Chapter 7
Cybercrime, Evidence and Territoriality: Issues and Options

Jan Kleijssen and Pierluigi Perri

Abstract This chapter aims to explore policy proposals to deal with one of the most complicated problems posed by the Internet, namely that of jurisdiction. While cybercrime is a phenomenon without borders, the effective prosecution of such a crime is seriously hampered by conflicts of territoriality and jurisdiction. These problems are exacerbated by the evolution of information technology, in particular cloud computing which creates 'loss of location' problems for collecting the electronic evidence indispensable for prosecuting crime. The Cloud Evidence Group—a Working Group established by decision of the Cybercrime Convention Committee (T-CY) of the Council of Europe—has proposed, within the limits of agreed legal principles of territoriality and jurisdiction, a series of measures which, together with proper implementation of the Convention, would enable fast and effective access to electronic evidence, while respecting human rights and the rule of law.

Keywords Council of Europe · Cloud computing · Territoriality · Budapest Convention on Cybercrime · Location of data · Jurisdiction

Jan Kleijssen is Director of Information Society and Action against Crime at the Council of Europe. Pierluigi Perri is Associate Research Professor at University of Milan, and Advisor on Cybercrime at the Council of Europe. The views and opinions expressed in this contribution are those of the authors and do not necessarily reflect the official position of the Council of Europe.

J. Kleijssen (✉)
Information Society and Action Against Crime, Council of Europe, Strasbourg, France
e-mail: jan.kleijssen@coe.int

P. Perri
University of Milan, Milan, Italy
e-mail: pierluigi.perri@unimi.it

M. Kuijer and W. Werner (eds.), *Netherlands Yearbook of International Law 2016*, Netherlands Yearbook of International Law 47,
DOI 10.1007/978-94-6265-207-1_7

Contents

7.1 Introduction

Millions of attacks against computers and data are recorded each day worldwide. At the same time, only a very small fraction of computer-related crime or cybercrime,[1] that is offences against and by means of computers, is actually prosecuted and adjudicated.

The difference with other forms of crime, for example 'ordinary' crimes or transnational crimes, may be found in the specifics of cybercrime, which can be performed from a distance, using different methods to hide IP addresses[2] or electronic traces,[3] and may not be detected for a long time.[4] Moreover, the general understanding of 'crime' as such is different in many ways.

There are five elements that characterise cybercrime that should be recalled. First is the change of the *scena criminis*, which becomes intangible; second, the emergence of completely new types of crime (i.e. phishing);[5] third, the impact on law

[1] Defined here as offences against and by means of computer data and systems in the sense of Articles 2 to 11 of the Budapest Convention on Cybercrime, ETS No 185, 23 November 2001.

[2] The IP address is a unique address represented by a number, which identifies the device over the Internet. It is important to underline, with regard to criminal investigations, that an IP address identifies only the device and not the user behind it.

[3] One of the best known tools with which to achieve a good anonymization is TOR (The Onion Router), which is a network of computers (nodes) that distributes the transactions over several places on the Internet, so that it is almost impossible from one single node to trace the user.

[4] Consider, for example, the recent case of hacking of the SWIFT global banking system that affected at least twelve central banks like the Bank of Bangladesh, the Bank of Vietnam, the Bank of Philippines, the Bank of Ecuador and the Ukrainian Bank, with a loss of hundreds of million dollars.

[5] Phishing is one of the most widespread cybercrimes that consists of computer fraud to obtain sensitive information of the victim, such as credit card numbers, usernames and passwords for internet banking platforms, personal data of the victim, etc. According to the draft version of the Comprehensive Study on Cybercrime of UNODC (United Nations Office on Drug and Crime), '[i]ndividual cybercrime victimization is significantly higher than for "conventional" crime forms. Victimization rates for online credit card fraud, identify theft, responding to a phishing attempt, and experiencing unauthorized access to an email account, vary between 1 and 17% of the online population'. UNODC 2013, at 25.

enforcement procedures, requiring international co-operation between law enforcement agencies and a multi-stakeholder approach;[6] fourth, the decentralisation of the control over digital networks, which has major consequences for the identification of the country, company or place where the evidence is transmitted or stored; fifth, the openness and interdependence of the Internet, which creates shared vulnerabilities affecting all people accessing a specific digital network.[7]

Other types of crime may not always be sufficiently prosecuted, for lack of resources in case of ordinary crime or for lack of specific provisions in case of transnational crimes. However, cybercrimes are hardly ever prosecuted due to the difficulties connected with the very nature of the network and of the electronic evidence, which requires immediate access to the data as well as cooperation between the law enforcement agencies and the providers.[8]

Moreover, nowadays evidence in relation to any crime is increasingly available only in electronic form on computer systems or storage devices and needs to be preserved for criminal proceedings.[9] Criminal investigations not relying on electronic evidence are becoming the exception, not only for cybercrime but also for 'ordinary' crime, because virtually every investigation now involves digital evidence.[10] Access to electronic evidence—in relation to cybercrime and any other type of crime—is thus essential for criminal justice authorities as well as for ensuring the rule of law in general, which requires that there can be no overall impunity for criminals.

[6] Some provisions of the Budapest Convention on Cybercrime are focused on the cooperation between the Parties (see Articles 23 and 25).

[7] Balkin et al. 2007.

[8] There are different definitions of 'provider', according to the service that they deliver to their customers. In fact, under the general category of the Internet Service Provider (ISP), we can identify for example access providers, hosting providers, cloud providers, VoIP providers and content providers.

[9] For example, the recent disputes over the encryption of iPhones were not related to cybercrime but to cases of terrorism and drug trafficking. D Chmielewski (2016) Apple-FBI Encryption Battle Shifts to New York, 8 April 2016, http://www.recode.net/2016/4/8/11585978/apple-fbi-encryption-battle-shifts-to-new-york, accessed 20 January 2017.

[10] Kerr 2015. Already in this paper of eleven years ago, the Author argues how the law of criminal procedure must be changed as a result of the increasing number of cases based largely on digital evidence. The rise of the number of mobile and personal devices that store not only our personal information (i.e. e-mail, instant messaging contents, bank account movements) but also other information automatically (i.e. location, heart rate, circadian rhythm) combined with the spreading of this information on social network platforms, is creating a large amount of data related to the person under investigation that must be taken into account.

However, the matter is complex. A major problem is that electronic evidence is often not located in the territory of the investigating criminal justice authority. Data is increasingly stored on, mirrored on, or fragmented or moving between servers 'somewhere in the cloud', in possibly multiple or unknown jurisdictions, while criminal justice authorities are normally limited by the principle of territoriality.[11] Even if data is stored in the territory of an investigating authority and a server or device could be lawfully searched and seized, this will not be sufficient if the natural or legal person in possession or control of the data—that is, the person with the 'keys' to the data—is elsewhere.[12] The question, therefore, is how electronic evidence can be secured lawfully and effectively for criminal justice purposes while meeting human rights and rule of law requirements and respecting the principles of State sovereignty.

To address this question, in December 2014 the Cybercrime Convention Committee (T-CY)–the entity representing the Parties to the Council of Europe's Budapest Convention on Cybercrime–established a Cloud Evidence Working Group (CEG) which was tasked with identifying solutions by the end of 2016.[13] This contribution is based on the findings and recommendations of this Group.

---

[11] Usually, the starting point of this endless debate is identified in the paper by Johnson and Post published in 1996 in the Stanford Law Review 'Law and Borders—The Rise of Law in Cyberspace', in which the Authors argued that 'The rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behavior; (2) the effects of online behavior on individuals or things; (3) the legitimacy of a local sovereign's effort to regulate global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply' (see Johnson and Post 1996, at 1370). But the debate is still open and many scholars focus their research on the new challenges for the principle of territoriality in cyberspace, for example Goldsmith 1998; Reidenberg 2005; Bach and Newman 2006; Kulesza 2008; Schultz 2008; de Hert and Kopcheva 2011; Daskal 2015; Osula 2015; Svantesson and Gerry 2015; Svantesson and van Zwieten 2016; Zoetekouw 2016.

