International Cooperation in Cybercrime: The Budapest Convention

Introduction

In today's increasingly digitized world where an increasing volume of information is being stored in the digital format, access to data generated by digital technologies and on digital platforms is important in solving crimes online and offline. However, the global nature of the internet challenges traditional methods of law enforcement by forcing states to cooperate with each other for a greater variety and number of cases than ever before in the past. The challenges associated with accessing data across borders in order to be able to fully investigate crimes which may otherwise have no international connection forces states to think of easier and more efficient ways of international cooperation in criminal investigations. One such mechanism for international cooperation is the Convention on Cybercrime adopted in Budapest ("**Budapest Convention**"). Drafted by the Council of Europe along with Canada, Japan, South Africa and the United States of America it is the first and one of the most important multilateral treaties addressing the issue of cybercrime and international cooperation.[1]

Extradition

Article 24 of the Budapest Convention deals with the issue of extradition of individuals for offences specified in Articles 2 to 11 of the Convention. Since the Convention allows Parties to prescribe different penalties for the contraventions contained in Articles 2-11, it specifies that extradition cannot be asked for unless the crime committed by the individual carries a maximum punishment of deprivation of liberty for atleast one year.[2] In order to not complicate issues for Parties which may already have extradition treaties in place, the Convention clearly mentions that in cases where such treaties exist, extradition will be subject to the conditions provided for in such extradition treaties.[3] Although extradition is also subject to the laws of the requested Party, if the laws provide for the existence of an extradition treaty, such a requirement shall be deemed to be satisfied by considering the Convention as the legal basis for the extradition.[4] The Convention also specifies that the offences mentioned in Articles 2 to 11 shall be deemed to be included in existing extradition treaties and Parties shall include them in future extradition treaties to be executed.[5]

The Convention also recognises the principle of "*aut dedere aut judicare*" (extradite or prosecute) and provides that if a Party refuses to extradite an offender solely on the basis that it shall not extradite their own citizens,[6] then, if so requested, such Party shall prosecute the

---

[1] Council of Europe, Explanatory Report to the Convention on Cybercrime, https://rm.coe.int/16800cce5b, para 304.

[2] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 24(1)(a). Except in cases where a different minimum threshold has been provided by a mutual arrangement, in which case such other minimum threshold shall be applied.

[3] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 24(5).

[4] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 24(3).

[5] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 24(2).

[6] Council of Europe, Explanatory Report to the Convention on Cybercrime, Para 304, https://rm.coe.int/16800cce5b, para 251.

offender for the offences alleged in the same manner as if the person had committed a similar offence in the requested Party itself.[7] The Convention also requires the Secretary General of the Council of Europe to maintain an updated register containing the authorities designated by each of the Parties for making or receiving requests for extradition or provisional arrest in the absence of a treaty.[8]

Mutual Assistance Requests

The Convention imposes an obligation upon the Parties to provide mutual assistance "to the widest extent possible" for investigations or proceedings of criminal offences related to computer systems and data.[9] Just as in the case of extradition, the mutual assistance to be provided is also subject to the conditions prescribed by the domestic law of the Parties as well as mutual assistance treaties between the Parties.[10] However, it is in cases where no mutual assistance treaties exist between the Parties that the Convention tries to fill the lacuna and provide for a mechanism for mutual assistance.

The Convention requires each Party to designate an authority for the purpose of sending and answering mutual assistance requests from other Parties as well as transmitting the same to the relevant authority in their home country. Similar to the case of authorities for extradition, the Secretary General is required to maintain an updated register of the central authorities designated by each Party.[11] Recognising the fact that admissibility of the evidence obtained through mutual assistance in the domestic courts of the requesting Party is a major concern, the Convention provides that the mutual assistance requests are to be executed in accordance with the procedures prescribed by the requesting Party unless such procedures are incompatible with the laws of the requested Party.[12]

Parties are allowed to refuse a request for mutual assistance on the grounds that (i) the domestic laws of the requested party do not allow it to carry out the request;[13] (ii) the request concerns an offence considered as a political offence by the requested Party;[14] or (iii) in the opinion of the requested Party such a request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.[15] The requested Party is also allowed to postpone any action on the request if it thinks that acting on the request would prejudice criminal investigations or proceedings by its own authorities.[16] In cases where assistance would be

[7] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 24(6).

