CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Anna-Maria Osula

# Accessing Extraterritorially Located Data: Options for States

Tallinn 2015

*www.ccdcoe.org*
*publications@ccdcoe.org*

# Table of Contents

# Executive summary

Preventing, responding to and investigating cyber incidents rely on time-critical access to relevant data. Operational cooperation between different private and public entities and national law enforcement agencies is one of the prerequisites of a successful investigation. However, given the structure of the internet and in particular the widespread use of cloud computing by citizens, private entities and States, the physical location of data necessary for an investigation is often difficult to determine. This raises several questions regarding the appropriate legal mechanisms to be used in accessing extraterritorially located data in the course of an investigation of a cyber incident. There is a need to analyse alternative and more effective legal tools, and to find a balance with the legal structures intended to protect the data and the privacy of individuals.

A number of different measures for accessing extraterritorially located data are currently employed. Since most known cyber incidents will be legally qualified as criminal offences, the entities involved are usually national law enforcement bodies. In the context of accessing extraterritorially located data as part of an investigation, the principal tools used are Mutual Legal Assistance (MLA) mechanisms, which allow to gain access to evidence by officially contacting the other State.

However, despite the frequent use of MLA, there are a number of factors that do not make the MLA framework entirely suitable for time-critical access to extraterritorial data. Therefore, States are actively looking for alternatives to the traditional MLA framework.

The alternative measures introduced in this paper can be divided into two groups. The first group includes options for formal and informal cooperation between States that, besides MLA, entails the use of multinational databases, exchange of information between national databases, use of international bodies such as Europol, Eurojust or Interpol, informal cooperation between law enforcement entities, and others. The second group comprises of formal and informal cooperation between States and third parties. This includes *inter alia* contacting the Service Provider (SP) directly (such as exemplified by the quoted Microsoft and Yahoo! cases) and practising 'direct' transborder access (such as prescribed by the Council of Europe (CoE) Convention Article 32 or under certain circumstances, by some national legal frameworks). The measures in both of these groups have their own pros and cons.

In discussing the possible way ahead, this paper concludes that, unless the identified inefficiencies pertaining to MLA are addressed, the traditional focus on territoriality and assuming that the other State is the primary counterpart for carrying out investigative measures requiring transborder access to evidence will continue to gradually shift to more operational mechanisms that do not necessarily require the prior authorisation of the State where the data is located. However, moving away from the formal MLA will entail challenges regarding the transparency of criminal investigations and will decrease the control of sovereign States over investigations and their conditions regarding data held in their territory.

In order to find a common ground between States, and overcome the inconclusive state of international law, viable options and conditions for transborder access should be examined in open discussions where States share their legal assessments together with examples of accepted State practice. These discussions could be facilitated, and continue to be supported, by international organisations such as the European Union (EU) and the CoE.

# 1. Introduction[1]

Investigations into cyber incidents are increasingly faced with complex jurisdictional puzzles where the victim, the perpetrator, the Service Provider (SP) and the evidence may each be in different jurisdictions.[2] Since most of the known cyber incidents are legally qualified as cyber crime and therefore investigated as part of criminal procedure, the bodies in charge of their investigation are national law enforcement agencies such as police, military police, security police, border guards and also possibly the entities dealing with tax and customs.

Law enforcement agencies have long realised that the success of such cross-border investigations relies to a significant degree on up-to-date legal and procedural frameworks as well as on functional mechanisms for international cooperation. Increasingly, to investigate any type of crime of transnational character, or involving evidence stored abroad, there is a need for timely measures to access the evidence that is located in a foreign jurisdiction.

This paper will first give a brief overview on the role of criminal procedure and law enforcement entities in investigating cyber incidents, and then move on to the options for States to access extraterritorially located data. Specifically, the mechanisms of Mutual Legal Assistance (MLA) and other established measures for international cooperation in the fight against cyber crime will be discussed. Due to the increasing volume and importance of digital evidence in investigations of cyber incidents, the need to access such data quickly will only increase. Therefore, the effectiveness of these MLA procedures is highly relevant and should be a priority for States. If alternative measures are to be used or proposed by State entities, these need to be in accordance with both national and international legal frameworks.

# 2. The role of law enforcement in criminal procedure

Most known cyber incidents will be investigated as part of domestic criminal procedure. The regulation for domestic criminal procedure may vary in different legal systems, but is generally built on similar founding principles. The following examples are based on Estonian domestic law, with the aim to give a brief overview of one nation's approach to criminal procedure.

Although different legal systems may vary in their specific approaches, criminal procedure usually includes pre-trial and court procedures as well as procedures for the enforcement of the decisions made in criminal matters.[3] Generally, the sources of criminal procedure law lie within a State's constitution, generally recognised principles and provisions of international law, international agreements binding on the State, relevant domestic legal acts, and the decisions of the State's Supreme Court on issues which are not regulated by other sources of criminal procedure law but which arise in the application of the law.[4]

---

[1] This research paper draws, and expands, upon earlier research published as: Anna-Maria Osula, 'Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data' (2015) Vol 9 Masaryk University Journal of Law and Technology. The views expressed are those of the author in her personal capacity and do not necessarily reflect those of any institution with which they are affiliated.

[2] According to United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, February 2013, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf., 'between 50 and 100 per cent of cybercrime acts encountered by the police involve a transnational element.' xxv, 117–118.

[3] E.g. § 1, Estonian Code of Criminal Procedure, RT I, 30.12.2014, 9.

[4] E.g. Ibid., § 2.

The proceedings are conducted by courts, prosecutors' offices and investigative bodies.[5] The investigative bodies involved in the proceedings are defined by law. For example, in Estonia investigative bodies include the Police and Border Guard Board, the Security Police Board, the Tax and Customs Board, the Competition Board, the Military Police, the Environmental Inspectorate, and the Prisons Department of the Ministry of Justice and the prison.[6] These bodies perform their functions directly or through institutions administered by them. According to Estonian law, an investigative body shall perform the procedural acts provided for in law independently, unless the permission of a court or the permission or order from a prosecutor's office is necessary for the performance of the act.[7] In Estonia, pre-trial proceedings are usually conducted by the Police and Border Guard Board and the Security Police Board, unless the investigative jurisdiction specifies a concrete set of acts that need to be investigated by specific bodies.[8] For example, the Military Police is in charge of the pre-trial procedures in the case of criminal offences relating to service in the Defence Forces and war crimes.[9]

The efficient struggle against cyber crime is based on a number of interlinked elements. Primarily, successful investigation and prosecution rely on harmonised and up-to-date substantial and procedural criminal law. The harmonisations of different national criminal laws continue to be important in order to avoid situations where behaviour legal in one jurisdiction is illegal in another, and this may hinder the prosecution of the case.[10] Of equal importance, national law must arm law enforcement with the necessary tools for carrying out modern investigations.

