webmail—is not yet felt in practice to a significant degree.

Thus, if we are to provide an anatomy of the main problems for criminal investigation, it will necessarily refer to general cyber-investigation problems rather than cloud-specific problems. The only particularly relevant cloud applications are webmail services, often offered by large multinational companies such as Yahoo! or Google, and, presumably, cloud storage services such as Dropbox that are increasingly used by individuals instead of local storage on the home computer or laptop. While webmail primarily involves communications, it can involve many types of data, as documents and photographs can be attached to mail. Webmail, as well as remote storage services, can also be used by criminals to exchange files without sending them: one person will store a file in the box ‘Draft messages’ or in a cloud folder, which another person will then pick up (and often then delete on the remote service).[142] Apart from communications, any type of document that suspects store in the cloud may be relevant for the investigation. Therefore, it will not make sense to distinguish between different types of data in determining the main problems for law enforcement.

In a similar vein, it is hard to say which types of crime are primarily at issue. Cyber-investigation is far from limited to cybercrimes, as digital evidence may be relevant in any criminal case, including traditional physical crimes such as burglary or sexual assault. This is why the Cybercrime Convention stipulates that its cyber-investigation powers also apply to ‘the collection of evidence in electronic form of a criminal offence’ in general, and not only to cybercrime (art. 14 para. 2). Obviously, transborder crime will raise transborder investigation issues sooner than national crime, but as national crimes can just as easily involve digital evidence, transborder

[139] Koops et al., 'Misdaad en opsporing in de wolken'.
[140] Ibid.
[141] Kaspersen, 'Cybercrime and Internet jurisdiction. Discussion paper (draft)', at 29-30.
[142] Ibid., at 29; R.C. Van Der Hulst and R.J.M. Neve, 'High-tech crime, soorten criminaliteit en hun daders - Een literatuurinventarisatie' (Den Haag: WODC, 2008), at 46.

cyber-investigation is relevant for local as well as for transborder crimes. One can say, in general, that the problem of cyber-investigation is larger for serious crime, which often involves more effort and urgency to acquire evidence, than for petty or high-volume crimes; however, what qualifies as a serious crime depends on the national context and cannot be defined in global terms. At present, there is no evident consensus on particular crimes that countries agree to be the most problematic in relation to cloud or cyber-investigations. It may be possible, nevertheless, to identify at a supranational level a list of crimes that countries mutually agree on as being important in the context of transborder cyber-investigation; current mutual-legal assistance instruments already feature such lists,[143] which could serve as a starting point for a new international legal instrument (see *infra*, section 5.1).

For an anatomy of the main law-enforcement problems, the main element that we can distinguish is the mode of acquiring data. There seems to be considerable agreement, both with practitioners and with academic cyber-investigation experts, that classic mutual legal assistance is inadequate.[144] Some seek solutions in (further) streamlining mutual legal assistance rather than allowing for some form of extraterritorial investigation.[145] Many, however, seek the solution rather in moving beyond classic mutual legal assistance and allowing law-enforcement authorities some form of 'self-help'. Under the umbrella term of 'transborder access to data', two main modes of investigation are envisioned as possible solutions, which raise discussions as they are not accommodated in the existing paradigm of international cooperation in criminal matters. These two main forms of transborder access to data are:

1. a cross-border search, which can take the form of
    a. an extended network search, i.e., when law-enforcement officials search a certain location and find a computer with a network connection, they may extend the search to the remotely connected computers (this is regulated in art. 19 para. 2 Cybercrime Convention, but restricted to computers on national territory);
    b. a remote search, i.e., a search in remote computers, independent of an initial local search (this is not regulated in the Cybercrime Convention; it is a power being discussed in several countries, see *infra* section 4.1.3); such a remote search could be:
        1. limited to lawfully accessible computers (for example with a user name and password that the police have lawfully acquired during an investigation), or
        2. unlimited, allowing the police to hack remote computers, including by infringing security measures;
2. directly contacting a foreign provider, which can be
    a. a voluntary request, with which the providers can comply at their own discretion and within the limits of what their contractual relationship with the consumer allows (this is regulated in art. 32(b) of the Cybercrime Convention, see *infra*, section 4.1.4);
    b. an order that the provider has to comply with (this is currently not regulated in the Cybercrime Convention).

It is primarily these two types of criminal investigation, and their different possible instantiations, that need to be considered from the perspective of international law. Within that perspective, it may be relevant to consider that there can be different constellations of national connections when police seek transborder access to data. Often, the police from state A seeking evidence from state B will be investigating a crime because the victim is a national or resident of A, while the suspect (if known) will be a national or resident of B, or vice versa. In the cyber-investigation context, however, it may well occur that both victim and suspect are located in A, while evidence is located in B, and there may be some logical connection between the data being in state B (for example, a foreign bank account held by the suspect) but the connection may also be more incidental, when B is using a webmail service offered by a company with its headquarters, or a cloud server park, in B. It can also occur that the location of the victim or the suspect is unknown, but that the data in state B are assumed to be of relevance for the police in state A. But it can also occur that the location of the evidence sought is unknown or uncertain (the police do not know that they are actually in state B), while the victim or suspect may or may not have some

[143] See, for example, art. 2(2) Framework Decision 2002/584/JHA (European Arrest Warrant), *Official Journal* L190, 18.07.2002, p. 1-20.
[144] Expert workshop 19 December 2013; see also *supra*, notes 57-58 and surrounding text.
[145] Gercke, 'Understanding cybercrime', at 278.

connection with B. And more variations and even more complex constellations are possible, of course. With a lack of empirical documentation of problematic cases, we do not know which of these constellations is more likely to occur or more problematic in practice. We will therefore have to consider both situations in which transborder access to data is targeted at a state that has, through a connection with victims or suspects, some substantive connection with the crime (and thus a stronger potential interest in the criminal investigation), and situations in which the remote state has only a cursory connection with the crime. We will also have to consider situations in which the location of the remote data is not or insufficiently known. As this latter situation is mentioned by practitioners to occur frequently —as they claim they often cannot 'see' 'where' the data are[146]—it is an important part of the problem framing, and requires some further scrutiny, which we will provide in the following section.

3.4.2. The role of the 'I don't know where the data are' argument

3.4.2.1. Spoenle's 'loss of location'

A powerful framing within the debate about transborder access to data is the 'loss of location' claim introduced by Jan Spoenle in a discussion paper for the Council of Europe's Project on Cybercrime.[147] According to Spoenle,

> 'Due to positive effects in terms of availability, power consumption and costs, the users' data is constantly moved around within the "cloud" by algorithms. Therefore, it's always possible to access a certain e-mail message; however it's not possible to tell where exactly the data representing this certain message might be located. (…) Like Google, Dropbox uses servers in different countries to store their users' data, which is being moved around constantly to minimize costs and maximize availability. Once again, the files stored in Dropbox folders are accessible at any time, but their exact location at a certain point of time is practically indeterminable. (…) [D]ata in the clouds is constantly shifted from one server to the next, moving within or across different countries at any time. Also, data in the clouds might be mirrored for security and availability reasons, and therefore could be found in multiple locations within a country or in several separate countries. Due to this and to cached versions of data, not even the cloud computing provider might know where the sought-after data is exactly located.'[148]

Consequently, location as a characteristic of objects 'has ceased to function under the conditions of cloud computing', which results in a 'loss of location' that 'is likely to cripple cybercrime investigations at a very early stage.'[149] The 'loss' of location is a metaphor, suggesting that objects—including data—'had' a location which they 'lose' when they are in the cloud. Assuming that Spoenle does not mean this in some quantum-mechanical sense (that particles do not have 'a' location, but have multiple locations at the same time that can only be expressed in terms of probabilities), the metaphor of 'loss' does not really aptly capture the situation of data in the cloud: they still *have* a location at any time, but the location may be difficult to *determine* at any point in time. It is thus not an ontological loss (i.e., a characteristic of the data), as the metaphor seems to suggest in the way that Spoenle uses it, but rather an epistemological loss (i.e., a characteristic of the observer of the object). The difference may sound unimportant to the average cyber-investigation expert, but it can matter considerably for an international law scholar: if the data *are* not on any identifiable territory, the legal assessment under international law may be quite different from the situation in which the data *are* on some territory but the person accessing the data does not (appear to) *know* which territory that is. Framing the problem as a 'loss of location' might therefore lead to different solutions than where the problem is framed as a 'loss of knowledge of location'.

[146] Expert workshop 19 December 2013.
[147] J. Spoenle, 'Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?' (Strasbourg: Council of Europe, 2010).
[148] Ibid., at 4-5.
[149] Ibid., at 5.

3.4.2.2. Geo-location technologies and cyberspace jurisdiction

The claim of a 'loss' of (knowledge of) location in the cloud has many similarities to the earlier claim in the Internet governance debate that in cyberspace, (physical) location no longer matters (see the 'exceptionalist' view, *supra*, section 3.2). As noted above, Internet regulation practice has largely sided with the non-exceptionalists, finding ways to establish jurisdiction on the basis of cyberspace's connections with objects, persons, or data processing activities on their territory.

This is facilitated partly through the rise of geo-location technologies, which enable the geographic (national) origin of an IP address to be identified.[150] Most IP addresses are allocated in batches to national registrars who distribute them across Internet access providers in their countries, who in turn provide their users with the IP addresses; thus, most IP address can be recognised as falling in a particular national batch. Geo-location service providers could extend this with other available information about IP addresses in use (e.g., host name translations or web content), enabling them to make educated guesses about the location of an IP address.[151] Also some other information about a computer that may be retrieved remotely, such as language and time zone, could provide some indication of geographic origin.[152] Although geo-location providers claim that they can identify IP addresses' location with 99% accuracy, this is contested as being unproven.[153]

Moreover, Internet users can apply anonymising services or use proxy servers to shield their IP address, so that the ostensible IP address of a computer may not reveal the location of the real user, but perhaps only that of an in-between computer, which can be located anywhere.[154] The claims of high accuracy rates of geo-location are based on average users and 'typically assume no evasive action by users; this is not particularly useful in adversarial applications.'[155] For the purposes of criminal investigation, in which evasive actions by suspects should be expected, there is not too much promise in relying on geo-location technologies to identify the likely location of a computer that is the object of a criminal investigation.

It should also be noted that the literature on geo-location in relation to establishing jurisdiction[156] almost only discusses the situation in which a website owner attempts or should attempt to determine the geographic origin of website visitors in order to decide whether or not certain content or services can be offered to a particular visitor (e.g., not to offer Nazi memorabilia in countries where these are prohibited, or offering music only to users from countries for which a license has been obtained). This is different from situations in which police officers try to identify the geographic origin of a computer they are trying to remotely access; in the former, the server tries to identify the client based on an http request (the protocol used for websites), while in the latter, the client tries to identify the server (possibly using another protocol, such as FTP or SMTP). We are not aware of literature that discusses the latter case in terms of accuracy of geo-locating an IP address.

Therefore, although geo-location technologies may provide part of the answer to addressing cyberspace jurisdiction issues in private or substantive criminal law related to the geographic reach of websites, it is unclear whether, and to some extent unlikely that, they can provide some foothold on which to determine jurisdiction in the context of criminal procedure. The combination of the fact that criminals may use proxy servers to hide the origin of their original Internet access computer, and the fact that they can frequently and speedily relocate data on servers, underlines the idea that there is a loss of knowledge of location of Internet data in the context of cyber-investigation. As Kaspersen concludes, if law enforcement needs to access data 'to obtain evidence of criminal activity (…), it will hardly be possible to take legal action around the internet,

---

[150] Dan Jerker B. Svantesson, 'How Does the Accuracy of Geo-Location Technologies Affect the Law', *Masaryk University Journal of Law and Technology,* 2 (2007), 11-21.
[151] Ibid., at 12, 16.
[152] Dan Jerker B. Svantesson, 'Geo-location technologies and other means of placing borders on the 'borderless' Internet', *Journal of Computer & Information Law,* 23 (2004), 101-39 at 120-21.
[153] Svantesson, 'How Does the Accuracy of Geo-Location Technologies Affect the Law', at 14-16.
[154] Ibid., at 16-19.; Kaspersen, 'Cybercrime and Internet jurisdiction. Discussion paper (draft)', at 28. See also James A. Muir and P.C. Van Oorschot, 'Internet Geolocation and Evasion' (Ottawa: School of Computer Science, Carleton University, 2006).
[155] Muir and Van Oorschot, 'Internet Geolocation and Evasion', at 20.
[156] Ibid.; Svantesson, 'Geo-location technologies and other means of placing borders on the 'borderless' Internet'; Svantesson, 'How Does the Accuracy of Geo-Location Technologies Affect the Law'.

because there is no certainty whatsoever of the physical location of the data, necessary as a nexus for the execution of investigative powers within the domestic sphere or *a fortiori* within the international sphere.'[157]

3.4.2.3. The locatability of data in the cloud

While location may already often be difficult to determine in general cyberspace contexts, it seems that the cloud compounds the complexity of locatability of data. 'An oft-cited feature of cloud computing is that data may automatically flow between different equipment, in the same or different data centres, even to different countries. Sometimes, even the supplier cannot precisely pinpoint certain data's location within a data centre.'[158] This feature has led various authors, analysing the implications of cloud computing for law enforcement, to conclude that it is, or is becoming, virtually impossible to determine the location of data in the cloud.[159] It should be noted, however, that these authors primarily have a legal background, largely in criminal or cybercrime law, and that they have not necessarily studied the technologies and practices of cloud computing services in depth. We should not conclude outright that locatability of data in the cloud is virtually impossible or, in principle, much more complicated than locatability of data on the Internet in general.

At the workshop we organised in the context of this study, it was remarked that the reports of the cloud-induced death of location were grossly exaggerated, as in practice data are often stored in a cloud server park close to the user to maximise speed.[160] There is also a trend of cloud providers offering to restrict data storage and processing to certain countries or regions, so that users are assured that the processing complies with their local data protection laws, or to ensure that the data remain out of the United States' long-arm's reach;[161] for example, several providers offer cloud storage in the 'European region'.[162] In line with a growing acknowledgement of the international nature of cloud storage, providers are increasingly mentioning the location(s) of their data processing,[163] and being generally more transparent about the location of their data centres.[164] These developments suggest that, to some extent at least, it is still possible to identify the likely location where data are stored in the cloud.

However, significant challenges to locatability of cloud data remain. Although efficiency might induce a preference for storage in certain data centres close to the user, cloud researchers acknowledge that, depending on the systems used, data may still move around, across and within data centres.[165] The providers offering local or regional storage usually do not commit contractually to keep the data in the chosen region,[166] which raises doubts over the actual or verifiable character of the geographic storage position. Moreover, the regions are broad or vague, such as 'Europe' or 'North Europe'. State-specific storage services are available for private cloud services (i.e., where a company hires a separate cloud infrastructure for its own use) but may be less available for public cloud services (i.e., where the cloud infrastructure is shared among various users, whose data are separated by access restrictions). Although law enforcement may sometimes have a need to investigate a large company that uses a private cloud, in most cyber-

[157] Kaspersen, 'Cybercrime and Internet jurisdiction. Discussion paper (draft)', at 29.
[158] Kuan Hon, Millard, and Walden, 'Public Sector Cloud Contracts', at 127.
[159] For example, Koops et al., 'Misdaad en opsporing in de wolken'; Schwerha Iv, 'Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers"', at 17(concluding that it 'is impossible to know where the sought after data resides'); J. Spoenle, 'Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?' Ibid.).
[160] Expert workshop 19 December 2013.
[161] Simon Bradshaw, Christopher Millard, and Ian Walden, 'Standard Contracts for Cloud Services', in Christopher Millard (ed.), *Cloud Computing Law* (Oxford: Oxford University Press, 2013), 39-72 at 55.
[162] W. Kuan Hon and Christopher Millard, 'How Do Restrictions in International Data Transfers Work in Clouds?', ibid., 254-82 at 274.
[163] Simon Bradshaw, Christopher Millard, and Ian Walden, 'Standard Contracts for Cloud Services', ibid., 39-72 at 56.
[164] W. Kuan Hon and Christopher Millard, 'How Do Restrictions in International Data Transfers Work in Clouds?', ibid., 254-82 at 275.
[165] W. Kuan Hon, Christopher Millard, and Ian Walden, 'Negotiated Contracts for Cloud Services', ibid., 73-107 at 88
[166] W. Kuan Hon and Christopher Millard, 'How Do Restrictions in International Data Transfers Work in Clouds?', ibid., 254-82 at 274.

investigation cases the type of cloud will be a public cloud. For determining cyber-investigation jurisdiction, a regional indication such as 'Europe' will not be useful.[167]

Moreover, other possible complications may arise. If the cloud service is part of a layered service—e.g., a cloud webmail service (SaaS) built on a cloud platform (PaaS) that uses a cloud infrastructure (IaaS)—determining the location of data may become very complex,[168] as it requires studying the terms, conditions, and practices of all different cloud providers involved, and the different providers may not be able to pinpoint where particular data are as they only see their limited part of the picture. If data are retrieved from the client side (the end user's account), which is typically the case when law enforcement officers conduct a transborder search of data in the cloud, the data need not necessarily come from the 'real' storage location but can also come from a caching server (i.e., a server closer to the user than the original server, in which data are temporarily stored to facilitate efficient data transport).[169]

Interesting complications will also arise when cloud infrastructures are located on ships, which is a distinct possibility as Google has a patent on floating data centres.[170] Although apparently 'currently intended to be based in territorial waters', it is 'not inconceivable that in [the] future providers could use data centres on ships (…) in international waters'.[171] Determining the 'location' for jurisdiction purposes would then imply determining the flag flown by the floating data centre, which will not be easy for law enforcement officers to see when they are searching in the cloud.

3.4.3. The role of human rights

A number of human rights issues arise in the context of cross-border data searches. The problems of human rights protection in the context of international co-operation for the suppression of transnational crime are well-known and form the context of our examination here.[172] The rights most affected by cross-border data searches are the right to privacy and the right to protection of correspondence. Article 12 of the Universal Declaration on Human Rights provides:

> 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks'.

According to Balboni & Pelinoa, the 'idea of privacy, in a modern sense, includes protection of all data in electronic form which can be linked to an individual, e.g. emails, tweets, posts and similar.'[173] Moreover, the rights contained in Article 12 protect both the target of any investigation and any third parties whose privacy or correspondence is interfered with as part of any data search.

Data protection, whilst undoubtedly an important limit to the actions of states, is not strictly speaking part of the international human rights canon. Rather, data protection is usually viewed internationally as part of the right to privacy; an exception here is the European Union Charter of Fundamental Rights and Freedoms, which enshrines data protection as a fundamental right distinct from the human right to privacy. Data protection here is, however, a fundamental right not

---

[167] It might become useful in the future if a certain region would agree on an instrument to allow unilateral transborder access to cloud data. Since the European Union already has a considerable development in criminal co-operation based on the principle of availability (see section 2.4.1), 'Europe'-limited cloud services could remove some of the problems of cloud data locatability. However, current 'Europe'-limited services often do not specify what 'Europe' means, and their data centres are not necessarily restricted to the EU or the European Economic Area (ibid.).

[168] Cf. Kuan Hon and Millard, 'Cloud Technologies and Services', at 15-16; W. Kuan Hon, Christopher Millard, and Ian Walden, 'Public Sector Cloud Contracts', ibid., 108-41 at 129-30.

[169] Schwerha Iv, 'Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers"', at 10 (claiming that '[s]ince systems could be using caching servers transparent to the end user, the person at the keyboard may not know where the actual data is coming from exactly').

[170] https://www.google.com/patents/US7525207.

[171] Kuan Hon and Millard, 'How Do Restrictions in International Data Transfers Work in Clouds?', at 275.

[172] Neil Boister, 'Human Rights Protections in the Suppression Conventions', *Human Rights Law Review,* 2 (2002), 199.

[173] Paolo Balboni and Enrico Pelino, 'Law Enforcement Agencies' activities in the cloud environment: a European legal perspective', *Information & Communications Technology Law,* 22/2 (2013), 165-90, p. 168.

a human right[174] and its status is as yet limited to the space of the European Union.[175] For that reason, we do not consider data protection in any depth here.[176]

The precise content of the right to privacy in relation to data searches remains unclear because of the lack of case-law in this area.[177] What is clear, in light of the proportionality requirement, is that law-enforcement authorities (LEAs) should restrict themselves to searches for specific data that are necessary in the context of a particular criminal investigation. Human rights bodies, notably the European Court of Human Rights, will look strictly at the copying and further processing of personal data of third parties. Further, while data obtained through cross-border searches is not significantly different in type to data issues that already arise in criminal investigations, the sheer amount of personal information stored in the cloud is likely to make such investigations more intrusive than non-cloud criminal investigations, and thus compliance with the right to privacy may require especially stringent safeguards to ensure that LEAs do not access accounts other than those of the person under investigation, and that no data about third parties are acquired unless strictly unavoidable or necessary. Moreover, since data stored in the cloud can encompass communications (e.g., webmail or other stored communications), the right to protection of correspondence should also be particularly safeguarded, so that LEA activities in accessing cross-border data meet with all national legal and ECHR requirements for acquiring communications, such as foreseeability and strict checks and balances.[178] What is more, correspondence of a professional kind that relies upon confidentiality, such as with a lawyer, doctor, or priest, must be strictly protected; short of preventing an immediate threat to life, there can be no justification for accessing such correspondence. Therefore, particular care must be taken that (cross-border as well as national) searches do not have any chilling effect on individuals seeking access to such professionals.

Other human rights possibly affected by data searches include freedom of speech (article 19 ICCPR; article 10 ECHR), which includes the right to receive and impart information across frontiers, freedom of association (article 22 ICCPR; article 11 ECHR), and the right to a fair trial (article 14 ICCPR; article 6 ECHR). The latter may be engaged by cross-border data searches, particularly where the data retrieved constitutes evidence in a criminal prosecution and where the legality of the search is dubious.[179] It seems nonetheless unlikely that cross-border data searches for the purpose of criminal prosecution of themselves would raise these broader human rights concerns, at least not in a different way than national data searches would do.

Given the current inevitable vagueness about the substantive content of the right to privacy in the context of cross-border data searches, the remainder of this section shall focus on a number of procedural or general human rights issues that may arise.

The first issue to note concerns the nature of human rights obligations; as observed in section 3.3.3 above, human rights are vertical obligations between the state and those within its jurisdiction, whether individuals, legal persons, or relevant groups. What this means is that relations between service providers and users in relation to issues such as privacy or data protection are not human rights issues. Rather, such matters are governed by the contract agreed between the provider and the user (and liability may arise within the domestic law governing the contract). The existence of such a contract, however, does not entail that the human rights responsibilities of a state are not engaged where it seeks the voluntary co-operation of a service provider to supply data. The state cannot sidestep its obligations to respect the privacy of the individual user by relying on the voluntariness of the service provider in providing the data sought,

[174] Fundamental rights and human rights are not the same thing, despite a good deal of overlap. Fundamental rights are rights of fundamental importance to a given social ordering – such as data protection or the right to academic freedom – but that make no claim to universal status. In contrast, human rights claim universal validity; as a consequence, the list of human rights is more limited.

[175] For the European view on data protection as a fundamental right, see Paul De Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalization in Action', in Serge Gutwirth et al. (eds.), *Reinventing Data Protection?* (Berlin: Springer, 2009), 57-71.

[176] For a discussion, see, e.g., Balboni and Pelino, 'Law Enforcement Agencies' activities in the cloud environment: a European legal perspective'.

[177] http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection.

[178] E.g., ECtHR, *Kruslin* v. *France*, app. 11801/85 (1990) and *Huvig* v. *France*, app. 11105/84 (1990).

[179] Jenny Schultz & Melissa Castan Sarah Joseph, *The international covenant on civil and political rights : cases, materials, and commentary* (Oxfrd: Oxford University Press, 2013).

for example. This is not to state that human rights obligations of the state *are* engaged by cross-border searches but simply to note that the actions of the service provider do not affect the obligations of the state to the individual.

Secondly, a state owes human rights protection not only to the natural individuals within its jurisdiction but also to legal persons, such as corporations or other incorporated actors. This is particularly relevant for certain rights, such as the right to property or freedom of speech. A state can thus also breach the human rights of service providers and not simply users.

The third element to note is the wide variation in implementation of a right such as privacy at the national level. Human rights are universal at the abstract level only and rely upon implementation in domestic law to be given concrete legal status. This means that there is no universally shared content for the right to privacy or data protection at the international level. This is likely to entail that it is the minimum standard that becomes the international norm, as a state cannot be held to standards above that to which it has consented. This may be problematic for Member States of the European Union or state parties to the Council of Europe, where standards on privacy may be higher than in some other parts of the world. That said, within the legal spaces of the Council of Europe and the European Union, it is possible to speak of shared standards.

