The limits of subjective territorial jurisdiction in the context of cybercrime

Jean-Baptiste Maillart¹

Published online: 3 September 2018
© The Author(s) 2018

Abstract Despite the ubiquitous nature of cyberspace, territorial jurisdiction remains the most fundamental principle of jurisdiction in the cybercrime context. The objective of this paper is, however, to point out the limits of subjective territorial jurisdiction, one of the two main forms of territoriality, over cybercrimes, and thereby call into question the territorial dogma in the digital age. Subjective territorial jurisdiction, which can be claimed and exercised by the state on the territory of which a criminal conduct occurred, is indeed of limited use in the context of cybercrime precisely because it is very difficult to pinpoint the location where the conduct of a cybercrime actually took place. Technical and legal considerations explain such a situation.

Keywords Territoriality · Cybercrime · Metadata · Transborder access · Public · Private partnerships

1 Introduction

Today no one can doubt that territorial jurisdiction is the most fundamental and commonly accepted method of exercising jurisdiction to prescribe in criminal matters. As underlined by Wong, it is indeed ‘indisputable that the generally accepted view in public international law is that the primary basis of criminal jurisdiction for any state is territorial’.¹ This is to be explained mostly by the existence of very strong ties

¹ Wong [50], p. 96. See also e.g. Kulesza [30], p. 2 (‘The execution of jurisdictional competence is, above all, a territorial phenomenon’); Ryngaert [36], p. 49 (‘The territoriality principle is the most basic principle of jurisdiction in international law’).

✉ J.-B. Maillart
j.maillart@mpicc.de

¹ Research Fellow, Max Planck Institute for Foreign and International Criminal Law, Freiburg, Germany

between the notions of state sovereignty and territoriality, the latter being the necessary corollary of the former in the Westphalian legal order. That said, one could have expected the development of the decentralised, borderless and pervasive cyberspace in the 1990s to prompt a paradigm shift regarding jurisdiction over cybercrimes. Yet, '[c]yberspace has not led to any innovation in jurisdictional rules':² the exercise of jurisdiction in the context of cybercrimes remains largely based on the principle of territoriality. Such predominance is notably highlighted in all the national reports submitted in the framework of Section IV's preparatory colloquium (Helsinki, 2013) to the *Association internationale de droit pénal's* XIXth International Congress of Penal Law (Rio de Janeiro, 2014).³ One could also mention the various international and regional instruments that aim at enhancing the fight against cybercrime since they all rely on territoriality as the primary basis for exercising jurisdiction.⁴

The objective of this paper is, however, to point out the limits of subjective territorial jurisdiction, one of the two main forms of territoriality, over cybercrimes, and thereby call into question the territorial dogma in the digital age. More specifically, this paper aims at demonstrating that, although territoriality constitutes one of the keystones of the international legal order, the '*pilier d'assises du droit pénal international*' to use the expression of Donnedieu de Vabres,⁵ the adequacy of its subjective facet with regard to the Internet is dubious as it prevents states from effectively investigating and prosecuting cybercrimes. Subjective territorial jurisdiction, which can be claimed and exercised by the state on the territory of which a criminal conduct occurred, is indeed of limited use in the context of cybercrime precisely because it is very difficult to pinpoint the location where the conduct of a cybercrime actually took place. Technical and legal considerations explain such a situation, particularly problematic with respect to so-called 'cybercrimes of conduct' whose *actus reus* only consists of a criminal conduct and which can therefore only be subjected to the territorial jurisdiction of the state where it originated from.⁶

²Hayashi [23], p. 80. See also e.g. Foggetti [16], p. 35 ('There is no change compared with traditional principles. The most important principle is always the place in which the criminal has committed a crime: the principle of territoriality').

³Reports available at: <http://www.penal.org/en/readip-2014-e-riapl-2014>.

⁴See e.g. Convention on Cybercrime, Budapest, 23.11.2001, ETS No. 185, Art. 22(1)(a); Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28.1.2003, ETS No. 189, Art. 4(1); Arab Convention on Combating Information Technology Offences, Cairo, 21.12.2001, Art. 30(1)(a); Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2001 on combating the sexual abuse and sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA [2011] OJ L 335, Art. 17(1)(a); Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2014] OJ L 218, Art. 12(1)(a).

⁵Donnedieu de Vabres [12], p. 443.

⁶A significant number of cybercrimes are construed as cybercrimes of conduct. See e.g. Art. 2 of the Convention on Cybercrime (*supra*, fn. 4) which defines the offence of illegal access as merely 'the access to the whole or any part of a computer system without right' (emphasis added). No result is required for the offence to be deemed to have been committed: '[t]he mere unauthorised intrusion, i.e. 'hacking', 'cracking' or 'computer trespass' should in principle be illegal in itself' (Explanatory Report of the Convention on Cybercrime, para. 44).

2 Subjective territorial jurisdiction in criminal matters: definition and scope

According to the modern and universally recognised theory of ubiquity,⁷ '[t]he widest application of the qualified territoriality principle',⁸ a state can exercise its jurisdiction over a crime when at least one of its constituent elements, either the criminal conduct (subjective territorial jurisdiction) or the result (objective territorial jurisdiction), occurred within its territory.