Some of these procedures may entail more intrusive measures such as surveillance[11] and such regulation must be especially transparent and undertaken in accordance with law. The law lists those law enforcement agencies which are entitled to carry out surveillance activities and the legal bases for these activities. For example, under Estonian law, the Military Police may conduct surveillance activities in the event of criminal offences specified in law: if there is a need to collect information about the preparation of a criminal offence for the purpose of detection and prevention thereof; for the purposes of the execution of a ruling on declaring a person a fugitive; if there is a need to collect information in confiscation proceedings; or if there is a need to collect information in a criminal

[5] E.g. Ibid., § 16.
[6] Ibid., § 31.
[7] Ibid., § 32 (2).
[8] In 2013, 95% of the criminal proceedings in Estonia were initiated by the Police and Border Guard Board. The Military Police initiated 17 cases in 2013. Prosecutor's Office, 'Riigi Peaprokuröri Ülevaade Riigikogu Põhiseaduskomisjonile Seadusega Prokuratuurile Pandud Ülesannete Täitmise Kohta 2013. aastal' (2014), 6 <http://www.prokuratuur.ee/sites/www.prokuratuur.ee/files/elfinder/article_files/riigi_peaprokurori_ettekanne_pohiseaduskomisjonile_2013_0.pdf>.
[9] 'The Military Police of the Estonian Defence Forces is a structural unit of the Defence Forces whose functions are the exercise of supervision over discipline in the Defence Forces, the conduct of proceedings regarding offences within the limits of its competence and, on the basis of the assessment of hazards, the protection of foreign defence ministers, the managerial staff of foreign troops, the managerial staff of civilian and military headquarters of the North-Atlantic Treaty Organisations, the minister responsible for the field Defence and the Commander of the Defence Forces and other persons designated' by law. § 21 (1) of the Estonian Defence Forces Organisation Act RT I, 16.12.2014, 9; § 212 (1), (2) 3) Estonian Code of Criminal Procedure.
[10] Marco Gercke, Understanding Cybercrime: Phenomena, Challenge and Legal Response (International Telecommunication Union, 2012), 82–83, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.
[11] E.g. Estonian Code of Criminal Procedure, Chapter 3 - Surveillance Activities.

proceeding about a criminal offence.[12] Accordingly, the Military Police may make enquiries to telecommunications undertakings to get the information needed to establish the end-user who is connected to the identified user in the electronic communication network, and to get access to the data stored by the phone, mobile phone, internet, email service and other similar providers,[13] provided that they have received an authorisation for making the enquiry from the prosecutor's office.[14]

The measures described above are usually regarded as being territorially limited to the territory of the State. However, investigative measures relevant to the purposes of this paper relate to obtaining data from outside the domestic jurisdiction. Usually, the channels for obtaining data located extraterritorially may be built on formal or informal relationships but must always be in line with international law and supported by domestic legislation and procedures. Among other restrictions, these measures need to take into account the boundaries set by jurisdiction that reflect the extent of a State's right to regulate the conduct or the consequences of events.[15] In the context of cyber crime, the interpretation and implementation of jurisdictional principles are relevant for both prosecuting the offence (prescriptive jurisdiction – the capacity to make law, judicial jurisdiction – the power of the courts to try cases) as well as for specific cross-border investigatory measures (jurisdiction to enforce – the capacity to ensure compliance with the adopted laws, also to investigate offences). Although jurisdiction is primarily territorial, there are a number of instances that allow for its extraterritorial application.[16]

A lot of research has been undertaken regarding the limits of prescriptive jurisdiction, whereas the territorial scope of jurisdiction to enforce has undeservedly received little attention. In fact, it is the interpretation of the latter that is especially relevant for outlining the rules for accessing and obtaining data from foreign jurisdictions. This is based on the international law principle according to which the exercise of jurisdiction to enforce on the territory of another State is permitted only if the latter provides consent for such behaviour (for example, based on a bi- or multilateral agreement) or such a right would be derived from international customary law.[17] States that fail to acquire consent for 'exercising power' on the foreign territory may therefore be acting contrary to the principle of non-intervention[18] and may violate the sovereignty of the States concerned.[19] The most common way for States to prevent such possible violation of international law, if in need of evidence located extraterritorially or other support in transnational criminal matters, is basing the cooperation on MLA treaties and another cooperation mechanisms and thus requiring the consent of the other State before exercising jurisdiction in its territory.

[12] Ibid., § $126^2$ (1).
[13] § $111^1$ (2) and (3) of the Estonian Electronic Communications Act RT I, 23.03.2015.
[14] § $41^1$ of the Estonian Defence Forces Organisation Act.
[15] L. Oppenheim, Oppenheim's International Law, 9th ed (London; New York: Longman, 1996), 456.
[16] For more on jurisdiction, see e.g. Malcolm N Shaw, *International Law* (Cambridge University Press 2008) 645–696.
[17] The Case of the S.S. Lotus, Fr. v. Turk, 1927 P.C.I.J. (ser. A) No. 10, at 4 (Decision No. 9), 45.
[18] United Nations, Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the Charter of the United Nations, A/RES/25/2625, 1970.
[19] Pierre Trudel, 'Jurisdiction over the Internet: A Canadian Perspective,' in Int'l L., vol. 32, 1998, 1047.

# 3. International cooperation for accessing stored data

Over recent decades international cooperation mechanisms have developed significantly, driven mainly by international communities or groups of like-minded States. Today, international cooperation in criminal procedure consists of a number of measures outlined in domestic legislation. Such measures usually entail extradition of persons to foreign States, mutual assistance between States in criminal matters, execution of the judgments of foreign courts, taking over and transfer of criminal proceedings, cooperation with the International Criminal Court and regional bodies such as Eurojust, as well as specific regional extradition arrangements such as between Member States of the European Union.[20] The law also lists reasons for refusing requests for international cooperation, which may include:

1) If it may endanger the security, public order or other essential interests of the State;
2) If it is in conflict with the general principles of domestic law; or
3) If there is reason to believe that the requested international cooperation assistance is requested for the purpose of bringing charges against or punishing a person on account of his or her race, nationality or religious or political beliefs, or if the situation of the person may deteriorate due to any such reasons.[21]

In the context of accessing extraterritorially located data, requests for assistance are, in conjunction with relevant national legislation, mostly based on:

1) Bi-lateral agreements on MLA;
2) Multilateral agreements such as the Council of Europe Convention on Cybercrime, European Convention on Mutual Legal Assistance in Criminal Matters and other Council of Europe treaties, United Nations and other international treaties, or
3) Reciprocity.[22]

Depending on the MLA framework to be used and the countries being asked, the exact content and conditions for submission and response differ.[23] For example, MLA requests may have to be sent to a central authorising authority such as the Ministry of Justice, they may be forwarded directly to the relevant national authorities, or other channels such as INTERPOL may be employed.[24] Also, the national bodies authorising, in response to a received MLA request, domestic access to stored computer data may vary according to the type of data to be accessed (e.g. subscriber data, traffic data or content data).[25] In Estonia, the national entities competent to engage in international cooperation in criminal procedure, to the extent provided by law and international agreements, are Courts, the Prosecutors' Offices, the Police and Border Guard Board, the Security Police Board, the Tax and Customs Board, the Environmental Inspectorate, the Competition Board and the Military

[20] E.g. § 433 (1), Estonian Code of Criminal Procedure.
[21] E.g. Ibid., § 436 (1).
[22] Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, December 3, 2014, 31, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf.
[23] Ibid.
[24] Ibid., 38.
[25] Ibid., 31–33.

Police.[26] In addition to traditional MLA measures, some countries also provide for more expedited procedures such as:

> *'in cases of urgency, a request for assistance submitted through the International Criminal Police Organisation (INTERPOL) or a notice in the Schengen Information System may be complied with before the request for assistance is received by the Ministry of Justice with the consent of the Office of the Prosecutor General.'*[27]

Two examples of international organisations that have attempted to provide more uniform approaches for MLA regarding accessing extraterritorially stored computer data are the European Union and the Council of Europe.