A final but significant human rights issue in the context of cross-border data searches concerns the 'loss of (knowledge of) location' problem. This raises issues of determining the 'location' of human rights protection. Human rights are protections offered by a state to those within its jurisdiction. If we do not know where data are in terms of their physical location, knowing which state is responsible for ensuring that the human rights of those under investigation are protected becomes more complicated, but not impossible. To ensure that a gap does not occur (whereby the acting state assumes that the state in which data are located provides protection and vice versa), it would be advisable to adopt the effective control test used by the ECtHR in, e.g., the *Al-Skeini* case (discussed above in section 3.3.1), thereby assuming the extra-territorial application of human rights standards. In such an approach, it is the state taking action, by taking effective control of a situation, that is understood to be extending its jurisdiction and hence its human rights protection to those it acts upon. Whilst such an approach addresses the 'loss of (knowledge of) location' issue, it raises others in terms of human rights. While human rights standards are universal in theory, in practice the human rights standards offered by many countries would not meet standards demanded by domestic legal orders, e.g., in the US in relation to sentencing policy, or Europe in relation to US rules on self-incrimination, where US rules are much more protective. It may be different where China is the state acting in relation to data belonging to a Dutch citizen. This question of the actual human rights standards to be applied needs to be resolved in the creation of any regime that allows for cross-border data searches.

3.4.4. Summary of the law-enforcement framing of cross-border cloud investigations

The notional impact of cloud computing compounding the challenges of cyber-investigation does not—with the exception of accessing webmail—seem to be felt yet in practice to a significant degree. The main problems for law enforcement will therefore tend to be general cyber-investigation problems rather than cloud-specific problems. This can, in principle, involve any type of data in relation to any type of crime. As cyber-investigation often involves a need for expeditious securing of data for criminal-investigation purposes, many practitioners as well as cyber-investigation scholars frame the problem as a need of moving beyond classic mutual legal assistance and allowing law-enforcement authorities some form of 'self-help' through transborder access to data. This can involve a) a cross-border search (an extension of a physical search or a separate remote online search, which may or may not be limited to lawfully accessible computers) or b) directly contacting a foreign provider (with a voluntary request or a compulsory order). Some of these modes of transborder access are provided for in the Cybercrime Convention, but with significant limitations; the potentially most effective ones—an unconsensual transborder search or a direct order to foreign service providers—are currently not allowed. One of the most pertinent questions raised by cloud computing for law enforcement is whether such more invasive forms of transborder access to data should be allowed, and if so under what conditions. The question gains urgency through the fact that the foreign state may lack a substantive connection with the crime, its victims, or suspects, and thus lack an incentive to assist in the criminal investigation. Moreover, we also have to consider situations in which the location of the remote data is not or insufficiently known.

It would be too easy, however, for law enforcement officers to claim (which they might want to do when intending to conduct a remote search and wanting to avoid jurisdiction problems) that they 'don't know where the data are' merely because it is difficult to determine the location of Internet-based or cloud-based data. To some extent, the location of data can be established, with reasonable likelihood, through geo-location technologies. The locatability of data on the Internet, which has to some extent ended the debate about cyberspace jurisdiction in favour of the non-exceptionalists, primarily resides in the private-law and average-user/abiding-citizen context. In criminal investigation, the possibilities for criminals of circumventing or obfuscating geo-locating data are substantial enough to raise considerable doubts on the feasibility, in practice, of the theoretical merit of geo-location technologies. Although determining the location of cloud-stored data is not as impossible as some authors are suggesting, the cloud does compound the locatability problem of data even further, not only through its feature of moving data around but also through complications such as layered services and, possibly, floating cloud centres. This effectively means a 'loss of location', not in the ontological sense but in the epistemological sense: it is becoming very difficult to know where cloud-based data are stored. To avoid the suggestion that the data do not *have* a location (with the connotation that they vaguely float somewhere in outer (cyber)space), however, it is important to speak of a 'loss of knowledge of location' rather than a 'loss of location'.

3.5. Conceptualising transborder access to data

Transborder access to data basically comes in two main forms: a transborder search and directly contacting a foreign provider (*supra*, section 3.4.1). Contacting a foreign provider to request (or order) certain data is a relatively straightforward type of activity; it entails using some communications medium (telephone, fax, email, snail mail) to send a request to a person or entity in a foreign state, and the person or entity then decides whether or not to send the data to the requesting law-enforcement authority. This is something that has been possible for a long time, and it does not require further investigation at the conceptual level in order to be able to assess it from the perspective of international law. The other mode, a transborder search, however, is a relatively new form; it has precedents in law-enforcement officers going to a foreign state and conducting some search activity there, but a computer network search is not exactly a functional equivalent of physically present persons searching on foreign territory. We need some further analysis in order to conceptualise what a transborder search comes down to, in technical and metaphorical terms, before we can draw on analogies and interpretation schemes under international law.

3.5.1. What does a transborder search amount to, technically?[180]

An adequate description of a transborder search should be technically correct but not phrased in too technical terms, in order for legal scholars to be able to make a legal assessment (which we will attempt to do below, see section 4.2). There are many ways in which a transborder search could be conducted, and an adequate description depends on the details, which makes it impossible here to give a comprehensive overview. We limit ourselves to what we think are the most typical cases and the main factors or dimensions that matter in a transborder search from a legal perspective.

In cloud investigations, law-enforcement authorities will usually want to access email or documents stored in the cloud. We assume that the standard way of doing so fits in the client-server model,[181] in which the LEA's computer functions as client and the cloud provider's computer where the data are stored (or collected from) functions as the server.[182] The server can be accessed through different protocols, depending on the software and applications used (e.g.,

[180] This section is partly based on a personal communication from Jaap-Henk Hoepman, 10 April 2014 (on file with first author).
[181] See http://en.wikipedia.org/wiki/Client-server.
[182] Other constellations are possible in transborder access; for example, in the Bredolab case (see note 215 and surrounding text), the LEA used a server (the botnet's command & control server) to send a message to all clients. To keep our analysis practicable, we limit ourselves to discussing only the LEA-client / cloud-provider-server constellation.

HTTP for web-based access, FTP for file transfer, or POP3 or SMTP for email programs[183]). Technically, these protocols differ, but conceptually they largely come down to the same thing, namely that the client sends a message to the server with a certain request, and the server interprets and acts upon this request; this can entail sending the requested data (e.g., a list of items included in a folder, or the content of a certain message or document, or all the data in a folder—all depending on the type and content of the request), or it can entail sending back a message of refusal or simply ignoring the request (e.g., because the requester is not authorised to access the account, folder, or data requested, or because the requested data are not available).

A relevant factor for the analysis is authorisation. We should distinguish between situations in which the LEA has the correct credentials to access the server account (e.g., the login name and password given by the suspect or found on a post-it note on the suspect's desk, or access information provided by the service provider[184]), and situations in which the LEA does not have such credentials, in which case they can attempt to break into the account (e.g., by the brute force of trying every possible password, or by trying to penetrate through the security measures by, for instance, a scan of all ports[185]—i.e., 'doors' into the computer—and subsequent exploitation of security weaknesses associated with available ports). Both trying to guess (by brute force) the password and a port scan entail sending messages with requests, but the types of request differ, and the way in which the server responds also. Roughly speaking, in the case of correct credentials, the server responds in ways it is programmed and intended to do, while in the case of security-circumvention attempts, the server responds in ways it has been programmed to do (by definition it can only respond as it is programmed to do) but arguably not necessarily as it is intended, by its user, to respond. For instance, if the server executes a script that exploits a security weakness to install malware, this falls within the range of programmed actions but outside the range of actions intentionally accepted by the user when putting the server into operation. Moreover, in the case of exploiting security weaknesses after a port scan (e.g., if a backdoor program is installed that allows sneak access by the police), the server not only responds in ways it was presumably not intended to respond by its user, but its functioning is also significantly affected. The legal assessment under international law may differ for the two situations involved in transborder access, i.e., access with correct credentials, which involves an element of deception (as the law-enforcement officer pretends to be the user) but does not alter the normal or intended functioning of the computer, and access through exploiting security weaknesses, which involves manipulation and does alter the normal or intended functioning of the computer.

Another important factor for analysis is the level of intrusion in the accessed (part of the) server. In the ('ethical' or 'white hat') hacker community, the following types of activities would often be distinguished as having increasing levels of intrusion:

1. looking around in the server at a meta level, i.e., at file names or message headings ('looking around' is a metaphor here for sending a request to send back the meta data of certain files or folders);
2. looking around in the server at the content level, i.e., opening certain files or messages and accessing their content;
3. copying or downloading files or messages;
4. manipulating files or messages, or adding files or messages;
5. deleting files or messages.

There is not a great practical difference between 2 and 3, since both involve the content of files being sent from the server to the client; the only difference is that with 'looking into' the content of a file, the content will usually be stored in the temporary memory of the client's computer (which may be lost when the computer is switched off, so it requires an additional act of the user to permanently store the content), while in downloading content the file will usually be stored in the permanent memory part of the client's computer.

[183] See http://en.wikipedia.org/wiki/Communications_protocol#Common_types_of_protocols for an introduction.
[184] Note that under article 32(b) Cybercrime Convention (see *infra*, section 4.1.1), LEAs can request (on a voluntary basis) foreign providers not only to send them data, but also to provide access to the data.
[185] See http://en.wikipedia.org/wiki/Port_scan.

A relevant factor related to the level of intrusion is whether the message sent to the server only contains command lines (within a suitable computer language and protocol, such as 'get this file' or 'show me the contents of the folder'), which the server—in line with how it has been programmed—determines how to deal with; or whether the message also contains executable code, such as scripts (small programmes that execute themselves on the remote computer) that would, for instance, install a backdoor program on the server. The latter could be relevant to get more, or more efficient, insight into the contents of the remote computer, or to manipulate or delete files; this is more intrusive than non-executable code, as it takes over some of the control of what is happening on the remote computer. Executable searches may be relevant, depending upon the goal or stage of an operation, for instance where a law enforcement official anticipates counter-action by the targeted user, or where the goal of an operation is not only to secure evidence of child pornography but also to restrict, temporarily or permanently, access to the offensive images or data.[186]

3.5.2. What does a transborder search amount to, metaphorically?

In the previous section, we have attempted to describe in plain terms what happens in a transborder (or, in fact, any remote) network search. We have not attempted to avoid metaphors, which in any case would be very hard to do, as natural language can hardly capture technical processes without resorting to metaphors. In everyday language, it is customary to speak of 'going to' a website, 'visiting' a server, and 'looking around' in a mailbox. Of course, computer users do not really go or visit anywhere, nor do they actually look into mailboxes; this is a manner of speech for situations in which computer users access content from remote computers. It is important to realise that the 'travel' metaphor is misleading, at least in our context: speaking of a police officer 'going to' a remote server tends to trigger a frame that is associated with police officers visiting a foreign state, and the physical presence of foreign police agents (acting in their capacity as law-enforcement officers) on their soil is something that states do not accept without their express consent. The physical presence of officials is a major factor in an international-law assessment of extraterritorial state activities, and since transborder computer searches do not involve the physical presence of persons, we should attempt to avoid metaphors associated with this frame.

Another metaphor that could be used to describe a transborder search (with copying but not altering data) is that law-enforcement authorities take snapshots of the situation in the remote server. The search is then conceptualised in terms of a sensor that records a situation. The search could be compared to making satellite images of the situation in another state, or sending a camera-equipped drone to another state to take photos. Although a computer search causes some activity on foreign territory (in the server, which has to respond to the client), and is more intrusive than a satellite that only passively records an image, it is comparable to an active satellite that emits radiation and measures the energy reflected back by objects.[187] An active satellite can still only measure the outside of objects, however, while a computer search enters into closed spaces. In addition, a satellite image cannot change the nature of an object – it simply records it; the simple fact of entering a computer system changes the data within it. Yet, it should be recalled that when satellites were first developed and used, their advent was viewed by states as deeply intrusive, since air space above states is part of a state's exclusive realm and thus before the advent of satellites the territory of a state was a closed space (with the exception, of course, of border areas or internationally-managed waterways). Thus, a satellite taking detailed images of topographical features or any activities, such as troop movement, within a state from outer space can also be seen (at least, it was initially seen) as a way of capturing data from a closed space, similarly to cross-border data searches.[188]

An alternative analogy would be that of sending a drone that swipes an ID to enter an access-controlled building (or that otherwise disguises itself as someone allowed to enter the building) and that makes photographs of the interior. Such a simile seems far-fetched, in the sense that we

[186] A comparison could be made to a legal search of a property used for the distribution of illegal drugs, where the property is not only secured in order to be searched but is then sealed in order to make the property unusable for criminal purposes.
[187] See *infra*, note 288 and surrounding text.
[188] See *infra*, section 4.3.5 for the international legal regime on satellite imaging.

have no experience with such drones, and it is therefore not a helpful comparison upon which to base a legal assessment. Moreover, there may be a difference between physical drones (moving through a nation's airspace) and non-physical electric signals (moving through cables) in terms of the way and degree in which territorial sovereignty is affected. Therefore, the metaphor of a search 'looking into' and 'taking a snapshot image' of a remote computer is altogether not the most suitable.

Another metaphor is to describe the transborder search as the sending and receiving of messages. In this way it is, to some extent, comparable to sending a letter to a foreign service provider, such as a bank, to request information about a customer's account. Although this is somewhat contested, directly contacting foreign providers seems to occur frequently in practice.[189] A relevant difference may be, however, that in the offline case, the service provider uses humans to decide whether or not to send back the requested information, which may involve a more discretionary form of decision-making than in the case of servers responding to requests they are programmed to respond to. Moreover, the provider—as a legal person or as a real person through its employees—would normally be aware that the request comes from a foreign authority, not from the client; while in the computer search scenario, the analogy would be rather that the bank is led to believe that the request comes from the client herself. The element of deception might be relevant in the assessment under international law, and it should be noted that where the computer server also 'believes' that the request comes from the client, as it is made with correct credentials, an 'automated belief' may have a different flavour—in terms of the degree of deception involved—than a human (or legal-institutional) belief.

Although the metaphor of sending and receiving messages may thus be associated with some connotations that are not precisely appropriate to describe a transborder search, we think that overall, it is the most suitable metaphor, and it should serve as a good frame on which to base the legal assessment under international law.

3.6. Conclusion

As in all areas of social life, metaphors play an important role in conceptualizing and framing cyberspace and hence in our understanding of what is involved in cross-border data searches. Cyberspace, as the language we use to describe our actions there suggests, is conceived by the majority of states as place and thus as subject to territorial jurisdiction. However, while our conception of jurisdiction remains largely wedded to notions of territory, recent developments, particularly in the area of human rights, have seen the spatial extension of legal authority extended beyond territorial boundaries and defined instead by effective control. These developments are not only important in revealing the contingency of the seemingly-natural relationship between authority and place but will also be central, we have suggested, in thinking about human rights safeguards in the context of cross-border searches.

Further, we have suggested in this chapter that the main difficulty confronting criminal investigations that seek to collect evidence from cyberspace is the *loss of knowledge* of location and not a loss of location itself. This is an important distinction. Moreover, it helps to highlight the key aspect of the problem, that is that those using the cloud to facilitate criminal activities are likely to, and can easily, obscure the location of their data.

Finally, it is important not to allow language to obscure the nature of what a cross-border search entails. Our suggestion here is that such a search is best characterised as the sending and receiving of messages. The legal qualification of a cross-border search—its lawfulness—will

[189] See *infra*, notes 210 and 234. An example would be the cross-border practice of tax authorities. Many tax codes, e.g., that of the US, require tax authorities to seek information from third parties where a citizen provides incomplete financial information. The legality of such action will depend upon the consent of the state where the third party is located. This consent can be given via national law where it explicitly allows for information to be supplied to foreign LEAs or via a treaty, where consent for such co-operation is explicitly given. For example, although the US tax code requires the Internal Revenue Service to seek information on the overseas assets of US citizens, the Swiss criminal code prohibits the supplying of such information without the client's consent. See Paolo S. Grassi & Daniele Calvarese, "The Duty of Confidentiality of Banks in Switzerland: Where It Stands and Where It Goes - Recent Developments and Experience - The Swiss Assistance to, and Cooperation with the Italian Authorities in the Investigation of Corruption among Civil Servants in Italy (The "Clean Hands" Investigation): How Much Is Too Much?', *Pace International Law Review,* 7/329 (1995), p. 347.

largely depend upon the question of consent and who has the lawful authority to consent. We pick up the question of the centrality of consent in the next chapter.

4. Analysis

4.1. Current framework, practices, and discussions on cross-border access to data

4.1.1. The legal framework for transborder access to data

Article 19 of the Cybercrime Convention provides for an extended network search, i.e., extending an existing search (e.g., in a house) to computers lawfully accessible to the computer on the search location; this extended search, however, should remain within the national borders, i.e. can only search on computers or servers within the state's territory. Article 32 of the Cybercrime Convention allows a cross-border search in two cases:

> '**Article 32 — Trans-border access to stored computer data with consent or where publicly available**
> A Party may, without the authorisation of another Party:
>
> a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
>
> b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.'[190]

The situation of publicly available or open-source data under a) is not very relevant for our purposes of cloud investigations, as in those situations (e.g., files in a Dropbox folder of which the URL is published online to facilitate access by the public) the police—just as anyone else—can easily retrieve the data. The law-enforcement problem with cloud data (*supra*, section 3.4.1) lies in situations where the data are not openly available. Thus, the relevant part is the situation under b) where there is voluntary consent of someone authorised to give permission. According to the Explanatory Report, both the person storing data abroad (in many cases, the suspect) and the service provider are authorised to give (voluntary) permission.[191] This means that authorisation from the foreign state is not always necessary; also private parties can give consent for the search.

What is considered 'lawful consent' and 'lawfully authorised' is to be determined by the state seeking access, which does not have to look into the law of the foreign state, since '[i]t is presumed that the Parties to the Convention form a community of trust and that rule of law and human rights principles are respected' (in line with article 15 of the Convention, which refers to, inter alia, the ECHR and the ICCPR).[192] This means that the lawfulness will depend on the national legal framework, which can vary considerably among party states. Moreover, determining the lawfulness of the authority to consent to data disclosure is complicated. One issue is that the Terms and Conditions of cloud contracts can (and often do) allow disclosure to law enforcement, so that the cloud provider can in principle decide to voluntarily cooperate with a law-enforcement request; however, some question whether a generic provision in General Terms and Conditions about disclosure to law enforcement constitutes explicit and informed consent.[193] It is also unclear what the consequences are if consent is revoked—data protection law requiring

[190] Convention on Cybercrime, CETS 185. A similar provision is included in article 40 of the League of Arab States' Arab Convention on Combating Information Technology Offences (available at https://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=3dbe778b-7b3a-4af0-95ce-a8bbd1ecd6dd).

[191] Convention on Cybercrime, CETS 185, *Explanatory Report*, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm, §293.

[192] Cybercrime Convention Committee (T-Cy), 'T-CY Guidance Note # 3. Transborder access to data (Article 32), Draft for discussion by the T-CY' (Strasbourg: Council of Europe, 2013a), at 7.

[193] Micheál O'floinn, 'It wasn't all white light before Prism: Law enforcement practices in gathering data abroad, and proposals for further transnational access at the Council of Europe', *Computer Law & Security Review,* 29 (2013), 610-15 at 612; see also Article 29 Data Protection Working Party, *Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime*, letter to Council of Europe, 5 December 2013, p. 3.

that consent be revocable—after the data have been secured.[194] Another issue is that data protection law only allows transfers of personal data outside of the European Economic Area if the foreign state has an 'adequate level' of data protection.[195] This implies that if the cloud provider (or the relevant data centre) is in an EU state and the state seeking access to data under article 32(b) is a non-EEA state (the Cybercrime Convention has 16 non-EEA parties), the cloud provider may not be able to consent to the data being transferred to the foreign law-enforcement authority, unless a) the access-seeking state is determined to have an adequate level of protection (which, of the Cybercrime Convention party states, applies to Switzerland,[196] b) there is some sort of safe-harbour agreement with the foreign LEA, or c) the transfer is necessary on important public-interest grounds—which is altogether a complicated matter.[197]

To complicate matters further, in addition to data protection law, there may be other legal rules that inhibit disclosure, for example rules protecting trade secrets or national security; Walden mentions, for example, the UK's Protection of Trading Interests Act 1980, which 'was specifically passed to restrain the extraterritorial reach of US regulatory agencies', and the French Loi 80-538 that prohibits 'certain disclosures of information of an "economic, commercial, industrial, financial, or technical" nature for the purposes of foreign legal proceedings.'[198] If such rules apply to particular data, the cloud provider does not have the lawful authority to disclose them.

Perhaps in light of these complications, the 2013 draft Guidance note on article 32 is more wary about private-party consent than the Explanatory Memorandum, observing that '[s]ervice providers are highly unlikely to be able to consent validly and voluntarily to disclosure of their users' data under Article 32' as they normally 'will not control or own the data, and they will, therefore, not be in a position validly to consent.'[199] In practice, most service providers generally seem not to voluntarily give permission to foreign investigating officials to search their servers – they are only willing to co-operate upon receiving a clear legal warrant. And while individuals may also have lawful authority to consent to disclosure, in most cases the persons storing data with a foreign provider will be suspects of a crime, who are unlikely to give permission.

All this makes article 32 of limited relevance in practice. Efforts during the drafting of the Convention to give article 32 a wider scope have failed, however. As the Explanatory Report explains:

> 'The issue of when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance was a question that the drafters of the Convention discussed at length. There was detailed consideration of instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules. Ultimately, the drafters decided to only set forth in Article 32 of the Convention situations in which all agreed that unilateral action is permissible. They agreed not to regulate other situations until such time as further experience has been gathered and further discussions may be held in light thereof. In this regard, Article 39, paragraph 3 provides that other situations are neither authorised, nor precluded.'[200]

Article 32(b) is 'controversial'[201], and perceived quite differently by experts. Cyber-investigation stakeholders tend to consider it a very limited provision, calling it, for example, a 'compromise

[194] Schwerha Iv, 'Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers"', at 12.
[195] Articles 25-26 Directive 1995/46/EC.
[196] See http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.
[197] See Walden, 'Law Enforcement Access to Data in Clouds', at 306-07 for a discussion.
[198] Ibid., at 295.
[199] Cybercrime Convention Committee (T-Cy), 'T-CY Guidance Note # 3. Transborder access to data (Article 32), Draft for discussion by the T-CY', at 7.
[200] Convention on Cybercrime, CETS 185, *Explanatory Report*, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm, §293.
[201] Walden, 'Law Enforcement Access to Data in Clouds', at 296.

without teeth'.[202] Dogmatic legal scholars, on the other hand, consider the provision too far-reaching, as it 'probably contradicts fundamental principles of international law'.[203]

It should be noted that article 32 applies only to situations in which the location of data is known. In situations 'where it is uncertain where the data are located', parties would need to determine the legitimacy of a cross-border search themselves.[204] While some states could allow a 'good faith' exception, if they do not know whether data are located abroad or obtain data from abroad by accident or mistake,[205] Belgium goes a step further in also allowing for the accessing of data known to be abroad in exigent circumstances, i.e., when there is significant risk of evidence being lost. In those cases, the data can be copied and the authorities of the state where the data are located shall be notified, with the caveat that it must be reasonably possible to determine what state is affected (which rarely seems to be the case).[206]

Interestingly, article 32(b) does not provide for notification to the foreign state in cases in which lawful consent was obtained from a private party. A precursor of article 32(b), namely one of the principles on transborder access adopted by the G8 in 1999, provided the following:

> 'a State need not obtain authorization from another State when it is acting in accordance with its national law for the purpose of (…) accessing, searching, copying, or seizing data stored in a computer system located in another State, if acting in accordance with the lawful and voluntary consent of a person who has the lawful authority to disclose to it that data. The searching State should consider notifying the searched State, if such notification is permitted by national law and the data reveals a violation of criminal law or otherwise appears to be of interest to the searched State.'[207]

Although the notification is voluntary, and aims at informing the foreign state only if that state presumably has an interest in the information, it might have been a valuable addition to article 32(b) and can in any case be understood as constituting good practice (one to which the Netherlands adheres). Moreover, 'with slight modifications,' Gercke observes, 'such a provision could ensure that affected states are aware of investigations taking place in their own territory. It would not prevent conflict with international law, but at least guarantee a certain degree of transparency.'[208] In the current regulation, it is entirely at the discretion of the accessed state whether or not it informs the accessed state after it has acquired the data sought.

4.1.2. The practice of transborder searches

In general, due to the difficulties of mutual legal assistance procedures (*supra*, section 2.4.2), practitioners sometimes resort to investigative (e.g., Internet or interception) activities on foreign territory without formal authorisation, although they often consult with local investigation officers in the foreign state.[209] In particular, given the additional challenges of cyber-investigation (*supra*,

---

[202] Koops et al., 'Misdaad en opsporing in de wolken', at 57, quoting a Dutch public prosecutor

[203] Gercke, 'Understanding cybercrime', at 277-78 (arguing that by 'creating Article 32 sub-paragraph b, the drafters of the Convention on Cybercrime ultimately violated the dogmatic structure of the mutual legal assistance regime in this Convention').

[204] Cybercrime Convention Committee (T-Cy), 'T-CY Guidance Note # 3. Transborder access to data (Article 32), Draft for discussion by the T-CY', at 6.