[12] The 'un-territoriality' of data in the cloud is, in fact, one of the most challenging problems for government authorities to search and seize digital evidence: firstly due to the difficulties of determining where the data is stored, so as to identify the applicable jurisdiction, and secondly due to the clash of different judicial systems. See Daskal 2015.

[13] The Cloud Evidence Group (CEG) was a Working Group established by decision of the Cybercrime Convention Committee (T-CY) in December 2014. The aim of this Group is to explore solutions on criminal justice access to evidence stored on servers in the cloud and in foreign jurisdictions, including through mutual legal assistance. The members of CEG are the members of the T-CY Bureau plus up to five extra additional members. The objective of the Cloud Evidence Group was to prepare a report on criminal justice access to data in the cloud. During its activity, the Cloud Evidence Group issued several reports, including the Guidance Note on Article 18 of the Budapest Convention (production order) and the final report "Criminal justice access to data in the cloud: recommendations for considerations by the T-CY", that are all published on http://www.coe.int/en/web/cybercrime/ceg (accessed 18 July 2017). During the last Plenary of 7-9 June 2017, the T-CY decided to follow one of the recommendations included in the final report and approved the Terms of Reference for an Additional Protocol to the Budapest Convention in order to help law enforcement to secure evidence on servers in foreign, multiple or unknown jurisdictions. This will be the second Additional Protocol to the Budapest Convention after the Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

7.2 Challenges

7.2.1 *Cybercrime and Electronic Evidence: The Globalization of Threats*

Reportedly, trillions of security incidents are noted on networks each year[14] and millions of attacks against computer systems and data are recorded every day.[15] The amount of daily news on ongoing threats is hard to follow.[16]

As pointed out by the members of the Cloud Evidence Group, cybercrime is not simply a matter of attacks against machines. A review of the current scale, scope and challenges related to cybercrime and electronic evidence (that is, evidence in the form of data generated by or stored on a computer system) suggests that cybercrime has become a serious threat to the fundamental rights of individuals, to the rule of law and to democratic societies.[17]

The theft and misuse of personal data processed and stored in electronic form (i.e. email account data, credit card details, address books, patient records, etc.) affect the right to private life (including the protection of personal data) of hundreds of millions of individuals. Recent examples of huge personal data breaches[18] include the theft of personal details of 37 million users—combined with extortion—from the website Ashley Madison,[19] of 15 million users from T-Mobile US, or of 150,000 customers of TalkTalk UK.[20] In May 2016, it was reported that the

[14] See Symantec Internet Security Threat Report, Volume 21, April 2016, http://www.symantec.com/deepsight-products, accessed 20 October 2016.

[15] See for example the Overview of current cyberattacks on Deutsche Telekom sensors, http://www.sicherheitstacho.eu/?lang=en, accessed 30 October 2016.

[16] To give an example, see the web page on the ongoing threats managed and constantly updated by the CERT-EU (Computer Emergency Response Team for the EU institutions, bodies and agencies): http://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html, accessed 30 October 2016.

[17] See T-CY 2015b, at 4.

[18] A personal data breach is defined by Article 4 of the EU General Data Protection Regulation (Regulation EU 2016/679) as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

[19] It is necessary to point out that the theft of subscribers' data from the Ashley Madison website is more sensitive if compared to other websites, considering that it is an online dating service and social networking service marketed to people who are married or in committed relationships. An unfortunate end of this story, among others, was the suicide committed by a pastor outed by the publication of Ashley Madison's account. Recently, the website settled the customer class action for 11.2 million dollars.

[20] See Talbot 2016.

passwords and sexual preferences of 40 million users[21] were up for sale on the dark web.[22]

Cybercrime thus represents an attack against the dignity and integrity of individuals, in particular children.[23] The Internet Watch Foundation, a UK independent organisation established in 1996 by the UK internet industry, recently reported a four-fold increase in child abuse imagery over the past two years[24] because new technologies reportedly help offenders groom and procure children for abuse and are 'fuelling a global boom in child sex tourism'.[25]

Other types of cyberattacks, such as distributed denial of service (DDOS) attacks,[26] website defacement[27] and others attacks aimed to compromise the availability of resources on the web, which can be used against media, civil society organisations, individuals or public institutions, also affect freedom of expression.

Consequently, cybercrime, even if carried out by ordinary criminals or terrorists, poses a grave threat to democracy and to our security. Governments, parliaments

[21] For more information, see J Murdock (2016) Fling.com Breach: Passwords and Sexual Preferences of 40 Million Users Up For Sale on Dark Web, IBTimes, 6 May 2016, http://www.ibtimes.co.uk/fling-com-breach-passwords-sexual-preferences-40-million-users-sale-dark-web-1558711, accessed 20 October 2016.

[22] Experts use the expression 'dark web' to identify websites that host illegal content and that are not indexed by normal search engines like Google, Yahoo!, Bing, etc. (the indexed web is called 'surface web'). The dark web is intentionally hidden, to some extent anonymous, and is inaccessible with the standard configuration of web browsers, requiring other tools to join in these websites and get the contents.

[23] *K.U. v Finland*, ECtHR, No. 2872/02, 2 March 2009.

[24] See Internet Watch Foundation (2015) Annual Report, https://www.iwf.org.uk/report/2015-annual-report, accessed 20 October 2016.

[25] See ECPAT (2016) Global Study on Sexual Exploitation of Children in Travel and Tourism, http://cf.cdn.unwto.org/sites/all/files/docpdf/global-report-offenders-move-final.pdf, accessed 21 October 2016.

[26] A distributed denial of service (DDOS) attack is an attack where multiple compromised servers are used to target a single system flooding it with many fake requests, with the result that the server becomes inaccessible for the legitimate users and the service is taken down.

[27] A defacement is an attack aimed to change the content of a webpage without the consent of the owner of the webpage. This type of attack is often used to cause reputational damages to companies or to spread political or other propaganda. For example, following the Charlie Hebdo attack of 7 January 2015, more than 20,000 websites in France were under attack, rendering websites inaccessible either by defacing them or by sending multiple requests to a server to render its services inaccessible. Another example are the attacks against the French channel TV5 that targeted their Facebook and Twitter accounts, Internet website as well as the broadcasting programme, shutting down the network for several hours. See J Campbell (2015) French TV network TV5Monde 'hacked by cyber caliphate in unprecedented attack' that revealed personal details of French soldiers, The Independent, http://www.independent.co.uk/news/world/europe/french-tv-network-tv5monde-hijacked-by-isis-hackers-in-unprecedented-attack-that-revealed-personal-10164285.html, accessed 21 October 2016.

and other public institutions as well as critical infrastructure[28] are faced with attacks every day that require specific competences and tools to investigate and contain possible damages. Last year, for example, the German Parliament was the victim of a cyberattack that infected 20,000 machines forcing the entire network to shutdown and set up a new system,[29] and recently ransomware[30] paralyzed a hydroelectric power plant in the United States by infecting its computer systems.[31]

In this scenario, where cybercrime is a direct threat to our societies, and information and communication technologies can be used to foster radicalisation and spread terrorist propaganda, the Internet serves as an echo chamber, and facilitates the process of radicalization,[32] criminal justice authorities are facing the problem that evidence in relation to almost any crime is now often stored in electronic form on computer systems placed abroad. In fact, the findings of a survey conducted by the Cybercrime Convention Committee (T-CY), involving 42 States that are Parties to the Convention, show that most international requests for data are related to fraud and financial crime, followed by violent and serious crimes. These may include murder, assault, smuggling of persons, trafficking in human beings, drug trafficking, money laundering, terrorism and the financing of terrorism, extortion and, in particular, child pornography and other forms of sexual exploitation and abuse of children.[33]

If we look at what could happen in the near future, with the Internet of Everything,[34] the widespread adoption of cloud services and the new forms of mobile payment, cybercrime can be expected to grow significantly.