## 3.1 European Union

The European Union is increasingly covering different aspects of pre- and post-trial measures. This has introduced a certain degree of harmonisation of criminal procedure across Member States while at the same time being far from enforcing a pan-European code of criminal procedure.[28] The founding documents of EU criminal assistance build to a great extent upon the Council of Europe Convention on Mutual Assistance in Criminal Matters,[29] parts of the Schengen Convention,[30] the EU Convention on Mutual Assistance in Criminal Matters,[31] and its Protocol.[32]

Development of a common European approach for more effective investigations has advanced in stages. In 2003, the EU addressed the need for immediate mutual recognition of orders to prevent the destruction, transformation, movement, transfer or disposal of evidence and adopted a Framework Decision outlining the rules under which a Member State recognises and executes in its territory a freezing order issued by a judicial authority of another Member State in the framework of criminal proceedings.[33] However, this instrument is restricted to the freezing phase, and therefore a freezing order is required to be accompanied by a separate request for the transfer of evidence to the State issuing the order in accordance with the rules applicable to mutual assistance in criminal

[26] § 435 (2), Estonian Code of Criminal Procedure.
[27] Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, 38; Estonian Code of Criminal Procedure, § 462, 'Processing of requests for assistance received from foreign States'.
[28] Samuli Miettinen, Criminal Law and Policy in the European Union, Routledge Research in European Union Law 3 (Abingdon, Oxon; New York: Routledge, 2013), 176.
[29] Council of Europe, European Convention on Mutual Assistance in Criminal Matters, 1959, http://www.conventions.coe.int/Treaty/en/Treaties/Html/030.htm.
[30] The Schengen Acquis - Convention Implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the Gradual Abolition of Checks at Their Common Borders, Official Journal L 239, 22.09.2000.
[31] Council of the European Union, Council Act of 29 May 2000 Establishing in Accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197, 12.7.2000.
[32] Council of the European Union, Council Act of 16 October 2001 Establishing, in Accordance with Article 34 of the Treaty on European Union, the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ 326, 21.11.2001.
[33] Council Framework Decision 2003/577/JHA of 22 July 2003 on the Execution in the European Union of Orders Freezing Property or Evidence, OJ L 196, 2.8.2003, para. 1.

matters; and such a two-step procedure has been reported to be detrimental to efficiency and seldom used in practice by the competent authorities.[34]

In 2008, the EU adopted the Council Framework Decision for the European Evidence Warrant in order to further enhance judicial co-operation by applying the principle of mutual recognition to judicial decisions for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters.[35] However, the instrument has been criticised as having a limited scope since it only applies to 'evidence which already exists' (and is readily available), and thus is not as useful to the investigators.[36]

The next development took place in 2009, when the Stockholm Programme proposed setting up a comprehensive system for obtaining evidence in cases with a transborder dimension that would be based on the principle of mutual recognition, and it was hoped thereby to tackle the EU's fragmented approach in matters related to evidence gathering in criminal proceedings.[37]

In the most recent development, in 2014 the EU adopted a Directive on the European Investigation Order (EIO) in criminal matters,[38] which outlines a framework for a judicial authority of one Member State to 'have one or several specific investigative measure(s) carried out in another Member State'[39] in order to obtain evidence. Law enforcement agencies should opt to use an EIO when the execution of such an investigative measure seems proportionate, adequate and applicable to the case in hand.[40] Such investigative measures also include interception of telecommunications, which should not be limited to the content of the telecommunications, but could also cover 'collection of traffic and location data associated with such telecommunications, allowing competent authorities to issue an EIO for the purpose of obtaining less intrusive data on telecommunications'.[41] In addition to the measures described in the Directive, EU Member States are also encouraged to use Joint Investigative Teams.[42]

Put in a more general context of the EU criminal procedures, the Directive is indeed a significant step forward since it indicates a gradual shift from the MLA mechanisms where the requested Member State has a wide discretion to comply with the request of another Member State, into a mutual recognition mechanism where each Member State must in principle recognise and execute a request

[34] European Union, Directive of the European Parliament and of the Council of Regarding the European Investigation Order in Criminal Matters, OJ L 130, 1.5.2014, para. 3.
[35] European Union, Council Framework Decision 2008/978/JHA of 18 December 2008 on the European Evidence Warrant for the Purpose of Obtaining Objects, Documents and Data for Use in Proceedings in Criminal Matters, OJ L 350, 30.12.2008.
[36] European Union, Directive of the European Parliament and of the Council of Regarding the European Investigation Order in Criminal Matters, OJ L 130, 1.5.2014, para. 4.
[37] European Union, 'The Stockholm Programme - An Open and Secure Europe Serving and Protecting the Citizen 2010/C 115/01' (Council of the European Union, December 2, 2009), OJ C 115 4.5.2010.
[38] European Union, Directive of the European Parliament and of the Council of Regarding the European Investigation Order in Criminal Matters, OJ L 130, 1.5.2014.
[39] Importantly, as of 22 May 2017, this Directive will replace most of the existing laws in the area of transferring evidence between Member States in criminal cases. European Union, Directive of the European Parliament and of the Council of Regarding the European Investigation Order in Criminal Matters, OJ L 130, 1.5.2014, para. 1 (1).
[40] European Union, Directive of the European Parliament and of the Council of Regarding the European Investigation Order in Criminal Matters, OJ L 130, 1.5.2014, para. 11.
[41] Ibid., para. 30.
[42] 'Joint Investigation Teams (JITs),' https://www.europol.europa.eu/content/page/joint-investigation-teams-989.

coming from another Member State.[43,44] It also underlines that the Member States of the EU trust each other sufficiently not to question each other's procedures.[45] However, for the purposes of transborder access, the Directive does still not solve the need for time-critical access to transborder data during an investigation because it allows 90 days for responding to such requests.[46] The Directive does, however, allow for a shorter deadline when required by the seriousness of the offence or in other particularly urgent circumstances, and this should be taken into account as much as possible when fulfilling the request.[47]

## 3.2 Council of Europe

The only international treaty that includes provisions regarding MLA specifically in cyber crime is the Council of Europe (CoE) Convention on Cybercrime.[48] As of 1st of July 2015, the Convention has been signed by 54 and ratified by 47 Parties.[49]

The founding principle of the chapter on international cooperation in the Convention is to invite its Parties to provide each other mutual assistance to the widest extent possible (Articles 23 and 25 (1)). This principle guides the Parties to provide extensive co-operation to each other based on various proposed measures, and to minimise possible impediments to the smooth and rapid flow of evidence and information across borders.[50] At the same time, the Convention makes it clear that its provisions do not 'supersede other similar provisions of international agreements on mutual legal assistance and extradition, reciprocal arrangements between the Parties, or relevant provisions of domestic law related to international co-operation.[51] The Convention also outlines procedures to be used for mutual assistance requests in the absence of an applicable international agreement (Articles 27 and 28), while underlining that the drafters of the Convention specifically rejected the creation of a separate general regime of mutual assistance that would be applied in lieu of other applicable instruments and arrangements.[52]

Specific provisions encourage 'expedited' means of communication (Article 25) which aim to accelerate the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted or

[43] European Union, Directive of the European Parliament and of the Council of Regarding the European Investigation Order in Criminal Matters, OJ L 130, 1.5.2014, para. 12.
[44] Steve Peers and Emilio De Capitani, 'EU Law Analysis: The European Investigation Order: A New Approach to Mutual Recognition in Criminal Matters,' Blog, EU Law Analysis, (May 23, 2014), http://eulawanalysis.blogspot.com/2014/05/the-european-investigation-order-new.html.
[45] Koops, B.-J. and Goodwin, M., 'Cyberspace, the Cloud, and Cross-Border Criminal Investigation' (2014) 25 <http://english.wodc.nl/images/2326-volledige-tekst_tcm45-588171.pdf>.
[46] European Union, Directive of the European Parliament and of the Council of Regarding the European Investigation Order in Criminal Matters, OJ L 130, 1.5.2014, article 12 (4).
[47] Ibid., article 12 (2).
[48] Council of Europe, Convention on Cybercrime 2001, ETS No. 185.
[49] Council of Europe, 'Convention on Cybercrime, List of Signatories and Ratifications.' (5 October 2014) <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG>.
[50] Council of Europe, 'Explanatory Report to the Convention on Cybercrime (ETS No. 185)' para 242 <http://conventions.coe.int/Treaty/EN/Reports/html/185.htm>.
[51] Ibid., 244.
[52] Ibid., 262.

responded to.[53] Use of 24/7 networks (Article 35) and sharing spontaneous information (Article 26) are also encouraged.