[205] This is the case in Dutch law, see C. Conings and J.J. Oerlemans, 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?', *Computerrecht,* /1 (2013), 23-32. Cf. also a memorandum of some US law enforcement authorities that recommend police officers to obtain a search warrant to directly access records stored with a service provider, using the exigency exception to the search warrant to preserve the records; and then remarking that the law-enforcement officer should be aware of the following: 'WARNING: if the records are stored outside of the United Sates you run the risk of violating a foreign jurisdictions computer crime laws and may be subject to arrest' (quoted in Schwerha Iv, 'Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers"', at 11), thus acknowledging the possibility that direct searches of remotely stored records may occur on foreign territory.

[206] Art. 88ter §1 (2) Belgian Code of Criminal Procedure [Wetboek van Strafvordering]. See Transborder Group, 'Transborder access and jurisdiction: What are the options?, Discussion Paper' (Strasbourg: Council of Europe, 2012), at 32-33.

[207] Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, 'Principles on Transborder Access to Stored Computer Data' (Moscow: G8, 1999).

[208] Gercke, 'Understanding cybercrime', at 278.

[209] Tak, 'Bottlenecks in International Police and Judicial Cooperations in the EU', at 346.

section 3.4.1), cross-border access to data is also frequently obtained in practice without permission from the foreign state, in a variety of circumstances.[210]

In addition to LEAs obtaining data from abroad through service providers (which we discuss *infra*, section 4.1.4), they may also use cross-border network searches. It is unknown how often the police engage in unilateral cross-border searches without permission from the foreign state, but a few cases have been published. The best-known example is the Gorshkov and Ivanov case, in which US law enforcement officers enticed two Russian hackers to come to the US for a (fake) job interview to demonstrate their skills; the FBI officers secretly recorded the hackers' passwords and used these to access their computers in Russia and download evidence. Gorshkov and Ivanov were arrested and convicted on the basis of this evidence.[211] Among the arguments why the evidence was admissible[212] were the court's assessment that the Fourth Amendment (which protects against unreasonable search and seizure) does not protect the rights of individuals abroad in the case of US access to extraterritorial computers, while Gorshkov's presence in the US (considered to be for criminal purposes) was insufficient to establish a minimum contact with the US; also, the Fourth Amendment allows access to a computer and securing data if vulnerable evidence is in danger of being destroyed or altered.[213] (Russia subsequently charged the FBI officers with hacking into Russian computers, but the FBI officers were never extradited.) This mode of criminal investigation seems an exception and not a regular practice in the US—not many opinions cite the Gorshkov/Ivanov cases as a proposition for transborder searches, while the American Bar Association discourages it in the International Guide to Combating Cybercrime: the Gorshkov case 'does not provide a sound basis for transborder searches and seizures because it would inevitably allow one state to transgress upon another state's sovereignty by searching and seizing property belonging to that second state's citizens, property that is physically located within that second state's territory.'[214]

Two Dutch cases of transborder access to data are the Bredolab case, in which Dutch law enforcement sent a message to all infected computers of a botnet (warning them of the infection), and the Descartes case in which Dutch law enforcement removed child pornography from a hidden TOR server that was probably located in the US.[215] In the latter operation, the law-enforcement officers had considered the possibility that the hidden server was located in the US, and they had informed US authorities of the pending operation. When the officers encountered a large amount of child sexual abuse images that appeared to have been newly made (indicating that the server was close to the source of on-going child abuse), they decided to remove the files themselves instead of using a mutual-legal assistance request, given the exigent circumstances. They notified the US authorities afterwards, which did not object to the operation.[216]

4.1.3. The debate about transborder searches

In Autumn 2004, Nicolai Seitz published an article discussing the legitimacy of cross-border searches. He concluded that non-consensual cross-border searches violate international law, *except* where states search US-located computers under exceptional circumstances. The reason he gives for the exception is that the US – as witnessed by the Gorshkov/Ivanov cases and the Department of Justice's digital investigation manual – apparently considers cross-border searches to be acceptable under international law in exigent circumstances.[217] At the same time, Seitz claimed that the consensual cross-border search, as stipulated in article 32(b) Cybercrime Convention, could now be considered a rule of international customary law, since no caveats

[210] See Transborder Group, 'Transborder access and jurisdiction: What are the options?, Discussion Paper', at 32-43 for a discussion of many countries' laws and practices.
[211] See N. Seitz, 'Transborder search: A new perspective in law enforcement?', *International Journal of Communications Law & Policy,* 9/2 (2004) and Schwerha Iv, 'Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers"', at 14-17 for a case description.
[212] See Schwerha Iv, 'Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers"', at 14-17 for an overview.
[213] Ibid.
[214] As quoted in ibid., at 17.
[215] See Transborder Group, 'Transborder access and jurisdiction: What are the options?, Discussion Paper', at 35 for a brief description.
[216] Koops et al., 'Misdaad en opsporing in de wolken', at 46.
[217] Seitz, 'Transborder search: A new perspective in law enforcement?'.

regarding the provision had been expressed by non-signatory states.[218] Soon after publication of this paper, however, Russia voiced its disagreement with article 32(b), arguing that the provision is contrary to international law and constituted a major obstacle to Russian adoption of the Convention.[219] Slovakia too, although it has ratified the Convention, does not accept the consent of a private party for accessing transborder data and considers the 'approval of a competent judicial authority of the Party where the computer data are located (…) necessary in all cases'.[220]

While Russia and Slovakia consider article 32(b) too far-reaching, several parties to the Cybercrime Convention consider the provision on transborder access too limited. In late 2011, the Cybercrime Convention Committee established an 'ad-hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows' (the 'Transborder Group'). Its task is to 'develop an instrument – such as an amendment to the Convention, a Protocol or Recommendation – to further regulate the transborder access to data and data flows, as well as the use of transborder investigative measures on the Internet and related issues.'[221] In December 2012, the group's mandate was extended so that they could prepare a first draft text of a possible Protocol to the Cybercrime Convention.[222]

The Transborder Group observes that the need for solutions to transborder access to data has become more pressing, as 'criminal justice authorities appear to be less and less able to meet their positive obligations to protect people against crime. This further weakens the rule of law in cyberspace.'[223] It has proposed a number of possible solutions that might be considered for a Protocol:

1. 'Transborder access with consent but without the limitation to data stored "in another Party" (...).
2. Transborder access without consent but with lawfully obtained credentials (...).
3. Transborder access without consent in good faith or in exigent or other circumstances (...).
4. Extending a search [from the original computer being searched to connected systems] without the limitation "in its territory" in Article 19 [paragraph 2] (...).
5. The power of disposal as connecting legal factor.'[224]

The latter option would entail that 'if the location of the data is not known, but the person having the power of disposal of the data is physically on the territory of, or a national of the searching Party, the LEA of this Party may be able [to] search or otherwise access the data.'[225]

In June 2013, the Cybercrime Convention Committee adopted terms of reference for a draft 2nd Additional Protocol[226] on Transborder Access to Data, with a mandate until end of 2015.[227] As

[218] Ibid., s. II(B)(3).

[219] Cf. Cybercrime Convention Committee (T-Cy), 'Compilation of responses to questionnaire for the parties concerning the practical implementation of the Cybercrime Convention' (Strasbourg: Council of Europe, 2008), at 28: 'Russia proceeds from the assumption that, in her opinion, the current wording of Article 32.b. of the Convention (…) can damage the state sovereignty and national security of the member-states, as well as rights and legal interests of their citizens and entities. The Russian Federation will make decision on her participation or non-participation in the Convention, considering also possible review of provisions of Article 32.b. (…) The Ministry of the Interior of the Russian Federation believes that Article 32.b. contradicts internationally recognized norms of respect of sovereignty and human rights fixed in many international documents. It is advisable to ask for the member-states' opinion on that matter. We propose to make amendments to the text of the Convention that will be in line with common practice and modern requirements.'

[220] Committee of Experts on the Operation of European Conventions on Co-Operation in Criminal Matters (Pc-Oc), 'Summary of the replies to the questionnaire on Mutual Legal Assistance in Computer-Related Cases' (Strasbourg: Council of Europe, 2009), at 6.

[221] Transborder Group, 'Transborder access and jurisdiction: What are the options?, Discussion Paper', at 4.

[222] Cybercrime Convention Committee (T-Cy), '(Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding transborder access to data' (Strasbourg: Council of Europe, 2013b), at 3.

[223] Transborder Group, 'Report of the Transborder Group for 2013' (Strasbourg: Council of Europe, 2013), at 7.

[224] Cybercrime Convention Committee (T-Cy), '(Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding transborder access to data'. See O'floinn, 'It wasn't all white light before Prism: Law enforcement practices in gathering data abroad, and proposals for further transnational access at the Council of Europe', at 613-14, for a critical discussion of these options.

[225] Cybercrime Convention Committee (T-Cy), '(Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding transborder access to data', at 6.

[226] The first Additional Protocol, CETS 189, concerns criminalisation of racist and xenophobic acts committed through computer systems.

the Committee observed, the 'fact that LEA of many States are already engaged in transborder access to data beyond the scope of the Budapest Convention on an uncertain legal basis, with risks to the procedural and privacy rights of individuals, and with concerns regarding national sovereignty would justify the difficult process of negotiating a binding international legal instrument.'[228] However, although the Transborder Group documents emphasise the need for appropriate safeguards, the fact that the Transborder Group consists 'almost without exception [of] members [who] are either current or previous criminal prosecutors or investigators' has raised questions on the balance in the proposals between law enforcement needs and protection of fundamental rights.[229]

Discussions in the Transborder Group about a draft Protocol are on-going.

4.1.4. Directly contacting foreign providers

Although article 32(b) Cybercrime Convention (somewhat implicitly) allows law-enforcement authorities to directly contact foreign service providers to request the delivery of data (see *supra*, 4.1.1), this is not a type of transborder access to data that is generally encouraged or accepted in international law or policy. This element of article 32(b) has been criticised by Gercke:

> 'By creating Article 32 sub-paragraph b, the drafters of the Convention on Cybercrime ultimately violated the dogmatic structure of the mutual legal assistance regime in this Convention. With Article 18, the drafters of the Convention on Cybercrime enabled investigators to order the submission of data in domestic investigations. If law-enforcement agencies were to be authorized to use this instrument in international investigations, it would have been sufficient to include it in the catalogue of instruments mentioned in the context of mutual legal assistance. However, the instrument cannot be applied in international investigations because the corresponding provision in Chapter 3 of the Convention on Cybercrime, dealing with international cooperation, is lacking. Instead of relinquishing the dogmatic structure by allowing foreign investigators to contact directly the person who has control over the data and ask for the submission of the data, the drafters could have simply implemented a corresponding provision in Chapter 3 of the Convention.'[230]

Indeed, the 2008 Council of Europe itself, in their guidelines for the cooperation between LEAs and service providers, discourages direct contacts: 'For requests addressed to non-domestic Internet service providers, domestic law enforcement authorities should be encouraged not to direct requests directly to non-domestic Internet service providers but make use of procedures as described in international treaties (...).'[231] In a similar vein, the Article 29 Working Party advocates the introduction in data protection law of a provision on 'the obligatory use of Mutual Legal Assistance Treaties (MLATs) in case of disclosures not authorised by Union or Member States law', in order to prevent that cloud service providers would directly provide data to non-EU-based LEAs without an explicit treaty basis or authorisation from a European supervisory authority.[232]

Thus, directly contacting foreign providers is a contested practice: 'many Parties would object – and some even consider it a criminal offence – if a person who is physically in their territory is directly approached by foreign law enforcement authorities who seek his or her cooperation.'[233] Nevertheless, apparently 'LEAs routinely request and are provided with data from foreign service

---

[227] Cybercrime Convention Committee (T-Cy), 'Cybercrime Convention Committee (T-CY) 9th Plenary, Strasbourg, 4-5 June 2013. Abridged meeting report' (Strasbourg: Council of Europe, 2013c),, Appendix 3.3.

[228] Transborder Group, 'Transborder access and jurisdiction: What are the options?, Discussion Paper', at 59. The need to develop 'common standards and safeguards concerning the circumstances, if any, under which direct access to extraterritorial data may be conducted by law enforcement' is also recognised by the United Nations, see United Nations Office on Drugs and Crime (Unodc), 'Comprehensive Study on Cybercrime, Draft' (New York: United Nations, 2013), at 216.

[229] O'floinn, 'It wasn't all white light before Prism: Law enforcement practices in gathering data abroad, and proposals for further transnational access at the Council of Europe', at 614.

[230] Gercke, 'Understanding cybercrime', at 278.

[231] Council of Europe, 'Guidelines for the cooperation between law enforcement and internet service providers against cybercrime, adopted by the global Conference Cooperation against Cybercrime, 1-2 April 2008' (Strasbourg: Council of Europe, 2008), at 5-6, guideline 36.

[232] Article 29 Working Party, 'Opinion 05/2012 on Cloud Computing' (Brussels: Article 29 Data Protection Working Party, 2012), at 23.

[233] T-CY 2013a, p. 8.

providers, without formal inter-State process such as mutual legal assistance'.[234] Part of these may be on a voluntary basis (in line with article 32(b) Cybercrime Convention), but some also involve the serving of court orders directly on foreign providers. Not many instances of this are published and the situation may perhaps not occur frequently in practice,[235] but two cases illustrate the possible complications arising from such practices.

A typical case is the Belgian Yahoo! case, in which Belgian law enforcement directly served an order on US-based Yahoo! to disclose webmail data of a Belgian user, which Yahoo! refused claiming that Belgium should use the formal MLAT route. The case has ping-ponged back and forth between the Supreme Court and three (!) Courts of Appeal, both on the issue of the definition of an electronic communications provider (which we leave aside here) and the jurisdiction issue. In November 2013, the Court of Appeal Antwerp decided that Yahoo! should comply with the order as it offers its webmail services also in Belgium; the fact that it does not have an office or residence in Belgium was not considered relevant.[236] This is compatible with the earlier judgement of the Belgian Supreme Court (Hof van Cassatie), which claimed that the fact that the order was sent from Belgium to an address abroad did not make the order unlawful (although the Supreme Court seemed to leave open the question of whether the order was legally binding[237]—a question that the Court of Appeal now has answered affirmatively).[238] The argumentation for this decision has been criticised, however, as arguments relating to substantive jurisdiction seem to have been confused with arguments relating to procedural jurisdiction. According to De Schepper and Verbruggen, Yahoo!'s place of residence was not relevant for the decision as to whether a material obligation existed for Yahoo! to cooperate with an order to provide data (in relation to the *substantive* question of whether Yahoo!'s refusal violated the Belgian provision on not cooperating with a lawful order—the order was lawful, as Yahoo! provided services in Belgium and could therefore be addressed to provide relevant data in Belgian proceedings);[239] however, the place of residence *is* relevant for the decision *how* the order can be served on Yahoo! (in relation to the procedural question of how compliance by Yahoo! with an order can be enforced). De Schepper and Verbruggen conclude that a company residing abroad can only be approached with a court order via the way of mutual legal assistance, not directly.[240]

A second interesting case is the Rackspace case, in which Italian law enforcement ordered, through an MLAT procedure, the US-based hosting and cloud company Rackspace to produce data concerning Indymedia, a media organisation. Relevant for our purposes here is that the requested files were not stored in the US but in the UK, and pursuant to the order Rackspace shut down the entire host server in the UK and delivered the drives to the FBI (claiming that the time-frame for complying with the order was too limited to find and select the requested files, and opting instead to provide the whole server drives instead).[241] UK authorities were not involved in the process at all, implying that the legality of this action under English law was not considered, which according to Walden illustrates that 'even a lawfully obtained and served order can still result in potential unlawfully obtained material'.[242] Although such extraterritorial effects of lawfully

---

[234] O'Floinn, 'It wasn't all white light before Prism: Law enforcement practices in gathering data abroad, and proposals for further transnational access at the Council of Europe', at 611.

[235] Cf. Vodafone's *Law Enforcement Disclosure Report*, Vodafone Group Plc, 'Sustainability Report 2013/14' (Newbury, Berkshire: Vodafone, 2014), at 66, which states 'that we *have not, in fact, received any such cross-border demands*. Were we ever to receive such a demand, in providing our refusal in response, we would inform the agency or authority that they should consider any mutual legal assistance treaty (MLAT) processes to seek the cooperation of the relevant domestic agency or authority with the necessary lawful mandate', emphasis added).

[236] Court of Appeal Antwerp 20 November 2013, *Openbaar Ministerie v. Yahoo! Inc.*, §4.4.1.

[237] Kristel De Schepper and Frank Verbruggen, 'Ontsnappen *space invaders* aan onze *pacmannen*? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners', *Tijdschrift voor Strafrecht,* /2 (2013), 143-66 at 147.

[238] Belgian Supreme Court [Hof van Cassatie] 4 September 2012, *Procureur-Generaal bij het Hof van Beroep te Brussel v. Yahoo! Inc*.

[239] De Schepper and Verbruggen, 'Ontsnappen *space invaders* aan onze *pacmannen*? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners', at 160.

[240] Ibid., at 161.

[241] Walden, 'Law Enforcement Access to Data in Clouds', at 298.

[242] Ibid.

given orders are considered by some as a potential infringement of sovereignty of the state on whose territory the data are stored (unless that state has indicated approval),[243] others consider it an acceptable practice that providers can give data stored in another state but under their control to law-enforcement authorities without resorting to MLAT or seeking approval from the foreign state.[244] Indeed, article 18 Cybercrime Convention stipulates that LEAs can give orders to persons (including providers) in their territory to submit data 'in that person's possession *or control*' (emphasis added),[245] which the Explanatory Memorandum explains as follows:

> 'The term "possession or control" refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely *control production* of the data *from within the ordering Party's territory* (for example, subject to applicable privileges, a person who is served with a production order for information stored in his or her account by means of a remote online storage service, must produce such information). At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision'[246]

In other words, the person addressed with a production order needs to produce data over which she has the control from within the territory, i.e., the *activity of (lawful) control* needs to be in the territory of the state requesting the data (whether or not on the basis of an MLAT); the data themselves do not necessarily have to be within the territory itself. This position has also been taken in a US case in which a US warrant was issued to Microsoft to produce the contents of a certain email account, which was hosted overseas in Ireland. Microsoft contended that it did not have to comply with the order since the data were stored overseas, but this was rejected by the court.[247] On appeal, which is pending as of August 2014, the government defended this position as follows: 'Overseas records must be disclosed domestically when a valid subpoena, order, or warrant compels their production. The disclosure of records under such circumstances has never been considered tantamount to a physical search under Fourth Amendment principles, and Microsoft is mistaken to argue that the SCA [Stored Communications Act, BJK/MG] provides for an overseas search here. As there is no overseas search or seizure, Microsoft's reliance on principles of extraterritoriality and comity falls wide of the mark.'[248] This interpretation seems to be in line with article 18 CCC as explained in the Explanatory Memorandum, provided that the service provider has lawful authority, through its General Terms & Conditions, to access the contents of the account.

Although this is a different situation than the case of directly contacting a provider residing abroad, the argument—although not uncontested[249]—that providers can retrieve data stored abroad under their control without infringing the other state's sovereignty can be relevant to include in an assessment of the acceptability of transborder access to data under international law.

---

[243] Transborder Group, 'Transborder access and jurisdiction: What are the options?, Discussion Paper', at 10, referring to Ulrich Sieber (2012), 'Straftaten und Strafverfolgung im Internet', Gutachten C zum 69. Deutschen Juristentag. München, p. C147/148.

[244] De Schepper and Verbruggen, 'Ontsnappen *space invaders* aan onze *pacmannen*? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners', at 161.

[245] Ibid.

[246] Convention on Cybercrime, CETS 185, *Explanatory Report*, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm, §173 (emphasis added).

[247] *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, __ F. Supp. 2d. __, No. 13 Mag. 2814, 2014 WL 1661004.

[248] Government's brief in support of the magistrate judge's decision to uphold a warrant ordering Microsoft to disclose records within its custody and control, *In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation*, 13 Mag. 2814, M9-150.

[249] De Schepper and Verbruggen, 'Ontsnappen *space invaders* aan onze *pacmannen*? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners', at 162.

4.2. Possibilities under international law–the strict interpretation

4.2.1. International law as it is

In their relations with one another, states remain wedded to the notion of exclusive territoriality and thus defend jealously their rights as territorial sovereigns, particularly in the sphere of crime control. This approach is clearly in evidence in relation to the regulation of cyberspace; despite the difficulties of doing so and the clear benefits with regard to regulatory efficiency to thinking more broadly about regulatory solutions, states have been keen to assert jurisdiction within cyberspace based upon territorial claims. The Cybercrime Convention facilitates co-operation between states in the combating of cybercrime but always within the frame of territorial sovereignty; for example, Art. 32(b) allows for transborder access to data with the consent of the provider, where that consent can be lawfully given, i.e., where the state in which the provider is domiciled allows for such consent through its legal regime.[250] Data are thus legally understood as being stored somewhere on the earth, whether or not that somewhere can be reliably identified at the moment at which access is sought. That 'somewhere' provides the ordinary jurisdiction.[251]

International law is a permissive system with the activities of states limited only by their obligation to respect the rights of other states. The obligation to respect the territorial integrity of fellow states is fundamental to the workings of the international order. As such, a non-territorially-based claim to jurisdiction – such as passive personality, based on the nationality of the victim, or nationality, based upon the nationality of the suspect – does not allow a state to breach the territorial integrity of another state in order to enforce its claim: jurisdiction to prescribe or legislate does not entail jurisdiction to enforce. Thus the most solid view on what international law permits is that accessing data that are, or later turn out to be, stored on a server located in the territory of another state constitutes a breach of the territorial integrity of that state and thus constitutes a wrongful act (where the action is attributable to the state[252]), except where sovereign consent has formally been given.[253] The US Third Restatement of Foreign Relations Law states: 'It is universally recognized, as a corollary of state sovereignty, that officials in one state may not exercise their functions in the territory of another state without the latter's consent.' It further notes that one state's law enforcement officials 'can engage in criminal investigation in a state only with that state's consent.'[254] Any evidence-gathering activity in a foreign state, also without officers being physically present, can be considered a breach of sovereignty, including making a phone call or sending a letter to a foreign state.[255]

It is worth noting here the strength of feeling among the international lawyers present in the workshop organised for this project as to the sensitivity of states to a breach of territorial integrity for the purpose of criminal law or security investigations. This feeling is based upon the dual observation that a state's first responsibility is traditionally understood to be ensuring public order and the fact that the enforcement of criminal law is explicitly connected to the coercive power of the state, i.e., its monopoly of violence that is the marker of its internal claim to sovereignty.

What this means in theory is that the inability of one state to determine the location of data at the moment of access does not mitigate the wrong caused to the affected state of a breach of

---

[250] As Guy de Val, Director-General for Legal Affairs for the Council of Europe, noted, the Convention 'does not provide for actual cross-border investigations, nor cross-border searches, "because the states which negotiated the draft were unable to agree on that point."' See Europe Information Service, 'Cybercrime: Community Accession to an International Convention', *European Report* (Mar 21, 2001). Cited in Goldsmith 2001, 107.

[251] Unless the provider is required to supply data that is stored abroad by the legal order where it is domiciled, such as in the Microsoft case (see section 4.1.4 above).

[252] For an action to constitute an international wrong, the action must be attributable to a state (Articles on State Responsibility, 53 UN GAOR Supp. (No. 10) at 43, U.N. Doc. A/56/83 (2001)).

[253] Consent is likely to take one of three forms: a) consent via a MLAT request in a particular instance; b) a state will legislate at the domestic level to allow service providers located within its jurisdiction to comply with requests for data from foreign LEAs; c) a state will commit itself to allowing such searches in the form of a treaty, such as article 32(b) of the Cybercrime Convention.

[254] US Third Restatement, § 432 comment b (1987).

[255] United States Attorneys' Manual, Title 9, §267, available at http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00267.htm; Tak, 'Bottlenecks in International Police and Judicial Cooperations in the EU', at 346; De Schepper and Verbruggen, 'Ontsnappen *space invaders* aan onze *pacmannen*? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners', at 158.

territorial integrity (in section 4.3 we consider how such actions might be mitigated in practice or understood from a less formal perspective). Nor does the consent of the user or the provider to access data located on the territory of another state constitute the consent of the sovereign, unless the state has otherwise also consented, as is the case with Article 32(b) of the Cybercrime Convention. Non-state actors cannot provide consent to the commission of an international wrong against another state and the proper view is that permission would still need to be sought from the state affected. Only the consent of the relevant sovereign – tacit or explicit – can prevent the accessing of data lodged outside one's own territory from constituting an international wrong and thus a breach of international law. This consent can also, in practice, be retrospective, i.e., while an international wrong is committed in theory by a search without consent, where the 'injured state' is notified after the fact and does not perceive itself as injured, the matter ends (see the Descartes case example in section 4.1.2).