One should recall, however, that the subjective and objective applications of the territorial principle first developed in the late 19th and early 20th century as independent and exclusive principles of jurisdiction.^{9,10} Traditionally, subjective territoriality relies upon three main principles. Firstly, it is usually where the criminal conduct took place that the most useful pieces of evidence to solve a crime are to be found. The place where the perpetrator engaged in the criminal conduct is indeed generally where most of the witnesses and indicia of criminal activity were, and are still likely to be.¹¹ Secondly, compared to its objective counterpart, subjective territoriality is supposed to better ensure due process and compliance with the principle of legality, according to which individuals must be warned that a certain act is criminalised. Contrary to the place of result, which may be random and unpredictable, the place of conduct is more or less always certain. This argument is notably put forward by Schultz.¹² Thirdly, subjective territorial jurisdiction relies upon the idea that, from a criminological point of view, it is more important for states to sanction the expression of a criminal will on their territory than to protect and restore their public order (objective territorial jurisdiction's main ratio). According to Foucault, one of its most keen advocates, the aim of territorial jurisdiction is indeed 'not so much to re-establish a balance as to bring into play, as its extreme point, the dissymmetry between the subject who has dared to violate the law and the all-powerful sovereign who displays his strength'.¹³

In this context, the only state on the territory of which the *locus delicti* may be located for the purpose of subjective territorial jurisdiction is the state where the perpetrator was physically present when he/she engaged in the criminal conduct. States cannot interpret subjective territoriality in a broader way so that they can apply it to an offence which was committed by someone abroad as this would be contrary to

⁷For more on the ubiquity theory, see e.g. Ryngaert [36], pp. 77-79.

⁸Gilbert [20], p. 430.

⁹The subjective and objective applications of the territoriality principle were then later combined, as complementary, upon the conclusion that, taken alone, none of them 'can be made sufficiently comprehensive to serve as a rationalisation of contemporary practice' (Harvard Research on International Law, Jurisdiction with respect to Crime, in AJIL Suppl. 1935, p. 494).

¹⁰With respect to subjective territorial jurisdiction, see e.g. *R. Keyn*, 1876, in LR 2 Ex D 63; Institut de droit international, Résolution sur les règles relatives aux conflits des lois pénales en matière de compétence, Session de Munich, 1883, Art. 1; PCIJ, *The Case of the S.S. 'Lotus' (France v. Turkey)*, judgment, 7.9.1927, dissenting opinion of Judge Weiss in C.P.J.I Recueil 1927, série A, n 10, p. 47.

¹¹For more on this, see e.g. *Donnedieu de Vabres* [13], p. 927.

¹²Schultz [38], pp. 313-314. See also e.g. *Huet/Koering-Joulin* [24], p. 226.

¹³Foucault [17], pp. 48-49.

the three aforementioned principles which, together, constitute the *ratio* of subjective territorial jurisdiction. The most relevant pieces of evidence are indeed only to be found in the state where the criminal conduct originated from. It is also only on the territory of that state that the criminal will of the perpetrator is expressed and that the principle of legality is best safeguarded. This narrow definition of the location of the criminal conduct is widely recognised by the doctrine, in particular with respect to cybercrimes.¹⁴ For instance, according to Schmitt, '[a]ny state from which the individual has operated enjoys jurisdiction because the individual, and the devices involved, were located on its territory when so used. [...] Actual physical presence is required, and sufficient for jurisdiction based on territoriality; spoofed presence does not suffice'.¹⁵ Another example is that of Jessberger, who, regarding the German legal framework, writes the following: '[A] person who uploads data to the Internet from outside Germany does, as a rule, not establish such a 'Handlungsort' in Germany. In this case, only the place in the country where the offender is physically present at the time of uploading the data defines the place where the offender acted ("Handlungsort")'.¹⁶

3 The technical difficulty to trace back cybercriminals

The first reason explaining the inadequacy of subjective territorial jurisdiction in the context of cybercrime is of technical nature, precisely because of the 'technical difficulties in tracing the origins of cybercrime perpetrators'¹⁷ and thereby pinpointing where the criminal conduct of a cybercrime actually took place.

Each computer system (computers, smart phones, tablets, etc.) connected to the Internet is assigned a unique Internet Protocol (IP) address, which consists of four (IPv4) to six (IPv6) numbers, between 0 and 255.¹⁸ The IP address space is managed globally by the International Corporation for Assigned Names and Numbers (ICANN). ICANN does not run the system but it does help to co-ordinate how IP addresses are supplied to avoid repetition or clashes. ICANN is also the central repository for IP addresses, from which ranges are supplied to the five regional Internet registries (RIRs¹⁹) who in turn are responsible in their designated territories for as-

¹⁴ *Contra*: Maillart [32]; Brenner/Koops [5], p. 15.

¹⁵ Schmitt [37], p. 19.

¹⁶ See also Sieber [42], p. 189 ('[T]he location of the criminal act in the legal sense of Sect. 9(1) 1st alternative StGB is thought to depend on the physical location of the offender'). With respect to the Swiss legal framework, Gless/Petrigl/Stagno/Martin [21], p. 5 ('[T]he place of acting is considered to be located in Switzerland if the alleged offender was physically present in Switzerland when entering the respective computer commands. Hence, the place of the data input is decisive for determining the place of acting, which, in turn, gives rise to a place of commission in Switzerland according to Article 8 Swiss Criminal Code').

¹⁷ Communication from the European Commission to the Council and the European Parliament, Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre, COM(2012) 140 final, Brussels, 28.3.2012, p. 3.

¹⁸ IPv6 addresses were developed in 1995, and standardised in 1998, because of the growth of the internet and the depletion of available IPv4 addresses.

¹⁹ There are currently five RIRs: RIPE-NCC (Europe and Middle East), ARIN (North America), APNIC (Asia-Pacific), LACNIC (Latin America and Caribbean) and AfriNIC (Africa).

signment to end users and local Internet registries, such as Internet service providers. In this context, considering that '[t]he IP address of a computer points at a physical address',²⁰ determining the place of origin of a cybercrime does not seem, at first glance, to raise any technical issue as it merely consists in identifying the IP address of the computer system used by the cybercriminal. However, the problem lies in the fact that 'no attacker worth his salt would make any intrusion directly from his own IP address', as Rosenzweig rightly observes.²¹ Instead, cybercriminals always find a way to conceal their true IP address and thereby the place where they engage in the criminal conduct. There are indeed 'a range of techniques, software programs and websites available on or accessible over the Internet which allow individual users to either hide who or where they are'.²²