At the same time, cybercrime is largely underreported. Among the offences reported and recorded by law enforcement authorities, only an infinitesimal part is

[28] 'Critical infrastructure' is defined by Article 2(a) of the Directive 2008/114/EC as 'an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions'.

[29] See C Von Ulrich (2015) Cyber-Angriff auf Kanzleramt und Bundestag, 7 January 2015, http://www.welt.de/politik/deutschland/article136114277/Cyber-Angriff-auf-Kanzleramt-und-Bundestag.html, accessed 21 October 2016.

[30] Ransomware is software able to restrict the access to a computer system and its content until a ransom is paid. Usually the ransomware encrypts the whole disk drive of the computer and show a message containing the procedure to pay the ransom and obtain the decrypting key.

[31] Lacy and Reed 2016.

[32] von Behr et al. 2013.

[33] T-CY 2013b, at 5.

[34] The Internet of Everything (IoE) is an evolution of the Internet of Things (IoT) and refers to a possible near future, in which everything will be connected: people, process, data, and things, intended as devices and consumer products. This 'hyperconnection' will improve the possibility to deliver services, but will also imply an incredible exposure of data that need to be protected. For more information please visit http://ioeassessment.cisco.com, accessed 30 October 2016.

eventually investigated. Of these only a very small fraction is prosecuted and of these, again, only a few are adjudicated.[35]

The *de facto* impunity of the perpetrators and the massive violations of the rights of victims of cybercrime are compelling reasons why it is urgent to provide concrete solutions to criminal justice authorities regarding the question of access to data in the cloud. One of the key messages at the occasion of the Octopus Conference organized by the Council of Europe in 2015 was that

> [t]he protection of victims and their rights should be put at the forefront in order to ensure the effectiveness of the criminal justice system. The impact of victims is often underestimated. More co-operation amongst law enforcement, private sector and victim services is needed.[36]

As stated by the Cloud Evidence Group:

> If only a minuscule fraction of offences involving computer data and systems can be prosecuted, victims have a very limited expectation of justice. This raises questions regarding the rule of law in cyberspace.[37]

7.2.2 Cloud Computing, Territoriality and Jurisdiction

The nature of cybercrime calls for an effective access to electronic evidence in investigations. The problem of these investigations, however, can be summarized as follows:

- The resources available to criminal justice authorities cannot keep pace with the increasing number of devices, services, users and victims of cybercrime.
- A range of technical challenges render investigations complex, including peer-to-peer networks, The Onion Router (TOR) and other anonymisers, the widespread use of encryption,[38] Voice over Internet Protocol (VOIP) or Carrier-grade Network Addressing Translators (CGN).[39]

[35] See Brown 2015. On this topic see also: Office of the Police and Crime Commissioner for Surrey (2015/16) South East Cybercrime Survey, https://www.cybersafesurrey.org/surveyresults, accessed 22 October 2016.

[36] See Octopus Conference 2015, Cooperation against Cybercrime, Key messages, http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680319026, accessed 22 October 2016.

[37] See T-CY 2015b.

[38] See C Metz (2016) Forget Apple vs the FBI: WhatsApp Just Switched on Encryption for a Billion People, 5 April 2016, http://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/, accessed 22 October 2016.

[39] See Huston 2013.

To complicate this scenario even more, cloud computing[40] and related questions about applicable law and jurisdiction add another layer of challenges that criminal justice authorities are confronted with.[41]

'Cloud computing' means that data—and thus also electronic evidence—is less held on a specific device or in closed networks but is distributed over different services, providers, locations and often jurisdictions. While in traditional computer forensics procedures, due to the centralized nature of the information technology system, investigators can have full control over the forensic artefacts (router, process logs, hard disks), in the cloud ecosystem, due to the distributed nature of the information technology systems, control over the functional layers varies among cloud actors, depending on the service model. Therefore, investigators have reduced visibility of and control over the forensic artefacts.[42]

Within this context, how can a State exercise its powers to investigate and prosecute? Is the principle of territoriality, firmly established in international law, still applicable?

The academic literature often considers the principle on territorial jurisdiction emerging from the famous *Lotus* case[43] as a general departure point for the study of public international law on conflict of jurisdiction between States.

In this case, on the one hand, the Permanent Court of International Justice (PCIJ) of 1927 determined that:

> 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.[44]

This principle means that a State cannot exercise its jurisdiction outside its territory, unless an international treaty or other laws permit to do so.

On the other hand, the PCIJ established as second principle that, within its territory, a State may exercise its jurisdiction on any matter even if there is no specific rule of international law permitting it to do so. With this principle, States have a wide measure of discretion in exercising their jurisdiction, unless it is expressly limited by some rules of international law.

---

[40] The definition of 'cloud computing' provided by NIST, a branch of the US Department of Commerce responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, is: '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.' See Mell and Grance 2011.

[41] See Narayanan 2012.

[42] See NIST 2014.

[43] *Case of the S.S. 'Lotus' (France v Turkey)*, PCIJ Series A, No 10, 7 September 1927 ('*Lotus*').

[44] Ibid., at 18–19.

The case, and the related issues about jurisdiction, was summarized by the Court as follow:

> The French Government contends that the Turkish Courts, in order to have jurisdiction, should be able to point to some title to jurisdiction recognized by international law in favour of Turkey. On the other hand, the Turkish Government takes the view that Article 15 allows Turkey jurisdiction whenever such jurisdiction does not come into conflict with a principle of international law.[45]

Within this framework, the Court issued its famous *dictum* about the nature of international law as permissive or prohibitive, stating that:

> International law governs relations between independent States. The rules of law binding upon States therefore 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. Restriction upon the independence of States cannot therefore be presumed.[46]

There are three possible interpretations of the *Lotus* principle about jurisdiction: the first is that the principle must be used as residual: when there are no other governing principles or rules of international law, States are free to act as they please; the second is that the *Lotus* principle could be intended as a residual principle with a presumption attached that, when it is not clear which international rule can be applied to a situation, it is possible to presume that there are no rules and that the States are free to act; the third possible interpretation, finally, is that the *dictum* of the PCIJ means that States are presumed to be unrestrained by international law, unless there are some rules providing such restraint.[47]

The *Lotus* principles, however, have been subjected to criticism by legal doctrine[48] and jurisprudence,[49] but despite their 'vagueness and generality'[50] are still

[45] Ibid., at 18.

[46] Ibid.

[47] This reflect the dissenting opinion posed by Judge Loder who commented that '[…] every door is open unless it is closed by treaty or by established custom' (*Lotus* case, Dissenting Opinion by M. Loder, at 34).

[48] Handeyside 2007.

[49] In the *Kosovo* Advisory Opinion, Judge Simma disagreed with the methodology used by the Court for deciding the case, which derive from the *Lotus* principles. In particular, he criticized the principle, declaring that 'by upholding the *Lotus* principle, the Court fails to seize a chance to move beyond this anachronistic, extremely consensualist vision of international law. The Court could have considered the scope of the question from an approach which does not, in a formalistic fashion, equate the absence of a prohibition with the existence of a permissive rule; it could also have considered the possibility that international law can be neutral or deliberately silent on the international lawfulness of certain acts.' *Accordance with international law of the unilateral declaration of independence in respect of Kosovo*, Advisory Opinion of 22 July 2010, Declaration of Judge Simma, para 3.

[50] Brownlie 2003, at 301.

considered valid in judgements concerning jurisdictional conflicts,[51] even if these principles were rarely used by the International Court of Justice.