Failure to obtain consent from the affected state (whether ex ante or ex post), as an international wrong, thus has consequences. The affected state is entitled to demand an apology, including an admission of wrong-doing and a commitment to desist from such behaviour in the future (cessation and non-repetition), and full restitution i.e. the situation must be restored to that before the wrong was committed. Where this is impossible or impractical, financial compensation takes its place. Breaching international law can be an expensive affair. In addition, failure to desist entitles other states to take countermeasures.[256] Countermeasures are actions that wronged states can lawfully take to ensure that obligations owed them are fulfilled. Obligations within international law are, with one or two exceptions, reciprocal. The first step in lawful countermeasures is that a wronged state will not fulfil their obligation owed the state that is committing the wrong and which refuses to cease its wrongful action; in short, where one state wrongs another by acting to access cross-border data and refuses to desist, other states will have no obligation towards that state to respect their territorial integrity with regard to data access. This situation will continue until the state that committed the wrong agrees to cease their wrongful action, agrees not to repeat it, apologizes and offers some form of reparation. Lawful countermeasures are by no means limitless and are designed so as not to aggravate conflict between states; the most important limitation is proportionality – any countermeasure taken must be proportional to the wrong committed. However, a state that commits a wrongful act may find that it is faced with illegal countermeasures by the wronged state that feels that its dignity has been affected. Such measures are rarely proportional to the original wrong committed and may strike at an interest dear to the state committing the wrong or dear to its citizens. For example, a state that acts illegally to access cross-border data i.e. without the consent of the affected state, may have a ship under its flay stopped on the high seas by the wronged state and its citizens taken into custody; or it may find that a contract to provide an essential service, such as gas, is broken; or that its products are boycotted. Acting in breach of international law, and persisting in that breach, is rarely without consequences of some kind.

4.2.2. What exceptions are allowed to states under international law?

International law provides a number of exceptions to the strict requirement of state consent laid out above. These are known as circumstances precluding wrongfulness. They are, however, strictly limited in their application and unlikely to be of relevance except in the most extreme of circumstances. Such exceptions or circumstances precluding wrongfulness in the context of cross-border data searches are the consent of the affected state (considered above); self-defence; where such action constitutes a counter-measure; force majeure and distress.[257]

Self-defence may allow a state to access data located abroad without consent in the context of a cybercrime attack, where the threat posed by such an attack is imminent and overwhelming.[258] This does not apply to situations of criminal investigation by LEAs.

A counter-measure is action taken by a state in response to the commission of an international wrong by another state. The accessing of data on the territory of another state without consent

[256] Articles on State Responsibility, 53 UN GAOR Supp. (No. 10) at 43, U.N. Doc. A/56/83 (2001), Articles 49-53.
[257] Ibid., Articles 20-24 respectively.
[258] The customary international law standard is, in full, 'a necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment of deliberation [and involving] nothing unreasonable or excessive' (Caroline case, 1851).

could thus only preclude wrongfulness if it were done in response to the same actions of another state, and where it was done openly and solely with the intention of ensuring the compliance of the breaching state with the rules on territorial integrity. This exception is thus not of assistance in the regular pursuit of criminal investigation.

Force majeure – a situation of sudden and unanticipated intensity, such as an earthquake, tsunami or landslide of such severity that, for example, alters the course of a river – provides an exception because it renders a state unable to fulfil its obligations. However, the strict limitation of its application ensures its irrelevance in the present context.

The final exception is distress, where a state has a choice about its actions but where one option entails sacrifice; this again is strictly interpreted and generally concerns a situation in which lives are immediately threatened. Action taken in that moment of extreme distress with the intention of saving lives precludes wrongfulness. Classic examples include an aircraft in distress that lands on the territory of a state without permission; or emergency vehicles crossing an international border to attend the scene of a disaster in order to administer life-saving treatment, where consent is sought retrospectively. It is possible to imagine a scenario in which access to data stored in the cloud could meet such conditions, where the situation was urgent and solely related to the saving of lives (kidnappings or terrorist attacks are the most obvious examples). This, however, will not be the case in the regular pursuit of criminal investigations.

In sum, the consent of states, however so agreed, is the only real option for precluding wrongfulness in ordinary cross-border criminal investigations.

4.2.3. An exception allowed under article 32(b) Cybercrime Convention: lawfully obtained credentials?

With article 32, member states of the Cybercrime Convention have given their consent to certain forms of cross-border access to data: either accessing publicly available data or accessing data with lawful consent of someone authorised to give consent (see *supra*, section 4.1.1). The consent of the user or provider is best conceptualised here as a trigger that activates the prior consent of the sovereign state. It is not the user's consent that renders the action legal under international law, but that of the state. Without this prior consent given through the convention, the act of a cross-border data search would constitute an international wrong even with the user's consent.

What interests us here is the question of what state parties to the Convention have consented to under article 32(b). Let us assume that a LEA of state A has reason to believe that relevant data are stored in state B, where both countries are party to the Cybercrime Convention. Since the Explanatory Memorandum includes the service provider as a possible candidate for giving lawful and voluntary consent, article 32(b) implicitly allows the LEA to directly approach the service provider in state B to ask for the data. To read the article otherwise would be nonsensical as it would otherwise not be possible for the LEA to obtain consent from the provider. It makes no sense to expect the provider to give consent to the foreign LEA without being asked to do so, and if the asking would have to be done via traditional mutual legal assistance, the service provider would not have been included in the Explanatory Memorandum as capable of giving consent. It is crucial to note, however, that the request can only be on a voluntary basis–legal orders or threats of sanctions are out of the question—and the provider should have lawful authority to provide the data, which will not ordinarily be the case (*supra*, section 4.1.1).

The other option allowed for by article 32(b) is to have consent of the user. This will usually be the suspect, who is unlikely to give voluntary permission (except in cases where only non-incriminating and possibly exculpatory data are stored abroad), although it may also be in certain cases a third party who is not under suspicion and who has relevant data about the suspect.

While both options seem to have limited value in practice—with the service provider often being unable or unwilling, and the user presumably being usually unwilling, to give voluntary consent—there may be scope for a wider reading of what article 32(b) allows. One of the options discussed by the Transborder Group is transborder access to data without consent but with lawfully obtained credentials (see *supra*, section 4.1.3). Credentials refer to the login data to an account (typically user name and password), and a LEA could have lawfully obtained these by finding them for example during a (lawful) search on a post-it note on the suspect's screen or in his notebook.

An argument can be constructed by which article 32(b) already allows cross-border access to data with lawfully obtained credentials (for state parties to the Convention). This argument builds

on the technical and metaphorical conceptualisation of a cross-border search. As we outlined in section 3.5.1, a transborder search by the LEA from state A using lawfully obtained credentials technically amounts to sending a request to the server in state B, to which the server responds in the way it has been programmed to respond—it does not affect the normal or intended functioning of the computer. Metaphorically, it amounts to sending a message to the service provider in state B requesting data (such as mails in a webmail account). Such a request is lawful under international law for state parties to the Cybercrime Convention, since they have given prior consent for this type of action. Moreover, if the server sends back the requested data, as it was programmed to do upon a request with the right credentials, this can be construed as voluntary and lawful consent by the service provider to give access to the data. There is voluntary consent because correct credentials are used and the server is not compelled to do what is was not intended to do; and the consent is lawful because the server is allowed, under the terms and conditions that regulate the provider-user relationship, to send data when it is approached with the right credentials. Although the service provider does not consciously and specifically give consent in this situation, by programming the server to respond in a certain way—sending data when approached with a request using the right credentials—it has implicitly given prior and generic consent for this type of cross-border access to data. The fact that no coercion is involved makes the consent by the service provider voluntary (the server is not in any way compelled to do anything it was not programmed to do), and the fact that the server sends data in response to a request with correct credentials ensures that the service provider has the lawful authority to disclose the data and makes the consent by the service provider lawful (in terms of private law). Thus, all elements of article 32(b)—' if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system'—have been met. The fact that state B has given prior consent, through the Cybercrime Convention, for its service providers to give access to data in this way thus makes the action lawful under international law.

This argument implies that article 32(b) already includes a possibility of cross-border searches with lawfully obtained credentials (if the LEA from state A knows that the data are in state B and that B has ratified the Convention). Since it is—to our knowledge—a new interpretation of article 32(b), it is unlikely that this reading is what the drafters of the Convention explicitly intended. At the same time, it is not ruled out that this reading may be acceptable to state parties, since it is compatible with both the letter (with the service provider consenting through the way it has programmed the server's functioning) and the spirit of article 32(b): as signatory states consider it acceptable that private parties such as service providers give data to foreign LEAs without case-by-case prior state consent, it should also be acceptable to them if entities to which the private parties have delegated consent-giving—namely, their servers—give data to foreign LEAs without case-by-case prior state consent.

Such an interpretation would need to be the subject of explicit discussion among the parties to the Cybercrime Convention before it can be accepted as a legitimate interpretation of article 32(b). However, a considerable advantage over an additional protocol is that a new interpretation of article 32(b) does not need to go through a cumbersome ratification procedure in all signatory states, but can be agreed upon by adapting the Guidance Note to article 32,[259] which is a considerably easier process.

4.2.4. Interim conclusion

In the strict—and dominant—interpretation of international law, any evidence-gathering activity in a foreign state, including the making of a mere phone call, can be considered a breach of sovereignty. Accessing data that are, or later turns out to be, stored on a server located in the territory of another state, without prior consent of that state, constitutes a breach of the territorial integrity of that state and thus a wrongful act. The fact that the searching state may have difficulty in determining the location of data at the moment of access does not mitigate the wrong of a breach of territorial integrity, nor does the consent of the user or the provider to access the data preclude wrongfulness. Exceptions such as self-defence, force majeure, and distress are not applicable in this context; only the latter might potentially apply in extreme circumstances, but not

[259] Cybercrime Convention Committee (T-Cy), 'T-CY Guidance Note # 3. Transborder access to data (Article 32), Draft for discussion by the T-CY'.

in the regular pursuit of criminal investigations. The only exception is where the foreign state has given prior consent, either for a specific search upon a specific request, or in a generic form for certain types of searches under certain conditions; the latter is the case with Article 32(b) of the Cybercrime Convention, which allows cross-border access to data with consent of the user or provider, if both countries are parties to the Convention.

Article 32(b) can also be interpreted as including the possibility of cross-border searches with lawfully obtained credentials, if the LEA from state A knows that the data are in state B and that B has ratified the Convention, but this interpretation needs to be agreed among the Cybercrime Convention member states before it can be accepted as a legitimate interpretation. Although the reading we suggest here does provide one way of opening the discussion about cross-border access to data, it should be pointed out that it provides only a limited exception to the general status of cross-border access to data under international law: it applies only to states that are party to the Cybercrime Convention; it applies only if the LEA knows, or has good reason to believe, that the data are stored on the territory of another signatory state; and it applies only to the form of access to data with lawfully obtained credentials, and not to other forms of cross-border searches (without consent of the user of provider). Therefore, the possibilities of international law for cross-border access to data without prior consent of the foreign state are, in the strict interpretation of international law, overall very limited.

4.3. Possibilities under international law—broadening the perspective

4.3.1. Introduction

While the law in relation to cross-border data searches within international law is in the process of development, the strict legal approach is one that is respectful of state sovereignty in the form of territorial integrity. Such an approach severely limits the possibility for unilateral state action in this area. However, it is possible to think beyond such a legal technical approach. What the strict analysis of international law presumes is that it is possible to state with certainty whether an action is legal or illegal. A critical approach to international law, as espoused by David Kennedy and Martti Koskenniemi among others,[260] is that international law is permanently caught in the need to compromise between the positivist (i.e., that law is the outcome of an authoritative process, regardless of its content) and naturalist (i.e., that law is only law if it is both made in the right (authoritative) process *and* speaks to some broader goal of the international order, such as justice or fairness) traditions of law. What this means is that international law has to make a claim to being something more than simply state interests – otherwise it is just brute power; yet at the same time it needs to reflect the actual practice of states – otherwise it is just wishful thinking. As a consequence, arguments made from a positivist position are vulnerable to a naturalist critique and vice versa. The result is that the rules of international law are indeterminate as soon as one attempts to apply them and thus it is impossible to give a 'right answer' to any legal question.[261] Critical scholars therefore have suggested that international law is a practice of argumentation by international lawyers, where the better question is not whether an action is legal or illegal but whether it can be legally justified.[262] Accepting this as the question entails moving away from the binary illegal/legal distinction to a sliding scale on which behaviour can be less or more justifiable

[260] M. Koskenniemi, *From Apology to Utopia: The Structure of International Legal Argument* (2nd Edition edn.; Cambridge: Cambridge University Press, 2005); D. Kennedy, *International Legal Structures* (Baden-Baden: Nomos, 1987).

[261] A good example is the question of the legality of nuclear weapons: where a naturalist perspective would argue that it is impossible to conceive of a situation in which the use of nuclear weapons would be legal, the positivist would respond that there is no explicit rule banning nuclear weapons. Both perspectives are good legal arguments and the question of the legality of nuclear weapons is thus indeterminate. This is more or less the opinion reached by the ICJ in its 1996 Advisory Opinion on Nuclear Weapons. *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, [1996] ICJ Reports, 226.

[262] Klabbers, *International Law* , 20; also H. Lauterpacht, *The Function of the Law in the International Community* (Oxford: Oxford University Press, 2011 [1933]).

in legal terms.[263] If we take this as our approach to international law, what happens to the question of cross-border data searches?

Cloud computing and the loss of knowledge of location conundrum pose a significant problem for international law. The centrality of territory as an organising principle hinders an appropriate response to the threat posed to state interests by data stored in the cloud; this is a problem for all states.[264] Moreover, it is helpful at this point to recall the justification for exclusive territorial sovereignty: the demonstration of effective control over a defined area does not only create rights for a state; rather the right to rule has, in the less oft-cited words of Arbitrator Huber in the *Island of Palmas* case, 'as a corollary a duty'.[265] Huber further noted that, '[t]erritorial sovereignty cannot limit itself to its negative side, i.e. to excluding the activities of other States; for it serves to divide between nations the space upon which human activities are employed, in order to assure them at all points the minimum of protection of which international law is the guardian.' The International Court of Justice (ICJ) has defined this duty in the *Corfu Channel* case, in the context of assigning state responsibility for wrongful acts, as 'every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.'[266] While this duty has not been extended beyond the understanding given it by the ICJ in the *Corfu Channel* case, this case and Huber's words serve to remind us of the original justification of territorial sovereignty under international law: the capacity to act. As Klabbers has recently noted, 'unless a state accepts responsibility for things happening in its territory, that very title to territory becomes difficult to justify.'[267]

A state cannot accept responsibility for data that are temporarily located on its territory where it cannot even know that the data are located there, any more than it can be held accountable for its territory being (temporarily) used to affect negatively the interests of other states.[268] This inability of states to take responsibility for data in the cloud that may be located on their territory entails, in a broader interpretation of international law, that it would be unreasonable of states to insist upon a strict interpretation of territorial integrity and thus claim territorial jurisdiction in situations in which they are not aware of data being stored on their territory and in which the material interests of other states are affected. (Note, however, that while it may be unreasonable, it remains the strict interpretation of the law.) Similarly, the claim of jurisdiction by a state over a person, object, or event requires that there is a strong and plausible link to that over which jurisdiction is being asserted. Where data is simply moving across territory in a random pattern, the argument can reasonably be made that territory does not provide a sufficiently strong connection to the data and that other forms of jurisdictional claim are stronger; for example, jurisdiction based upon the nationality of the suspect (nationality jurisdiction) or on the nationality of the victim (passive personality), or universal jurisdiction, where the loss of knowledge of location can be seen as rendering territorial claims impossible, as with the high seas (see section 4.3.3 below).

At the same time, it seems reasonable to conclude that all states have an interest in ensuring that the cloud cannot be used to facilitate cross-border criminal activities and thus an interest in working together to conceive of a legal framework that protects their interests. While territoriality is the dominant organising principle in international law and while states are often resistant to claims that impinge upon their right to strict exclusivity of action within their territory, this right is limited by the obligations owed to other states. Moreover, where territorial sovereignty does not serve their interests or where states accept that they have responsibilities to future generations,

[263] As Klabbers puts it: "if state A sends its troops into state B, it should be able to justify this in legal terms, and if the justification is strong enough, the behaviour can be deemed 'lawful'. … Once a crucial point is passed (when the justification is not strong enough) the behaviour may be deemed unlawful." *Ibid.*

[264] State interests are many and varied but should not be confused with the concept of national interest within international relations theory. State interests are defined by reference to legal obligations owed by other states, such as non-interference in internal affairs.

[265] *Island of Palmas* case.

[266] *Corfu Channel* case, ICJ Reports, 1949, 6.

[267] Klabbers, *International Law* , 90.

[268] As the quotation from the ICJ's judgement in the previous paragraph makes clear, for a state to be held accountable for the use of its territory to harm the interests of another state it must know that its territory is being so used.

states are capable of creating special legal regimes outside the dominant frame of territorial sovereignty.

In this section of the report we examine a number of these special regimes[269] in order to help us in imagining an approach to cloud computing and cross-border access to data that is not based upon strict territoriality. The aim of what follows is not to suggest that international law, via analogies with certain special regimes, already allows for cross-border data searches; it is to suggest avenues that might be worth pursuing in developing international law in this area. By definition such suggestions remain *lege ferenda*. By analogising to existing forms of co-operation outside the usual strictures of exclusive territoriality, efforts to develop the law in a certain direction can become more plausible and less strange to states.

4.3.2. The common heritage of mankind

The principle of the common heritage of mankind is well-established in international law. It provides a limit to the sovereign claims of states by declaring certain spaces to be the common heritage of mankind and thus beyond the claims of any one or groups of states. There is much talk about the common heritage principle in relation to realms as distinct as UNESCO world heritage sites, the rainforest and the human genome. It is generally applied to natural spaces and cultural objects, and it is important to distinguish between common heritage as a legal principle and as a moral statement that some space or artefact should belong to all of mankind. The actual extent to which the common heritage principle serves as the basis of a legal regime is strictly limited and agreement among states to be guided by the principle should not be presumed.[270] There are, however, clear examples where the common heritage of mankind acts as the foundational principle for a legal regime. An example is the deep seabed. Under the terms of the 1982 Law of the Sea Convention, the deep seabed, ocean floor and its subsoil are held to be the common heritage of mankind. No state can claim sovereign rights or exploit these resources; instead the International Seabed Authority is charged with ensuring that any activities carried out in the deep seabed are 'for the benefit of mankind as a whole'.[271] Another arena in which the common heritage of mankind functions as the founding principle is outer space. The key treaty regarding the law of outer space is the 1967 Outer Space Treaty, which explicitly recognises 'the common interest of all mankind in the progress of the exploration and use of outer space for peaceful purposes'. Moreover, Article 1 of the Treaty codifies the belief, as provided in the preamble, 'that the exploration and use of outer space should be carried on for the benefit of all peoples irrespective of the degree of their economic or scientific development'. It further provides that '[t]he exploration and use of outer space, including the Moon and other celestial bodies, (…) shall be the province of all mankind.'[272]

However, despite the acceptance of states in these areas of the existence of a principle of common heritage and a willingness to see the scope of sovereign rights limited in this way, such examples are very rare. Moreover, more recent developments may suggest that the common heritage principle is waning as technological developments allow states to imagine the exploitation of realms that were once beyond their scope. It is to be expected that sovereign claims will quickly follow on from the realisation of those ambitions. As Klabbers has commented, 'there can be little doubt that if the geostationary orbit had been conveniently located above Western industrialized nations, it would have been subject to national appropriation by now.'[273] There has been recent media speculation – driven by the landing by the Chinese space programme of a lunar rover on the surface of the moon that is widely viewed as searching for possibilities to mine Helium-3 – that the Chinese government views the appropriation of space

[269] The choice of special regimes considered reflects the discussions among the participants of the workshop we organised for this research.

[270] Some indication of the weight of the principle within international law can be derived from the fact that the indexes of the contemporary leading handbooks do not contain an entry for common heritage (e.g. Klabbers, *International Law* ; Malcolm D. Evans, *The Law of the Sea*, ed. Malcolm D. Evans (International Law; Cambridge: Cambridge University Press, 2006)).

[271] 1982 UN Convention on the Law of the Seas, Articles 136-140; see also, Evans, *The Law of the Sea* , 645-646.

[272] Preamble & Article 1 of the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies [Outer Space Treaty].

[273] Klabbers, *International Law* , 251.

and celestial bodies as a natural development by states. If true, this view is a direct challenge to the basic principle of outer space law and to the principle of the common heritage of mankind.[274] This trend, as well as the determination by the major Internet states to refuse to countenance the idea of cyberspace as a realm apart, would suggest that any attempt to characterise cyberspace as the common heritage of mankind – and hence beyond the frontier of claims to territorial jurisdiction – is highly unlikely to succeed.

4.3.3. High seas and flag jurisdiction

The principle of the freedom of the high seas is a core principle of international law. It is founded not upon the principle of common heritage but upon the principles of state sovereignty and of sovereign equality. At its essence, it entails that the high seas are not subject to the jurisdictional claim of any one state; instead, all states may freely use and exploit the oceans subject only to their own will.[275] The freedom of the high seas is better understood as an obligation upon States rather than as a right; as expressed by the International Law Commission: 'All maritime flag-states have an equal right to put the high seas to legitimate use. But the idea of equality of usage comes only in second place. The essential idea contained in the principle of the freedom of the high seas is the idea of interdiction of all flag-states from interference in navigation in time of peace with all other flag-states.'[276] It follows from this that ships on the high seas are subject only to the jurisdiction of the state whose flag they lawfully fly.

Ships on the high seas do not however enjoy absolute freedom of passage. Customary international law recognises a number of scenarios in which a state may interfere with the passage of a ship flying a different flag.[277] These are: a) where the ship is involved in acts of piracy; b) where it is involved in the slave trade; c) where it constitutes a threat to the state (conceived narrowly to concern terrorism, weapons of mass destruction and drug trafficking)[278]; d) where it is without nationality, i.e., not flying a flag; e) where the ship is actually a ship of the interfering state but is flying an alternate flag; and f) hot pursuit (i.e., the pursuit of a ship from territorial waters into the high seas). According to Reuland's study of this subject, the right of interference on the high seas takes two forms:

> 'right of reconnaissance and the droit de visite (right of visit). The least obtrusive mode of interference is the right of reconnaissance – a simple right permitting a warship to request that the encountered ship show her flag. The droit de visite, on the other hand, involves physical interference with the suspect vessel. The droit de visite is actually composed of two distinct operations: the droit d'enquête du pavillon (right of investigation of flag) and the right of search. A state may exercise her droit d'enquête du pavillon to ascertain whether the encountered ship is entitled to the flag she flies. In the most extreme cases, a state may proceed to search the vessel.'[279]

The high seas are an obvious analogy for cyberspace because they represent an anomalous legal regime at the heart of international law, in which states have limited their sovereign rights and in which they accept the principle of free navigation.[280] The concept of flag jurisdiction

---

[274] See, e.g., China Moon Landing Raises Big Questions, 15 December 2013, http://guardianlv.com/2013/12/china-moon-landing-raises-big-questions/. There is also a subtle but arguably crucial shift in the language being used by state delegations in relation to outer space. Note the statement by the Chinese delegation on Outer Space at the thematic debate at the first committee of the UN General Assembly on 28 October 2013 that "The security of outer space bears on the common welfare of the mankind." http://www.un.org/disarmament/special/meetings/firstcommittee/68/pdfs/TD_28-Oct_OS_China.pdf While similar in language, it is not the same as recognising that outer space is the common heritage or province of mankind.

[275] "[A]ll nations being equal, all have an equal right to the uninterrupted use of the unappropriated parts of the ocean for their navigation. In places where no local authority exists, where the subjects of all states meet upon a footing of entire equality and independence, no one state, or any of its subjects, has a right to assume or exercise authority over the subjects of another." *Le Louis*, 2 Dods. 210, 243, 165 Eng. Rep. 1464, 1475 (1817).

[276] *Memorandum par le Secretariat*, U.N. Doc. A/CN.4/32, reprinted in [1950] 2 Y.B. I.L.C. 67, 69, U.N. Doc. A/CN.4/SER.A/1950/Add.1 (our translation).

[277] These powers cannot be used against a military vessel of another state or any other vessel entitled to immunity. See Evans, *The Law of the Sea* , 637.

[278] Ibid., 637-641.

[279] Reuland, 'Interference with Non-National Ships on the High Seas: Peacetime Exceptions to the Exclusivity Rule of Flag-State Jurisdiction', 1169.

[280] See, for example, the use of the principles underlying the high seas as the basis for a suggested instrument to regulate against cyber-attacks in W.M. Stahl, 'The Uncharted Waters of Cyberspace: Applying the Principles of

means, however, that the vast expanse of the high seas is not unregulated. Jurisdiction is instead exercised on a nationality basis rather than a territorial one. What is interesting here, though, is the described willingness of states to allow one another to interfere with the territorial-like rights represented by flag jurisdiction – however limited in scope and action.[281] States permit the idea that another state can enter the bounded area of its exclusive jurisdiction, as represented by its flag, for certain agreed purposes. These purposes are limited in scope to exploration of identity and the pursuit of universally condemned actions such as slavery and terrorism. Were we to suggest a view of cyberspace as the high seas, data movement as akin to free navigation, and jurisdiction being provided by the nationality of the service provider, interference with the free movement of data would be, in this analogy, strictly limited to investigating the authenticity of the service provider's nationality claim and to the investigation of crimes that are universally abhorred. Such crimes would most likely be limited to terrorism, child pornography, and the activities of organised crime in relation to drugs and human trafficking.