First of all, the perpetrator of a cybercrime can easily replace the IP address of the computer system which he/she uses by the one allotted to another computer system so that the offence purports to come from a location other than the one from which it truly stems. In the absence of a strong authentication rule²³ and considering that '[t]here are many 'open proxies' on the Internet which can be accessed by anyone',²⁴ this technique, called 'IP spoofing', is relatively easy to implement. Another technique is the use of proxy servers, public or private, which enables cybercrime offenders to establish a connection to a network via an intermediary server and thereby conceal their online activity.²⁵ That said, the most commonly used and efficient method to hide the geographical origin of an offence committed in cyberspace is still to take control over a remote computer system in a foreign country and then use that computer as a staging ground from which to perpetrate the offence. This computer system, which is said to be 'zombified', is often the last link in a very long chain involving numerous computer systems and jurisdictions. Indeed, '[b]y moving from stepping stone to stepping stone on their way to the final target, attackers can obscure the true origin of the attack, making tracking and tracing the attackers an extremely difficult task'.²⁶ In this regard, China, in particular, is a convenient stepping stone because of the large number of computer systems that outsiders from around the world can easily compromise and 'commandeer as their unwitting launchpads'.²⁷

Moreover, one should note that anonymity inherent in Internet-based activities greatly contributes to the technical difficulty to trace back criminals in cyberspace. For Greenemeier, anonymity is actually 'the hardest problem' in geolocating the

²⁰ *Klip* [28], p. 387.

²¹ *Rosenzweig* [35], p. 78.

²² *Davies* [9], p. 53.

²³ *Rosenzweig* [35], p. 78; *Lipson* [31], p. 14.

²⁴ *Muir/Van Oorschot* [34], p. 15.

²⁵ For more on the use of proxy servers, see e.g. *Brown* [7], p. 80; *Muir/Van Oorschot* [34], p. 14.

²⁶ *Lipson* [31], p. 16. See also e.g. *Brenner* [4], p. 28; *De Hert/Gonzalez Fuster/Koops* [10], p. 518; *Morris* [33], p. 14; *Rosenzweig* [35], p. 78.

²⁷ *Thornburg* [46]. See also e.g. *Gable* [18], p. 115 ('Cyberterrorists often use China as a jumping off point due to its relatively lax security. This complicates efforts to pinpoint the identity and location of attackers, as the fact that the apparent source of an attack was a Chinese computer does not necessarily mean that the attack actually came from China').

source of cybercrimes.²⁸ Law enforcement authorities could indeed more easily locate the place of origin of a cybercrime if they could previously identify its perpetrator. Yet, there exist many tools, such as Tor,²⁹ Anonymouse,³⁰ The Cloak³¹ or email encryption software, which allow to remain anonymous online and keep Steiner's dictum from 1993 – 'On the Internet, nobody knows you're a dog' –³² accurate in today's reality.

4 The unfit character of traditional cooperation mechanisms to access metadata abroad

In addition to the technical difficulty to trace back criminals in cyberspace, efforts to pin down the location where a cybercriminal engaged in a prohibited conduct and thereby identify the state which can claim and exercise its subjective territorial jurisdiction also encounter legal obstacles.

4.1 The issue at stake

Unlike offences which are committed offline, there is no crime scene in cyberspace, at least not in the traditional sense, where it is possible to find material evidence, like DNA or fingerprints, or interview witnesses to attempt determining where exactly the criminal act was performed.³³ To quote Smit, '[c]ybercrime offences are committed without any climbing over fences, balaclavas or angry dogs and property owners. There is only somewhere in the world a computer, which is controlled by a particular person'.³⁴ In this context, the law enforcement authorities which are trying to pinpoint the physical origin of a cybercrime can only rely upon available computer data, in particular metadata, i.e. subscriber information and traffic data. These data can indeed be very useful to geolocate cybercriminals. The Convention on Cybercrime defines them 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;

²⁸Greenemeier [22]. See also e.g. Rosenzweig [35], p. 78 ('The difficulty of identification is perhaps the single most profound challenge for cybersecurity today').

²⁹<http://www.torproject.org>.

³⁰<http://anonymouse.org>.

³¹<http://www.the-cloak.com/anonymous-surfing-home.html>.

³²<http://emilebela.mondoblog.org/2013/07/15/sur-internet-personne-ne-sait-que-tu-es-un-chien/imageszzzz/>.

³³Brenner [3], p. 78.

³⁴Smit [44], p. 4.

- 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'.³⁵
- '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.³⁶

However, the problem lies in the fact that metadata are very often held by service providers outside the territory of the investigating law enforcement agency and therefore outside its jurisdiction and that, as detailed below, traditional cooperation mechanisms – direct transborder access and mutual legal assistance – are unfit to access and secure data stored in foreign jurisdictions in an effective and timely manner. To this must be added the fact that computer data are increasingly stored 'in the cloud'³⁷ where the location of the data may be very difficult to determine at any point in time³⁸ and that such cooperation mechanisms cannot be used in these circumstances.

Three main factors explain the international dimension of metadata, in particular in relation to cybercrimes. First, the ubiquitous architecture of the internet itself allows technology companies significant flexibility as to the geographical location where they may store the data which are in their possession or control. Second, data are by nature extremely volatile and can therefore be easily moved from one jurisdiction to another just with a few mouse clicks. Third, considering that cybercrimes are inherently transnational,³⁹ metadata related to these crimes are necessarily spread around several jurisdictions as well. As highlighted by the European Commission (Commission), 'no crime is as borderless as cybercrime'.⁴⁰ Very early observed,⁴¹ this distinctive feature is notably reflected in the Comprehensive Study on Cybercrime conducted by the United Nations Office on Drugs and Crime (UNODC) in 2013.⁴² Countries responding to the Study questionnaire indeed reported regional averages of between 30 and 70 per cent of cybercrime acts that involve a transnational dimension and more than half of countries reported that between 50 and 100

³⁵Convention on Cybercrime (*supra*, fn. 4), Art. 18(3).

³⁶Convention on Cybercrime (*supra* fn. 4), Art. 1(d).

³⁷*Siebert/Neubert* [43], p. 243; *Velasco* [47], p. 345.