[8] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 24(7).

[9] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 25(1).

[10] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 25(4).

[11] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 27(2).

[12] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 27(3) read with para 267 of the Explanatory Note to the Budapest Convention.

[13] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 25(4).

[14] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 27(4)(a).

[15] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 27(4)(b).

[16] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 27(5).

refused or postponed, the requested Party may consult with the other Party and consider whether partial or conditional assistance may be provided.[17]

In practice it has been found that though States refuse requests on a number of grounds,[18] some states even refuse cooperation in the event that the case is minor but requires an excessive burden on the requested state.[19] A case study of a true instance recounted below gives an idea of the effort and resources it may take for a requested state to carry out a mutual assistance request:

> "In the beginning of 2005, a Norwegian citizen (let's call him A.T.) attacked a bank in Oslo. He intended to steal money and he did so effectively. During his action, a police officer was killed. A.T. ran away and could not be found in Norway. Some days later, police found and searched his home and computer and discovered that A.T. was the owner of an email account from a provider in the United Kingdom. International co-operation was required from British authorities which asked the provider to put his email account under surveillance. One day, A.T. used his email account to send an email message. In the United Kingdom, police asked the ISP information about the IP address where the communication came from and it was found that it came from Spain.
>
> British and Spanish authorities installed an alert system whose objective was to know, each time that A.T. used his email account, where he was. Thus, each time A.T. used his account, British police obtained the IP address of the computer in the origin of the communication and provided it immediately to Spanish police. Then, Spanish police asked the Spanish ISPs about the owner or user of the IP address. All the connexions were made from cybercafés in Madrid. Even proceeding to that area very quickly, during a long period of time it was not possible to arrive at those places before A.T. was gone.
>
> Later, A.T. began to use his email account from a cybercafé in Malaga. This is a smaller town than Madrid and there it was possible to put all the cybercafés from a certain area permanently under physical surveillance. After some days of surveillance, British police announced that A.T. was online, using his email account, and provided the IP address. Very rapidly, the Spanish ISP informed Spanish police from the

---

[17] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 27(6).

[18] Some of the grounds listed by Parties for refusal are: (i) grounds listed in Article 27 of the Convention, (ii) the request does not meet formal or other requirements, (iii) the request is motivated by race, religion, sexual orientation, political opinion or similar, (iv) the request concerns a political or military offence, (v) Cooperation may lead to torture or death penalty, (vi) Granting the request would prejudice sovereignty, security, public order or national interest or other essential interests, (vii) the person has already been punished or acquitted or pardoned for the same offence "*Ne bis in idem*", (viii) the investigation would impose an excessive burden on the requested State or create practical difficulties, (ix) Granting the request would interfere in an ongoing investigation (in which case the execution of the request may be postponed). Council of Europe, *Cybercrime Convention Committee assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime*, December 2014, pg. 34.

[19] Council of Europe, *Cybercrime Convention Committee assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime*, December 2014, pg. 34.

concrete location of the cybercafé what allowed the officers in the street to identify and arrest A.T. in place.

A.T. was extradited to Norway and prosecuted."[20]

It is clear from the above that although the crime occurred in Norway, a lot of work was actually done by the authorities in the United Kingdom and Spain. In a serious case such as this where there was a bank robbery as well as a murder involved, the amount of effort expended by authorities from other states may be appropriate but it is unlikely that the authorities in Britain and Spain would have allocated such resources for a petty crime.