One interesting exception to free navigation is that of hot pursuit.[282] Hot pursuit is an exception to the exclusive flag state jurisdiction to address the problem of vessels that commit offences within internal or territorial waters evading arrest by moving beyond territorial waters onto the high seas. Where warships or military aircraft of a coastal state have already begun the pursuit of a vessel within its territorial waters or contiguous zone,[283] they may continue that pursuit as long as the pursuit is continuous (although the actual ships or aircraft in pursuit need not be the same). The hot pursuit analogy allows the list of crimes for which such action can be taken to increase substantially. However, it should be noted that hot pursuit concerns the pursuit of a suspect object that is in sight; in cases of cross-border data searches, there is likely to be a lack of clarity as to the data that are being sought (or pursued). In addition, the data sought are not pursued as they move from state A to cyberspace but are already in cyberspace (the high seas). These caveats suggest that hot pursuit is less suitable as an analogy than on first consideration.

In the context of pursuit of cross-border data, the most appropriate means of using the high seas analogy appears to be to liken the cloud to the high seas and to imagine the service providers as ships, subject to the jurisdiction of the flag they fly (either where they are registered or where the headquarters are located). Likening the providers to ships (as opposed to the data themselves) reduces the difficulties for LEAs in locating data; all they would need to do is identify the provider. This approach does not necessarily absolve an LEA of the need to seek consent from the state in which the provided is based. Yet, the exceptions allowed for under international law in relation to the high seas suggests that states may be willing to accept the need to access data in the pursuit of (certain) crimes, in much the same way as they allow for intrusion onto the 'territory' of their flag vessel where certain crimes are suspected. Moreover, by analogising cyberspace to the high seas, in scenarios in which the cloud is used to escape the territorial jurisdiction of a state in which crimes have been committed – by, for example, hiding evidence of the crime in the cloud – it may be possible for an investigating state to claim hot pursuit if at the moment of arrest or of the execution of a search warrant an effort is made to hide data.

4.3.4. Piracy as an analogy for (certain types of) cybercrime

The flipside to the notion that certain objects or areas of the earth constitute the common heritage of the high seas is the position of the pirate, labelled by Cicero as the common enemy of mankind.[284] In being framed as an enemy to all, pirates are denied the protection of any state and are subject to universal jurisdiction. This is why the act of piracy constitutes an exception to the

---

International Maritime Law to the Problem of Cybersecurity', *Georgia Journal of International and Comparative Law* 40/247 (2011).

[281] Although flag jurisdiction is based upon nationality, the rights are territorial-like in that the vessel represents a defined space of exclusive jurisdiction.

[282] Article 111 UNCLOS. See Evans 2006, 638-639.

[283] The contiguous zone is a zone of 12 additional nautical miles from the baseline in which a coastal state may enforce certain of its laws; it is a zone in between territorial waters and the high seas, although not all states have chosen to claim it. Article 33 UNCLOS. Hot pursuit from the contiguous zone is only allowed for breaches of laws that are applicable within it.

[284] Marcus Tullius Cicero, 'On Duties (De Officiis)', *Trans. MT Griffin and EM Atkins. New York: Cambridge University Press,* (1991), 3.107, 141.

exclusivity of flag state jurisdiction. Piracy is defined in the UN Convention on the Law of the Seas (UNCLOS) as:

> '(a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:
>
> (i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;
>
> (ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;
>
> (b) any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;
>
> (c) any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).'[285]

Piracy is interesting as an analogy for cybercriminals because of the widely-recognised status of universal jurisdiction that arises and because of the reason for which universal jurisdiction arises: the basis for universal jurisdiction for piracy flows not from the near-universal abhorrence of pirates as enemies of all mankind but from the principle of freedom of the high seas. The lack of jurisdiction of any one state entailed that all states had jurisdiction in relation to piracy. Likewise, because no single state has jurisdiction over vessels that fail to fly any flag, all do. International law is in essence a practical means for states of solving common problems. It is for this reason that UNCLOS includes a strongly worded and far-reaching provision requiring state parties to the Convention to 'co-operate to the fullest possible extent in the repression of piracy on the high seas or in any other place outside the jurisdiction of any State.'[286] The fear that the high seas could become a nautical 'wild west', in which crime goes unpunished, has not only led states to accept universal jurisdiction for those crimes but to accept a far-reaching obligation to co-operate to suppress piracy.

A similar provision in UNCLOS relating to vessel discharge allows port states to investigate and prosecute vessels that illegally discharge waste on the high seas, where those vessels voluntarily enter port.[287] The aim of this provision is to prevent polluters from evading prosecution because of the freedom of the high seas and of difficulty of the flag-state in obtaining sufficient evidence to prosecute. By voluntarily seeking the services of the port, vessels can be subject to searches by the authorities of the port state (at least in relation to discharge).

It could be claimed that it serves the interests of no states to allow cross-border criminal activities that make use of the cloud for criminal purposes to go unpunished because of the practical difficulties inherent to locating data. Universal jurisdiction would be one means of expressing this shared interest of states. Another would be to view the investigating state as port authorities, where service providers voluntarily 'enter port' by providing services within the jurisdiction of the investigating ('port') state and can therefore be subjected to searches by that state.

It is important to distinguish from the pirate example in one key way: piracy gives states jurisdiction over the physical persons of the pirates. Universal jurisdiction in relation to cross-border data would need to be explicitly limited to the jurisdiction to search for cross-border data; it would not imply the ability for LEAs to enter territory in order to arrest suspects. This would still require an international arrest warrant within existing forms of co-operation. Rather, the powers of universal jurisdiction are more akin to those of the port state investigating vessel discharge.

An alternative way of using the pirate analogy is to label as pirates not the data users but the service providers. For example, where providers do not openly identify themselves by 'flying a flag' they could be conceived of as a pirate against whom universal jurisdiction applies and all (human rights compliant) action is justified. This could include the right of access to data stored

[285] Article 101 UNCLOS. This definition of piracy is most likely complemented by a broader definition in customary international law. See Evans, *The Law of the Sea* , 637; Evans does, unfortunately, not specify how the customary international law definition is broader.

[286] Article 100, UNCLOS.

[287] See article 218(1) UNCLOS: 'When a vessel is voluntarily within a port or at an off-shore terminal of a State, that State may undertake investigations and, where the evidence so warrants, institute proceedings in respect of any discharge from that vessel outside the internal waters, territorial sea or exclusive economic zone of that State in violation of applicable international rules and standards established through the competent international organization or general diplomatic conference.'

by providers who operate as 'pirates' in cyberspace. Again, this universal jurisdiction, and the pirate analogy, would apply only to the act of cross-border data searches and not to the legal person of the provider or to the physical persons connected to it. It is possible to imagine that certain service providers that seek to conceal their identity (such as the so-called 'bullet-proof' providers) do so precisely because they offer data storage for illicit purposes. However, a technical equivalent of the flag for Internet or cloud service providers would need to be implementable by all providers storing data, which—if technically feasible at all—would require considerable investment to alter the service architecture; and it is very unlikely that states will agree upon creating such a 'flag' regime for providers.

The discussion in this and the previous section have been intended to highlight the ability and willingness of states to co-operate outside the usual pattern of territorial sovereignty where the physical attributes of a space—the high seas—make territorially-based claims of jurisdiction impractical. Faced with the alternative that criminals would be left to operate freely, states have adopted universal jurisdiction for violent acts, plunder, and certain forms of pollution.

4.3.5. The right to acquire remote sensing imagery and the principle of 'Open Skies'

An alternative, yet similar, line of reasoning exists in the legal regime of satellite imaging. Satellite imaging or remote sensing imagery denotes the collection of data in either photographic or digital form by space-located devices without any physical contact with the sensed object and by using electromagnetic radiation. There are two types of remote sensing satellites: passive satellites that observe radiation emitted by the sensed object itself, and active satellites, which themselves emit radiation and measure the energy reflected back by the object.[288] Both types of satellite imaging are available to and used within both the military and civilian domains by more than a hundred countries. Satellites and satellite imaging for any purpose are governed by international law, in particular the law of outer space.

The 1967 Outer Space Treaty is the cornerstone of the legal regime on outer space. Central to this regime is the principle of the freedom of outer space. With the launch of the first satellites in the mid-twentieth century by the US and USSR, no State protested at the passage of these satellites over their territory; this implied consent of States to allow free passage of satellites over their territory was given formal recognition in the 1967 Treaty and is now held to be a peremptory norm of the international order.[289] It is important to note, however, that the freedom of outer space is not without limits, the most important of which is the obligation upon States to exercise their rights in such a way that it does not constitute an abuse of rights and impinge upon the rights of other States.

The specific rules relating to satellite imagery are located in a 1986 UN General Assembly Resolution: the Principles Relating to Remote Sensing of the Earth from Outer Space.[290] The rules on satellite imaging are particularly interesting in the context of this report for the controversy that they settled. Prior to the adoption of the principles, there were two strongly opposed views about the legality of satellite imaging: the first advocating the unrestricted use of satellites for imaging purposes and the freedom of distribution of those images. The second view, advanced mainly by the Socialist and Latin American countries but also including France, held that the reception, processing and distribution of satellite images were earth-bound and hence governed by state sovereignty. What this principle was taken to require in the context of satellite images was the need for the prior consent of the sensed state before satellite imagery could be distributed to a third party. This proposed need for consent did not, however, appear in the UN Principles: it is the first view that prevailed and has defined the legal regime in this area. The sensing State thus has the right to collect and distribute satellite imaging without regard to the wishes of the sensed state. In compensation, the main obligation upon sensing states is to make the imaging available to the sensed state on a non-discriminatory basis and on reasonable cost

[288] R Jakhu, 'International Law Governing the Acquisition and Dissemination of Satellite Imagery', *Journal of Space Law,* 29/65 (2003) 65, at 66.
[289] *Ibid*., at 76.
[290] The UN Principles Relating to the Remote Sensing of the Earth from Outer Space, G.A. Res. 41/65, UN GAOR, 41th Sess. 95th Plen Mtg, UN Doc. A/RES/41/65 (adopted without vote on 3 December 1986 i.e. adopted unanimously).

terms.[291] The freedom to collect and distribute images and the non-discriminatory dissemination of those images together constitute the principle of open skies; this principle (although perhaps not all of the 1986 Principles) is acknowledged to have achieved the status of customary international law. In addition, the Principles note the need for sensing states to inform the UN Secretary-General of any remote sensing programme, allowing public access to this information.[292]

Why, though, did those States that strongly advocated the need for consent eventually accept the principle of open skies (it took 16 years to gain the necessary agreement)? One reason is the compromise that the open skies represents: the right of States to collect and distribute satellite images but the obligation to offer those images on a non-discriminatory basis and at reasonable cost. Underlying this is the idea that satellite images contribute to a public good, notably environmental protection and management. More importantly, the acceptance that a prior consent regime would entail was simply unworkable as satellites were unable to recognise invisible political boundaries, and the need to obtain the consent of every state on the satellite's arc would be prohibitively time-consuming and complicated. According to one commentator, 'science and technology thwarted the possibility of enforcing a regime based on notions of national privacy stemming from national sovereignty.'[293]

Satellite imaging provides a helpful analogy to the problem of cloud-based data. Satellite imaging does not simply take a snapshot from outer space but most commonly functions by emitting radiation and measuring the way in which the radiation bounces back off objects, similar to the idea of cross-border searches as the sending and receiving of messages to a server. Moreover, the radiation can be viewed as a breach of territorial integrity in much the same way as a cross-border data search, at least where the search is simply to locate and copy data (as opposed to disrupting it). Although the analogy is limited in technological terms, insofar as the potential scale and reach of computer searches move far beyond what satellites can record, the analogy is useful in terms of the perception of intrusiveness at the time of introduction of the technology at issue. The levels of intrusiveness of satellites in the 1970s and of cross-border searches today are quite comparable, in terms of the reaction of states to other states using these technologies. It is interesting to see how states have been willing to accept, eventually, a principle such as open skies that limited the notion of territorial integrity and non-interference in quite a dramatic way. They did so because of a compromise that ensured that some benefits of satellite imaging were shared, and gradually all states began to recognise a common interest in the open skies principle. Also of importance is that these negotiations were not conducted in the abstract but in a world where one or two states were nonetheless forging ahead with the development, and hence use, of satellite imaging technology. For rules to be formed in this way, one or two states must suggest a normative regime and act in accordance with it.

It may therefore be possible for states to start conceptualising the cloud and cross-border data as a new form of open sky, where the only requirements upon states actively pursuing cross-border data is that they share some of the benefits with other states (for example, to share data where a state is affected by the data recovered) and where those states that pursue this policy register this fact openly (for example, with the UN Secretary-General or the institutional setting of the Cybercrime Convention).

4.3.6. The common concern of mankind

The final possibility for re-conceptualising how we think about the cloud considered here is the common concern of mankind. The idea of there being common concerns of mankind is not to be confused with the principle of the common heritage of mankind, although they stem from the same moral-philosophical roots, and common concern is seen by some to have replaced the failed concept of common heritage. Common concern is a principle that has emerged very recently in the context of international environmental law to frame the cross-border nature of

[291] This obligation relates only to images taken for civilian purposes, particularly in relation to natural resources management and the protection of the environment.

[292] Principle IX; this Principle builds upon obligations laid down in the 1975 Registration Convention and the 1967 Outer Space Treaty.

[293] H. Feder, 'The Sky's The Limit? Evaluating the International Law of Remote Sensing', *New York University Journal of International Law and Policy,* 23/599 (1990) 611.

global environmental problems in relation to the biosphere, such as air pollution, loss of biodiversity, ozone depletion and, of course, climate change.[294] The aim is to provide a legal principle to counteract the seemingly unbreakable loop of the tragedy of the commons.[295]

However, the principle, despite its increased presence in international documents, lacks bite. While states recognise the existence of common concerns and the need to co-operate to combat common threats, the decentralised nature of the international order means that there is no governance structure to make good on the sentiments expressed by the notion of common concern. The lack of organisational structures is a direct consequence of the unwillingness of states to move beyond what is effectively the counter-concept to common concern: the principle of permanent sovereignty over natural resources. This principle is well-established as a corollary of state sovereignty. Labelling a problem as one of common concern is not the same as establishing a legal regime governed by the principle of common concern to address it. While there is a marked increase in the former, there is no evidence that states are willing to do the latter. For this reason, while it may be useful to label the problem of cybercrime in the cloud as a common concern of mankind, particularly where it can be linked to the pursuit of terrorist activities or other types of crime that constitute a grave threat to the survival of the planet, the legal principle provides an insubstantial basis for re-framing how we conceptualise the cloud.

4.3.7. Developing a plausible account

There exists at present no special legal regime within international law governing cyberspace, the cloud or cross-border data searches.[296] This, coupled with the fact that the 'loss of location' of data is in fact a loss of knowledge of location that undermines the claims of states to be capable of regulating what takes place within their territories i.e. the capacity argument that underpins the concept of territorial sovereignty (see section 3.3.1), provide some scope for a state to actively attempt to develop this area of law. If a state were so minded to attempt this, there are some key steps that it should take and some general issues to take into account.

Territorial integrity and non-interference provide the background against which any actions are judged within international law. For a state to breach these rules without committing an international wrong, and where it wishes its actions to constitute state practice within the meaning of customary international law, it needs to do a number of things. The first is to provide an alternative legal account, e.g., by suggesting a new principle of 'open cyberspace' in the context of cross-border access to data, similar to the principle of open skies in the context of remote sensing. The acting state must see its behaviour as conforming to an alternative legal interpretation rather than simply as the exercise of brute power or of relying on the fact that most states will never notice that they were the target of a cross-border data search. The second key step follows on necessarily from the first: any state attempting to offer an alternative legal account to justify its actions must be open about what it is doing. In other words, state practice is not the mere act of doing (or not doing) something; a state attempting to develop this area of law must actually conduct cross-border data searches according to the principles derived from its alternative legal account and state openly that it is doing so.

If such a state can, over time, induce other states to follow its lead and where key states do not object to the alternative legal account presented, it may be possible to form new rules of customary international law; or to persuade other states of the need to codify a developing practice through a set of principles, either under UN auspices or any suitable organisation, as

[294] A. Kiss, 'The Common Concern of Mankind', *Environmental Policy and Law,* 27/4/244 (1997); Thomas Cottier, 'The Emerging Principle of Common Concern: A brief outline', (2012).

[295] The tragedy of the commons is a theory, developed by Garrett Hardin, according to which individuals, acting independently and rationally according to each one's self-interest, behave contrary to the whole group's long-term best interests by depleting some common resource. Garret Hardin, 'The Tragedy of the Commons', *Science,* 162/1243 (1968).

[296] The Cybercrime Convention can certainly make a claim to be moving in this direction, particularly as it is open to non-European states and has been ratified by the US, Australia, and Japan, but the lack of a number of key states, such as Russia, China, and Andorra, among the signatories suggest that it is not yet sufficiently general to form part of general international law (as opposed to regional international law) and thus cannot be considered to have binding effects on non-signatory states.

happened with remote sensing.[297] If this occurs, states that forged ahead will be seen as early adopters rather than poor members of the international community.

How other states react in general will depend in part on how convincing the alternative legal account is, but more importantly on whether they perceive their interests to be served by the developments proposed and on whether the benefits of such searches will be shared (where appropriate and in keeping with human rights obligations).

How states react to specific searches conducted under an alternative account will depend upon a number of case-specific factors. These factors can help provide a more nuanced legal account.

The first factor that will affect how a state that is the subject of a cross-border search reacts concerns the seriousness of the case and the immediacy of action. Where there is broad agreement among states about the seriousness of certain types of crime, such as child pornography, or where the case concerns an immediate risk to life, action will be perceived as more reasonable, though only where the action undertaken is strictly limited to the case at hand and proportionate to the justification given. Fishing expeditions must on all counts be excluded from the practice, and states should offer a plausible account that what they do in practice is really limited to what is strictly necessary.

The second factor concerns the locatability of the data sought, i.e., the ease or difficulty with which its location can be determined. One of the more plausible bases for currently arguing for an alternative account of international law that allows for cross-border data searches in certain, defined, circumstances is the unknowability of the location of data. In a number of cases, it is possible to identify the location of data with reasonable likelihood, in part because data is most likely to be stored at a server close to the user. In such circumstances, arguments for accessing the data without seeking the prior consent of the affected state will be weak. However, where it is genuinely not possible to ascertain, with reasonable efforts, the location of the data, arguments for accessing the data without prior consent become stronger. The question thus arises what a 'reasonable' effort is to ascertain the location of data. In a plausible account, some threshold must be proposed for the efforts that can be expected of law enforcement authorities to make before they can claim that the location of data is unknowable. The question of what such a threshold should consist in, is both a technical and a political question, which we cannot address in this report. States aiming to develop this area of law should attempt to come to an agreement on such a threshold, making explicit what are good practices through identifying the necessary technical and operational measures for various situations of cross-border searches. The standard should be periodically reviewed to stay abreast of new technical developments.

Although we, as legal scholars, cannot indicate what threshold could or should be adopted in a plausible account, we need to emphasise that, from the legal perspective, it remains the case that any breach of territorial integrity without the prior consent of the affected state constitutes an international wrong, even if the law enforcement authorities acted in good faith and assumed that the data were located in their own territory or reasoned that they could not determine the location with sufficient likelihood. A state official accidentally crossing a border violates the sovereignty of the other state, even if she is not aware of the border-crossing. This implies that any threshold of the effort that can be expected of law enforcement authorities to determine the location of data must be high in order to be plausible; how high can only be determined by states themselves. We suggest that gaining agreement on the nature of the problem – the inability to ascertain with reasonable efforts the location of data sought for the purpose of criminal investigation of a list of circumscribed crimes (as agreed between states) – and in developing a threshold for searches without prior consent within the frame of one or more relevant international fora (see section 5.1) is a valuable approach to moving forward.

The third factor relates to the extent to which *both* the affected state and the acting state are genuinely affected by the data. Relevant factors here include the nature of the action (accessing or copying data, alteration, or deletion); the purpose to which the data will be put (acting to save lives or criminal investigation and evidence gathering), and, where the purpose is that of criminal investigation, the seriousness of the crime (the 'four horsemen of the Internet apocalypse'[298] that

[297] The UN is the traditional route because of its superior claim to global representation; however, the Council of Europe may be a better forum, given the leadership that it has taken in this area (see section 5.1 below).
[298] See http://en.wikipedia.org/wiki/Four_Horsemen_of_the_Infocalypse.

are more commonly considered serious—child pornography, terrorism, drugs, and organised crime—as opposed to, for example, mortgage fraud); and the nationality of the victim and of the suspect (if both are nationals of the acting state, or if the suspect is a national of the affected state). Also other factors affecting the strength of a jurisdictional claim should be taken into account, such as the location or impact of the criminal activity; if most of the action takes place within the territory of the acting state or elsewhere; the strength of the link between the data and the territory, in other words, whether the data have been intentionally stored in the affected state—e.g., to benefit from the legal protection in that state—or whether the data just happen to be located in the affected state as an inadvertent consequence of someone's using a cloud service. These factors are used to weigh up the interests of the affected state and the acting state. Where the acting state is strongly impacted by the criminal activity in question and the impact upon the affected state of action to retrieve the data sought is minimal, the concern of the affected state is likely to be itself minimal.

Forging ahead may have a number of advantages: although it may not enable a state to conduct all searches it might find necessary, it does allow for some searches in defined situations; moreover, the state forging ahead gets to play an important role in shaping the developing legal regime, e.g., through defining what the accepted types of situations will be. This might be particularly attractive for a smaller state that would otherwise not play such an influential role in more formal law-making forums. Another advantage is that, while there may remain some level of doubt as to how the international community or particular states will react to unilateral actions, this in itself does not have to jeopardise the prosecution of suspects if data have been acquired through cross-border searches. Various countries apply a 'Schutznorm' in criminal legal doctrine, which holds that unlawfully obtained evidence does not necessarily have to be declared inadmissible if the norm that was breached protects the interest of others than the suspect.[299] In this case, if a cross-border search were eventually to be considered unlawful under international law, the breach would be of an obligation owed to another state—respect for territorial integrity and non-interference in domestic affairs—but not that of the suspect. Hence, if the search were otherwise in conformity with the law of the searching state (in terms of the infringement of the suspect's privacy interest being legitimated, e.g., through a warrant), the data can be used as evidence in a criminal trial (in countries applying the *Schutznorm*) regardless of whether or not international law was violated.

However, there are a number of risks to such a strategy. For this strategy to have any validity within international law, as already noted, a state needs to be open about its behaviour. Other states may require that consent be sought *ex post* and this may result in the demand for an apology, an acknowledgment of a wrongful act, and a commitment not to act in such a way in the future. This assumes that it is possible to locate the data in terms of territorial sovereignty at all. States cannot claim that a wrongful act has been committed in the abstract. This may make the approach of a plausible alternative account more attractive in this particular case. There are nonetheless some other general risks that are worth considering.

The first risk is a broad one, relating to the nature of international law, and, although unlikely to be of importance in the present context, nonetheless worth mentioning. Positive international law can seem ridiculous in its seemingly blind attachment to state sovereignty, particularly in the context of almost overwhelmingly global challenges; climate change would be one such problem. To such a mind-set, international law is part of the problem by preventing those who wish to act from doing so. However, before rushing to push the self-interested claims of sovereignty to one side in the service of the common good, it is wise to recall the purpose of sovereignty and its attendant doctrines. The doctrine of sovereignty, for example, underpins the concept of sovereign equality, granting small states an equal voice irrespective of the political and military power of the larger states. Sovereign equality determines the need for consent before a state can be bound; more powerful states cannot simply create law that serves their interests and for this reason it is important that consent cannot be presumed. There are thus reasons to be cautious about any move that may undermine the protection that the doctrine of sovereignty affords smaller, less powerful states. That said, it seems unlikely that actions by one or more states to access data

[299] See, for example, in Dutch law Hoge Raad [Dutch Supreme Court] 30 March 2004, ECLI:NL:HR:2004:AM2533, §3.5.

stored in the cloud without seeking prior consent will cause any serious damage to the centrality of state sovereignty or the territorial integrity it presumes. The key point here, however, is that is unwise to under-estimate the importance that states attach to safe-guarding their individual sovereignty, even if the destruction of the planet from climate change is the result. As such, international problems can only be solved by working within the framework of state sovereignty and not either by ignoring it or by attempting to wish it away.

A more substantial risk concerns the near certainty that where a state acts in a unilateral manner to access data stored in the cloud, other states will act in a similar manner. Further, the state forging ahead would be estopped from protesting about such behaviour or from claiming an infringement of their territorial integrity where the data was located on their territory. Estoppel is a general principle of international law, drawn from municipal law, that holds that once a state takes a position on an issue and relies upon it in its relations with other states, it is prevented (estopped) from altering its position in relation to what other states are doing. Where, for example, a state relies upon a claim of universal jurisdiction to pursue data in the cloud, it cannot refute the claim of other states to universal jurisdiction on the same matter. What this means is that once a state starts down this path, it cannot reverse its position because the strategy turns out to negatively affect its interests in certain circumstances. There are no *sui generis* situations in international law: each claim can be used as a precedent.[300] Any state pursuing such a strategy should think hard about how the alternative legal account proposed could be used in a way which harms their interests or those of its citizens.