³⁸For more on this, see *Jessberger* [25], p. 2; *Kaspersen* [27], p. 29; *Schwerha* [39], p. 9; *Taylor/Haggerty/Gresty/Lamb* [45], p. 6.

³⁹For more on this, see e.g. *Brenner* [2], pp. 189–190; *Broadhurst* [6], p. 414; *Faraldo Cabanal/Catalina Benavente* [15], p. 3; *Del Tufo/Rafaraci* [11], p. 6; *Vestergaard/Fuchsel* [48], p. 3.

⁴⁰Communication from the European Commission to the Council and the European Parliament, Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre, COM(2012) 140 final, Brussels, 28.3.2012, p. 2.

⁴¹See e.g. Council of Europe, Committee of Ministers, Recommendation No. R (89) 9 ('[C]omputer-related crime often has a transfrontier character').

⁴²Available at: https://www.unodc.org/documents/.../crime/.../CYBERCRIME_STUDY_210213.pdf.

per cent of cybercrime acts encountered by the police involve a transnational element.⁴³

4.2 Direct transborder access

First, in order to obtain metadata held abroad, law enforcement authorities may consider to remotely access the foreign servers where the sought-after data are located directly from their home state. However, self-service is not permitted. Such a transborder online search amounts to an extraterritorial exercise of enforcement jurisdiction and therefore requires, from the point of view of international law,⁴⁴ the consent of the territorial state.⁴⁵ The fact that the law enforcement officer carrying out the investigative measure is not physically located on foreign soil is completely irrelevant. Indeed, as recalled by Sieber and Neubert, '[e]ver since the famous Trail Smelter Arbitration, it has been an accepted principle in international law that acts attributable to a state that are conducted from the territory of one state but that take effect within the territory of another state infringe the sovereignty of the affected state'.⁴⁶

Consent from the state where the data are physically located can be obtained in two different ways. Yet, these two options very often prove unsatisfactory.

Firstly, consent can be obtained on a case-by-case basis. However, in addition to the potentially very high number of jurisdictions to get in touch with, the problem is that the legal process to obtain consent is usually time-consuming, which is incompatible with the volatile nature of data.⁴⁷

Secondly, consent can be granted in advance by virtue of a treaty provision, such as Article 40 of the Arab Convention on Combating Information Technology Of-

⁴³ See p. 183 of the study.

⁴⁴ PCIJ, *The Case of the S.S. 'Lotus' (France v. Turkey)*, judgment, 7.9.1927, p. 18 ('[T]he first and foremost restriction imposed by international law upon a State is that – failing a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State'); ICJ, *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)*, judgment, 25.3.1948, p. 35 ('Between independent States, respect for territorial sovereignty is an essential foundation of international relations').

⁴⁵ Bourguignon [1], p. 362; Gercke [19], p. 171; Koops/Goodwin [29], p. 9; Sieber [41], pp. 211–212; Ziolkowski [51], pp. 163–164.

⁴⁶ Sieber/Neubert [43], p. 257. In the same vein, see e.g. Seitz [40], p. 36 ('[A] transborder search brings about physically perceptible changes to the outside world in the territory of the third country because data processing is initiated on servers that are located in the foreign state. [...] [I]t cannot make a difference whether the acting officer is physically present at the foreign site of the server when undertaking the measure, or whether he accesses the server over the Internet or in some cases also over an intranet. The result of his activity is the same in both cases: data processing is initiated on servers which are located in foreign territory. The decisive criterion to answer the question whether or not a violation of the principle of territoriality occurs is thereafter not the physical presence in foreign sovereign territory but whether the measure causally precipitates a perceptible change in the outside world in foreign territory'). *Contra*, see e.g. Bourguignon [1], pp. 362–363; Ehlscheid/Von Briel [14], pp. 451–452; Jofer [26], p. 193; Kaspersen [27], p. 27.

⁴⁷ Schwerha [39], p. 18; Taylor/Haggerty/Gresty/Lamb [45], p. 5.

fences⁴⁸ or Article 32(b) of the Convention on Cybercrime.⁴⁹ The issue here is not time-related but is that these provisions have strong limitations. Let's take the example of Article 32(b) of the Convention on Cybercrime which represents a minimum consensus as the drafters of the Convention 'ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area'.⁵⁰ Article 32(b) provides that states parties can 'access or receive, through a computer system in its territory, stored computer data located in another Party'.⁵¹ Therefore, this provision does not apply if the metadata are held on the territory of a non-state party or 'somewhere online', in the cloud. This is a serious shortcoming as more than 130 states are not parties to the Convention on Cybercrime⁵² and the use of cloud computing is growing. Moreover, Article 32(b) permits transborder access only 'if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.' Yet, the question as to 'who' is the person who is 'lawfully authorized' to disclose the data may vary depending on the circumstances, laws and regulations applicable. For example, it may be a physical individual person, providing access to his email account or other data that he stored abroad, or it could be a service provider. Service providers will, however, unlikely be able to consent validly and voluntarily to disclosure of their users' data under Article 32(b). As noted by the Cybercrime Convention Committee (T-CY), '[n]ormally, service providers will indeed only be holders of such data; they will not control or own the data, and they will, therefore, not be in a position validly to consent'.⁵³ In the same vein, it is very unlikely that the person who stored the data abroad consents to disclosure, especially if he/she is subject to a criminal investigation (pursuant to the *nemo tenetur se ipsum accusare* principle).

4.3 Mutual legal assistance

In addition to direct transborder access, one could think of mutual legal assistance (MLA) as an option to access and secure metadata held abroad in view of identifying the state of origin of a cybercrime. However, although the MLA process remains

⁴⁸ *Supra*, fn. 4.

⁴⁹ *Supra*, fn. 4.

⁵⁰ Explanatory Report of the Convention on Cybercrime, para. 293. It should be noted, however, that the drafters of the Convention on Cybercrime 'agreed not to regulate other situations until such time as further experience has been gathered and further discussions may be held in light thereof' (*ibid*).