In sensitive cases where the requests have to be kept secret or confidential for any reason, the requesting Party has to specify that the request should be kept confidential except to the extent required to execute the request (such as disclosure in front of appropriate authorities to obtain the necessary permissions). In case confidentiality cannot be maintained the requested Party shall inform the requesting Party of this fact, which shall then take a decision regarding whether to withdraw the request or not.[21] On the other hand the requested Party may also make its supply of information conditional to it being kept confidential and that it not be used in proceedings or investigations other than those stated in the request.[22] If the requesting Party cannot comply with these conditions it shall inform the requested Party which will then decide whether to supply the information or not.[23]

In the normal course the Convention envisages requests being made and executed through the respective designated central authorities, however it also makes a provision, in urgent cases, for requests being made directly by the judicial authorities or even the Interpol.[24] Even in non urgent cases, if the authority of the requested Party is able to comply with the request without making use of coercive action, requests may be transmitted directly to the competent authority without the intervention of the central authority.[25]

The Convention clarifies that through these mutual assistance requests a Party may ask another to (i) either search, seize or disclose computer data within its territory,[26] (ii) provide real time collection of traffic data with specified communications in its territory;[27] and (iii)

---

[20] Pedro Verdelho, *Discussion Paper: The effectiveness of international cooperation against cybercrime: examples of good practice*, 2008, pg. 5, https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/DOC-567study4-Version7_en.PDF, accessed on March 28, 2019.

[21] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 27(8).

[22] However, disclosure of the material to the defence and the judicial authorities is an implicit exception to this rule. Further the ability to use the material in a trial (which is generally a public proceeding) is also a recognised exception to the right to limit usage of the material. *See* para 278 of the the Explanatory Note to the Budapest Convention.

[23] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 28.

[24] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 27(9)(a) and (b).

[25] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 27(9)(d) read with para 274 of the Explanatory Note to the Budapest Convention.

[26] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 31.

[27] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 33.

provide real time collection or recording of content data of specified communications.[28] The provision of mutual assistance specified above has to be in accordance with the domestic laws of the requested Party.

The procedure for sending mutual assistance requests under the Convention is usually the following:

1. Preparation of a request for mutual assistance by the prosecutor or enforcement agency which is responsible for an investigation.
2. Sending the request by the prosecutor or enforcement agency to the Central Authority for verification (and translation, if necessary).
3. The Central Authority then submits the request either, (i) to the foreign central authority, or (ii) directly to the requested judicial authority.

The following procedure is then followed in the corresponding receiving Party:

1. Receipt of the request by the Central Authority.
2. Central Authority then examines the request against formal and legal requirements (and translates it, if necessary).
3. Central Authority then transmits the request to the competent prosecutor or enforcement agency to obtain court order (if needed).
4. Issuance of a court order (if needed).
5. Prosecutor orders law enforcement (e.g. cybercrime unit) to obtain the requested data.
6. Data obtained is examined against the MLA request, which may entail translation or using a specialist in the language.
7. The information is then transmitted to requesting State via MLA channels.[29]

In practice, the MLA process has generally been found to be inefficient and this inefficiency is even more pronounced with respect to electronic evidence. The general response times range from six months to two years and many requests (and consequently) investigations are often abandoned.[30] Further, the lack of awareness regarding procedure and applicable legislation of the requested State lead to formal requirements not being met. Requests are often incomplete or too broad; do not meet legal thresholds or the dual criminality requirement.[31]

Preservation Requests

The Budapest Convention recognises the fact that computer data is highly volatile and may be deleted, altered or moved, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. The Convention therefore envisioned the concept of preservation orders which is a limited, provisional measure intended to take place much more rapidly than the execution of a traditional mutual assistance. Thus the Convention gives the Parties the legal ability to obtain the expeditious preservation of data stored in the territory of

[28] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 34.

[29] Council of Europe, *Cybercrime Convention Committee assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime*, December 2014, pg. 37.