An additional consideration for any efforts to develop the law in this area concerns the risk of unintended consequences. Any claims made in relation to cross-border access to data (where those claims find some traction) are likely to influence the development of rules in relation to cyberspace and cyber commerce, and may influence the development of rules further afield. The nature of international law entails that arguments can be used, in good faith, to support opposing positions. Arguments about universal jurisdiction or about cyberspace as an open sky may not suit the interests of the original proposing state where they resurface in other areas. While this cannot be avoided, it would be worth a close consideration of the consequences such arguments might have in disputed areas of cyberspace law in particular.

Finally, any state that takes a unilateral stance may find that other states become less co-operative than they might usually expect, whether in relation to matters of cross-border policing or more broadly.[301] Some states can ride such a response more easily than others because of their relative importance and size. Smaller states are more exposed to the need for co-operation than larger ones. It is not surprising that those states that tend to forge ahead in developing new legal regimes most often are those that are less dependent on the co-operation of their fellow states in the international order.

4.4. Conclusion

The current options for legally accessing data in cross-border searches are limited. Article 32(b) has been watered down in the 2013 Guidance and, in any case, is only of relevance where the location of the data can be determined to be in another state that is party to the Convention. Nonetheless, a number of states are attempting to access data for the purposes of cross-border investigation, leading to a variety of practices, most of which are legally dubious from the perspective of international law and operate within (or perhaps exploit) this grey legal zone. This suggests a need for clarity as to the legal position of such searches and, arguably, the development of a legal regime that addresses the apparent needs of states to conduct cross-border data searches for the purposes of criminal investigations.

[300] See Russia's claims in relation to the Crimea employing arguments used earlier in the western claims about Kosovo; Russia's claims parrot – quite deliberately and hence irrefutably – the claims made by western powers in relation to Kosovo, their claims about the *sui generic* nature of the Kosovan situation notwithstanding.

[301] Cf. Cedric Ryngaert, *Jurisdiction in international law* (Oxford monographs in international law; Oxford; New York: Oxford University Press, 2008) at 83 (arguing that 'Europeans may indeed reason that arguments of reciprocity counsel against unilateral assertions of jurisdiction in the field of the law of evidence. Although such assertions may confer short term litigation benefits, such benefits may be outweighed by the burdens of future unilateral assertions of jurisdiction of other States').

While the strict legal interpretation is that cross-border data searches breach the obligations that all states owe one another to refrain from breaching territorial integrity and interfering in internal affairs, a non-doctrinal approach to international law sees behaviour as more or less justifiable depending upon the strength of the arguments that one makes. There are several more or less plausible arguments that can be made on the basis of existing legal regimes that could advance an alternative legal account of how states could better relate to one another within the space of the cloud to achieve shared aims.

Where states have sufficient interest in doing so, they can develop legal regimes that put claims based on territorial sovereignty to one side. Such regimes are rare. However, the legal framework applicable to outer space, and to satellite imaging in particular, suggests that where technology makes assertions of territorial sovereignty untenable and where states perceive a shared interest in an alternative framing principle, a principle such as open skies can develop. Similarly, where the nature of a space, such as the oceans or the wildness of Antarctica, limits states' ability to make that space into place, capable of being subjected to territorial claims, states will create a regime that recognises that limitation and co-operate to ensure that such 'space' does not become a haven for criminals.

For the creation of a more or less plausible alternative account of the space of the cloud to gather plausibility momentum, one or two states—better still, a group of states—need to forge ahead in developing an alternative legal account and in acting openly in accordance with that account. The more states that can be persuaded to do so, the stronger the legal argument will become.

5. Ways forward

The rapid spread of cloud computing and the constraint that the loss of knowledge of location of data constitute a serious practical and legal constraint on modern law enforcement practices. The strict interpretation of international law is that where officials are unable to identify the location of data in order to seek a MLAT, they must stop in their efforts to access it. It is important to be aware that without a coherent attempt to addresses this problem LEA officials are unlikely to exercise the necessary self-restraint, particularly where the data sought is in the context of an investigation into child pornography for example. This will lead to a sort of 'free for all', in which data is accessed cross-borders without sufficient guarantees for the rights of individuals. In addition, such a practical approach cannot lead to the development of an alternative legal account. As noted above in section 4.3.7, in order to develop an alternative legal account for accessing cross-border data, it is necessary for a state or group of states not only to actually access cross-border data (practice) but to do so openly by offering a plausible account from within international law of why such behaviour is permissible (*opinion juris*).

This section contains pragmatic suggestions for how states could best proceed to develop the law on cross-border searches in a way that achieves some of their law enforcement goals. A general rule of thumb is that there is a necessary trade-off between substance and process; phrased differently, the less ambitious a proposal is in scope and substance, the easier it will be to persuade more states to agree to it, and vice versa. It should be recognised that, given the complexity and sensitivity of the issue, various efforts may not succeed or turn out to be unachievable; and it is possible that efforts will take a long time and require considerable investment of effort. However, our suggestion is that where a plausible account can be developed of the need for injecting new powers into cyber-investigation, states may be willing to overcome, in a limited way, their territorial approach towards cyberspace.

Before an alternative account can begin to be effective, however, it is necessary, as we have emphasised in this report, to do substantial preliminary work aimed at creating a shared basis of common understanding. This preliminary work should comprise at least three types of efforts. First, the challenges of cyber-investigations, in particular the need for expeditious cross-border access to data in the cloud era, need to be recognised at the international level. It is not sufficient that law enforcement authorities publicly voice the problems they are facing—these problems need to be acknowledged by state officials in international fora, before they can be recognised as challenges of international law. Second, the problems need to be conceptualised carefully and explicitly. Stakeholders should be aware of the effect of metaphors employed in debates, and care should be taken to use the most appropriate metaphors. Framing cyberspace as 'space' (a more abstract area) rather than as 'place' (a physical area) makes a difference in terms of thinking about solutions, as does conceiving of cross-border searches as the sending and receiving of messages rather than as 'going to' a server. And defining legal authority in terms of effective control rather than controlling territory within national boundaries may also help to understand jurisdiction in relation to 'space' instead of purely connected to 'place'. Third, the communities of cyber-investigation and international law need to get acquainted and familiarise themselves with the other community's language, concepts, and assumptions much more than is currently the case. In our research, we were struck by the lack of understanding with cyber-investigation experts of basic principles and developments of international law as well as by the lack of understanding with international law experts of the basic principles and developments of cyber-investigation. Bringing these communities together is not only a matter of bridging theory (international law) and practice (cyber-investigation), but also of developing a shared understanding of the problem and the framework within which the problem needs to be addressed, before an account can be developed of cross-border cyber-investigations that is plausible both in technical and in international law terms.

When preliminary work along these lines is undertaken, states can take steps forward to addressing the challenge of cross-border cyber-investigation. We will first discuss actions that can be undertaken at the international level, and then zoom in on actions that can be taken at the national level of individual states, in particular with the Dutch context.

5.1. Actions at the international level

5.1.1. United Nations

5.1.1.1. UN General Assembly

The UN General Assembly is a global forum for discussion, co-operation, and co-ordination on any topic of interest to states that falls within the broad remit of the UN Charter.[302] It is charged with 'promoting international co-operation' and 'encouraging the progressive development of international law'.[303] With limited exceptions, it has no power to take any decisions that create legal obligations for states; yet, according to Boyle and Chinkin, 'although not a legislative body in any sense, [the General Assembly's] ability to adopt resolutions on any subject, convene law-making conferences, adopt treaties and initiate codification projects has given it a central role in the development of international law.'[304] One avenue for legal development in relation to cross-border data searches is therefore the creation of a General Assembly resolution that creates (declares) legal principles in this area. One of the advantages of the General Assembly is that decisions are taken on a simple majority, one state one vote, with no states possessing a veto.[305] This means that to pass a resolution it is necessary only to persuade 96 other states (96 + 1 proposing state) to vote in favour.

In an area such as cyberspace law, where the legal regime is under-developed, declarations of the General Assembly can be the beginning of a process of seeking binding agreements, either where the Declaration forms the basis for later treaty negotiations, i.e., as a means for seeking a basic consensus for the need for a multilateral treaty. In such scenarios, a Declaration tends to declare a general intention to co-operate to address specified problems. Alternatively, a resolution can be the basis for customary international law. As resolutions are themselves not binding, and as multilateral treaty creation and customary international law formation are excruciatingly slow and complex processes, resolutions of the General Assembly cannot be recommended as a means of creating binding international law.

However, General Assembly resolutions are not simply political statements or part of a process of creating binding legal obligations (i.e., as evolving law). They are also soft law instruments. Boyle and Chinkin write, in their leading account of international law-making, that 'soft law instruments will tend to legitimise conduct and make it harder to sustain the legality of opposing positions.'[306] While a General Assembly resolution cannot create binding obligations for states upon which other states can rely, cross-border data searches do not actually require other states to act. Such searches only require states to permit the actions of other states. A declaration that stated the intention of states to co-operate in this area and that provided for cross-border data searches (in a limited set of circumstances) would go quite some way towards providing a legitimate basis for action, most particularly because it does not require other states to act to be effective.

Existing General Assembly resolutions, in which states recognise the need to co-operate in the field of transnational crime, particularly in relation to the Internet, provide a basis on which any attempt to create the political momentum for a resolution on cross-border data searches could be based.[307] The most likely route for a General Assembly resolution on matters of criminal justice is via the Commission on Crime Prevention and Criminal Justice (see below).

---

[302] Articles 10-11 UN Charter. For the extent of the UN's remit in the area of economic and social co-operation, Article 55 UN Charter.
[303] Article 13 UN Charter.
[304] Alan Boyle and Christine Chinkin, *The Making of International Law* (Oxford University Press, 2007), p. 116.
[305] Article 18 UN Charter.
[306] Boyle and Chinkin, *The Making of International Law* , p. 212. Soft law is a term that encompasses a wide variety of non-legally binding instruments used by states in the pursuit of their international relations.
[307] See, e.g. the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, annexed to GA Resolution 65/ 230, A/RES/65/230, 1 April 2010, notably para. 8, which calls for greater international co-operation in the preventing, prosecution and punishment of crime by 'building, modernizing and strengthening' criminal justice systems; and para. 39, where UN Member States highlight that ICT developments and the Internet 'create new opportunities for offenders and facilitate the growth of crime.'

5.1.1.2. Commission on Crime Prevention and Criminal Justice

Within the almost limitless substantive remit of the UN,[308] it has also claimed specific competence in relation to facilitating co-operation between states in relation to crime and criminal justice.[309] This competence is given concrete life in the form of the Commission on Crime Prevention and Criminal Justice (CCPCJ), which is one of the functional committees of the UN Economic and Social Council.[310] The principal policymaking body of the United Nations in the field of crime prevention and criminal justice, the CCPCJ also functions as a forum for exchanging expertise, experiences, and information in order to develop national and international strategies, and to identify priorities for combating crime. In addition, this body is responsible for the organisation and agenda-setting of the United Nations Crime Congresses that take place every five years.

The 2010 Crime Prevention and Criminal Justice Congress paid attention to the issue of cybercrime. A working paper for this congress observed that existing legal instruments have limited reach. It observed that 26 Council of Europe member states and one non-member state (the US) had ratified the Cybercrime Convention to date (2010), while acknowledging that it had a wider reach since several other countries had used the Convention as a model for national legislation. It considered that the number and speed of ratifications 'remains an issue' compared to global standards,[311] and that '[e]xperience has shown that States are generally reluctant to ratify or accede to conventions that they have not contributed to developing and negotiating'.[312] Thus, at 'regional preparatory meetings (…), calls were made for the development of an international convention on cybercrime', which the working paper supported.[313] Subsequently, in December 2010, the United Nations General Assembly adopted a resolution in which it

> '*Requests* the Commission on Crime Prevention and Criminal Justice to establish (…) an open-ended intergovernmental expert group (…) to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.'[314]

The expert group was established and in its first meeting in 2011 'agreed that the decision on whether a global instrument should be developed will be made after the [comprehensive] study was conducted.'[315] A draft of the comprehensive study, released in February 2013, listed numerous binding and non-binding regional cybercrime-combating instruments – in addition to the Cybercrime Convention, for example, the Commonwealth of Independent States (CIS) Agreement on Cooperation in Combating Offences related to Computer Information (2001) and the League of Arab States Convention on Combating Information Technology Offences (2010) – but observed that no single instrument 'has received signatures or ratifications/accessions with global geographic reach' (with the exception of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, which has a limited substantive scope).[316] The study indicated that there was 'insufficient harmonization of "core" cybercrime offences, investigative powers, and admissibility of electronic evidence', and proposed as possible policy options to develop 'a multilateral instrument on international cooperation regarding electronic evidence in criminal matters' and/or 'a comprehensive multilateral instrument on cybercrime'.[317] At the second meeting of the Expert Group in February

[308] Two of the four key purposes of the United Nations as an organisation, justifying its existence, are to 'achieve international co-operation in solving international problems of an economic, social, cultural or humanitarian character' and to be a forum for the 'harmonizing' of states' actions towards common goals. Article 1 UN Charter.
[309] General Assembly resolution 415 (V) of 1 December 1950.
[310] The CCPCJ was established by the Economic and Social Council (ECOSOC) resolution 1992/1, upon request of General Assembly (GA) resolution 46/152.
[311] Un Commission on Crime Prevention and Criminal Justice, 'Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime. Working paper': United Nations, 2010), at 11.
[312] Ibid., at 12.
[313] Ibid., at 12, 15.
[314] UN General Assembly Resolution 65/230, 21 December 2010.
[315] Gercke, 'Understanding cybercrime', at 120.
[316] United Nations Office on Drugs and Crime (Unodc), 'Comprehensive Study on Cybercrime, Draft', at 65-67.
[317] Ibid., at xii.

2013, although there was broad support for a UNODC role in capacity-building and technical assistance, '[d]iverse views were expressed regarding the content, findings and options presented in the study', suggesting that a consensus on the direction of a comprehensive multilateral instrument is not within sight.[318] Although the open-ended expert group has been asked to 'continue its work towards fulfilling its mandate',[319] the group is currently awaiting funding for translation of the draft study and comments by Member States,[320] and a date has not been set for a third meeting. It is therefore – given these developments – highly uncertain, whether the work of the expert group has real potential to lead to a new international legal instrument in the area of cybercrime. Given the current momentum of the Cybercrime Convention, that forum currently seems a more promising alternative space for harmonising and globalising cybercrime law (see *infra*, section 5.1.2).

Nevertheless, the issue of international co-operation in criminal justice matters and on 'alternative forms of co-operation' that go beyond extradition and mutual legal assistance remain on the CCPCJ's agenda. At a thematic discussion on international co-operation in criminal justice matters, on 13-14 May 2014, members of the CCPCJ explicitly discussed the need for further co-operation to address cybercrime.[321] Similarly, at a meeting of the same session, at which the CCPCJ reflected upon 'world crime trends', specific reference was made to the challenges posed by new technologies, specifically 'the challenges posed by various forms of cybercrime, including online financial crime, illegal access to computer systems, cyberbullying and the online exploitation of children'. According to the same report, '[m]any speakers highlighted the need for effective prevention, including (...) strengthened international cooperation to address such crimes.'[322] The threat posed to traditional forms of international criminal justice co-operation by cyberspace is clearly an issue of serious concern within the CCPCJ. This provides a platform for directing those concerns towards the need for cross-border data searches.

A concrete opportunity for putting the issue of cross-border access to data on the international agenda is the next CCPCJ Congress is in April 2015. While such events are not designed as a forum for law-making or for the discussion of detailed rules, the declarations that are drafted and issued during such congresses set the agenda for the next five-year period for international co-operation in the area of crime and criminal law. The topic of this conference, to be held in Doha, is very broadly formulated: 'Integrating crime prevention and criminal justice into the wide United Nations agenda to address social and economic challenges and to promote the rule of law at the national and international levels, and public participation'.[323] Having cloud-stored data explicitly acknowledged as a problem in the fight against crime in an article in the 2015 declaration would be an important recognition of the existence of a shared problem by states. Such recognition is not only a necessary first step in building a consensus on the existence of a problem, on the nature of the problem, and on possible solutions to it; it also provides some legitimacy to early adopters who seek to address the problem together or unilaterally – at least where such action does not cause (material) harm to other states. Such an opportunity for shaping the debate on cybercrime seems to present itself in the next Congress with the decision that one of the workshops of the Congress (Workshop 3) will focus on 'strengthening crime prevention and criminal justice responses to evolving forms of crime such as cybercrime and trafficking in cultural property, including lessons learned and international cooperation.'[324]

---

[318] UNODC, *Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 25 to 28 February 2013*, UNODC/CCPCJ/EG.4/2013/3, 1 March 2013, available at http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_3_E.pdf.

[319] Commission on Crime Prevention and Criminal Justice, Resolution 22/7, 2013. Also, Commission on Crime Prevention and Criminal Justice, Report on the twenty-third session (13 December 2013 and 12 to 16 May 2014), Economic and Social Council, Official Records, 2014, Supplement No. 10, E/CN.15/2014/20, p. 94.

[320] UNODC Organized Crime Branch, personal communication, 15 September 2014.

[321] Ibid., p. 81.

[322] Ibid., para. 77, p. 94.

[323] Ibid., p. 47.

[324] Ibid., p. 49.

The Netherlands is not currently a member of the CCPCJ and to have real influence on the agenda of the CCPCJ, it would ideally seek to be elected to the body.[325] Alternatively, the Netherlands could co-operate with a state with a similar approach to the problem of cross-border data that is a CCPCJ member, such as the United States or Italy. Influencing the agenda of the CCPCJ will require the construction of a narrative of cross-border searches that fits into and complements the CCPCJ's existing agenda. This agenda is focused on three key areas: combatting transnational organised crime, fighting terrorism, and tackling the trade in illegal drugs.[326] In addition, the topic of the 2015 Congress suggests that the relationship of crime and criminal justice to development ('social and economic challenges') is an important part of the current efforts of the CCPCJ. Success in directing attention to the problem of cross-border data searches – and in securing its inclusion in Congress declarations or future draft resolutions of the CCPCJ[327] – will depend to a large extent on the ability of would-be early adopters of tying their concerns into this existing agenda.

5.1.1.3. The ITU and the Internet Governance Forum

The Commission on Crime Prevention and Criminal Justice is not the only actor within the UN policy space. The International Telecommunications Union (ITU), for example, is also active in cybercrime law and policy. As part of its global cybersecurity agenda, the ITU has developed a toolkit and a guide for developing countries to assist 'in understanding the legal aspects of cybersecurity in order to move towards harmonizing legal frameworks';[328] and it has likewise commissioned a comprehensive report for this purpose.[329]

The ITU itself does not seem an appropriate forum to establish some international agreement on cyber-investigation, since its remit focuses more on the telecommunications infrastructure itself than on how the infrastructure is used. Nevertheless, the ITU has attempted to move into broader Internet governance issues, through two World Summits on the Information Society (WSIS), in Geneva (2003) and Tunis (2005).[330] Following the Tunis Agenda,[331] the UN Secretary-General set up the Internet Governance Forum (IGF) as a multi-stakeholder platform to discuss wider issues of Internet governance. The IGF's purpose is 'to support the United Nations Secretary-General in carrying out the mandate from the World Summit on the Information Society (WSIS) with regard to convening a new forum for multi-stakeholder policy dialogue'.[332] The multi-stakeholder approach encompasses a wide range of stakeholders from across the globe, including industry, government (both executive and legislative branches), international organisations, NGOs, and individuals who are interested in Internet governance. Its mandate includes broad Internet policy goals:

> 'Discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet.
>
> Facilitate discourse between bodies dealing with different cross-cutting international public policies regarding the Internet and discuss issues that do not fall within the scope of any existing body. (…)'[333]

Given the law-enforcement problems of cyberspace investigations to combat the serious threat of cybercrime (*supra*, section 3.4.1), it may well be argued that cross-border access to data

---

[325] Details on elections to the CCPCJ are available in a factsheet on the CCPCJ website: http://www.unodc.org/documents/commissions/CND/Membership/Fact_sheet_on_elections_and_membership.pdf.
[326] See Draft Resolution V: Rule of law, crime prevention and criminal justice in the United Nations development agenda beyond 2015, in Commission on Crime Prevention and Criminal Justice, E/CN.15/2014/20, p. 44-48.
[327] The CCPCJ drafts resolutions for the Economic and Social Council, which can then be put forward to the full General Assembly. This seems the most likely route to bringing a resolution to the General Assembly; see section 5.1.1.1 *supra*.
[328] International Telecommunications Union, 'Global Cybersecurity Agenda Brochure' (Geneva: International Telecommunications Union, s.a.), at 14.
[329] Gercke, 'Understanding cybercrime'.
[330] See http://www.itu.int/wsis/index.html.
[331] Tunis Agenda for the Information Society, 18 November 2005, WSIS-05/TUNIS/DOC/6 (Rev. 1)-E, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.
[332] http://www.intgovforum.org/cms/aboutigf.
[333] Tunis Agenda, *supra* n. 331, §72.

is a public policy issue of significant concern for the security and stability of the Internet. The multi-stakeholder character of the IGF may also make this a useful forum to discuss issues of cyber-investigation, since this ensures that the broad range of perspectives and implications – including technical aspects, human rights issues, and the interests of small or developing countries – can be taken up in policy development. At the same time, the general and multi-stakeholder character of the IGF makes it unlikely that agreement can be reached on police investigations, which always raise controversy as to how far they should be allowed. Moreover, only states can create obligations under international law, and the IGF cannot function as a platform for state-to-state decision-making. Thus, it cannot solve the sovereignty question, but it could serve as a useful forum for gaining wider acceptance, and thus legitimacy, for a more or less plausible account that some early-adopter states may advance for certain forms of cross-border access to data.

5.1.2. Actions in the context of the Cybercrime Convention

An alternative international platform for discussing and developing a policy framework for cross-border cyber-investigation is the Council of Europe, which has set the stage for harmonising cybercrime and cyber-investigation legislation with its Cybercrime Convention. Different opinions circulate in policy circles concerning the usefulness of the Cybercrime Convention as a basis for a global legislative approach, as opposed to developing a new instrument within the UN context. It may be relevant to observe that since the CPJPC 2010 working paper voiced concern over the limited reach of the Cybercrime Convention (*supra*, section 5.1.1.2), an additional twelve Council of Europe member states have ratified the convention (leaving Greece, Poland, Romania, Russia, Sweden, and Turkey as the only larger member states not to have ratified it). Moreover, five additional non-member states (Australia, Dominican Republic, Japan, Mauritius, and Panama) have ratified the Convention, giving it a rather more global reach than it had in 2010.[334] Moreover, the Council of Europe provided assistance to states to develop legislation that is harmonised with the Convention, supporting around 100 activities on all continents, and cooperating with almost 130 countries in cybercrime matters.[335]

The Council of Europe also has the support of the European Union in this regard. Responding to the comprehensive UN study, the EU voiced opposition to the idea of developing a new international instrument. It argued that the Cybercrime Convention is 'a very efficient international instrument' while negotiating a new instrument 'would prolong the response of the international community to the immediate need to strengthen existing forms of cooperation and could delay the adoption of new legislation in countries' that have already started adopting legislation modelled on the Cybercrime Convention.[336]

In light of these developments, we consider a multilateral approach to cross-border access to data within the context of the Cybercrime Convention, rather than in the context of the UN (in drafting a completely new instrument), as more likely to succeed. The fact that Russia is not on board the Convention is a significant drawback, but given its position (*supra*, section 4.1.3), the likelihood of Russia agreeing to a new international instrument that allows cross-border access to data without prior state consent is minimal in any event.

The Cybercrime Convention seems a more appropriate venue for a multilateral approach also for the simple reason that the Convention states have already taken steps towards developing a new instrument for cross-border searches in the form of discussing a Second Additional Protocol (*supra* section 4.1.3). Such a Protocol has a clear advantage of being able to focus narrowly on cross-border searches because it is auxiliary to the main Convention. As noted in the introduction to this section, the more limited the scope of a multilateral agreement, the easier it generally is to reach agreement between states. At the same time, a protocol also has the additional advantage of, while being auxiliary and hence limited, being capable of being designed as a free-standing instrument. What this would mean is that it would not be necessary for states to ratify the full

[334] Situation as of October 2014. See http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG for an overview of ratifications.

[335] Council of Europe, 'Cooperation against cybercrime: Progress made in 2012' (Strasbourg: Council of Europe, 2013).

[336] Delegation of the European Union to the Council of Europe, 'EU Statement on the UN study on cybercrime (26/02/2013)' (Strasbourg: European Union, 2013).

Cybercrime Convention in order to be eligible to join the Protocol. This would have the double advantage of enabling a limited, targeted content, while keeping the possible pool of ratifying states as wide as possible.