Concerning cyberspace and the relevance of the *Lotus* case to address the problems posed by the new technologies, it may be useful to recall the general principle stated by PCIJ in the *Lotus* case about jurisdiction:

> Though it is true that in all systems of law the principle of the territorial character of criminal law is fundamental, it is equally true that all or nearly all these systems of law extend their action to offences committed outside the territory of the State which adopts them, and they do so in ways which vary from State to State. The territoriality of criminal law, therefore, is not an absolute principle of international law and by no means coincides with territorial sovereignty.[52]

The implications of this principle applied to cloud computing are highly relevant, if the bottom line is that States are not limited to their territorial boundaries in applying their laws,[53] but of course it is clear that other boundaries need to be identified to guarantee respect for the rule of law.

The problem of jurisdiction in cyberspace is still an issue before international courts, and it was recently addressed by the European Court of Justice in Case C-618/15, where the Advocate General Wathelet noted that '[t]he issue of crime committed on the internet ("cybercrime") is not a straightforward one inasmuch as, since the internet is a network which is by definition universal, the location of such crime, be it the causal event or the loss sustained, is particularly difficult to determine.'[54]

---

[51] Ireland-Piper 2014.

[52] *Lotus* case, at 20.

[53] Some suggestions could come from other sources, like the Restatement of the Law (Third) of the Foreign Relations Law of the United States, that provides the following rules: '(2) Whether exercise of jurisdiction over a person or activity is unreasonable is determined by evaluating all relevant factors, including, where appropriate: (a) the link of the activity to the territory of the regulating state, i.e., the extent to which the activity takes place within the territory, or has substantial, direct, and foreseeable effect upon or in the territory; (b) the connections, such as nationality, residence, or economic activity, between the regulating state and the person principally responsible for the activity to be regulated, or between that state and those whom the regulation is designed to protect; (c) the character of the activity to be regulated, the importance of regulation to the regulating state, the extent to which other states regulate such activities, and the degree to which the desirability of such regulation is generally accepted; (d) the existence of justified expectations that might be protected or hurt by the regulation; (e) the importance of the regulation to the international political, legal, or economic system; (f) the extent to which the regulation is consistent with the traditions of the international system; (g) the extent to which another state may have an interest in regulating the activity; and (h) the likelihood of conflict with regulation by another state'. See Hixson 1988; and Swanson 2011.

[54] Opinion of Advocate General Wathelet delivered on 9 November 2016, *Concurrence SARL v Samsung Electronics France SAS and Amazon Service Europe Sàrl*, ECJ, Case C-618/15, ECLI: EU:C:2016:843, para 2. This case is just one of the newest discussed in front of a superior Court, but cases regarding the jurisdiction in cyberspace are quite numerous. We can cite, for example: *LICRA v Yahoo! & Yahoo France*, Tribunal de Grande Instance de Paris, 22 May 2000; *R v Töben*, BGH, 12 December 2000; *R v Perrin*, EWHC Criminal Division, 22 March 2002; *Arzneimittelwerbung im Internet*, BGH, 30 March 2006; *Persönlichkeitsverletzungen durch ausländische Internetveröffentlichungen*, BGH, 2 March 2010; *Vidal-Hall & Ors v Google Inc*,

This is why some have therefore called for a 'paradigm shift' and to abandon traditional concepts of jurisdiction corresponding to territorial sovereignty.[55] However, such a 'shift', if at all possible, will take a very considerable time. Meanwhile, therefore, the best and likely the only way forward would appear to be finding innovative solutions compatible with the *Lotus* principles of State jurisdiction.

Against this backdrop, a number of challenges have been identified for criminal justice in combating cybercrime, particularly with regard to the applicable law and the jurisdiction to enforce.[56]

The first challenge is about location of data to set the applicable law. Unfortunately, location is of limited relevance in cloud computing. A service provider may have its headquarters in one jurisdiction and apply the legal regime of a second jurisdiction while the data is stored in a third jurisdiction. Data may be mirrored in several, or move between, jurisdictions. It is unclear which legal regime applies and it is far from clear which rules apply for lawful access by criminal justice authorities.[57] If the location of data determines the jurisdiction, it is conceivable that a cloud service provider systematically moves data to prevent criminal justice access.

Moreover, a service provider may be under different layers of jurisdictions for various legal aspects related to its services at the same time. The sharing and pooling of resources is a key characteristic of cloud computing. Cloud services may entail a combination of service models (Cloud Software as a Service (SaaS), Cloud

(Footnote 54 continued)

EWHC, 16 January 2014; *Google Spain SL, Google Inc v Agencia Española de Protección de Datos*, ECJ Grand Chamber, 13 May 2014; *Yahoo! v Belgium*, Court of Cassation, P.13.2082.N, 1 December 2015.

[55] Svantesson 2015, at 79, proposes to focus on the following 'core principles':

'In the absence of an obligation under international law to exercise Jurisdiction, a State may only exercise jurisdiction where:

(1) there is a substantial connection between the matter and the State seeking to exercise jurisdiction

(2) the State seeking to exercise jurisdiction has a legitimate interest in the matter and

(3) the exercise of jurisdiction is reasonable given the balance between the State's legitimate interests and other interests.'

[56] See T-CY 2015b.

[57] This topic was recently discussed in front of the Second Circuit Court of Appeal in the case *Microsoft v United States*, USCA II Circuit, 14-2985, 14 July 2016, where the Court stated that the government cannot compel Microsoft, or other companies, to turn over customer emails stored on servers outside the United States. The main question presented was whether the Section 2703(a) of the Stored Communications Act (SCA)–the provision under which the government sought and received a search warrant for the email account–applies extraterritorially. The government argued that when the SCA used the word 'warrant', the statute was actually referring not to a traditional warrant, but to legal process or 'compelled disclosure' more akin to a subpoena. A warrant, according to the Second Circuit, and conceded by the government, has domestic boundaries. This important decision complicates even more an already uncertain framework. See Svantesson and Gerry 2015.

Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)) and it is often unclear which service provider—when providing one or more types of services—is in possession or control of which type of data (subscriber information, traffic data, content data) so as to be served a production order.

Cloud services also make unclear whether data is stored or in transit and thus whether production orders, search and seizure orders, interception or real-time collection orders are to be served.

The non-localised nature of cloud computing causes problems for live forensics (online forensics) and searches because of the architecture of the cloud (multi tenancy, distribution and segregation of data) as well as legal challenges related to the integrity and validity of the data collection, evidence control, ownership of the data or jurisdiction.[58]

In short, the Cloud Evidence Group identified these questions:

> What governs jurisdiction to enforce for criminal justice purposes: Location of data? Nationality of owner of data? Location of owner of data? Nationality of data owner? Location of data controller? Headquarters of a cloud service provider? Subsidiary of a cloud service provider? Territory where a cloud provider is offering its services? Laws of the territory where the data owner has subscribed to a service? The territory of the criminal justice authority?[59]

The crucial question to address is therefore which options are available to permit effective and lawful access to electronic evidence for criminal justice purposes? This question gives rise to a number of issues and options that will be briefly described in the next section of this chapter.

7.3 Issues and Recommendations for a Jurisdiction 'in the Cloud'

7.3.1 Issues

As stated in the introduction, the analysis of the issues and recommendations is based on the findings of the Cloud Evidence Group (CEG) of the Cybercrime Convention Committee (T-CY). The CEG consulted external experts from academia and private consultants. In light of the challenges posed by cloud computing to the territoriality principle, the Cloud Evidence Group identified the following specific issues.[60]

[58] See NIST 2014.

[59] See T-CY 2015b, at 15.

[60] See T-CY 2016a.

7.3.1.1 Types of Data Required

The first question that the CEG tried to address was: which type of data are necessary for investigating a computer-related crime? This topic is important because it involves data protection regulation[61] and is open to different regional approaches even in the EU, at least until the EU General Data Protection Regulation will be in force.

The CEG finds that criminal justice authorities typically need three types of data to investigate, that is:

- subscriber information[62] indicating the user of a service (such as a webmail account) and which may also include the login Internet Protocol (IP) address;
- traffic data;[63]
- content data.