[30] Council of Europe, *Cybercrime Convention Committee assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime*, December 2014, pg. 123.

[31] *Ibid* at 124.

another (requested) Party, so that the data is not altered, removed or deleted during the time taken to prepare, transmit and execute a request for mutual assistance to obtain the data.

The Convention therefore provides that a Party may request another Party to obtain the expeditious preservation of specified computer data in respect of which such Party intends to submit a mutual assistance request. Once such a request is received the other Party has to take all appropriate measures to ensure compliance with such a request. The Convention also specifies that dual criminality is not a condition to comply with such requests for preservation of data since these are considered to be less intrusive than other measures such as seizure, etc.[32] However in cases where parties have a dual criminality requirement for providing mutual assistance they may refuse a preservation request on the ground that at the time of providing the data the dual criminality condition would not be met, although in regard to the offences covered under Articles 2 to 11 of the Convention, the requirement of dual criminality will be deemed to have been satisfied.[33] In addition to dual criminality a preservation request may also be refused on the grounds that (i) the offence alleged is a political offence; and (ii) execution of the request would likely to prejudice the sovereignty, security, *ordre public* or other essential interests of the requested Party.[34]

In case the requested Party feels that preservation will not ensure the future availability of the data or will otherwise prejudice the investigation, it shall promptly inform the requesting Party which shall then take a decision as to whether to ask for the preservation irrespective.[35] Preservation of the data pursuant to a request will be for a minimum period of 60 days and upon receipt of a mutual assistance request will continue to be preserved till a decision is taken on the mutual assistance request.[36] If the requested Party finds out in the course of executing the preservation request that the data has been transmitted through a third state or the requesting Party itself, it has a duty to inform the requesting Party of such facts as well as provide it with sufficient traffic data in order for it to be able to identify the service provider in the other state.[37]

Jurisdiction and Access to Stored Data

The problem of accessing data across international borders stems from the international law principle which provides that the authority to enforce (an action) on the territory of another State is permitted only if the latter provides consent for such behaviour. States that do not acquire such consent may therefore be acting contrary to the principle of non-intervention and may be in violation of the sovereignty of the other State.[38] The Convention specifies two situations in which a Party may access computer data stored in another Party's jurisdiction;

---

[32] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 29(3) read with para 285 of the Explanatory Note to the Budapest Convention.

[33] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 29(4).

[34] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 29(5).

[35] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 29(6).

[36] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 29(7).

[37] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 30.

[38] Anna-Maria Osula, *Accessing Extraterritorially Located Data: Options for States*, http://ccdcoe.eu/uploads/2018/10/Accessing-extraterritorially-located-data-options-for-States_Anna-Maria_Osula.pdf, accessed on March 28, 2019.

(i) when such data is publicly available; and (ii) when the Party has accessed such data located in another state through a computer system located in its own territory provided it has obtained the "lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system".[39] These are two fairly obvious situations where a state should be allowed to use the computer data without asking another state, infact if a state was required to take the permission of the state in the territory of which the data was physically located even in these situations, then it would likely delay a large number of regular investigations where the data would otherwise be available but could not be legally used unless the other country provided it under the terms of the Convention or some other legal instrument. At the time of drafting the Convention it appears that Parties could not agree upon any other situations where it would be universally acceptable for a state to unilaterally access data located in another state, however it must be noted that other situations for unilaterally accessing data are neither authorized, nor precluded.[40]

Since the language of the Budapest Convention stopped shy of addressing other situations law enforcement agencies had been engaged in unilateral access to data stored in other jurisdictions on an uncertain legal basis risking the privacy rights of individuals raising concerns regarding national sovereignty.[41] It was to address this problem that the Cybercrime Committee established the "ad-hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows" (the "Transborder Group") in November 2011 which came out with a Guidance Note clarigying the legal position under Article 32.