While we will not speculate here on the likely success or not of the Convention states agreeing a draft of a Second Additional Protocol, it is worth noting that the success of any draft in gaining broad global support from states will depend upon the creation of a plausible account within international law of *why* a strict interpretation of sovereignty undermines states' own interests and *how* it can be otherwise imagined. Moreover, the success of any draft will also depend, obviously enough, upon the content: where the Protocol is highly specific and limited in ambition, it will be easier to gain agreement on a draft and broad global support for the instrument. This avenue of possibility thus requires interested states to be clear on their priorities and to limit their scope to what they consider absolutely necessary to achieve those goals.

An alternative possibility within the Cybercrime Convention, which may offer greater possibility within the short term, concerns the existing article 32(b) of the Convention. As we discussed in section 4.2.3 above, it is possible to interpret the existing wording of article 32(b) as providing greater scope to LEAs, by interpreting the meaning of the term 'lawful and voluntary consent of the person who has the lawful authority' as covering accessing data with lawfully obtained credentials. A broader interpretation along the lines suggested in section 4.2.3 could be contained in a Guidance Note to article 32 of the Convention. A Guidance Note does not require the agreement of all parties to the Convention but is the product of the Cybercrime Convention Committee (T-CY). Such a Note, while not strictly authoritative unless all parties to the Convention explicitly acknowledge that they accept the interpretation that the Note contains,[337] can nonetheless provide some legitimacy to the actions of early adopters. Moreover, as a draft Note on article 32 is already being discussed, it may be possible to amend that Note rather than beginning the process of creating a new Note from scratch.

5.1.3. Other international action

The United Nations and the Council of Europe do not exhaust possibilities for action at the international level. For example, the Netherlands will host the fourth international Cyberspace Conference in 2015.[338] As this conference is being jointly organised by the Ministry of Foreign Affairs and the Ministry of Security and Justice, it seems to be an excellent opportunity to: 1) reiterate the challenges that cybercrime poses; 2) restate the conclusion of the CCPCJ that international co-operation is necessary to combat these challenges; 3) raise the importance of cross-border data searches in tackling (a limited list of) cybercrime(s), comprised of those most likely to gain broad international agreement, e.g., financial crime and crimes against children; 4) rehearse an alternative account of international law that allows for cross-border data searches and gain feedback on its plausibility from the wide array of stakeholders present at the conference.

5.2. Actions at the national level

5.2.1. Regulating cross-border searches

The Netherlands is taking steps to move forward in the area of cross-border access to data. There have been a few cases in which Dutch LEAs acquired cross-border access to computers of which the location was not (at least not with certainty) known,[339] which although widely published have not raised protests from the international community. Possibly triggered by the success of such cases, and being aware of the Belgian legislation,[340] the Dutch legislator is now proposing a power for Dutch LEAs to acquire cross-border access to data if the location of the data is not

[337] Under general international law, only the parties to a treaty can interpret that treaty unless its terms specify otherwise. Article 46 of the Cybercrime Convention that establishes the Committee does not grant it the authority to interpret the Convention on behalf of the parties to it.
[338] http://www.government.nl/news/2013/10/18/netherlands-to-host-international-cyberspace-conference-in-2015.html.
[339] *Supra*, section 4.1.2.
[340] *Supra*, note 206 and surrounding text.

known (and even leaves open the possibility of cross-border access if the location is known), without prior consent of the foreign state where the data reside.

5.2.1.1. The proposal

A draft Computer Crime III Bill was circulated for consultation in May 2013.[341] After the consultation, a somewhat revised draft was submitted to the Council of State for advice and, as of October 2014, the Ministry is finalising the Bill, taking into account the Council's advice, for submission to the Second Chamber. We base our discussion on the draft Bill as proposed in May 2013 and an internal draft version of the Explanatory Memorandum from September 2014, which is somewhat more elaborate than the May 2013 explanatory text. Note that the text may yet be adapted when the final Bill is submitted to Parliament.

The Bill contains a power in proposed article 125ja Dutch Criminal Procedure Code (DCCP) [Wetboek van Strafvordering] for remotely accessing computers, and using tools (such as trojan software, i.e. malware with a backdoor that is covertly installed on the remote computer) to investigate data, copy data, or block access to data (by deleting or encrypting the data). Although generally such a power would only be allowed to be used on Dutch territory (given the procedural territoriality principle embedded in the DCCP), the draft Explanatory Memorandum explains that this power may also be exercised if the location of data is unknown. According to the Memorandum, 'the factual location of data can in many cases not be reasonably determined. This happens especially frequently when almost all data are stored in the Cloud, or through the Internet behaviour of certain persons that is targeted at anonymity—and thus at not being able to retrieve a geographical place.'[342]

In the case of the data's location being unknown, the Memorandum considers unilaterally accessing, copying, or deleting the data to be compatible with international law:

> 'In such cases, a request for mutual legal assistance is impossible, since no state can be identified to which such a request can be directed. There is, then, no violation of the sovereignty of another state, nor is there a risk of reciprocity [i.e., that another state would retaliate or 'strike back', BJK/MG]. If the location of data is unknown, it would be objectionable to refrain from performing investigatory actions concerning the data; otherwise, this would mean that the Internet is an unregulated legal sphere and thus a free haven for crime. That is unacceptable.'[343]

The Explanatory Memorandum goes further, however, in suggesting that unilateral access may even be allowed if the location *is* known, provided that the Netherlands has material jurisdiction over the crime that is being investigated. This should happen within the boundaries of article 359a DCCP, which stipulates that investigation powers can be applied outside the (territorial) jurisdiction of a court (art. 359a(1)) but only to the extent that the law of nations and international law allow this (art. 359a(3)). Although the Memorandum does not explicitly say so, it suggests that international law allows some form of unilateral cross-border application of investigation powers to retrieve data. This suggestion lies in the fact that the Memorandum, in the paragraph directly following the remark about investigation powers being applicable outside the court's jurisdiction within the limitations of international law, emphasises that using coercive powers against *people* should follow procedures of mutual assistance, since 'independent action by the enforcing state is less likely given that the person at issue is not present on the territory of that state. The enforcing state cannot act without the help of the state in which the perpetrator is located (…)'.[344] Implicitly, the suggestion then is that when it comes to using coercive powers against *data*, mutual assistance does not necessarily have to be sought since there is no problem of factual need of assistance. Further on, the Explanatory Memorandum suggests more explicitly that, according to its drafters, international law allows, to some extent, unilateral cross-border access to data:

> 'Also in cases where the police does have knowledge of the factual location of data, it is possible—within the limits of article 359a DCCP and under condition of (extra)territorial jurisdiction [i.e., having

[341] http://www.internetconsultatie.nl/computercriminaliteit.
[342] Draft Explanatory Memorandum Computer Crime III Bill, unpublished version September 2014 (our translation).
[343] Ibid.
[344] Ibid., §2.8.1.

> material jurisdiction over a crime committed abroad]—to act independently. It will depend greatly on the nature of the actual act as to whether independent action by the enforcing state breaches international law. The nature and intensity of the mutual-assistance relationship with the state at issue is also relevant here.'[345]

The conclusion summarises the argumentation as follows:

> 'It is assumed that powers such as rendering inaccessible or securing data pertains to the own territorial power of disposition [i.e., jurisdiction to enforce, BJK/MG] insofar as Dutch criminal law is applicable to the offence under investigation [i.e., where there is material jurisdiction, BJK/MG]. The need for immediate action makes this inevitable and also well defensible under international law. This means that when the location of data storage is unknown, independent action is possible. Such action is moreover not excluded from the outset where the data location is known, depending upon the concrete facts and circumstances of the case.'[346]

5.2.1.2. Assessment of the proposal

The proposal is far-reaching and seems to rely more on pragmatic than doctrinal argumentation. The Explanatory Memorandum explains the current problem of cyber-investigation in relation to cloud data well and the urgency of finding ways to address the challenges is evident from the text. It then uses this argument, in particular the need for expediency and, in various cases, the difficulty or impossibility of mutual legal assistance, to conclude that unilateral cross-border access to data (provided there is material jurisdiction over the crime) is in principle allowed, or at least defensible, under international law.

That conclusion is not in line with our analysis in the previous chapters. The epistemological loss of location does not imply a factual loss of location: the data are still somewhere, and unilateral access in principle violates the sovereignty of the state, even though the state is not known and the state may not be aware of the unilateral data-access action. International law—in the dominant strict interpretation—considers any action on a state's territory by a foreign state as a breach of sovereignty, regardless of whether or not the action was intentional or whether or not the foreign state realised it was acting on the state's territory.[347] Exigency may excuse this, but only in extremely serious cases (notably, cases in which life is at risk), and this is much narrower than is suggested by the Explanatory Memorandum's 'need for immediate action' to prevent the Internet from becoming a free haven for crime in light of cloud developments.

Another aspect that is weakly addressed in the Explanatory Memorandum is reciprocity. If the Netherlands considers it compatible with international law to unilaterally access and delete data in accordance with the proposed law, it should expect other states to act in the same manner, and it cannot complain if other countries access or delete data on Dutch territory in this manner.[348] The Memorandum argues that this risk is negligible since, if the location of data is unknown, there is no particular foreign state that will retaliate or reciprocate. This, however, first ignores that, even though location data is unknown by the accessing state, it could nevertheless be known by the accessed state, possibly also at a later time, which is not totally unlikely if data are deleted rather than merely accessed. Second, and more importantly, the Memorandum confuses concrete single-case reciprocity with general reciprocity; and it ignores the latter. Although the Netherlands, if it unilaterally accesses or deletes data in an unknown state X, may perhaps not face reciprocal actions by state X directly in response to this particular action, it may well face reciprocal actions by X, or any other state for that matter, in general. Countries can, in response to the Dutch proposal being enacted, unilaterally access or delete data in the Netherlands in general, arguing that they were not aware that the data were stored in the Netherlands or that there were exigent circumstances that prevented seeking mutual assistance. This may not be problematic in cases that the Netherlands would also consider serious crime, but may well be problematic if the action relates to an investigation of something that the Netherlands does not consider a serious offence. It is questionable whether this general risk of reciprocal actions by any other state is sufficiently factored into the balance in the current proposal.

---

[345] Ibid., §2.8.2.
[346] Ibid., §2.8.4.
[347] *Supra*, section 4.2.
[348] *Supra*, section 4.3.7.

It should also be noted that the proposal goes further than the Belgian legislation in one important respect. Belgian law only allows copying data, in exigent circumstances, but not, as the Dutch proposal entails, deletion of data, which is a significantly stronger form of intrusion than copying. Moreover, Belgian law explicitly contains a requirement to notify the foreign state (if the state can be determined with reasonable effort); such a requirement is absent in the Dutch proposal.[349] Nor does the Memorandum provide any insight into how much effort Dutch police should make to find out where the data are located or, if the location is known, to seek mutual assistance; the Memorandum therefore seems to provide considerable discretionary room for the police to argue that the location is unknown or that the need for accessing or deleting data is too imminent to seek mutual assistance. Such discretionary room will not help to strictly limit the application of this form of trans-boundary law enforcement to cases where 'self-help' would be absolutely necessary.

For these reasons, although the proposed Computer Crime III Bill would seem a good starting point to raise international awareness and to take a first step in moving forward in this field as an early adopter of a new interpretation of international law, the proposed unilateral cross-border access to data is as yet insufficiently substantiated. It falls short of the standard required for a plausible account,[350] both in terms of a too shallow explanation of why the proposal is compatible with international law and in terms of limiting the proposed power to the minimum that is absolutely necessary. The proposal to unilaterally delete data and the suggestion that unilateral access might also be enacted in cases where the location of data is known go beyond what is absolutely necessary to collect digital evidence in the face of cloud computing and the challenges of cyber-investigation. The lack of sufficient safeguards (such as notification to the foreign state as soon as it becomes known where the data were located, or an international registry of performed actions; and a duty of demonstrable effort to determine the data location or to seek expedient mutual legal assistance) also diminish the plausibility of the account in the proposal.

5.2.2. Seeing things in a broader perspective

While stimulating both explicit recognition of the loss of knowledge of data location as a problem within international fora and the development of a plausible account for some—limited—form of unilateral access to data (section 5.2.1) provides a path to addressing some of the problems facing LEAs in investigating crimes in the cyber-era, the process will be long and slow and, if it succeeds, will only address part of the challenges. This is clearly unsatisfactory to those working in cyber-investigation practice, as this means that certain investigations into cybercrimes over which the Netherlands has substantive jurisdiction will run into the limits of enforcement jurisdiction. But this needs to be seen in perspective.

First, the rationale of international law needs to be taken into consideration. Although territory-based sovereignty may sound outdated to 21st-century netizens, it still serves a point in allowing each and every state—regardless of its ranking in the international power balance—to determine (within some limits set by international humanitarian law) what happens within its territory. And while it is common to see the state and its related sovereignty as a *cause* of problems at the international level, no other type of actor is currently able to combine the two essential features of accountability – capacity and legitimacy – to the same degree and in the same way. Put differently, states remain an essential part of the international landscape, protecting those within their jurisdiction and picking up the pieces when bad things happen. It is essentially within the broader interest of all that state agencies work within the framework of state sovereignty and not against it.

Second, the challenges of cyber-investigation in general are considerable and complex; the impact of international law is only one piece of the puzzle, and not necessarily the largest or most central piece. Many cybercrimes go un-investigated or unprosecuted not because of a lack of enforcement jurisdiction, but because the capacity of LEAs has limits in expertise and resources. While considerable investments have been, and are being, made to improve the capacity of LEAs to combat cybercrime, and the Netherlands is in relatively good shape compared to many other

[349] The Explanatory Memorandum (*supra* n. 342 at §2.8.3) mentions that the regular notification requirement applies, but this refers to notifying the persons that have an interest in the data, not the state on whose territory the data are stored.
[350] *Supra*, section 4.3.7.

countries in this respect, there are only so many investigations that can be conducted each year. A considerable additional number of cybercrimes might be effectively addressed with existing legal powers if more resources were available. This does not mean that we should simply leave the law as is, but it does mean that we should not focus all our attention on the current limits of the law if that means underestimating the current limits of the practical capacity of LEAs to enforce the law.

Third, the problem of unintended consequences is a well-known part of attempting to regulate anything and it is particularly problematic in a rapidly developing field such as technology.[351] What this means is that it would be unwise to focus on accessing cross-border data without viewing each context within its broader perspective and in the clear light of the goals to be achieved. For example, where absolute poverty pushes parents in developing countries into using their children in live web-cam sessions, interrupting the streaming might sometimes be more harmful to the children in the end, who could be removed from their home environment and put into prostitution at a truck-stop or a major urban area. If the goal is protecting children from sexual exploitation, the only sustainable approach will be one that addresses the absolute poverty that drives it. The challenges facing LEA agencies in the digital age must thus be viewed as a whole and prospective solutions considered in the light of a plurality of governmental goals, i.e., a whole-of-government approach.

Fourth, crime-fighting practitioners and policy-makers should realise that not all problems can be solved in real life. Enough food is produced every year to ensure that no one of the 7 billion people on the planet need go hungry, yet 1 billion of the world population face starvation on a daily basis and a second billion lack regular access to food such that they are physically and mentally stunted by the lack of nutrients. The fact that it is conceptually feasible to imagine a working system for unilateral cross-border access to data by LEAs does not mean that such a system can realistically be achieved in the current world order and certainly not within a short time-frame. We live in an imperfect world. Sometimes, this may mean that it is more productive to count one's losses and to focus attention on other regulatory challenges where progress is more feasible. In the present case, it might be a wise approach to actively contribute to the international debate and to take small first steps in cross-border access with a plausible account, but without setting too much hope on fundamental changes in the short term. International law develops slowly, even in the Internet age.

5.2.3. Overcoming misunderstandings

In our discussions during this research with those working in the field of cyber-investigation, we observed that there are various misunderstandings and gaps in basic knowledge about international law. This is not surprising given the nature of most legal education, which continues to focus overwhelmingly on national law,[352] and the likely recruitment patterns of LEAs, which will prefer graduates trained in the national law, rather than those who have specialised in international or global law. While some of this missing expertise can be provided by external specialists—as this report demonstrates—if officials within LEAs, who are best placed to understand investigation needs, are to be effective at developing and implementing a plausible alternative *international law* account of cross-border data access, they need a better awareness of the constraints and possibilities of international law. In the short-term, this need can be met by providing additional training for the relevant officials in international law as it relates to cross-border investigations. In the longer-term, recruitment policies may need to be adapted to take account of the need to hire more individuals with a greater knowledge of international and global law.

5.3. Conclusion

The analysis in this report leads to the conclusion that there are strict limits within international law for cross-border cyber-investigations. The dominant interpretation of international law implies

[351] Roger Brownsword and Morag Goodwin, *Law and the technologies of the twenty-first century: text and materials* (Law in context series; Cambridge, UK; New York: Cambridge University Press, 2012), 285-295.
[352] Most students in the Bachelor Rechtsgeleerdheid will have only six compulsory classes on international law in the whole of their bachelor education.

that accessing data that are, or later turns out to be, stored on a server located in the territory of another state, without prior consent of that state, constitutes a breach of the territorial integrity of that state and thus a wrongful act. The wrongfulness is not mitigated by the fact that the searching state may have difficulty in determining the location of data at the moment of access, nor by the consent of the user or the provider to access the data. The exceptions of exigency or distress might potentially apply in extreme circumstances, but not in the regular pursuit of criminal investigations. The only possibility for lawful cross-border cyber-investigation is where the foreign state has given prior consent, either for a specific search upon a specific request, or in a generic form for certain types of searches under certain conditions. The latter is the case with Article 32(b) of the Cybercrime Convention, which allows cross-border access to data with consent of the user or provider, if both countries are parties to the Convention. Overall, the possibilities of international law for cross-border access to data without prior consent of the foreign state are, in the strict interpretation of international law, very limited.

International law is not set in stone, however, and the first possibility of moving forward is to make efforts to change the status quo. The urgency of the need to do something about the increasing challenges of cyber-investigation, not least through the development of the cloud, seems increasingly felt. Cybercrime is high on the agenda of international policy-making institutions, including the UN's Commission on Crime Prevention and Criminal Justice. The 2010 UN General Assembly resolution calling, among other things, for proposals for new international legal or other responses to cybercrime[353] opens up pathways to discuss new instruments in which states agree to allow certain forms of cross-border access to data. Since the resolution, not much progress has been made in proposing new international legal responses to cybercrime; moreover, efforts within the UN may suffer from policy fragmentation as cybercrime legislation is also being discussed with the context of the ITU. The momentum for moving forward in developing a new legal instrument seems rather to lay with the Council of Europe in the context of the Cybercrime Convention, and in which already a protocol on cross-border access to data is being discussed.

In developing a new instrument, there is a necessary trade-off between substance and process: the less ambitious a proposal is in scope and substance, the easier it will be to persuade more states to agree to it. An instrument is also more likely to be successful if state concerns are adequately addressed about over-reaching powers and about lack of transparency. Strong safeguards should be built in, both relating to individuals in the context of data protection and human rights,[354] and in relation to concerns states have about the infringement of sovereignty. It will be necessary to reassure particularly those smaller or less powerful states who are likely to view cross-border data searches by states of the global North as threatening and as something from which they do not benefit. Therefore, in addition to clear limitations on the scope and content of data searches, attention should also be paid to benefit-sharing.

Another pathway that may be possible within the Council of Europe's Cybercrime Convention is to re-interpret article 32(b) as including the possibility of cross-border searches with lawfully obtained credentials, if the LEA from state A knows that the data are in state B and that B has ratified the Convention.[355] This interpretation needs to be agreed among the Cybercrime Convention member states before it can be accepted as a legitimate interpretation, but this could be done by agreeing on a Guidance Note, which may be easier than a new instrument that needs to be ratified by member states. This pathway provides a relatively limited exception to the general status of cross-border access to data under international law, as it applies only if the LEA knows, or has good reason to believe, that the data are stored on the territory of another signatory state, and it does not apply to cross-border data access without lawfully obtained credentials, so this should not preclude other pathways to create possibilities for cross-border access to data.

Seeing the changing landscape of the Internet and the rise of the cloud, which compounds already existing challenges to cyber-investigation, states should invest serious effort in

[353] *Supra*, note 314 and surrounding text.
[354] Note that a number of states have clearly flagged human rights concerns about transnational co-operation on criminal justice matters within the CCPCJ. See Commission on Crime Prevention and Criminal Justice, E/CN.15/2014/20.
[355] See the argument proposed *supra*, section 4.2.3.

developing some form of agreement on cross-border cyber-investigation. But such agreement will not be easy or expeditious, regardless of whether it concerns a treaty or a Protocol, within the UN or the Council of Europe. It simply concerns too complex and too sensitive an issue for some kind of consensus to be reached within the short term.

Therefore, a second possibility for moving forward is for one or a few countries to take the initiative and develop a certain practice of cross-border cyber-investigation, while at the same time advancing a plausible theoretical account of why these countries consider this practice compatible with international law. Such countries could be considered early adopters of an emerging practice that takes time to be accepted by the wider international community. While the strict legal interpretation remains that cross-border data searches are unlawful, a non-doctrinal approach to international law sees behaviour as being more or less justifiable depending upon the strength of the arguments that one makes. There are several more or less plausible arguments that can be made on the basis of existing legal regimes that could advance an alternative legal account of how states could better relate to one another within the space of the cloud to achieve shared aims.

Legal regimes that put claims based on territorial sovereignty aside are rare but not unheard of. The legal framework for outer space, and to satellite imaging in particular, suggests that where technology makes assertions of territorial sovereignty untenable and where states perceive a shared interest in an alternative framing principle, a new principle such as open skies can develop. Similarly, where the nature of a space, such as the oceans, limits states' ability to subject that space to territorial claims, states will co-operate to create a regime that ensures that such a space does not become a haven for criminals. These regimes can provide inspiration but also arguments to draw from, in developing an alternative account of cyberspace or the cloud in which some form of unilateral action within that space is plausibly acceptable.

To gather plausibility momentum, one or two states—better still, a group of states—need to forge ahead in developing an alternative legal account. Belgian law provides one step in that direction, and the current Dutch proposal another. The latter is, however, less plausible in its current form, as it does not limit itself to what can be considered the minimum intrusion necessary in cross-border cyber-investigations. The account can be improved by limiting the scope (e.g., only accessing but not deleting data; only for investigations into (almost) universally penalised serious crimes, such as child pornography), including more safeguards (e.g., notification to states where possible), and better substantiation (e.g., connecting cross-border access to data more explicitly and in more detail to existing legal regimes for non-standard spaces).

Where early adopters advance an alternative legal account for criminal investigation in cyberspace, it is crucial that they act openly in accordance with that account. The more forums in which an alternative account of the sovereignty question is presented and discussed—such as the Octopus conferences of the Council of Europe, the CCPPCJ Congress, the Internet Governance Forum, and the fourth international Cyberspace Conference in 2015—the more credence it may gain, even where it is not formally adopted. The more states that can be persuaded to similarly adopt the alternative account, the stronger the legal argument will become.

Further, other states are more likely to be reassured where early adopters are open about their actions and allow their actions to be overseen by an independent body. The inclusion of the role of the UN Secretary-General as a repository for satellite-owning states of all information of their satellites' trajectories in the Principles Relating to Remote Sensing of the Earth from Outer Space was an important factor in the Principles overcoming the sustained opposition of certain states. The United Nations, whether in the person of the Secretary-General or the CCPCJ, is likely to provide a greater level of reassurance, particularly to non-European states, than any other similar body. However, also within the Council of Europe context, attention can be paid to creating a mechanism by which early adopters are required to make public the nature and scope of searches that they conduct, i.e., a precise and detailed account of the types of searches that their legislation allows and of the safeguards that limit the scope and intrusion of these searches. Moreover, it would also help credibility and transparency if certain basic details of particular cross-border actions (such as date and time of access, type of crime under investigation, type and amount of data accessed, and some identifying information of the servers accessed) were deposited somewhere. The body overseeing the lodging of such information could take on a confidential role of notifying the affected states, when or as soon as it is known where the accessed information was located, or of allowing states to request information from the

overseeing body when they have reason to believe that servers on their territory may have been remotely accessed by foreign states.

Overall, international law therefore presents considerably larger limits than possibilities for cross-border cyber-investigations, and overcoming these limits and creating new possibilities will require much effort and patience. The focus of short-term efforts could be towards creating and enhancing the legitimacy of narrowly defined, transparently conducted, and strongly safeguarded unilateral actions of early adopters who advance an alternative account of sovereignty in cyberspace. At the same time, longer-term efforts can be undertaken that seek to create binding law at the international level in the form of an international or widely shared multilateral legal instrument allowing narrowly defined and strongly safeguarded forms of cross-border cyber-investigations. Neither will be an easy pathway to successfully solving the problems that cyber-investigation is facing in the cloud era, but both are necessary embarking upon if law enforcement is to move along in the 21st century.