The type of data most often needed in criminal investigations is 'subscriber information', that is less privacy-sensitive than traffic and in particular content data. Obtaining subscriber information therefore represents a lesser interference with the rights of individuals than obtaining other types of data.[64] However, this is not always reflected in domestic laws on access to evidence. In some States, the requirements for criminal justice access to subscriber information in specific investigations are rather low, while in others court orders may be required. This

[61] See Sect. 7.3.1.7.

[62] Defined in Article 18 of the Budapest Convention as follows:

'[…] the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

(a) the type of communication service used, the technical provisions taken thereto and the period of service;

(b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.'

[63] Defined in Article 1 of the Budapest Convention as follows: '[…] "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.'

[64] The same conclusions are reported in the Conference Report of the Presidency Conference 'Crossing Borders: Jurisdiction in Cyberspace' held in Amsterdam on 7–8 March 2016 (7323/16). On this specific issue, the conclusions of the policy experts and practitioners participating in the Conference are summarized as follows: 'Subscriber data is the most often requested type of data for the purposes of criminal proceedings, followed by traffic data and finally content data. It was acknowledged by participants that the interference with the rights of the investigated person is lower in the case of subscriber data compared to traffic data and content data and therefore a lighter regime for obtaining such data could be reasonably envisaged. It was concluded that this distinction should be systematically reflected in the current legal frameworks (both national and international) and that such a solution could substantially release pressure from the existing system for international cooperation for obtaining e-evidence.' (at 6).

affects domestic investigations and hampers international co-operation. In this sense, further harmonisation of rules for access to subscriber information is needed.[65]

In this context, it is also worth pointing out that subscriber information is normally held by private sector service providers and is typically obtained through production orders[66] that usually represent a lesser interference with the rights of individuals and the interests of third parties than the search and seizure of computer systems or the interception of communications.[67]

7.3.1.2 Mutual Legal Assistance to Obtain Data Required for Investigation

Connected with the problems of the data that are required for investigation is the issue of obtaining these data when stored outside of the country. Here the issues of territoriality and jurisdiction in the cloud come into play. As the jurisdiction to enforce is normally limited to the territory of the criminal justice authority, mutual legal assistance (MLA) is and is likely to remain the primary mean to obtain evidence located in foreign jurisdictions.

The Council of Europe has developed a large number of treaties on international co-operation in criminal matters, including in particular the European Convention on Mutual Assistance in Criminal Matters[68] and its Additional Protocols.[69] The application of these treaties is monitored by the Council of Europe Committee of Experts on the Operation of European Conventions on Co-operation in Criminal Matters (PC-OC). In order to facilitate the use by practitioners of the MLA treaties, the PC-OC developed guidelines on practical measures to improve co-operation in respect of transfer of proceedings[70] and a model request form for mutual assistance in criminal matters.[71] In addition, subject-matter specific treaties contain provisions

[65] See T-CY 2014.

[66] See Article 18 of the Budapest Convention.

[67] The production order aims to get some information in possession of a person—typically an Internet Service Provider or a telecommunication company—under request. This means that the amount of data is by itself less intrusive than in a search and seizure of computer systems or in an interception of communications, which can allow data dragnet. In fact, the production order must identify precisely the scope and the extension of the request.

[68] 1959 European Convention on Mutual Assistance in Criminal Matters, ETS No 030.

[69] 1978 Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, ETS No 099; 2001 Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, ETS 182.

[70] See PC-OC 2012.

[71] See PC-OC 2014.

on mutual legal assistance[72] such as the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse,[73] the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime[74] and the Convention on the Prevention of Terrorism.[75]

However, it seems that the feasibility of mutual legal procedures is limited with regard to electronic evidence in a cloud context. In 2013 and 2014, the Cybercrime Convention Committee (T-CY) carried out a detailed assessment of the functioning of the mutual legal assistance provisions of the Budapest Convention and concluded that 'mutual legal assistance procedures are considered too complex, lengthy and resource intensive, and thus too inefficient'[76] to permit effective measures against cybercrime and other offences involving electronic evidence, given the transnational and volatile nature of electronic evidence.[77] Therefore, the MLA process needs to be made more efficient in view of the scale of requests concerning electronic evidence and the volatility of such evidence.

7.3.1.3 'Loss of Location'

Apart from its shortcomings, situations also arise where mutual legal assistance is not a feasible option at all. For specific situations, such as where the origin of an attack is unknown, where servers in multiple jurisdictions are involved, or other 'loss of location' situations[78] where the principle of territoriality is not applicable, solutions need to be found, including transborder access to data in specific criminal investigations.

However, the current Article 32b of the Budapest Convention on transborder access to data is too limited because it requires knowledge on where the data are located. In fact, as noted by the T-CY, Article 32b would not cover situations where the data are not stored in another Party or where it is uncertain where the data are located, and a Party may not use Article 32b to obtain disclosure of data that is stored domestically.[79]

As pointed out by the Cloud Evidence Group, 'in the absence of international solutions, governments increasingly pursue unilateral solutions. This creates risks

[72] See PC-OC 2015.

[73] 2007 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No 201.

[74] 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, ETS No 141.

[75] 2005 Council of Europe Convention on the Prevention of Terrorism, CETS No 196.

[76] See T-CY 2013b.

[77] The same conclusions are drawn by some scholars. See Svantesson and van Zwieten 2016, at 673; Walden 2011, at 11.

[78] For example, in cloud computing it could happen that the provider does not know where the data are exactly located. On this issue see Vaciago 2011, at 7.

[79] See T-CY 2013a.

for State to State relations and the rights of individuals. A common international solution is required to provide a framework for lawful transborder access to data.'[80]

While Article 19.2 of the Budapest Convention requires Parties to authorise competent authorities to extend searches from an initial computer system to a connected system 'in its territory', this territorial limitation has been dropped in a number of States, including in Europe and in the United States. For example, a change of the US Federal Rule 41 of Criminal Procedure will allow remote searches if the origin of an attack 'has been concealed through technological means', with inevitable concerns from the civil rights associations.[81] Similarly in Europe the recent UK Investigatory Powers Act 2016 expressly allows the use of bulk equipment interference to obtain overseas-related communications, information or data.[82]

Thus, a clearer, generally accepted framework that includes conditions and safeguards for transborder searches is urgently required.

7.3.1.4 'Offering a Service in the Territory' of a State

Another problem typically posed by the ubiquitous nature of internet services is that a service provider or other natural or physical person located in the territory of a State, which is subject to the laws of that State, may have possession or control of data stored in another jurisdiction and may also be coerced to retrieve and produce such data.

A more complicated situation arises when a service provider is offering a service in the territory of a State without being present in the State. Examples are webmail, social media or cloud storage services. In this sense, some clarifications are needed as to when a service provider is indeed present or 'offering a service in the territory' of a State and is thus subject to a domestic production order or other type of coercive order. This would help clarify the applicable law and which jurisdiction has the power to enforce.

Moreover, if subscriber information can be obtained lawfully through domestic orders, the need for international co-operation and thus the pressure on the mutual legal assistance system would be reduced considerably.

7.3.1.5 'Voluntary Co-Operation' by Providers

Some providers—in particular US-based service providers—may respond directly to lawful requests for subscriber information by criminal justice authorities in other jurisdictions where they are offering a service. Voluntary disclosure of 'customer

[80] T-CY 2016a, at 2.

[81] See on this topic the action taken by the Electronic Frontier Foundation at the following URL: https://act.eff.org/action/stop-the-changes-to-rule-41, accessed 30 October 2016.