The Guidance Note # 3 on Article 32 by the Cybercrime Committee specifies that Article 32(b) would not cover situations where the data is not stored in another Party or where it is uncertain where the data is located. A Party is also not allowed to use Article 32(b) to obtain disclosure of data that is stored domestically. Since the Convention neither authorizes nor precludes other situations, therefore if it is unknown or uncertain that data is stored in another Party, Parties may need to evaluate themselves the legitimacy of a search or other type of access in the light of domestic law, relevant international law principles or considerations of international relations.[42] The Budapest Convention does not require notification to the other Party but parties are free to notify the other Party if they deem it appropriate.[43] The "voluntary and lawful consent" of the person means that the consent must be obtained without force or deception. Giving consent in order to avoid or reduce criminal charges would also constitute lawful and voluntary consent. If cooperation in a criminal investigation requires explicit consent in a Party, this requirement would not be fulfilled by agreeing to the

[39] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 32.

[40] Council of Europe, Explanatory Report to the Convention on Cybercrime, Para 304, https://rm.coe.int/16800cce5b, para 293.

[41] Council of Europe, Cybercrime Convention Committee, Report of the Transborder Group, *Transborder access and jurisdiction: What are the options?*, December 2012, para 310.

[42] Council of Europe, Cybercrime Convention Committee Guidance Note # 3, Transborder access to data (Article 32), para 3.2.

[43] Council of Europe, Cybercrime Convention Committee Guidance Note # 3, Transborder access to data (Article 32), para 3.3.

general terms and conditions of an online service, even if the terms and conditions indicate that data would be shared with criminal justice authorities.[44]

The person who is lawfully authorized to give consent is unlikely to include service providers with respect to their users' data. This is because normally service providers would only be holders of the data, they would not own or control the data and therefore cannot give valid consent to share the data.[45] The Guidance Note also specifies that with respect to the location of the person providing access or consent, while the standard assumption is that the person would be physically located in the requesting Party however there may be other situations, "It is conceivable that the physical or legal person is located in the territory of the requesting law enforcement authority when agreeing to disclose or actually providing access, or only when agreeing to disclose but not when providing access, or the person is located in the country where the data is stored when agreeing to disclose and/or providing access. The person may also be physically located in a third country when agreeing to cooperate or when actually providing access. If the person is a legal person (such as a private sector entity), this person may be represented in the territory of the requesting law enforcement authority, the territory hosting the data or even a third country at the same time." Parties are also required to take into account the fact that third Parties may object (and some even consider it a criminal offence) if a person physically located in their territory is directly approached by a foreign law enforcement authority to seek his or her cooperation.[46]

Production Order

A similar problem arises in case of Article 18 of the Convention which requires Parties to put in place procedural provisions to compel a person in their territory to provide specified stored computer data, or a service provider offering services in their territory to submit subscriber information.[47] It must be noted here, that the data in question must be already stored or existing data, which implies that this provision does not cover data that has not yet come into existence such as traffic data or content data related to future communications.[48] Since the term used in this provision is that the data must be within the "possession or control" of the person or the service provider, therefore this provision is also capable of being used to access data stored in the territory of a third party as long as the data is within the possession and control of the person on whom the Production Order has been served. In this regard it must be noted that the Article makes a distinction between computer data and subscriber information and specifies that computer data can only be asked for from a person (including a service provider) located within the territory of the ordering Party even if the data is stored in the

[44] Council of Europe, Cybercrime Convention Committee Guidance Note # 3, Transborder access to data (Article 32), para 3.4.
[45] Council of Europe, Cybercrime Convention Committee Guidance Note # 3, Transborder access to data (Article 32), para 3.6.
[46] Council of Europe, Cybercrime Convention Committee Guidance Note # 3, Transborder access to data (Article 32), para 3.8.
[47] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 18.
[48] Council of Europe, Explanatory Report to the Convention on Cybercrime, Para 304, https://rm.coe.int/16800cce5b, para 170.