As a possibly useful measure for urgent requests, the Convention includes options for expedited preservation of stored computer data where the other Party is requested to preserve information stored in its territory before the mutual assistance request has been formally submitted (Article 29). Such preservation is a limited, provisional measure intended to be used much more quickly than the execution of traditional mutual assistance and does not require dual criminality.[54] Besides allowing for the provision on expedited disclosure of preserved traffic data (Article 30), the Convention also provides for 'mutual assistance regarding accessing of stored computer data' (Article 31).

For the purposes of accessing extraterritorially located data, Article 31 is one of the principal legal constructs informing Parties about possible options for access. It prescribes an option for one Party to ask another to 'search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29' (Article 31 (1)). Importantly, the provision also allows requests for such assistance on an expedited basis where 'there are grounds to believe that relevant data is particularly vulnerable to loss or modification' or there are other legal grounds for providing for expedited co-operation (Article 31 (3a)). Unfortunately, there are currently no statistics on the frequency of the use of mutual assistance to access stored computer data amongst the Parties to the Convention. One of the main reasons for this is the increasingly decentralised nature of MLA where a growing number of requests are sent or received directly between relevant judicial authorities and not only via central authorities.[55] Even if such proposed measures should in principle be less time-consuming than traditional MLA requests, they are still fraught with practical challenges such as how to identify the State in which the desired data is stored at (e.g. if cloud computing is used), the relative ease with which perpetrators can host their data in countries that are not Parties to the Convention or other MLA treaties, and the ability of perpetrators to move from one IP address to another or use temporary storage facilities.[56]

# 4. MLA mechanisms

According to a global survey carried out by the United Nations, approximately 70% of the means of international cooperation in cybercrime investigations are based on traditional MLA mechanisms.[57] Although there is no universal approach to MLA treaties' format, content or other requirements, MLA is widely regarded as the official channel for obtaining evidence, even to the extent that in some countries only material received via MLA, as opposed to data being obtained via alternative channels, can be used as evidence in court.[58] In other national frameworks national legislation offers more flexibility and requires a formal MLA request when accessing only certain types of data (such as content data).[59] There are also countries that do not put forward a detailed regulatory framework and

[53] Ibid., 256.
[54] Ibid., 282, 285.
[55] Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, 6.
[56] Koops, B.-J. and Goodwin, M., 27.
[57] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, 201.
[58] Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, 7.
[59] Ibid.

only require the evidence to be gathered in accordance with the legislation of the other State and not to be in conflict with the principles of domestic criminal procedure.[60]

However, recent studies have reported that the high percentage of the use of MLA is in contrast with the characteristics of MLA procedures, which generally do not satisfy the needs of modern time-critical cyber crime investigations.[61]

In the context of accessing extraterritorially stored computer data, MLA procedures have been deemed to have a number of weaknesses. According to a recent CoE study, MLA is considered 'too complex, lengthy and resource intensive' and thus often abandoned.[62] Indeed, with MLA it may take months or even years for the requested evidence to reach the requesting State.[63] In a recent case *In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation*[64] the appellant, Microsoft, argued that, instead of the procedure undertaken by the US government and directed at Microsoft as a company based in the US, the US should have used MLA procedures to gain access to the desired data stored on Microsoft servers located in Ireland. In the Brief in Support of the Magistrate Judge's Decision, the government argued that:

> *'Microsoft's rosy view of the efficacy of the MLAT [Mutual Legal Assistance Treaty] 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.'*[65]

In addition to the inherent slowness of MLA procedures, they may always not cover all the required investigative measures. Also, there may be situations where there is no MLA treaty in place, the other State is simply uncooperative, accessing the data is urgent in order to avoid it being destroyed, or it is impossible to identify the jurisdiction of the data altogether due to, for example, the characteristics of cloud computing.[66] Further problems include refusals to cooperate for 'small' offences, lack of information from the requested country about the receipt or the status of the request, problems with the content of the requests (too broad, unclear criteria for urgent requests, problems with language, terminology) and differences in legal systems.[67]

Taking into account all of these factors, it is no surprise that the CoE has concluded, based on responses from 39 States, that the MLA process is inefficient in general and with respect to obtaining

[60] E.g. Estonian Code of Criminal Procedure, para. 65 (1).
[61] E.g. Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, 38–39.
[62] Ibid., 123.
[63] Ibid., 39.
[64] *In the Matter of a Warrant to Search a Certain E-mail Account: Controlled and Maintained by Microsoft Corporation*, F. Supp. 2d., 2014 WL 1661004 (S.D.N.Y. 25 April 2014).
[65] United States District Court Southern District of New York, 'In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation' (2014) Government's Brief in Support of the Magistrate Judge's Decision to Uphold a Warrant Ordering Microsoft to Disclose Records Within its Custody and Control 13 Mag. 2814 M9-150, 25–26.
[66] New Zealand and Law Commission, Search and Surveillance Powers (Wellington, N.Z.: Law Commission, 2007), 226.
[67] Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, 38–39.

electronic evidence in particular.[68] Individual States have also acknowledged that current mutual assistance arrangements may not be 'sufficiently tailored to facilitate intangible evidential material being efficiently collected from other jurisdictions.'[69] Similarly, some scholars have suggested that it is time to 'move beyond classical mutual legal assistance' that would enable law-enforcement authorities to exercise other forms of access to extraterritorially located data.[70] It has been noted, however, that there are currently conflicting views on who is responsible for solving the problems related to the MLA system and whether possible solutions should be global in application.[71]

At the same time, according to the CoE, the Parties to the Convention appear not to be making full use of the opportunities offered by the Convention and other specific agreements.[72] A set of recommendations for both Parties and other relevant entities on how to improve MLA in the context of accessing stored computer data has therefore been proposed by the CoE. Keeping in mind that MLA foresees procedures that are in the interests of the sovereign States since they allow for certain transparency and an overview of the activities of law enforcement targeting data stored in foreign territory, States should show more initiative in updating bilateral MLA treaties or reaching a consensus on more effective multilateral terms. In addition to MLA, alternative cooperation mechanisms must be considered.

# 5. Alternative cooperation mechanisms

As it is clear that States are in need of more effective investigatory mechanisms for fighting cyber crime, several formal and informal alternatives for transborder data access have already emerged or are currently under discussion. These options for transborder access do not solve all the issues that were previously discussed in relation to the MLA system, but each targets a certain type of a situation where these measures may be preferred over the traditional MLA.

In general, different approaches for accessing and obtaining data as part of an investigation from a foreign jurisdiction can be divided into two groups.

## 5.1. Formal and informal cooperation between States

The first group of measures consists of formal and informal mechanisms that guide the cooperation between the law enforcement agencies of two or more countries and involve formal or informal State authorisation in allowing for the requesting entity to access the data.