⁵¹ Similarly, Art. 40 of the Arab Convention on Combating Information Technology Offence (*op. cit.*) provides that a state party may, without obtaining an authorization from another state party, 'access or receive – through information technology in its territory – information technology information found in the other State Party, provided it has obtained the voluntary and legal agreement of the person having the legal authority to disclose information to that State Party by means of the said information technology.'

⁵² Only 60 States have ratified the Convention on Cybercrime so far (15.7.2018).

⁵³ T-CY, Guidance Note No. 3: Transborder Access to Data (Article 32), Adopted by the 12th Plenary of the T-CY (2-3.12.2014), T-CY(2013)7, p. 7.

the primary channel for obtaining digital evidence abroad,⁵⁴ it is largely inefficient. Numerous authors,⁵⁵ but also states,⁵⁶ denounce this state of affairs.

First of all, mutual legal assistance is such a cumbersome and slow process that it does not fit the time-critical need of cyber-investigations. Response time to requests of 6 to 24 months appear to be the norm for parties to the Cybercrime Convention.⁵⁷ According to the 2013 President's Review Group on Intelligence and Communications Technologies, MLA requests submitted to the United States (US) take an average of approximately 10 months to complete.⁵⁸ This legal scheme cannot compete in an environment where data can be deleted or moved across borders so easily and so quickly, often without human intervention.

Second of all, the admissibility of MLA requests is traditionally subject to the dual criminality principle. Yet, with respect to cybercrimes, the problem is that the definition and scope of cybercrimes may vary considerably from one state to another, which may then result in a refusal of the MLA request. According to a recent survey conducted by the Commission, Member States have actually identified the lack of dual criminality as one of the main grounds for rejecting a MLA request.⁵⁹

Third of all, the question of the language of international requests for mutual assistance is also considered a major problem by most states. According to the T-CY, the main problems in this respect are the delays caused by translations; the cost of translations; the limited quality of translations, including unclear terminology, [and] limited foreign language skills of practitioners'.⁶⁰

⁵⁴European Commission (Services), Non-Paper on Improving Cross-border Access to Electronic Evidence, 2017, p. 10 ('Cross-border access to electronic evidence is often obtained on the basis of formal cooperation between the relevant authorities of two countries. The main mechanism for the formal cooperation between the competent authorities of different countries for obtaining cross-border access to electronic evidence is currently based on mutual legal assistance (MLA), both within the European Union and with third countries'). In the same vein, see also e.g. T-CY, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Final report of the T-CY Cloud Evidence Group, 16.9.2016, T-CY(2016)5, p. 12.

⁵⁵See e.g. *Koops/Goodwin* [29], pp. 7 and 41.

⁵⁶See e.g. New Zealand Law Commission, Search and Surveillance Powers, Report 97, June 2007, p. 227 ('We acknowledge that current mutual assistance arrangements may not be sufficiently tailored to facilitate intangible evidential material being efficiently collected from other jurisdictions'). See also US District Court, S.D.N.Y., *In the Matter of a Warrant to Search a Certain E-mail Account: Controlled and Maintained by Microsoft Corporation*, 25.4.2014, in F.Supp.3d., 2014, vol. 15, p. 466 ('Microsoft's rosy view of the efficacy of the MLAT process bears little resemblance to reality. [...] [A] MLAT request typically takes months to process, with the turnaround time varying widely based on the foreign country's willingness to cooperate, the law enforcement resources it has to spare for outside requests for assistance, and the procedural idiosyncrasies of the country's legal system').

⁵⁷T-CY, The mutual legal assistance provisions of the Budapest Convention on Cybercrime, Adopted by the T-CY at its 12th Plenary (2-3.12.2014), T-CY(2013)17, p. 123.

⁵⁸*Clarke/Morell/Stone/Swire* [8], p. 171.

⁵⁹European Commission (Services), Non-paper on Improving Cross-border Access to Electronic Evidence, 2017, p. 5.

⁶⁰T-CY, The mutual legal assistance provisions of the Budapest Convention on Cybercrime, Adopted by the T-CY at its 12th Plenary (2-3 December 2014), T-CY(2013)17, p. 35.

Last but not least, the MLA process may simply not be an option if there is no available MLA treaty⁶¹ or when the physical location of the sought-after metadata is unknown or uncertain because it is stored in the cloud.⁶² Indeed, ‘if investigators do not know where the data are stored, they cannot file an application for mutual legal assistance because they do not know which country to file it with’.⁶³ Yet, as noted above, more and more data are migrating into the cloud.

5 Moving forward through an increasing use of public-private partnerships

As explained *supra*, subjective territorial jurisdiction does not fit the cybercrime context, in particular because traditional cooperation mechanisms do not permit states to access, in an effective and timely manner, metadata stored in foreign jurisdictions or in the cloud and thereby pin down the location where a cybercriminal engaged in the prohibited conduct. That said, subjective territorial jurisdiction is not dead yet and could still be of a certain relevance if more efficient and innovative cooperation mechanisms to access traffic data and subscriber information held abroad were used. One solution is to be found in public-private partnerships, i.e. direct cooperation mechanisms between law enforcement authorities and service providers. A brief overview of already available and forthcoming options under the Convention on Cybercrime, US law and European Union (EU) law is provided below.

5.1 Article 18(1) of the Convention on Cybercrime

Article 18(1)(a) of the Convention on Cybercrime provides that each state party shall ensure that its competent law enforcement authorities have the power to order ‘a person in its territory to submit specified computer data in that person’s possession or control, which is stored in a computer system or a computer-data storage medium’. According to the Explanatory Report of the Convention, the term ‘possession or control’ refers to ‘physical possession of the data concerned in the ordering Party’s territory, and situations in which the data to be produced is outside of the person’s physical possession but the person can nonetheless freely control production of the data from within the ordering Party’s territory’.⁶⁴ Article 18(1)(a) therefore offers an important tool for law enforcement authorities to access metadata held outside their territorial jurisdiction as the physical location of the data does not matter. What matters instead is that the service provider which has control over the data is established in the territory of the ordering state party.

