UNIVERSITEIT VAN TILBURG

Cyberspace, the cloud, and cross-border criminal investigation

The limits and possibilities of international law

Summary

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

Cyberspace, the cloud, and cross-border criminal investigation: the limits and possibilities of international law

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.