Besides the already mentioned MLA, other formalised procedures and communication channels include *inter alia*:

1) Multinational databases such as the Schengen Information System – a large-scale information system that supports external border control and law enforcement cooperation in the

[68] Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, 123.
[69] New Zealand and Law Commission, Search and Surveillance Powers, 227.
[70] Koops, B.-J. and Goodwin, M., 8.
[71] Gail Kent, 'Sharing Investigation Specific Data with Law Enforcement - An International Approach' [2014] Stanford Public Law Working Paper, 9 <http://ssrn.com/abstract=2472413>.
[72] Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, 123.

Schengen States. The system allows competent authorities, such as police and border guards, to enter and consult alerts on certain categories of wanted or missing persons and objects;[73]

2) Exchange of information stored in national databases under frameworks such as the European Information Exchange Model, or other bi- or multilateral arrangements for expedited information exchange,[74] and

3) Europol, Eurojust or Interpol or similar regional or international bodies that facilitate cooperation between countries, as well as joint investigation teams,[75] or law enforcement liaison officers or networks.[76]

States also engage in different types of more informal cooperation. One of the measures most frequently used is informal cooperation between the law enforcement agencies of different countries. Such cooperation is generally aimed at exchanging information that could lead to the commencement of criminal proceedings, even if, as in many cases, the information obtained through such alternative cooperation cannot be used as evidence in those proceedings.[77]

States have diverse rules as to what data may be shared with other States outside the MLA framework.[78] Some countries may share specified traffic and subscriber data for investigative purposes, others may share subscriber information based on reciprocity, while there are also States that are able to share only data that can be obtained domestically by the police without compulsory measures and thus without a court order.[79] CoE has suggested that the opening of a domestic investigation following a foreign request or receipt of spontaneous information should facilitate the sharing of information without an MLA, or even accelerate MLA.[80]

The CoE Convention also proposes to maintain and use 24/7 networks,[81] and encourages spontaneously disclosing information to the foreign law enforcement[82] 'where it appears relevant to

[73] Read more at Schengen Information System, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm.

[74] E.g. for the information exchange mechanisms in the EU, read more at Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security, COM(2015) 185 Final.

[75] The competent authorities of two or more EU Member States can set up a JIT for a specific purpose and a limited period of time to carry out criminal investigations in one or more of the EU Member States setting up the team. In particular, a JIT can be set up when: (i) an EU Member State's investigations into criminal offences require difficult and demanding investigations having links with other EU Member States; (ii) a number of EU Member States are conducting investigations into criminal offences in which the circumstances of the case necessitate coordinated, concerted action in the EU Member States involved. Also seconded members from other EU Member States, Europol, Eurojust and OLAF may take part in the JIT and support the team. Read more at European Commission, Migration and Home Affairs, Operational cooperation, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/operational-cooperation/index_en.htm

[76] Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, 91.

[77] It must be noted that the distinction between police-to-police cooperation and MLA is not always very clear. Read more: Ibid., 7–8.

[78] Ibid., 8.

[79] Ibid.

[80] Ibid.

[81] Except for the use of MLAs, however, these methods are under-used and handle only approximately 3 per cent of the cyber crime cased confronted by LEAs; United Nations Office on Drugs and Crime, Comprehensive

conduct seemingly connected to the foreign territory, rather than waiting for the foreign LEA to commence an investigation and initiate a formal MLA request'.[83]

## 5.2. Formal and informal cooperation between States and third parties

The second group of mechanisms for accessing and obtaining extraterritorial data by law enforcement is characterised by 'sidestepping' the State as the determining factor for the location of the data, and thus not always asking for nor requiring the authorisation of any of the formal State entities. Examples of such a pathway include:

1) Directly contacting the SP;
2) Accessing data publicly available;
3) Accessing data with the consent of the 'lawfully authorised entity'; and
4) Directly accessing the data either knowing or not knowing its physical location.

Whereas there is emerging evidence of State practice as well as developments in international organisations supporting such mechanisms, the approaches to regulating law enforcement's mandate for accessing and acquiring data are largely divided and usually not sufficiently clear in national legislation. One reason for not paying more attention to formalising or codifying these options may also be that States realise that such measures decrease the control of the sovereign State over the foreign law enforcement's requests as well as activities for accessing evidence stored in its own territory.

### 5.2.1. Directly contacting the Service Provider

It is not uncommon for law enforcement agencies to directly request the foreign SP to disclose the required data.[84] Such cooperation can be based on the terms and conditions provided to the users which often clearly states that data may be shared with law enforcement under specific circumstances.[85] SPs may require due legal process for data disclosure, or they may in some circumstances comply voluntarily with direct requests.[86] Some SPs, such as eBay and Facebook, even have dedicated portals for facilitating such exchanges.[87]

---

Study on Cybercrime, xxv. About the role of 24/7 contact points pertaining to mutual legal assistance for accessing stored computer data, see Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, 88–89.

[82] Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, 9–10.

[83] Ian Walden, 'Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent' (Social Science Research Network 2011) SSRN Scholarly Paper ID 1781067, 12 <http://papers.ssrn.com/abstract=1781067>.

[84] E.g. Micheál O'Floinn, 'It Wasn't All White Light before Prism: Law Enforcement Practices in Gathering Data Abroad, and Proposals for Further Transnational Access at the Council of Europe,' Computer Law & Security Review 29, no. 5 (October 2013), 611; United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, xxii–xxiii.

[85] Simon Bradshaw, Christopher Millard, and Ian Walden, 'Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services,' International Journal of Law and Information Technology 19, no. 3 (September 21, 2011), 187–223.

[86] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, xxii–xxiii.

[87] eBay Inc., 'Law Enforcement eRequest System', https://lers.corp.ebay.com/AIP/portal/home.do; Facebook, 'Law Enforcement Online Requests', https://www.facebook.com/records/x/login/ quoted in O'Floinn, 'It Wasn't All White Light before Prism,' 611.

At the same time, there are on-going legal debates whether the SP is in the position to provide the foreign law enforcement the requested data or whether this would require a separate MLA request. This is illustrated by two recent court cases.

The *Yahoo! Inc* case revolves around a criminal prosecution of fraud committed through the use of Yahoo! email accounts. During the investigation of the case, the Public Prosecutor requested subscriber information from Yahoo! under Art 46bis of the Belgian Code of Criminal Procedure which obliges electronic communication SPs to disclose identification data to law enforcement agencies when these agencies request them. Yahoo! refused to provide the requested information on the bases that was established in the US and did not have a branch office in Belgium. After series of judgements, the Court of Appeal of Antwerp finally agreed in November 2013 that, among other conclusions, Yahoo! was indeed obliged to disclose the identity of the persons who committed fraud via their Yahoo! e-mail accounts because it is a was "virtually" located in Belgium by offering electronic communications services in Belgium.[88]

In the already mentioned *Re Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp*[89] case the Magistrate ordered by way of a warrant under the Stored Communications Act that Microsoft should disclose the content of emails in connection with a criminal investigation that were stored by Microsoft's wholly owned subsidiary in a data center in Ireland. Microsoft refused to disclose content data physically stored in Ireland, citing presumption against extraterritorial reach of laws. The Federal District Court took the stance that such a request for information was not an extraterritorial application of the law because the data requested was 'within [Microsoft's] control'.[90] Microsoft has appealed the judgment and the case will be discussed again in the United States Court of Appeals for the Second Circuit.[91]

Both of the cases underline how national law may be interpreted by domestic courts in the light of the need for law enforcement to get access to the data related to the offences under investigation, regardless of the where the data is stored or where the Service Provider is based. These cases also exemplify the confusion that a certain reading of national legislation may bring about regarding the interpretation of international law.