territory of a third Party.[49] However subscriber information[50] can be ordered only from a service provider even if the service provider is not located within the territory of the ordering Party as long as it is offering its services in the territory of that Party and the subscriber information relates to the service offered in the ordering Party's territory.[51]

Since the power under Article 18 is a domestic power which potentially can be used to access subscriber data located in another State, the use of this Article may raise complicated jurisdictional issues. This combined with the growth of cloud computing and remote data storage also raises concerns regarding privacy and data protection, the jurisdictional basis pertaining to services offered without the service provider being established in that territory, as well as access to data stored in foreign jurisdictions or in unknown or multiple locations "within the cloud".[52] Even though some of these issues require further discussions and a more nuanced treatment, the Cybercrime Committee felt the need to issue a Guidance Note to Article 18 in order to avoid some of the confusion regarding the implementation of this provision.

Article 18(1)(b) may include a situation where a service provider is located in one jurisdiction, but stores the data in another jurisdiction. Data may also be mirrored in several jurisdictions or move between jurisdictions without the knowledge or control of the subscriber. In this regard the Guidance Note points out that legal regimes increasingly recognize that, both in the criminal justice sphere and in the privacy and data protection sphere, the location of the data is not the determining factor for establishing jurisdiction.[53]

The Guidance Note further tries to clarify the term "offering services in its territory" by saying that Parties may consider that a service provider is offering services if: (i) the service provider enables people in the territory of the Party to subscribe to its services (and does not, for example, block access to such services); and (ii) the service provider has established a real and substantial connection that Party. Relevant factors to determine whether such a connection has been established include "the extent to which a service provider orients its activities toward such subscribers (for example, by providing local advertising or advertising in the language of the territory of the Party), makes use of the subscriber information (or associated traffic data) in the course of its activities, interacts with subscribers in the Party,

---

[49] Council of Europe, Explanatory Report to the Convention on Cybercrime, Para 304, https://rm.coe.int/16800cce5b, para 173.

[50] Defined in Article 18(3) as "any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
a. the type of communication service used, the technical provisions taken thereto and the period of service;
b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

[51] Council of Europe, Explanatory Report to the Convention on Cybercrime, Para 304, https://rm.coe.int/16800cce5b, para 173.

[52] Council of Europe, Cybercrime Convention Committee Guidance Note #10, Production orders for subscriber information (Article 18 Budapest Convention), at pg.3.

[53] Council of Europe, Cybercrime Convention Committee Guidance Note #10, Production orders for subscriber information (Article 18 Budapest Convention), para 3.5 at pg. 7.

and may otherwise be considered established in the territory of a Party".[54] A service provider will not be presumed to be offering services within the territory of a Party just because it uses a domain name or email address connected to that country.[55] The Guidance Note provides a very elegant tabular illustration of its requirements to serve a valid Production Order on a service provider:[56]

<table>
<tr><th colspan="3">PRODUCTION ORDER CAN BE SERVED</th></tr>
<tr><td colspan="3">IF
The criminal justice authority has jurisdiction over the offence</td></tr>
<tr><td colspan="3">AND
The service provider is in possession or control of the subscriber information</td></tr>
<tr><td colspan="3">AND</td></tr>
<tr><td>The service provider is in the territory of the Party
(Article 18(1)(a))</td><td>Or</td><td>A Party considers that a service provider is "offering its services in the territory of the Party" when, for example:
- the service provider enables persons in the territory of the Party to subscribe to its services (and does not, for example, block access to such services);
and
- the service provider has established a real and substantial connection to a Party. Relevant factors include the extent to which a service provider orients its activities toward such subscribers (for example, by providing local advertising or advertising in the language of the territory of the Party), makes use of the subscriber information (or associated traffic data) in the course of its activities, interacts with subscribers in the Party, and may otherwise be considered established in the territory of a Party.
(Article 18(1)(b))</td></tr>
<tr><td colspan="3">AND</td></tr>
<tr><td></td><td colspan="2">the subscriber information to be submitted is relating to services of a provider offered in the territory of the Party.</td></tr>
</table>

[54] Council of Europe, Cybercrime Convention Committee Guidance Note #10, Production orders for subscriber information (Article 18 Budapest Convention), para 3.6 at pg. 8.
[55] *Id.*
[56] Council of Europe, Cybercrime Convention Committee Guidance Note #10, Production orders for subscriber information (Article 18 Budapest Convention), para 3.8 at pg. 9.