⁶¹One should note, for instance, that the United States has MLA treaties with only 60 nations around the world, which accounts for less than one third of the nations in the world (15.7.2018).

⁶²See e.g. T-CY, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Final report of the T-CY Cloud Evidence Group, 16.9.2016, T-CY(2016)5, p. 9 (‘MLA is not always a realistic solution to access evidence in the cloud context’); Walden [49], p. 310 (‘International rules governing the transborder gathering of evidence, ‘mutual legal assistance’, are poorly suited to cloud-based processing activities, as with other forms of computer and networking environments’).

⁶³Sieber/Neubert [43], p. 296.

⁶⁴Explanatory Report of the Convention on Cybercrime, para. 173.

Article 18(1)(b) addresses the situation in which the service provider is not physically present on the territory of the state party but offers its services within its territory. According to this Article, each Party shall empower its competent authorities to order ‘a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider’s possession or control’. The T-CY Guidance Note No. 10 specifies that ‘the storage of subscriber information in another jurisdiction does not prevent the application of Article 18 Budapest Convention as long as such data is in the possession or control of the service provider’.⁶⁵

5.2 US law

5.2.1 Cooperation between US law enforcement and US-based service providers

In a significant development for U.S. law enforcement’s ability to access data stored abroad, the US Congress enacted the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) at the end of March 2018. The Act enables US law enforcement to compel Internet service providers based in the US and subject to the Stored Communication Act (SCA)⁶⁶ to hand over data, whether that data is located within or outside the US, by adding the following extraterritoriality provision to the SCA:

‘A [provider] shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider’s possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.’⁶⁷

The CLOUD Act’s enactment mooted the Microsoft Ireland case that the Supreme Court was set to resolve. This case involved a dispute between Microsoft and the US government regarding the extraterritorial reach of the SCA. More specifically, the issue at stake was whether a warrant obtained under the SCA could compel a US company to produce information under its control but stored outside the US. The government argued that its warrant authority required US-based service providers to turn over responsive data, regardless of where these data happened to be held. Microsoft, by contrast, argued that this authority only extended to data located within the territorial boundaries of the US. If the data was stored in a foreign country, Microsoft’s view was that the US could not compel production via a US-issued warrant. Rather, it would be required to make a MLA request for the data and rely on the foreign government to access the data and turn it over back to the US. After the CLOUD Act’s enactment, the US obtained a new warrant seeking the emails at issue in its dispute with Microsoft under the authority of the new law.⁶⁸ Because both the US

⁶⁵T-CY, Guidance Note No. 10: Production orders for subscriber information (Article 18 Budapest Convention), adopted by the T-CY following the 16th Plenary by written procedure (28.2.2017), T-CY(2015)16, p. 7.

⁶⁶The SCA applies to a provider of an ‘electronic communications service,’ defined in 18 U.S.C. § 2510(15), and a ‘remote computing service,’ defined in 18 U.S.C. § 2711(2).

⁶⁷CLOUD Act, § 103(a)(1), adding 18 U.S.C. § 2713.

⁶⁸*United States v. Microsoft Corp.*, No. 17-2, 548 U.S. ___, 2018 WL 1800369, slip op. at 2 (U.S. Apr. 17, 2018) (per curiam).

and Microsoft agreed that the new warrant replaced the prior warrant, the Supreme Court concluded on 17 April 2018 that the case had become moot, and vacated the lower court's rulings with instructions to dismiss.⁶⁹

5.2.2 *Cooperation between foreign law enforcement and US-based service providers*

The SCA does not prohibit US-based providers of electronic communication services or remote computing services⁷⁰ from disclosing metadata to foreign governments.⁷¹ As a result, US-based service providers can cooperate as much as they want on a voluntary basis with foreign law enforcement authorities. This is particularly important considering that technology companies headquartered in the US hold a majority of the world's electronic communications on their server and that foreign governments frequently seek data held by US companies.

It should be noted that the CLOUD Act fails to require that foreign countries meet any standards for transborder metadata request. On the contrary, Section 105 of the CLOUD Act removes the SCA's blocking provision on disclosure of content data to foreign governments⁷² but sets forth a long list of restrictions on the type of governments which can enter into an executive agreement with the US and thereby be able to issue production orders directly to US providers. First, foreign governments are only eligible if the Attorney General, in conjunction with the Secretary of State, certifies in writing, and with an accompanying explanation, that the foreign government 'affords robust substantive and procedural protections for privacy and civil liberties' with respect to relevant data collection activities. Second, the CLOUD Act requires the executive branch to certify that the foreign government has adopted 'appropriate' procedures to minimise the acquisition, retention, and dissemination of information concerning U.S. persons. Third, partner foreign governments are required to have adopted appropriate minimisation procedures with respect to the acquisition, retention, and dissemination of U.S. person data. Fourth, the CLOUD Act mandates that any data sharing agreement concluded under the Act contain a set of requirements related to foreign governments' orders issued to service providers. These include, among other things, requirements that all orders identify a specific person, account, or other identifier that is the object of the order; be premised on a 'reasonable justification based on articulable and credible facts, particularity, and severity regarding the conduct under investigation'; not intentionally target a U.S. person (or person located in the U.S.) or target a non-U.S. person with the intention of obtaining information about a U.S. person; be issued for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution or a 'serious 'crime'—a term that the CLOUD Act states includes terrorism, but otherwise does not define; comply with the domestic law of the issuing country; not be used to infringe freedom of

⁶⁹ *United States v. Microsoft Corp.*, No. 17-2, 548 U.S. ___, 2018 WL 1800369, slip op. at 2 (U.S. Apr. 17, 2018) (per curiam).

⁷⁰ 18 U.S.C. § 2702(a)(1)-(2).

⁷¹ 18 U.S.C. § 2702(c)(6).