### 5.2.2. Transborder access

Other means for formal and informal cooperation between States and third parties include accessing data where publicly available, accessing data with the consent of the 'lawfully authorized entity', and directly accessing the data either knowing on unknowing its physical location. These options have been described in literature as 'transborder access'.

[88] 2012/CO/1054 Yahoo! Inc (Court of Appeal of Antwerp, 12th chamber for criminal cases 2013). For a review, see, e.g. Stibbe, ICT Law Newsletter, N49, http://www.stibbe.com/en/news/2014/july/benelux-ict-law-newsletter-49-court-of-appeal-of-antwerp-confirms-yahoo-obligation.

[89] United States District Court, In the Matter of a Warrant to Search a Certain E-mail Account: Controlled and Maintained by Microsoft Corporation (2014).

[90] *United States District Court of Texas Houston Division, In Re Warrant to Search a Target Computer at Premises Unknown, Case no H-13-234M,* 18.

[91] Brief for Appellant in the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation on Appeal from the United states District Court for the Southern District of New York, (14-2985-cv December 18, 2014), available at: http://digitalconstitution.com/wp-content/uploads/2014/12/Microsoft-Opening-Brief-120820141.pdf

The term 'transborder access' is mostly used as signifying unilateral access (i.e., accessing, copying, seizing) to computer data stored in another jurisdiction without previously seeking specific mutual assistance.[92] Despite deriving from the wording of the CoE Convention on Cybercrime, the term has not found univocal support in literature or in legislation, and consequently, different authors are using several almost synonymous terms (e.g. 'direct law enforcement access to extra-territorial data', 'remote search and seizure', 'direct penetration').[93]

One of the bases for discussing transborder access is Article 32 of the CoE Convention on Cybercrime. The article puts forward regulation for 'Transborder access to stored computer data with consent or where publicly available', prescribing the following:

> *'A Party may, without the authorisation of another Party:*
>
> *a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or*
>
> *b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.'*[94]

The option for transborder access as proposed by the Convention to its Parties has generated a lot of controversy, leading to some countries citing it as a reason not to join the Convention.[95] In fact, Article 32 (b) can be interpreted as allowing for remote search and seizure,[96] however, with a number of uncertainties as regards to the exact conditions for such an investigative measure. The explanatory memorandum explains the difficulties in reaching an agreement on transborder access:

> *'The issue of when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance was a question that the drafters of the Convention discussed at length. There was detailed consideration of instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules. Ultimately, the drafters decided to only set forth in Article 32 of the Convention situations in which all agreed that unilateral action is permissible. They agreed not to regulate other situations until such time as*

[92] Definition adapted from Council of Europe, 'T-CY Guidance Note # 3: Transborder Access to Data (Article 32)' (Cybercrime Convention Committee (T-CY) 2014) T-CY (2013)7 E <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)7REV_GN3_transborder_V12adopted.pdf>.

[93] See Anna-Maria Osula, 'Transborder access and territorial sovereignty', Computer Law and Security Review 2015, footnote 13 (forthcoming).

[94] Council of Europe, Convention on Cybercrime.

[95] Keir Giles, 'Russia's Public Stance on Cyberspace Issues,' in 2012 4th International Conference on Cyber Conflict, ed. C. Czosseck, R. Ottis, and K. Ziolkowski (NATO CCD COE Publication, 2012), 66–67, http://www.ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf.

[96] Ian Walden, Computer Crimes and Digital Investigations (Oxford; New York: Oxford University Press, 2007), 319.

*further experience has been gathered and further discussions may be held in light thereof.'*[97]

The explanatory report does not offer much clarity in regards of the exact meaning of the terms put forward in the clause, and the further guidance published by the CoE[98] also leaves some questions up in the air. The guidance note does, however, confirm that Article 32 (b) is an exception to the principle of territoriality in the sense that it permits 'unilateral transborder access without the need for mutual assistance under limited circumstances.'[99] Given that the current wording is not clear about the exact meaning of 'lawful authority', some commentators suggest that the provision in its current wording probably contradicts fundamental principles of international law since law enforcement agencies are not allowed to carry out investigations in another State without the consent of the competent authorities in that State.[100] It has been argued that the decision on whether such investigative measures should be allowed should not be dependent on the authorisation of an individual but should remain with the States, also for purposes for overall transparency.[101]

In an attempt to address MLA inefficiencies, and building on examples of national legislations allowing for transborder access under certain conditions, the CoE proposed in 2013 the adoption of an Additional Protocol to the Convention on Cybercrime regarding transborder access to data.[102] The draft element of an Additional Protocol included five proposals: [103]

1) 'Transborder access with consent without the limitation to data stored "in another Party"' – this option may entail access when the location of the data is unknown or be further expanded to include situations where the data is known to be stored in the territory of non-Parties;

2) 'Transborder access without consent but with lawfully obtained credentials' – this option may also need to include access to data the location of which is unknown or where the data is known to be stored in the territory of non-Parties;

3) 'Transborder access without consent in good faith or in exigent or other circumstances' – this option would expand the original requirement of the consent of a lawful authority and add a number of circumstances under which transborder access would be allowed without such consent (e.g. prevent imminent danger, physical harm, the escape of a suspect, risk of destruction of relevant evidence) or in 'good faith' where law enforcement is not able to

[97] Council of Europe, 'Explanatory Report to the Convention on Cybercrime (ETS No. 185)', 293.
[98] Council of Europe, 'T-CY Guidance Note # 3: Transborder Access to Data (Article 32)'.
[99] Ibid., 3.
[100] Gercke, Understanding Cybercrime: Phenomena, Challenge and Legal Response, 277.
[101] Ibid., 278. See also Nicolai Seitz, 'Transborder Search: A New Perspective in Law Enforcement,' Yale JL & Tech. 7 (2004), 40.
[102] Council of Europe Cybercrime Convention Committee (T-CY), (Draft) Elements of an Additional Protocol to the Budapest Convention on Cybercrime Regarding Transborder Access to Data, April 9, 2013, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY%282013%2914transb_elements_protocol_V2.pdf.
[103] Summarised from Council of Europe, '(Draft) Elements of an Additional Protocol to the Budapest Convention on Cybercrime Regarding Transborder Access to Data' (2013) T-CY (2013)14 <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY%282013%2914transb_elements_protocol_V2.pdf>.

determine the location of the data during an investigation, or may have obtained evidence from a foreign territory by mistake or accident;

4) 'Extending a search without the limitation "in its territory" in Article 19.3' – or in other words, clearly allowing for remote search and seizure on the territory of other Parties, possibly to be expanded to also cover non-Parties, and

5) 'The power of disposal as connecting legal factor' – this option is related to the 'loss of location' situation where it is not possible to determine the location of the data. CoE suggests that the connecting factor that would provide an alternative to territorial jurisdiction could be the 'power of disposal', i.e. data can be connected to a person having the power to 'alter, delete, suppress or to render unusable as well as the right to exclude others from access and any usage whatsoever'.

Detailed analysis of these proposals is out of the scope of this paper. However, it can be observed that while these proposals may be seen as offering needed discussion starters for further developments, they lack concreteness regarding the territorial limits of the proposed measures as well as clarity regarding sufficient safeguards. Therefore, not surprisingly, there has been a lack of consensus on the way forward, and the CoE concluded in 2014 that the 'negotiation of a Protocol on transborder access to data would not be feasible'.[104]

# 6. The way ahead

The previous section discussed formal and informal cooperation between States and third parties. These options for accessing extraterritorially located data do not usurp the central role of the State where the data is located, but instead, prioritise quick access to the evidence. In addition to raising the obvious question of violating the sovereignty of the other State, such access may also raise data protection and privacy concerns among the individuals whose data has been accessed.