[82] For this Act also some civil rights associations have filled a complaint addressing the ECtHR for alleged violations of fundamental rights, especially Articles 8, 10 and 14 of ECHR.

records'—and of contents in emergency situations—is possible under US law, that is, the Electronic Communications Privacy Act.[83] Parties to the Budapest Convention—other than the US—send every year more than 100,000 such requests to Apple, Facebook, Google, Microsoft, Twitter and Yahoo. According to the result of a survey conducted between the Parties to the Budapest Convention, these companies disclose data in about 60% of all cases.[84]

While the voluntary disclosure of data by US providers is highly useful for criminal justice authorities worldwide, it raises a number of concerns. For example, providers tend to notify customers of such requests and this compromises investigations. Providers also frequently change their policies and procedures for data request, which makes co-operation volatile and unpredictable. It must be considered also that, in some States, data obtained in this way is not admissible as evidence in court.

Furthermore, such voluntary disclosure raises concerns regarding data protection and confidentiality requirements.[85] Therefore, European providers already do not disclose data directly to criminal justice authorities in foreign jurisdictions, and this protection could be enforced under the forthcoming EU General Data Protection Regulation. Again, to address this issue, a clearer and more stable framework is required.

7.3.1.6 Emergency Procedures

In certain circumstances, to prevent imminent danger to life and public security, emergency procedures would be needed to obtain electronic evidence stored in foreign jurisdictions through mutual legal assistance but also via direct co-operation with a service provider in a foreign jurisdiction. While such procedures are in place in the US and while US service providers may also disclose content in emergency situations, in most other Parties to the Budapest Convention this is not the case, as a recent survey conducted by the Cloud Evidence Group shows.[86]

7.3.1.7 Data Protection

The processing of personal data requires a legal basis. In principle, criminal justice authorities can access, collect, share or otherwise process data if provided for by law. The international sharing of a personal data would be lawful if it is based on bilateral or multilateral co-operation agreements. The mutual legal assistance process is designed to ensure that rule of law requirements are met and that the rights of

[83] 18 U.S. Code §2702.
[84] See T-CY 2016b.
[85] See Sect. 7.3.1.7.
[86] See T-CY 2016c.

individuals are protected, in particular if the data sought are to be used as evidence in criminal proceedings.

At present, out of 49 Parties to the Budapest Convention,[87] 40 are Parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,[88] and 25 are member States of the European Union and thus subject to European data protection rules.[89] At the Council of Europe level, the negotiation of an Amending Protocol[90] to modernise the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data is ongoing. However, the question of transborder disclosure of data from a private sector entity in one Party to the criminal justice authority of another Party, that is the asymmetric transfer of data, is not specifically addressed at present.

7.3.2 Recommendations

Several approaches are proposed in the academic literature[91] trying to provide a solution to the issues described above, and the Council of Europe's Cloud Evidence Group suggested to pursue several specific options that combine immediate and practical measures with the negotiation of an Additional Protocol to the Budapest Convention on Cybercrime. The analysis of these options is valuable because they must take into account the suggestions and the complexities coming from the Parties of the Budapest Convention.

---

[87] See the Chart of signatures and ratifications of the Budapest Convention, Council of Europe Treaty Office, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=EIwx3ZYf, accessed 30 October 2016.

[88] 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No 108. See Chart of signatures and ratification of Convention 108, Council of Europe Treaty Office, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=etR46XGN, accessed 30 October 2016.

[89] The main data protection instruments referred to are the following: 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No 108; Council of Europe Recommendation R(87)15 Regulating the Use of Personal Data in the Police Sector; European Union Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data; Framework Decision 2008/977/JHA of the European Union on the Protection of Personal Data Processed in the Framework of Police and Judicial Co-Operation in Criminal Matters. At the European Union level, a new comprehensive data protection framework, the so-called new 'data protection package' was adopted in April 2016 and include the EU General Data Protection Regulation, which, among other things, will replace Directive 95/46/EC and which will be directly applicable in EU member States, and a Directive on data protection in the criminal justice sector.

[90] On this negotiation please see http://www.coe.int/t/dghl/standardsetting/dataprotection/Cahdata_en.asp and http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/CAHDat.%203_Report_CM(2015)40_En.pdf, accessed 30 October 2016.

[91] See Daskal 2015; Svantesson and van Zwieten 2016.

7.3.2.1 Rendering Mutual Legal Assistance More Efficient

Mutual legal assistance remains the accepted and primary tool to obtain evidence in foreign jurisdictions. In December 2014, the Cybercrime Convention Committee adopted a report with 24 recommendations.[92] The first fifteen of them fall under the responsibility of domestic authorities and do not necessarily require a new international legal instrument. Their implementation is primarily a question of resources, skills and streamlining procedures. States should also fully implement the provisions of the Budapest Convention, in particular Article 18 on domestic production orders and Articles 16, 17, 29 and 30 on expedited preservation.[93]

In particular, Recommendation 8 concerns emergency procedures: 'Parties are encouraged to establish emergency procedures for requests related to risks of life and similar exigent circumstances. The T-CY should document practices by Parties and providers.' Emergency procedures seem particularly important but are not available in most Parties.[94] If necessary, provisions for emergency procedures may need to be made available in the forthcoming second Additional Protocol to the Budapest Convention.

7.3.2.2 Domestic Production Orders (Article 18 Budapest Convention)

Article 18 of the Budapest Convention covers production orders with respect to two distinct situations. It would seem that this provision has not been fully understood and implemented by all Parties to the Budapest Convention. The Cloud Evidence Group has, therefore, drafted a Guidance Note for consideration by the Cybercrime Convention Committee,[95] which suggests the following:

- Under Article 18.1.a, competent authorities are to compel any natural or legal person to produce subscriber information in its possession or control irrespective of where the data are actually stored.[96]
- Under Article 18.1.b, competent authorities of a Party are to compel a service provider 'offering a service on its territory'[97] to produce subscriber information when:

---

[92] See T-CY 2013b.

[93] These provisions have not been fully implemented by all Parties as shown in assessments carried out by the Committee: http://www.coe.int/en/web/cybercrime/assessments, accessed 30 October 2016.

[94] See T-CY 2016c.

[95] T-CY 2015a.

[96] In fact, Article 18.1.a covers any type of data. However, the draft Guidance Note is focusing on subscriber information only.

[97] As reported into the final version of the Article 18 Guidance Note approved by the T-CY by written procedure last 20th of February 2017, Parties could consider that a service provider is 'offering a service in the territory of a Party' when the service provider enables persons in the territory of the Party to subscribe to its services and the service provider has established a real and

- the service provider enables persons in the territory of the Party to subscribe to its services;
- orients its activities at subscribers, or makes use of the subscriber information in the course of its activities, or interacts with subscribers in the Party;
- the subscriber information to be produced is relating to services of a provider offered in the territory of the Party.

If accepted, this interpretation of Article 18 could make a major difference at least with respect to subscriber information and offer a legal basis for the disclosure of such data by service providers in one State to the criminal justice authorities of a State where they are offering a service. As this is a domestic measure, it would considerably reduce the pressure on the mutual legal assistance system.

7.3.2.3 Practical Measures to Facilitate Co-Operation with Providers

Pending domestic legal measures and the negotiation of international legally binding instruments—namely the second Additional Protocol to the Budapest Convention—a number of practical measures may help improve consistency in the co-operation between US service providers and Parties to the Budapest Convention.

The Cloud Evidence Group held meetings with providers on 30 November 2015[98] and—in a less formal setting—on 25 April 2016. Proposals include: regular meetings of the Cybercrime Convention Committee with service providers; the establishment of an online tool with up-to-date provider policies and procedures as well as information on relevant legislation and criminal justice authorities responsible in the Parties; and common templates for requests for subscriber information.

Such increased co-operation with the private sector is also one of the expected results of the Internet Governance Strategy for 2016–2019 recently adopted by the Council of Europe Committee of Ministers,[99] that is to establish 'a platform between governments and major Internet companies and representative associations on their respect for human rights online, including on measures (such as model contractual arrangements for the terms of service of Internet platform, and principles of accountability and transparency to the multi-stakeholder community regarding the collection, storage, and analysis of personal data) to protect, respect

(Footnote 97 continued)

substantial connection to a Party. To identify this connection some factors could be the following: providing local advertising or advertising in the language of the territory of the Party, make use of the subscriber information in the course of its activities or interact with subscribers in the Party.