Appendices

1. Workshop 19 December 2013

Participants

Name	Affiliation	Areas of expertise
Stephen Allen	Queen Mary, University of London, UK	International law, territoriality
Daniel Augenstein	Tilburg University, NL	International law, legal philosophy, transnational human rights
Charlotte Conings	Katholieke Universiteit Leuven, BE	criminal law
Reiner Franosch	Upper public prosecutor, Public Prosecutor's Office, Hessen, Germany	Internet crime
Morag Goodwin	Tilburg University, NL	International law; law & technology; global law
Paul de Hert	Vrije Universiteit Brussel, BE Tilburg University, NL	ICT law, criminal law, legal philosophy
Alex de Joode	Senior regulatory counsel, Leaseweb, NL	Internet, hosting
Simone van der Hof	Leiden University, NL	cyberspace law
Rik Kaspersen	Free University Amsterdam, NL	cybercrime law, Convention on Cybercrime
Merel Koning	Radboud University / PI.lab, NL	cyber-investigation law
Eleni Kosta	Tilburg University, NL	ICT law, cybersecurity
Aldo Kuijer	judge, Court of Appeal The Hague / Expertise centre cybercrime, NL	cybercrime
Bas van der Leij	WODC, Ministry of Security & Justice, NL	security & justice research
Philippe van Linthout	Investigative judge, Court of First Instance, Mechelen, BE	cyber-investigation
Bert-Jaap Koops	Tilburg University, NL	cybercrime law, ICT law
Lokke Moerel	Tilburg University, NL; De Brauw Blackstone Westbroek	transnational data protection law
David Nelken	University of Macerata, Italy King's College London, UK	criminal law, legal sociology, legal cultures, comparative law, transnational law
Carl-Wendelin Neubert	Max Planck Institute for Foreign and International Criminal Law, DE	cybercrime law
Jan-Jaap Oerlemans	Leiden University / Fox-IT, NL	cybercrime law
Philip Paiement	Tilburg University, NL	Legal philosophy, legal sociology, transnational law
Erik Planken	Ministry of Security & Justice, NL	cybercrime
David G. Post	Temple University, US	cyberspace law
Ulrich Sieber	Max Planck Institute for Foreign and International Criminal Law, DE	cybercrime law
Ian Walden	Queen Mary, University of London, UK	cybercrime law, ICT law
Lodewijk van Zwieten	National prosecutor cybercrime, Public Prosecutor's Office, NL	cyber-investigation

Workshop agenda

Workshop Cloud computing and cross-border criminal investigation: international law perspectives

Thursday 19 December 2013, 09:30-17:30
Amsterdam

09:30 – 10:00 Coffee, welcome
10:00 – 10:15 Introduction

10:15 – 12:30 **Part I. Theoretical approaches and developments**
Chair: Morag Goodwin
1. Classic interpretation of 'place', territory and jurisdiction in international law
2. 'Extra-territorialising' and 'de-territorialising' conceptions of sovereignty?
3. Conceptualising cyberspace and the cloud

12:30 – 13:30 Lunch

13:30 – 15:00 **Part II. Practical approaches and problems**
Chair: David Nelken
4. Classic interpretation of cross-border criminal investigation
5. Current practices of criminal investigation (in relation to the cloud)

15:00 – 15:30 Tea break

15:30 – 17:00 **Part III. Towards solutions**
Chair: Bert-Jaap Koops
6. Possible directions for solutions

17:00 – 17:30 Conclusions and future steps

The meeting is held under the **Chatham House Rule**: participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed. http://www.chathamhouse.org/about-us/chathamhouserule

Workshop discussion questions

1. Do existing principles of jurisdiction provide sufficient scope for addressing the "loss of location" problem associated with cloud computing?
2. Why does international law provide more room for extraterritorial jurisdiction to prescribe than for extraterritorial jurisdiction to enforce? What does this difference tell us about our understanding of "sovereignty"?
3. Can the duty element of territorial sovereignty i.e. not only the right but the duty to assert effective control within one's territory, be interpreted as allowing other states to 'intervene' where a state cannot or refuses to assert effective control over the use of the cloud for criminal purposes (where a server, corporation or individual able to assist in the investigation is located on their territory)?
4. Is there a risk, should certain stages agree to co-operate in cloud investigations, of the so-called 'Delaware effect', should certain states agree, whereby corporations 'move' to the location with the least regulation?
5. Has the 'diffusion' of sovereignty changed the underlying notion of what sovereignty is?
6. How does the fragmentation of international law into specialised functional regimes affect our understanding of cyberspace as a functional regulatory realm?
7. Is it possible to conceive of the Internet as the common heritage of mankind; or of a regime of regulation for cloud services based upon ideas of the common management of resources?
8. How can or should the cloud be conceptualised in terms of 'space' or 'place', in light of police activities (such as remote searches) 'taking place in' the cloud?
9. How can or should the cloud be interpreted in terms of 'territory', in light of the need to determine jurisdiction to enforce?
10. Does a criminal investigation by a country of data in the cloud (a cross-border search, or a production order to the cloud provider) impinge upon the sovereignty of other countries? If so, in what way?
11. Advanced cooperation in criminal matters, in which states compromise on the right to take autonomous decisions on all aspects of cases in return for enhanced efficacy and efficiency, seems to work largely in local settings: neighbouring countries with much cross-border interaction and a common socio-cultural background. How does that translate into cyberspace? Can the international community of cyber-investigators be considered a 'local' community with shared values and interests?
12. How should current practices of transborder access to data be assessed under international law?
13. What are the implications for non-signatory countries if certain countries (e.g., Cybercrime Convention parties adopting an additional protocol) were to create an agreement allowing for transborder access to data?
14. In regulating transborder access to data, what should be the role of situations where 'the location of data are not known', given that in cloud computing environments, the 'location of data' is by default unknown?
15. Does/ how does the general principle of estoppel[356] in international law impact on the legality of non-consensual cross-border data searches?
16. What fundamental rights questions are raised by the current practices of cross-border data searches?

[356] Although the precise usage of estoppel in international law is not clear, it frequently has the effect of making it impossible for a state to contradict its previous behaviour or statements. In other cases, it makes it difficult to do so.

2. Advisory committee

Prof. S. (Simone) van der Hof (chair)	eLaw@Leiden, Leiden University
E.J.H. (Eric) Planken	Netherlands Ministry of Security and Justice
L.J.A. (Lodewijk) van Zwieten	Netherlands Public Prosecutor's Office
Dr. J.B.J. (Bas) van der Leij	WODC

3. About the authors

Prof.dr. Bert-Jaap Koops is Professor of Regulation & Technology at the Tilburg Institute for Law, Technology, and Society (TILT), the Netherlands. His main research fields are cybercrime, cyber-investigation, privacy, and data protection. He is also interested in topics such as DNA forensics, identity, digital constitutional rights, 'code as law', and regulatory implications of human enhancement, genetics, robotics, and neuroscience. He co-edited eight books in English on technology regulation, including *Emerging Electronic Highways* (1996), *Cybercrime and Jurisdiction: A Global Survey* (2006), *Constitutional Rights and New Technologies* (2008), *Engineering the Human* (2013) and *Responsible Innovation*,Vol. 1 (2014). He has published many articles and books in English and Dutch on a wide variety of topics. His WWW Crypto Law Survey is a standard publication on crypto regulation of worldwide renown.

With a personal postdoc (1999), VIDI (2003) and VICI (2014) grant, Koops is one of the few Dutch researchers who received all three stages of NWO's (Netherlands Organisation for Scientific Research) personal research-grant scheme. From 2005-2010, he was a member of *De Jonge Akademie*, a young-researcher branch of the Royal Netherlands Academy of Arts and Sciences.

Dr. Morag Goodwin is Associate Professor at Tilburg Law School, the Netherlands. Her fields of interest include international law, notably law and development; international and European human rights law, with a particular interest in development and human rights; non-discrimination law; Roma in the European legal context; and law and technology. Her current work focuses on the phenomenon of global law, concepts of law and space in relation to participation in decision-making and questions of Romani exclusion in the context of Europe's Horizon 2020 project. She is Programme Director of the EU-funded European Joint Doctorate in Law and Development and series editor of the new Cambridge University Press series, *Global Law*.

Bibliography

Arendt, Hannah (1958), *The human condition* ([Chicago: University of Chicago Press).

Article 29 Working Party (2012), 'Opinion 05/2012 on Cloud Computing', (Brussels: Article 29 Data Protection Working Party), 27.

Balboni, Paolo and Pelino, Enrico (2013), 'Law Enforcement Agencies' activities in the cloud environment: a European legal perspective', *Information & Communications Technology Law,* 22 (2), 165-90.

Bernstoff, J. Von (2003), 'Democratic Global Internet Regulation? Governance Networks, International Law and the Shadow of Hegemony', *European Law Journal,* 9 (511).

Birk, Dominik, Heinson, Dennis, and Wegener, Christoph (2011), 'Virtuelle Spurensuche. Digitale Forensik in Cloud-Umgebungen', *Datenschutz und Datensicherheit,* (5), 329-32.

Boister, Neil (2002), 'Human Rights Protections in the Suppression Conventions', *Human Rights Law Review,* 2, 199.

Boyle, Alan and Chinkin, Christine (2007), *The Making of International Law* (Oxford University Press).

Bradshaw, Simon, Millard, Christopher, and Walden, Ian (2013), 'Standard Contracts for Cloud Services', in Christopher Millard (ed.), *Cloud Computing Law* (Oxford: Oxford University Press), 39-72.

Brems, Eva and Gerards, Janneke (2014), *Shaping Rights in the ECHR* (Cambridge University Press).

Brownlie, Ian (1973), *Principles of public international law* (Oxford: Clarendon Press).

Brownsword, Roger and Goodwin, Morag (2012), *Law and the technologies of the twenty-first century: text and materials* (Law in context series; Cambridge, UK; New York: Cambridge University Press) xxi, 469.

Calvarese, Paolo S. Grassi & Daniele (1995), "The Duty of Confidentiality of Banks in Switzerland: Where It Stands and Where It Goes - Recent Developments and Experience - The Swiss Assistance to, and Cooperation with the Italian Authorities in the Investigation of Corruption among Civil Servants in Italy (The "Clean Hands" Investigation): How Much Is Too Much?', *Pace International Law Review,* 7 (329).

Choo, Kim-Kwang Raymond, et al. (2007), *Future directions in technology-enabled crime: 2007-09* (Research and public policy series; Canberra: Australian Institute of Criminology) xxxi, 131 p.

Cicero, Marcus Tullius (1991), 'On Duties (De Officiis)', *Trans. MT Griffin and EM Atkins. New York: Cambridge University Press*.

Committee of Experts on the operation of European conventions on co-operation in criminal matters (PC-OC) (2009), 'Summary of the replies to the questionnaire on Mutual Legal Assistance in Computer-Related Cases', (Strasbourg: Council of Europe).

Conings, C. and Oerlemans, J.J. (2013), 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?', *Computerrecht,* (1), 23-32.

Cottier, Thomas (2012), 'The Emerging Principle of Common Concern: A brief outline'.

Council of Europe (2008), 'Guidelines for the cooperation between law enforcement and internet service providers against cybercrime, adopted by the global Conference Cooperation against Cybercrime, 1-2 April 2008', (Strasbourg: Council of Europe).

--- (2013), 'Cooperation against cybercrime: Progress made in 2012', (Strasbourg: Council of Europe).

Cuthbertson, Shannon (2012), 'Mutual assistance in criminal matters: cyberworld realities', in Saskia Hufnagel, Clive Harfield, and Simon Bronitt (eds.), *Cross-border law enforcement: regional law enforcement cooperation - European, Australian and Asia Pacific perspectives* (Abingdon, Oxon; New York, NY: Routledge), 127-42.

Cybercrime Convention Committee (T-CY) (2008), 'Compilation of responses to questionnaire for the parties concerning the practical implementation of the Cybercrime Convention', (Strasbourg: Council of Europe).

--- (2013a), 'T-CY Guidance Note # 3. Transborder access to data (Article 32), Draft for discussion by the T-CY', (Strasbourg: Council of Europe).

--- (2013b), '(Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding transborder access to data', (Strasbourg: Council of Europe).

--- (2013c), 'Cybercrime Convention Committee (T-CY) 9th Plenary, Strasbourg, 4-5 June 2013. Abridged meeting report', (Strasbourg: Council of Europe).

De Hert, Paul and Gutwirth, Serge (2009), 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalization in Action', in Serge Gutwirth, et al. (eds.), *Reinventing Data Protection?* (Berlin: Springer), 57-71.

De Schepper, Kristel and Verbruggen, Frank (2013), 'Ontsnappen *space invaders* aan onze *pacmannen*? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners', *Tijdschrift voor Strafrecht,* (2), 143-66.
De Schutter, Olivier (2014), *International Human Rights Law: Cases, Materials, Commentary* (2nd edn.: Cambridge University Press).
Delegation of the European Union to the Council of Europe (2013), 'EU Statement on the UN study on cybercrime (26/02/2013)', (Strasbourg: European Union).
Dicken, P. (1998), *Global Shift: Transforming the World Economy* (3rd Edition edn.; London: Sage Publications).
Evans, Malcolm D. (2006), *The Law of the Sea*, ed. Malcolm D. Evans (International Law; Cambridge: Cambridge University Press).
Feder, H. (1990), 'The Sky's The Limit? Evaluating the International Law of Remote Sensing', *New York University Journal of International Law and Policy,* 23 (599).
Fijnaut, Cyrille (2012), 'The globalisation of police and judicial cooperation: drivers, substance and organisational arrangements, political complications', in Saskia Hufnagel, Clive Harfield, and Simon Bronitt (eds.), *Cross-border law enforcement: regional law enforcement cooperation - European, Australian and Asia Pacific perspectives* (Abingdon, Oxon; New York, NY: Routledge), 1-15.
Fuller, L. L. (1964), *The Morality of Law: Revised Edition* (New Haven: Yale University Press).
Geist, Michael A. (2001), 'Is There a There There? Toward Greater Certainty for Internet Jurisdiction', *Berkeley Technology Law Journal,* 16, 1345-406.
Gercke, Marco (2012), 'Understanding cybercrime: phenomena, challenges and legal response', (Geneva: ITU), 356.
Goldsmith, Jack L. (1998a), 'Against Cyberanarchy', *University of Chicago Law Review,* 65, 1199-250.
--- (1998b), 'The Internet and the Abiding Significance of Territorial Sovereignty', *Indiana Journal of Global Legal Studies,* 5, 475-91.
Goodwin, Morag (2006), 'The Romani claim to non-territorial nationhood: taking legitimacy-based claims seriously in international law', (Florence).
Hardin, Garret (1968), 'The Tragedy of the Commons', *Science,* 162 (1243).
Hufnagel, Saskia (2012), '(In)security crossing borders: a comparison of police cooperation within Australia and the European Union', in Saskia Hufnagel, Clive Harfield, and Simon Bronitt (eds.), *Cross-border law enforcement: regional law enforcement cooperation - European, Australian and Asia Pacific perspectives* (Abingdon, Oxon; New York, NY: Routledge), 177-208.
Hunter, Dan (2003), 'Cyberspace as Place and the Tragedy of the Digital Anticommons', *California Law Review,* 91 (2), 439-519.
International Telecommunications Union (s.a.), 'Global Cybersecurity Agenda Brochure', (Geneva: International Telecommunications Union).
Jakhu, R (2003), 'International Law Governing the Acquisition and Dissemination of Satellite Imagery', *Journal of Space Law,* 29 (65).
Jennings, R. Y. (1963), *The acquisition of territory in international law* (Manchester; New York: Manchester University Press ; Oceana Publications).
Johnson, David R. and Post, David G. (1996), 'Law and Borders – The Rise of Law in Cyberspace', *Stanford Law Review,* 48, 1367-402.
Kaspersen, H. W. K. (2009), 'Cybercrime and Internet jurisdiction. Discussion paper (draft)', (Strasbourg: Council of Europe Project on Cybercrime).
Keating, M. (2001a), *Plurinational Democracy. Stateless Nations in a Post-Sovereignty Era* (Oxford: Oxford University Press).
--- (2001b), ''Nations without States: The Accommodation of Nationalism in the New State Order'', in M. Keating & J. McGarry (ed.), *Minority Nationalism and the Changing International Order* (Oxford: Oxford University Press).
Kennedy, D. (1987), *International Legal Structures* (Baden-Baden: Nomos).
Kiss, A. (1997), 'The Common Concern of Mankind', *Environmental Policy and Law,* 27/4 (244).
Klabbers, J. (2013), *International Law* (Cambridge: Cambridge University Press).
Kleiven, Maren Eline (2012), 'Nordic police cooperation', in Saskia Hufnagel, Clive Harfield, and Simon Bronitt (eds.), *Cross-border law enforcement: regional law enforcement cooperation - European, Australian and Asia Pacific perspectives* (Abingdon, Oxon; New York, NY: Routledge), 63-71.
Koops, B.J. (2013), 'The role of framing and metaphor in the therapy versus enhancement argument', in Federica Lucivero and Anton Vedder (eds.), *Beyond Therapy v. Enhancement. Multidisciplinary analyses of a heated debate* (Pisa: Pisa University Press), 35-68.
Koops, Bert-Jaap, et al. (2012), 'Misdaad en opsporing in de wolken. Knelpunten en kansen van cloud computing voor de Nederlandse opsporing', (Tilburg / Den Haag: TILT / WODC).

Koskenniemi, M. (2005), *From Apology to Utopia: The Structure of International Legal Argument* (2nd Edition edn.; Cambridge: Cambridge University Press).
Kuan Hon, W. and Millard, Christopher (2013a), 'Cloud Technologies and Services', in Christopher Millard (ed.), *Cloud Computing Law* (Oxford: Oxford University Press), 3-17.
--- (2013b), 'How Do Restrictions in International Data Transfers Work in Clouds?', in Christopher Millard (ed.), *Cloud Computing Law* (Oxford: Oxford University Press), 254-82.
Kuan Hon, W., Millard, Christopher, and Walden, Ian (2013a), 'Negotiated Contracts for Cloud Services', in Christopher Millard (ed.), *Cloud Computing Law* (Oxford: Oxford University Press), 73-107.
--- (2013b), 'Public Sector Cloud Contracts', in Christopher Millard (ed.), *Cloud Computing Law* (Oxford: Oxford University Press), 108-41.
Ladeur, K-H. (2004), *Public Governance in the Age of Globalization* (Aldershot: Ashgate Pub Ltd).
Lakoff, George and Johnson, Mark (1980 (2003)), *Metaphors We Live By* (Chicago, London: University of Chicago Press).
Lauterpacht, H. (2011 [1933]), *The Function of the Law in the International Community* (Oxford: Oxford University Press).
Legg, Andrew (2012), *The Margin of Appreciation in International Human Rights Law: Deference and Proportionality* (Oxford University Press).
Leino, M. Koskenniemi & Päivi (2002), 'Fragmentation of International Law? Postmodern Anxieties', *Leiden Journal of International Law,* 15 (03), 553-79.
Lindahl, H. (2013), *Fault Lines of Globalization. Legal Order and the Politics of A-Legality* (Oxford: Oxford University Press).
Loughlin, M. (2013), 'Ten Tenets of Sovereignty', in Walker (ed.), *Sovereignty in Transition* (Oxford: Hart Publishing).
Lowe, Vaughan (2006), 'Jurisdiction', in Malcolm D. Evans (ed.), *International Law* (2nd edn.; Oxford: Oxford University Press).
McClean, J.D. (2012), *International co-operation in civil and criminal matters* (3rd edn.; Oxford, U.K.: Oxford University Press) xlviii, 366 p.
McVeigh, S. Dorsett & S (2012), *Jurisdiction* (Abingdon, Oxon; New York, NY: Routledge).
Mell, Peter and Grance, Timothy (2011), 'The NIST Definition of Cloud Computing', (Gaithersburg, MD: National Institute of Standards and Technology).
Milanovic, M. (2011), *Extraterritorial Application of Human Rights Treaties: Law, Principles and Policy* (Oxford: Oxford University Press).
Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime (1999), 'Principles on Transborder Access to Stored Computer Data', (Moscow: G8).
Moore, M. (2001), *The Ethics of Nationalism* (Oxford: Oxford University Press).
Muir, James A. and Van Oorschot, P.C. (2006), 'Internet Geolocation and Evasion', (Ottawa: School of Computer Science, Carleton University).
Mundlak, G. (2009), 'Deterritorializing Labour Law', *Law & Ethics of Human Rights,* 3, 189-222.
O'Floinn, Micheál (2013), 'It wasn't all white light before Prism: Law enforcement practices in gathering data abroad, and proposals for further transnational access at the Council of Europe', *Computer Law & Security Review,* 29, 610-15.
Odinot, G., et al. (2012), 'Het gebruik van de telefoon- en internettap in de opsporing', *Onderzoek en beleid* (304; Meppel: Boom Lemma), 302.
Ortony, Andrew (1993), 'Metaphor, language, and thought', in Andrew Ortony (ed.), *Metaphor and Thought* (2nd edn.; Cambridge, etc.: Cambridge University Press), 1-16.
Pulkowski, B. Simma & D. (2006), 'Of Planets and the Universe: Self-contained Regimes in International Law', *European Journal of International Law,* 17 (483).
Reuland, R. C. F. (1989), 'Interference with Non-National Ships on the High Seas: Peacetime Exceptions to the Exclusivity Rule of Flag-State Jurisdiction', *Vanderbilt ournal of Transnational Law,* 22 (1161).
Ruggie, J. G. (1993), "Territoriality and Beyond: Problematizing Modernity in International Relations', *International Organization,* 47 (139).
Ryngaert, Cedric (2008), *Jurisdiction in international law* (Oxford monographs in international law; Oxford; New York: Oxford University Press) xxiii, 241 p.
Sarah Joseph, Jenny Schultz & Melissa Castan (2013), *The international covenant on civil and political rights : cases, materials, and commentary* (Oxfrd: Oxford University Press).
Scholte, J. A. (2000), *Globalization: A Critical Introduction* (London: Macmillan).

Schön, Donald A. (1993), 'Generative metaphor: A perspective on problem-setting in social policy', in Andrew Ortony (ed.), *Metaphor and Thought* (2nd edn.; Cambridge, etc.: Cambridge University Press), 137-63.
Schreuer, Christoph (1993), "The Waning of the Sovereign State: Towards a New Paradigm for International Law", *European Journal of International Law,* 4.
Schwerha IV, Joseph J. (2010), 'Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers"', *Council of Europe Project on Cybercrime Discussion Paper* (Strasbourg: Council of Europe).
Seitz, N. (2004), 'Transborder search: A new perspective in law enforcement?', *International Journal of Communications Law & Policy,* 9 (2).
Shaw, Malcolm N (1982), 'Territory in International Law', *Netherlands Yearbook of International Law,* 13, 61-91.
--- (1997), 'Peoples, territorialism and boundaries', *Eur. J. Int'l L.,* 8, 478.
Slaughter, A-M. (2004), *A New World Order* (Princeton: Princeton University Press).
Spoenle, J. (2010), 'Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?', *Council of Europe Project on Cybercrime Discussion Paper* (Strasbourg: Council of Europe).
Spruyt, H. (1994), *The Sovereign State and Its Competitors* (Princeton: Princeton University Press).
Stahl, W.M. (2011), 'The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity', *Georgia Journal of International and Comparative Law* 40 (247).
Svantesson, Dan Jerker B. (2004), 'Geo-location technologies and other means of placing borders on the 'borderless' Internet', *Journal of Computer & Information Law,* 23, 101-39.
--- (2007), 'How Does the Accuracy of Geo-Location Technologies Affect the Law', *Masaryk University Journal of Law and Technology,* 2, 11-21.
Tak, P.J.P. (2000), 'Bottlenecks in International Police and Judicial Cooperations in the EU', *European Journal of Crime, Criminal Law and Criminal Justice,* 8 (4), 343-60.
Transborder Group (2012), 'Transborder access and jurisdiction: What are the options?, Discussion Paper', (Strasbourg: Council of Europe).
--- (2013), 'Report of the Transborder Group for 2013', (Strasbourg: Council of Europe).
UN Commission on Crime Prevention and Criminal Justice (2010), 'Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime. Working paper', (United Nations).
United Nations Office on Drugs and Crime (UNODC) (2013), 'Comprehensive Study on Cybercrime, Draft', (New York: United Nations).
Van der Hulst, R.C. and Neve, R.J.M. (2008), 'High-tech crime, soorten criminaliteit en hun daders - Een literatuurinventarisatie', (Den Haag: WODC).
Vodafone Group Plc (2014), 'Sustainability Report 2013/14', (Newbury, Berkshire: Vodafone).
Walden, Ian (2013), 'Law Enforcement Access to Data in Clouds', in Christopher Millard (ed.), *Cloud Computing Law* (Oxford: Oxford University Press), 285-310.
Walker, N. (2000), 'Flexibility within a metaconstitutional frame: reflections on the future of legal authority in Europe', in G. de Búrca & J. Scott (ed.), *Constitutional Change in the EU: From Uniformity to Flexibility* (Oxford: Hart Publishing).
--- (2003), 'Late Sovereignty in the European Union', in Walker (ed.), *Sovereignty in Transition* (Oxford: Hart Publishing).
Zielonka, J. (2003), 'Enlargement and the Finality of European Integration', in Mény & Weiler Joerges (ed.), *What Kind of Consitution for What Kind of Polity: Responses to Joschka Fischer* (Florence: Robert Schuman Center).