Since the need for more operational tools in the fight against cyber crime will not decrease, countries will have to actively look for solutions.[105] Generally speaking, countries are facing two courses of action that are not necessarily incompatible.

Firstly, countries may take steps to find consensus on the use of alternative measures for accessing transborder data, such as is reflected in the work undertaken by the CoE. This would, however, require wider discussions and reaching consensus on a number of interrelated issues that broadly touch upon the '(re)-conceptualization of the extent to which 'data location' can still be used as a guiding principle',[106] especially in circumstances where the exact location of the data cannot be identified. To do that, the debates on the interpretation of the limits of territorial sovereignty that would allow for, under certain circumstances, direct access to the data or the SP without the prior authorisation of the other State must be revisited. Also, the extraterritorial reach of jurisdiction must

[104] Council of Europe Cybercrime Convention Committee (T-CY), Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY, December 3, 2014, 12–13, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf.

[105] For a comprehensive set of possible solutions, see Gail Kent, 'Sharing Investigation Specific Data with Law Enforcement - An International Approach,' Stanford Public Law Working Paper, February 14, 2014, http://ssrn.com/abstract=2472413.

[106] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, 223.

be further addressed, especially in light of examples of some recently adopted national legislation such as Brazil, which has announced that its laws apply to companies that collect, store, retain or process personal or communications data whenever at least one of these activities occurs in Brazilian territory, also applying to every piece of data collected domestically as well as communication content when at least one of the terminals involved in the traffic is located in Brazil, and also in situations where the service is offered to the Brazilian public or when the provider has a branch in that country. [107]

Most importantly, transparency is needed concerning States' official positions in such legal assessments together with examples of accepted State practice. This is would serve two purposes: (i) creating trust between States and within the international community that would facilitate reaching further agreements on transborder access, and (ii) crystallising the (hopefully) emerging consensus on the interpretation of international law. Without more evidence of State practice and views, the traditional understanding of the territorial limits of jurisdiction to enforce will continue to prevail.

Koops and Goodwin conclude that the 'strict limits within international law' present an obstacle for more effective transborder investigations.[108] They propose this to be tackled in stages. They suggest that: (i) the challenges of cross-border investigations be more (formally) recognised within the international community, and not only by law enforcement, (ii) the terms used should be more carefully conceptualised which may facilitate more flexible interpretation of international law, and that (iii) law enforcement and international law community become more familiarised with each other's views and language, in order to develop solutions that are suitable for both technical and legal communities.[109]

Secondly, and assuming that this would be the preferred choice of States keen to protect their sovereignty, States may support the reform of current MLA procedures.[110] These reforms may include efforts to make the MLA process less time-consuming (e.g. adding more staffing and resources to relevant domestic authorities, coming up with a uniform format for specific type MLA requests), critically review the existing MLAs to ensure that they include all needed possibilities for operational cooperation as well as enhancing the cooperation and communication of other relevant national entities. This will not be an easy process since as despite the clear need for more effective investigative tools, States have largely refrained from open discussions on how to enhance these traditional frameworks. It is unclear what the motivation of the States could be in avoiding reaching an agreement on clearer rules for more effective international cooperation. Perhaps one of the reasons could be the general lack of statistics related to cybercrime (lack of reporting, a lack of initiation of prosecutions, and a lack of statistics on the use of different cooperation measures). Hence, there is insufficient underlining of the urgency of dealing with these issues. Assuming, however, that the gap in awareness will be bridged, an initiative could be taken or efforts continue to be pursued by international organisations such as the EU, the CoE, or a group of likeminded States. The latter option has also been supported by Koops and Goodwin who see the focus of short term

[107] Brazil, Presidency of the Republic, Law No. 12.965, April 23rd 2014, Article 11; Francis Augusto Medeiros and Lee A Bygrave, 'Brazil's Marco Civil Da Internet: Does It Live up to the Hype?' (2015) 31 Computer Law & Security Review, 127.
[108] Koops, B.-J. and Goodwin, M., 12.
[109] Ibid 12–13.
[110] A comprehensive list of proposals has been put forward by Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime.

efforts on 'narrowly defined, transparently conducted, and strongly safeguarded unilateral actions of early adopters who advance an alternative account on of sovereignty in cyberspace'.[111] Of course, such geographically restricted agreements would have their limitations regarding global cooperation, but they would nevertheless set an example of effective and transparent measures to other States and encourage them to follow the lead.

# 7. Conclusion

As an increasing number of crimes involve electronic evidence, transborder access to data is relevant not only for the investigation of cyber crime but for all crime. Previous sections of this paper have introduced the different cooperation mechanisms used for transborder access to evidence.

Examples of two organisations actively seeking to provide better conditions for transborder access are the EU and the CoE. Developments in these organisations include the EU's Directive on the European Investigation Order and the option for Joint Investigative Teams, as well as the CoE's work on analysing options for transborder access and carrying out an extensive study of MLA procedures. These initiatives are to be commended, but their efforts do not address the full spectrum of challenges to transborder access.

The widely used MLA mechanisms rely on the authorisation of the other State before gaining access to the data. Such mechanisms are therefore guided by the territoriality principle that focuses on the country in whose territory the data being sought is to be found. Thereby, the sovereignty of the other State is not being breached and the State remains in control of the investigative measures being carried out on its territory or involving data held on its territory.

However, despite the frequent use of MLA, this paper has indicated a number of factors that do not make the MLA framework entirely suitable for time-critical access to extraterritorial data. In spite of the efficiency of MLA procedures in accessing such data being criticised for some years, little meaningful improvement can be observed.

The alternative measures introduced in this paper can be divided into two. The first group includes options for formal and informal cooperation between States that, besides MLA, include the use of multinational databases, exchange of information between national databases, use of international bodies such as Europol, Eurojust or Interpol, informal cooperation between law enforcement entities, and others. The second group entails formal and informal cooperation between States and third parties. This includes *inter alia* contacting the SP directly (such as exemplified by the quoted Microsoft and Yahoo! cases) and practising 'direct' transborder access (such as prescribed by the CoE Convention Article 32 or under certain circumstances, by some national legal frameworks). The measures in both of these groups have their own pros and cons.

Finally, the paper offers an account on the way ahead. It concludes that unless the identified inefficiencies pertaining to MLA are addressed, the traditional focus on territoriality and assuming the other State being the primary counterpart for carrying out investigative measures requiring transborder access to evidence will continue to gradually shift to more operational mechanisms that do not necessarily require the prior authorisation of the State where the data is located. However, distancing from formal MLA will bring along challenges regarding the transparency of criminal

[111] Koops, B.-J. and Goodwin, M., 13.

investigations, and decrease the control of the sovereign State over investigations and their conditions regarding the data held in their territory.

In order to find a common ground between States, and overcome the inconclusive state of international law, viable options and conditions for transborder access should be examined in open discussions where States share their legal assessments together with examples of accepted State practice. These discussions could be facilitated, and continue to be supported, by international organisations such as the EU and the CoE.

# 8. References


2012/CO/1054 Yahoo! Inc (Court of Appeal of Antwerp, 12th chamber for criminal cases 2013).

Anna-Maria Osula, 'Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data' (2015) Vol 9 Masaryk University Journal of Law and Technology.

Anna-Maria Osula, 'Transborder access and territorial sovereignty', Computer Law and Security Review 2015, footnote 13 (forthcoming).