[98] For a general overview of the policies adopted by the providers, please see http://www.coe.int/en/web/cybercrime/hearing.

[99] See Council of Europe (2016) Internet Governance—Council of Europe Strategy 2016–2019, CM(2016)10-final, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c1b60, accessed 30 October 2016.

and remedy challenges and violations to them'. Several practical measures are expected due to this strategy in the future and, among these, there is also '[d]eveloping solutions regarding the access by law enforcement officers to data on cloud servers and related issues of jurisdiction. Solutions may include a Protocol to the Budapest Convention.'

Following this suggestion, the expected results of the second Additional Protocol to the Budapest Convention are the following:

- Provisions for more effective mutual legal assistance;
  i) a simplified regime for mutual legal assistance requests for subscriber information;
  ii) international production orders;
  iii) direct cooperation between judicial authorities in mutual legal assistance requests;
  iv) joint investigations and joint investigation teams;
  v) requests in English language;
  vi) audio/video hearing of witnesses, victims and experts;
  vii) emergency MLA procedures.
- Provisions allowing for direct cooperation with service providers in other jurisdictions with regard to requests for subscriber information, preservation requests, and emergency requests.
- Clearer framework and stronger safeguards for existing practices of transborder access to data.
- Safeguards, including data protection requirements.

The second Additional Protocol is expected to be finalised by December 2019, but the drafting of such a new legally binding text is still in the early stages and much intense and substantive negotiation between the Parties to the Budapest Convention is to be expected. Certain Governments consider that, in view of the global nature of the issue, the United Nations should be the framework for a new binding instrument, but solutions at the level of the United Nations are unlikely to be found for several reasons, mainly related to the difficult process in achieving an international consensus at UN level. In fact, there is no consensus between UN member States whether a UN treaty or other instrument is needed and what it would be all about, while the Budapest Convention is at present the recognized international reference to combat cybercrime and other computer-related crimes. In addition to this, a global instrument probably might set a lower standard while two-thirds of States already make use of the Budapest Convention. The proponents of a new treaty seem to want to exercise stronger control of contents. This may adversely affect free speech and other fundamental rights.

An important number of problems encountered are operational in nature and these should be addressed through improved information exchange and capacity building. There is global consensus on capacity building as an effective mean for immediate progress.

7.4 Conclusions

As argued in this chapter, cybercrime is a serious threat to the core values of societies, that is, human rights, democracy and the rule of law, which—without doubt—will become more serious every day. One only needs to consider the particular threat of cyberterrorism, for instance against nuclear facilities or other critical infrastructures, to understand the potentially disastrous consequences on our way of life.[100] Moreover, the ubiquitous use of cloud services poses various challenges in combating cybercrime and other computer-related crime. One of these challenges is the principle of territoriality and consequently the applicable jurisdiction.

The increasing threats posed by the switch of almost every human activity into a digital form require new ways to address the problem of territoriality and to distinguish between what is 'here' and 'there' in an electronic form.

The approach followed by the academic literature is often focused on specific requirements of domestic law,[101] but trying to draw a solution demands a more comprehensive approach that fully takes into account the transnational nature of the online world. Here, the basic principles of territoriality established under international law do not provide for clear solutions.[102] However, as States will not wish to

[100] Terrorism and the Internet is one of the priority areas for the biennium 2016–2017 of the Council of Europe Committee of Experts on Terrorism (CODEXTER), http://www.coe.int/t/dlapil/codexter/about_en.asp?expandable=0, accessed 30 October 2016.

[101] For example, the academic literature of US scholars is mainly focused on the Fourth Amendment issues posed by online investigations. See Kerr 2015; Daskal 2015; Daskal and Woods 2015.

[102] For a summary of different decisions in applying territoriality principles in cyberspace, see Daskal 2015, at 334–365. From an EU perspective, an important decision, already referred to in footnote 55 is *Yahoo! v Belgium*, where the Belgian Court of Cassation in December 2015 found that, unlike Yahoo!'s opinion, there was no issue of extraterritorial jurisdiction because the request for disclosure to an operator of an electronic communication network or an electronic communications service provider who is active in Belgium does not imply any intervention outside the territory of Belgium. Also, notwithstanding the place of location of such an operator or provider, its refusal to comply with such request constitutes an offence that takes place in Belgium. The Court of Cassation then concluded that Yahoo! 'voluntarily' submits itself to the Belgian law due to some peculiarities, like for example using the domain name.be or by displaying ads referred to Belgian users (see *Yahoo! v Belgium*, Court of Cassation, P.13.2082.N, 1 December 2015). The European Court of Justice dealt with the problem of territoriality in the *Weltimmo* case where, among other questions related to data protection law and the Directive 94/46/EC, the ECJ discussed the meaning of 'establishment' to decide the applicable law. On this specific issue the Court broadly follows the approach of the Advocate General, especially points 28 and 32 to 34 of his Opinion, agreeing upon a flexible definition of the concept of 'establishment', 'which departs from a formalistic approach whereby undertakings are established solely in the place where they are registered. Accordingly, in order to establish whether a company, the data controller, has an establishment, within the meaning of Directive 95/46, in a Member State other than the Member State or third country where it is registered, both the degree of stability of the arrangements and the effective exercise of activities in that other Member State must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned. This is

move away from these principles, solutions are required which, if not found within these agreed principles, should at least be compatible with them.

To start the discussion about such an approach to the problem, in June 2015, at the Council of Europe's Octopus Conference on Cybercrime, cybercrime experts from all over the world were asked about the rule of law online. Survey results showed they did not consider that 'cyberspace is basically safe, that crime and violation of rights are the exception and that offenders are brought to justice.' The ability of governments to protect society against crime and the right of individuals in cyberspace was considered to be limited.[103]

Solutions need to be identified and agreed upon that permit effective access to electronic evidence. In this respect, it is fundamental that these solutions meet human rights and rule of law requirements at the same time. The Cybercrime Convention Committee—based on proposals of its Cloud Evidence Group—is now considering a set of measures:

- rendering mutual legal assistance more efficient;
- differentiating between types of data to be secured, with a lighter regime for the production of subscriber information;
- ensuring proper implementation of Article 18 of the Budapest Convention based on the Guidance Note on the production or subscriber information;
- facilitating direct public/private transborder co-operation;
- establishing a framework with safeguards for transborder access to data in specific circumstances.

Similar efforts are now also underway within the European Union and have been promoted in particular by the Netherlands Presidency.[104] Common solutions, however, cannot be limited to the European Union[105] nor to the Council of Europe, but will need to be of a global nature as outlined before.

Therefore, the Council of Europe's Budapest Convention on Cybercrime with its currently 48 Parties[106] from all over the world, and including the US where much of the Internet infrastructure is based, remains at present the best framework to provide

(Footnote 102 continued)

particularly true for undertakings offering services exclusively over the Internet.' (see *Weltimmo s. r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, ECJ, ECLI:EU:C:2015:639, 1 October 2015, para 29).

[103] See Octopus Conference 2015, Cooperation against Cybercrime, Key messages, http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680319026, accessed 22 October 2016.

[104] See http://english.eu2016.nl/events/2016/03/07/crossing-borders-jurisdiction-in-cyberspace, accessed 30 October 2016.

[105] See EU Directive 2013/40/EU on Attacks Against Information Systems, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF, accessed 30 October 2016.

[106] Another 18 States are signatories or have been invited to accede the Convention. This number is constantly increasing.

the urgently needed solutions on securing cloud evidence for criminal justice purposes while respecting human rights and the established principles of State jurisdiction.