⁷² 18 U.S.C. § 2702(a)(3).

speech; and satisfy additional requirements for real-time communications captured by wiretap.

5.3 The proposed E-evidence regulation of the European Union

At the moment, most national legislations within the EU do not allow law enforcement authorities to order a service provider established in another Member State to disclose data. Indeed, as highlighted by the European Commission Services in December 2017, '[t]he majority of EU legislations either do not cover or explicitly prohibit that service providers established in the Member State respond to direct requests from law enforcement authorities from another EU Member State or third country'.⁷³ In this context, foreign governments which want to access data, in particular metadata, held by EU-based service providers must proceed through the burdensome MLA process.

However, this situation may change if the recent proposal of the European Commission for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters is adopted by the European Parliament and the Council.⁷⁴ The proposal indeed makes it easier for EU Member States to secure and gather electronic evidence for criminal proceedings held by a service provider established or represented in the EU, whether the data is physically stored within or outside the EU. First, the European Commission proposes to create a European Production Order which will allow a judicial authority in one Member State to request electronic evidence, in particular metadata, directly from a service provider offering services in the Union and established or represented in another Member State, regardless of the location of data.⁷⁵ The service provider will be obliged to respond within 10 days, and within 6 hours in cases of emergency (as compared to 120 days for the existing European Investigation Order (EIO) or much longer for a MLA procedure).⁷⁶ Second, the proposal will prevent data from being deleted with a European Preservation Order.⁷⁷ This will allow a judicial authority in one Member State to oblige a service provider offering services in the Union and established or represented in another Member State to preserve specific data to enable the authority to request this information later via mutual legal assistance, a EIO or a European Production Order.

Acknowledgements Open access funding provided by Max Planck Society.

⁷³European Commission (Services), Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, 2017, p. 4. In the same vein, T-CY, Criminal justice access to data in the cloud: Cooperation with 'foreign' service providers: Background paper prepared by the T-CY Cloud Evidence Group, 3.5.2016, T-CY(2016)2, p. 23 ('European providers are not disclosing data directly to foreign authorities and only respond to orders received via domestic authorities following mutual legal assistance requests').

⁷⁴European Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, 17.4.2018.

⁷⁵For more on the European Production Order, see Chap. 2 of the Proposal.

⁷⁶Art. 9 of the Proposal.

⁷⁷For more on the European Preservation Order, see Chap. 2 of the Proposal.

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

1. Bourguignon, J.: La recherche des preuves informatiques et l'exercice extraterritorial des compétences de l'Etat. In: *Internet et le droit international*, Colloque de Rouen. Pedone, Paris (2014)
2. Brenner, S.W.: Cybercrime jurisdiction. *Crime Law Soc. Change* (2006)
3. Brenner, S.W.: Toward a criminal law for cyberspace: distributed security. *Boston Univ. J. Sci. Technol. Law* (2004)
4. Brenner, S.W.: Toward a criminal law for cyberspace: product liability and other issues. *Pittsbg. J. Technol. Law* (2004)
5. Brenner, W./Koops B-J, S.: Approaches to cybercrime jurisdiction. *J. High Technol. Law* (2004)
6. Broadhurst, R.: Developments in the global law enforcement of cyber-crime. *Policing, Int. J. Police Strateg. Manag.* (2006)
7. Brown, C.S.D.: Investigating and prosecuting cybercrime: forensic dependencies and barriers to justice. *Int. J. Cyber Criminol.* (2015)
8. Clarke, R.A., Morell, M.J., Stone, G.R., Swire, P.: *The NSA Report: Liberty and Security in a Changing World*. Princeton University Press, Princeton (2014)
9. Davies, D.J.: Criminal law and the internet: the investigator's perspective. *Crim. Law Rev., Special edition: Crime, Criminal Justice and the Internet* (1998)
10. De Hert, Fuster, P., B-J, G.: Fighting cybercrime in the two Europes: the added value of the EU framework decision and the council of Europe convention. *Rev. Int. Droit Pénal* (2006)
11. Del Tufo, V./Rafaraci T, M.: Report on the Italian legal framework. Preparatory Colloquium of AIDP Section IV (International Criminal Law) in View of the XIXe International Congress of Penal Law, Information Society and Criminal Law, Helsinki, 10–12 June 2013 (2014). Available at <http://www.penal.org/sites/default/files/files/RH-9.pdf>
12. Donnedieu de Vabres, H.: *Les principes modernes du droit pénal international*. Sirey, Paris (1928)
13. Donnedieu de Vabres, H.: *Traité de droit criminel et de législation pénale comparée*, 3rd edn. Sirey, Paris (1947)
14. Ehlscheid, D., Briel, O.G.: *Steuerstrafrecht*, 2nd edn. Dt Anwaltverl, Bonn (2001)
15. Faraldo Cabana, P., Catalina Benavente, M.: Report on the Spanish legal framework. Preparatory Colloquium of AIDP Section IV (International Criminal Law) in View of the XIXe International Congress of Penal Law, Information Society and Criminal Law, Helsinki, 10–12 June 2013 (2014). Available at <http://www.penal.org/sites/default/files/files/RH-13.pdf>
16. Foggetti, N.: Transnational cyber crime, differences between national laws and development of European legislation: by repression? *Masaryk Univ. J. Law Technol.* (2008)
17. Foucault, M.: *Discipline and Punish: The Birth of the Prison*. Random House, New York (1995)
18. Gable, K.A.: Cyber-apocalypse now: securing the internet against cyberterrorism and using universal jurisdiction as a deterrent. *Vanderbilt J. Transnatl. Law* (2010)
19. Gercke, M.: *Rechtswidrige Inhalte im Internet: eine Diskussion Ausgewählter Problemfelder des Internet-Strafrechts unter Berücksichtigung Strafprozessualer Aspekte*. Selbstverl, Köln (2000)
20. Gilbert, G.: Crimes Sans Frontières: Jurisdictional Problems in English Law. In: *British Yearbook of International Law* (1993)
21. Gless, S., A./Stagno D./Martin, J.: Report on the Swiss legal framework. Preparatory Colloquium of AIDP Section IV (International Criminal Law) in View of the XIXe International Congress of Penal Law, Information Society and Criminal Law, Helsinki, 10–12 June 2013 (2014). Available at <http://www.penal.org/sites/default/files/files/RH-17.pdf>
22. Greenemeier, L.: Seeking address: why cyber attacks are so difficult to trace back to hackers (2011). Available at <http://www.scientificamerican.com/article/tracking-cyber-hackers/>
23. Hayashi, M.: The Information revolution and the rules of jurisdiction in public international law. In: Dunn, M., Krishna-Hensel, S.F., Mauer, V. (eds.) *The Resurgence of the State: Trends and Processes in Cyberspace Governance*. Ashgate, Aldershot (2007)
24. Huet, A., Koering-Joulin, R.: *Droit pénal international*, 3rd edn. Presses Universitaires de France, Paris (2005)