Brazil, Presidency of the Republic, Law No. 12.965, April 23rd 2014, Article 11.

Brief for Appellant in the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation on Appeal from the United states District Court for the Southern District of New York, (14-2985-cv December 18, 2014).

Case of the S.S. Lotus, Fr. v. Turk, 1927 P.C.I.J. (ser. A) No. 10, at 4 (Decision No. 9).

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security, COM(2015) 185 Final.

Council Framework Decision 2003/577/JHA of 22 July 2003 on the Execution in the European Union of Orders Freezing Property or Evidence, OJ L 196, 2.8.2003.

Council of Europe Cybercrime Convention Committee (T-CY), (Draft) Elements of an Additional Protocol to the Budapest Convention on Cybercrime Regarding Transborder Access to Data, April 9, 2013, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY%282013%2914transb_elements_protocol_V2.pdf.

Council of Europe Cybercrime Convention Committee (T-CY), The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, December 3, 2014, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf.

Council of Europe Cybercrime Convention Committee (T-CY), Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY, December 3, 2014, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf.

Council of Europe, 'Convention on Cybercrime, List of Signatories and Ratifications.' (5 October 2014) <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG>.

Council of Europe, 'Explanatory Report to the Convention on Cybercrime (ETS No. 185)' para 242 <http://conventions.coe.int/Treaty/EN/Reports/html/185.htm> .

Council of Europe, 'T-CY Guidance Note # 3: Transborder Access to Data (Article 32)' (Cybercrime Convention Committee (T-CY) 2014) T-CY (2013)7 E <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)7REV_GN3_transborder_V12adopted.pdf>.

Council of Europe, Convention on Cybercrime 2001, ETS No. 185.

Council of Europe, European Convention on Mutual Assistance in Criminal Matters, 1959, http://www.conventions.coe.int/Treaty/en/Treaties/Html/030.htm.

Council of the European Union, Council Act of 16 October 2001 Establishing, in Accordance with Article 34 of the Treaty on European Union, the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ 326, 21.11.2001.

Council of the European Union, Council Act of 29 May 2000 Establishing in Accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197, 12.7.2000.

eBay Inc., 'Law Enforcement eRequest System', https://lers.corp.ebay.com/AIP/portal/home.do.

Estonian Code of Criminal Procedure, RT I, 30.12.2014, 9.

Estonian Defence Forces Organisation Act RT I, 16.12.2014, 9

Estonian Electronic Communications Act RT I, 23.03.2015.

European Commission, Migration and Home Affairs, Operational cooperation, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/operational-cooperation/index_en.htm.

European Union, 'The Stockholm Programme - An Open and Secure Europe Serving and Protecting the Citizen 2010/C 115/01' (Council of the European Union, December 2, 2009), OJ C 115 4.5.2010.

European Union, Council Framework Decision 2008/978/JHA of 18 December 2008 on the European Evidence Warrant for the Purpose of Obtaining Objects, Documents and Data for Use in Proceedings in Criminal Matters, OJ L 350, 30.12.2008.

European Union, Directive of the European Parliament and of the Council of Regarding the European Investigation Order in Criminal Matters, OJ L 130, 1.5.2014.

Facebook, 'Law Enforcement Online Requests', https://www.facebook.com/records/x/login/.

Francis Augusto Medeiros and Lee A Bygrave, 'Brazil's Marco Civil Da Internet: Does It Live up to the Hype?' (2015) 31 Computer Law & Security Review, 127.

Gail Kent, 'Sharing Investigation Specific Data with Law Enforcement - An International Approach,' Stanford Public Law Working Paper, February 14, 2014, http://ssrn.com/abstract=2472413.

Ian Walden, 'Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent' (Social Science Research Network 2011) SSRN Scholarly Paper ID 1781067, 12 <http://papers.ssrn.com/abstract=1781067>.

Ian Walden, Computer Crimes and Digital Investigations (Oxford; New York: Oxford University Press, 2007), 319.

*In the Matter of a Warrant to Search a Certain E-mail Account: Controlled and Maintained by Microsoft Corporation*, F. Supp. 2d., 2014 WL 1661004 (S.D.N.Y. 25 April 2014).

Joint Investigation Teams (JITs), https://www.europol.europa.eu/content/page/joint-investigation-teams-989.

Keir Giles, 'Russia's Public Stance on Cyberspace Issues,' in 2012 4th International Conference on Cyber Conflict, ed. C. Czosseck, R. Ottis, and K. Ziolkowski (NATO CCD COE Publication, 2012), 66–67,

http://www.ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf.

Koops, B.-J. and Goodwin, M., 'Cyberspace, the Cloud, and Cross-Border Criminal Investigation' (2014) 25 <http://english.wodc.nl/images/2326-volledige-tekst_tcm45-588171.pdf>.

L. Oppenheim, Oppenheim's International Law, 9th ed (London; New York: Longman, 1996).

Malcolm N Shaw, *International Law* (Cambridge University Press 2008).

Marco Gercke, Understanding Cybercrime: Phenomena, Challenge and Legal Response (International Telecommunication Union, 2012), https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.

Micheál O'Floinn, 'It Wasn't All White Light before Prism: Law Enforcement Practices in Gathering Data Abroad, and Proposals for Further Transnational Access at the Council of Europe,' Computer Law & Security Review 29, no. 5 (October 2013).

New Zealand and Law Commission, Search and Surveillance Powers (Wellington, N.Z.: Law Commission, 2007).

Nicolai Seitz, 'Transborder Search: A New Perspective in Law Enforcement,' Yale JL & Tech. 7 (2004).

Pierre Trudel, 'Jurisdiction over the Internet: A Canadian Perspective,' in Int'l L., vol. 32, 1998.

Prosecutor's Office, 'Riigi Peaprokuröri Ülevaade Riigikogu Põhiseaduskomisjonile Seadusega Prokuratuurile Pandud Ülesannete Täitmise Kohta 2013. aastal' (2014), 6 <http://www.prokuratuur.ee/sites/www.prokuratuur.ee/files/elfinder/article_files/riigi_peaprokuror i_ettekanne_pohiseaduskomisjonile_2013_0.pdf>.

Samuli Miettinen, Criminal Law and Policy in the European Union, Routledge Research in European Union Law 3 (Abingdon, Oxon; New York: Routledge, 2013).

Schengen Information System, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm.

Simon Bradshaw, Christopher Millard, and Ian Walden, 'Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services,' International Journal of Law and Information Technology 19, no. 3 (September 21, 2011).

Steve Peers and Emilio De Capitani, 'EU Law Analysis: The European Investigation Order: A New Approach to Mutual Recognition in Criminal Matters,' Blog, EU Law Analysis, (May 23, 2014), http://eulawanalysis.blogspot.com/2014/05/the-european-investigation-order-new.html.

Stibbe, ICT Law Newsletter, N49, http://www.stibbe.com/en/news/2014/july/benelux-ict-law-newsletter-49-court-of-appeal-of-antwerp-confirms-yahoo-obligation.

The Schengen Acquis - Convention Implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the Gradual Abolition of Checks at Their Common Borders, Official Journal L 239, 22.09.2000.

United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, February 2013, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

United Nations, Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the Charter of the United Nations, A/RES/25/2625, 1970.

*United States District Court of Texas Houston Division, In Re Warrant to Search a Target Computer at Premises Unknown, Case no H-13-234M,* 18.

United States District Court Southern District of New York, 'In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation' (2014) Government's Brief in Support of the Magistrate Judge's Decision to Uphold a Warrant Ordering Microsoft to Disclose Records Within its Custody and Control 13 Mag. 2814 M9-150.