References

Bach D, Newman AL (2006) Local Power, Global Reach: The Domestic Institutional Roots of Internet Governance. http://www18.georgetown.edu/data/people/aln24/publication-25786.pdf. Accessed 20 October 2016

Balkin J, Grimmelmann J, Katz E, Kozlovski N, Wagman S, Zarsky T (2007) Cybercrime: Digital Cops in a Networked Environment. NYU Press, New York

Brown CSD (2015) Investigating and Prosecuting Cyber Crime: Forensics Dependencies and Barriers to Justice. International Journal of Cyber Criminology 9:55–119

Brownlie I (2003) Principles of Public International Law, 6th edn. Oxford University Press, Oxford

Daskal J (2015) The Un-Territoriality of Data. Yale Law Journal 125:326–398

Daskal J, Woods AK (2015) Cross-Border Data Requests: A Proposed Framework. https://lawfareblog.com/cross-border-data-requests-proposed-framework. Accessed 30 October 2016

Goldsmith J (1998) The Internet and the Abiding Significance of Territorial Sovereignty. Indiana Journal of Global Legal Studies 5:475–491

Handeyside H (2007) The *Lotus* Principle in ICJ Jurisprudence: Was the Ship Ever Afloat? Michigan Journal of International Law 29(1):71–94

de Hert P, Kopcheva M (2011) International Mutual Legal Assistance in Criminal Law Made Redundant: A Comment on the Belgian Yahoo! Case. Computer Law & Security Review 27:291–297

Hixson K (1988) Extraterritorial Jurisdiction Under the Third Restatement of Foreign Relations Law of the United States. Fordham International Law Journal 12(1):127–152

Huston G (2013) IP Addresses and Traceback. APNIC Labs. https://labs.apnic.net/?p=433. Accessed 22 October 2016

Ireland-Piper D (2014) The Enrica Lexie and St Antony: A Voyage into Jurisdictional Conflict. QUT Law Review 14(2):74–89

Johnson DR, Post DG (1996) Law and Borders: The Rise of Law in Cyberspace. Stanford Law Review 48(5):1367–1402

Kerr OS (2015) Search and Seizure in a Digital World. Harvard Law Review 119:531–585

Kulesza J (2008) Internet Governance and the Jurisdiction of State: Justification of the Need for an International Regulation of Cyberspace. https://www.researchgate.net/profile/Joanna_Kulesza3/publication/228228013_Internet_Governance_and_the_Jurisdiction_of_States_Justification_of_the_Need_for_an_International_Regulation_of_Cyberspace/links/564e522108ae4988a7a62701.pdf. Accessed 20 October 2016

Lacy E, Reed SR (2016) BWL cyberattack bills reach nearly $2M. http://www.lansingstatejournal.com/story/news/local/2016/09/22/bwl-ransomware-attack-costly-details-emerging/90826176/. Accessed 22 October 2016

Mell P, Grance T (2011) The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800–145. http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf. Accessed 23 October 2016

Narayanan V (2012) Harnessing the Cloud: International Law Implications of Cloud-Computing. Chicago Journal of International Law 12(2):783–809

NIST (2014) Cloud Computing Forensic Science Challenges. Draft NISTIR 8006. http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf. Accessed 25 October 2016

Osula A-M (2015) Transborder Access and Territorial Sovereignty. Computer Law & Security Review 31:719–735

PC-OC (2012) Guidelines on Practical Measures to Improve Co-Operation in Respect of Transfer of Proceedings, Including a Model Request Form. PC-OC INF 78. http://www.coe.int/t/dghl/standardsetting/pc-oc/Source/PC_OC_INF_78%20Guidelines%20and%20model%20request%20form%20on%20transfer%20of%20proceedings.doc. Accessed 25 October 2016

PC-OC (2014) Model Request Form for Mutual Assistance in Criminal Matters. PC-OC Mod (2014) 10rev.6. http://www.coe.int/t/dghl/standardsetting/pc-oc/PCOC_documents/Documents%202015/PC-OC%20Mod%20(2014)10rev6%20Model%20request%20form%20for%20MLA.pdf. Accessed 25 October 2016

PC-OC (2015) Mutual Legal Assistance in the Treaties of the Council of Europe: Note for Practitioners. PC-OC(2015)03. http://www.coe.int/t/dghl/standardsetting/pc-oc/PCOC_documents/Documents%202015/PC-OC%20(2015)03%20Note%20for%20practitioners%20on%20mutual%20legal%20assistance.pdf. Accessed 25 October 2016

Reidenberg JN (2005) Technology and Internet Jurisdiction. University of Pennsylvania Law Review 153:1951–1974

Schultz T (2008) Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface. European Journal of International Law 19(4):799–839

Svantesson D (2015) A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft. AJIL Unbound 109:69–74

Svantesson D, Gerry F (2015) Access to Extraterritorial Evidence: The Microsoft Cloud Case and Beyond. Computer Law & Security Review 31:478–489

Svantesson D, van Zwieten L (2016) Law Enforcement Access to Evidence Via Direct Contact With Cloud Providers – Identifying the Contours of a Solution. Computer Law & Security Review 32:671–687

Swanson SR (2011) Google Sets Sail: Ocean-Based Server Farms and International Law. Connecticut Law Review 43(3):709–751

Talbot D (2016) Cybersecurity: The Age of the Megabreach. MIT Technology Review. https://www.technologyreview.com/s/545616/cybersecurity-the-age-of-the-megabreach/. Accessed 30 October 2016

T-CY (2013a) Guidance Note#3: Transborder Access to Data (Article 32). http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a. Accessed 27 October 2016

T-CY (2013b) Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime. http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c. Accessed 23 October 2016

T-CY (2014) Rules on Obtaining Subscriber Information. Report. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7ad1. Accessed 25 October 2016

T-CY (2015a) Guidance Note#10 (Draft): Production Orders for Subscriber Information (Article 18 Budapest Convention). https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77c. Accessed 28 October 2016

T-CY (2015b) Criminal Justice Access to Data in the Cloud: Challenges. Discussion Paper. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59. Accessed 22 October 2016

T-CY (2016a) Criminal Justice Access to Electronic Evidence in the Cloud - Informal Summary of Issues and Options Under Consideration by the Cloud Evidence Group. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a53c8. Accessed 25 October 2016

T-CY (2016b) Criminal Justice Access to Data in the Cloud: Co-Operation with 'Foreign' Service Providers. Background Paper. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d. Accessed 27 October 2016

T-CY (2016c) Emergency Requests for The Immediate Disclosure of Data Stored in Another Jurisdiction Through Mutual Legal Assistance Channels or Through Direct Requests to Service

Providers: Compilation of Replies to the Questionnaire. http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680644318. Accessed 27 October 2016

UNODC (2013) Comprehensive Study on Cybercrime. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Accessed 20 October 2016

Vaciago G (2011) Cloud Computing and Data Jurisdiction: A New Challenge for Digital Forensics. CYBERLAWS 2012: The Third International Conference on Technical and Legal Aspects of the e-Society

von Behr I, Reding A, Edwards C, Gribbon L (2013) Radicalisation in the Digital Era. The Use of the Internet in 15 Cases of Terrorism and Extremism. http://www.rand.org/pubs/research_reports/RR453.html. Accessed 22 October 2016

Walden I (2011) Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent. Queen Mary School of Law Legal Studies Research Paper No 74/2011. https://ssrn.com/abstract=1781067. Accessed 27 October 2016

Zoetekouw M (2016) Ignorantia Terrae Non Excusat. https://english.eu2016.nl/binaries/eu2016-en/documents/publications/2016/03/7/c-mzoetekouw—ignorantia-terrae-non-excusat—discussion-paper-for-the-crossing-borders—jurisdiction-in-cyberspace-conference-march-2016—final/c-mzoetekouw-ignorantia-terrae-non-excusat-discussion-paper-for-the-crossing-borders-jurisdiction-in-cyberspace-conference-march-2016-final.pdf. Accessed 20 October 2016