25. Jessberger, F.: Report on the German legal framework. Preparatory Colloquium of AIDP Section IV (International Criminal Law) in View of the XIXe International Congress of Penal Law, Information Society and Criminal Law, Helsinki, 10–12 June 2013 (2014). Available at <http://www.penal.org/sites/default/files/files/RH-8.pdf>
26. Jofer, R.: *Strafverfolgung im Internet*. Lang, Frankfurt (1999)
27. Kaspersen, H.W.K.: Cybercrime and internet jurisdiction. Council of Europe discussion paper (2009). Available at <https://rm.coe.int/16803042b7>
28. Klip, A.: XIXe International Congress of Penal Law (Information Society and Criminal Law), Section IV, general report. *Rev. Int. Droit Pénal* (2014)
29. Koops, B.M.: Cyberspace, the cloud, and cross-border criminal investigation (2014). Available at <https://www.gccs2015.com/sites/default/files/documents/Bijlage1-CloudOnderzoek.pdf>
30. Kulesza, J.: *International Internet Law*. Routledge, Oxon (2012)
31. Lipson, H.F.: Tracking and tracing cyber-attacks: technical challenges and global policy issues (2002). Available at https://resources.sei.cmu.edu/asset_files/SpecialReport/2002_003_001_13928.pdf
32. Maillart, J-B.: Article 12(2) (a) Rome statute: the missing piece of the jurisdictional puzzle (2014). Available at <https://www.ejiltalk.org/article-122a-rome-statute-the-missing-piece-of-the-jurisdictional-puzzle/>
33. Morris, D.A.: Tracking a computer hacker. *US Attorneys Bull.* (2001)
34. Muir, J.A., Van Oorschot, P.C.: Internet geolocation and evasion. *ACM Computer Survey* (2009)
35. Rosenzweig, P.: *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*. Praeger, Santa Barbara (2013)
36. Ryngaert, C.: *Jurisdiction in International Law*, 2nd edn. Oxford University Press, Oxford (2015)
37. Schmitt, M.N.: *Tallinn Manual on the International Law Applicable to Cyber Warfare*: Prepared by the Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge University Press, Cambridge (2013)
38. Schultz, H.: Compétence des juridictions pénales pour les infractions commises à l'étranger. *Rev. Sci. Crim. Droit Pénal Comp.* (1967)
39. Schwerha J. J. I.V., Law: Law enforcement challenges in transborder acquisition of electronic evidence from 'cloud computing providers'. Council of Europe discussion paper (2010). Available at <https://rm.coe.int/16802fa3dc>
40. Seitz, N., Search, T.: A new perspective in law enforcement? *Yale J. Law Technol.* (2005)
41. Sieber, U.: Collecting and using evidence in the field of information technology. In: Eser, A., Thorundsson, J. (eds.) *Old Ways and New Needs in Criminal Legislation* Max-Planck-Institute für ausländisches und internationales Strafrecht, Freiburg-im-breisgau (1989)
42. Sieber, U.: Cybercrime and jurisdiction in Germany: the present situation and the need for new solutions. In: Brenner, S.W., Koops, B-J. (eds.) *Cybercrime and Jurisdiction*. Asser Press, The Hague (2006)
43. Sieber, U., Neubert, C-W.: Transnational criminal investigations in cyberspace: challenges to national sovereignty. In: *Max Planck Yearbook of United Nations Law* (2017)
44. Smit, A.M.G.: Report on the Dutch legal framework. Preparatory Colloquium of AIDP Section IV (International Criminal Law) in View of the XIXe International Congress of Penal Law, Information Society and Criminal Law, Helsinki, 10–12 June 2013 (2014). Available at <http://www.penal.org/sites/default/files/files/RH-11.pdf>
45. Taylor, M., J./Gresty D./Lamb, D.: Forensic investigation of cloud computing systems. *Netw. Secur.* (2011)
46. Thornburg, N.: The invasion of Chinese cyberspies. *Time* (29.8.2005)
47. Velasco, C.: Cybercrime jurisdiction: past, present and future. *ERA Forum* (2015)
48. Vestergaard J./Füchsel, M.R.: Report on the Danish legal framework. Preparatory Colloquium of AIDP Section IV (International Criminal Law) in View of the XIXe International Congress of Penal Law, Information Society and Criminal Law, Helsinki, 10–12 June 2013 (2014). Available at <http://www.penal.org/sites/default/files/files/RH-5.pdf>
49. Walden, I.: Law enforcement access to data in cloud. In: Millard, C. (ed.) *Cloud Computing Law*. Oxford University Press, Oxford (2013)
50. Wong, C.: Criminal jurisdiction over internet crimes. In: Hohloch, G. (ed.) *Recht und Internet. Nomos, Baden-Baden* (2000)
51. Ziolkowski, K.: General principles of international law as applicable in cyberspace. In: Ziolkowski, K. (ed.) *Peacetime Regime for State Activities in Cyberspace*. NATO CCD COE Publications, Tallinn (2013)