The existing processes for accessing data across international borders, whether through MLATs or through the mechanism established under the Budapest Convention are clearly too slow to be a satisfactory long term solution. It is precisely for that reason that the Cybercrime Committee has suggested alternatives to the existing mechanism such as granting access to data without consent in certain specific emergency situations;[57] or access to data stored in another country through a computer in its own territory provided the credentials for such access are obtained through lawful investigative activities.[58] Another option suggested by the Cybercrime Committee is to look beyond the principle of territoriality, specially in light of the recent developments in cloud computing where the location of the data may not be certain or data may be located in multiple locations,[59] and look at a connecting legal factor as an alternative such as the "power of disposal". This option implies that even if the location of the data cannot be determined it can be connected to the person having the power to "alter, delete, suppress or render unusable as well as the right to exclude other from access and any usage whatsoever".[60]

Language of Requests

It was found from practice that the question of the language in which the mutual assistance requests were made was a big issue in most States since it created problems such as delays due to translations, costly translations, quality of translations, etc. The Cybercrime Committee therefore suggested that an additional protocol be added to the Budapest Convention to stipulate that requests sent by Parties should be accepted in English atleast in urgent cases since most States accepted a request in English.[61] Due to these problems associated with the language of assistance requests, the Cybercrime Convention Committee has already released a provisional draft Additional Protocol to address the issue of language of mutual assistance requests for public comments.[62]

24/7 Network

Parties are required to designate a point of contact available on a twenty-four hour, seven-day-a week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence, in electronic form, of a criminal offence. The point of contact for each Party is required to have the capacity to carry out communications with the

---

[57] Situations such as preventions of imminent danger, physical harm, the escape of a suspect or similar situations including risk of destruction of relevant evidence.

[58] Council of Europe, Cybercrime Convention Committee, Subgroup on Transborder Access, (Draft) Elements of an Additional Protocol to the Budapest Convention on Cybercrime Regarding Transborder Access to Data, April 2013, pg. 49.

[59] Council of Europe, Cybercrime Convention Committee Cloud Evidence Group, *Criminal justice access to data in the cloud: challenges (Discussion paper)*, May 2015, pgs 10-14.

[60] Council of Europe, Cybercrime Convention Committee, Subgroup on Transborder Access, (Draft) Elements of an Additional Protocol to the Budapest Convention on Cybercrime Regarding Transborder Access to Data, April 9, 2013, pg. 50.

[61] Council of Europe, *Cybercrime Convention Committee assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime*, December 2014, pg. 35.

[62] https://www.coe.int/en/web/cybercrime/-/towards-a-protocol-to-the-budapest-convention-further-consultatio-1

points of contact for any other Party on an expedited basis. It is the duty of the Parties to ensure that trained and properly equipped personnel are available in order to facilitate the operation of the network.[63] The Parties recognized that establishment of this network is among the most important means provided by the Convention of ensuring that Parties can respond effectively to the law enforcement challenges posed by computer-or computer-related crimes.[64] In practice however it has been found that in a number of Parties there seems to be a disconnect between the 24/7 point of contact and the MLA request authorities leading to situations where the contact points may not be informed about whether preservation requests are followed up by MLA authorities or not.[65]

Drawbacks and Improvements

The Budapest Convention, whilst being the most comprehensive and widely accepted document on international cooperation in the field of cybercrime, has its own share of limitations and drawbacks. Some of the major limitations which can be gleaned from the discussion above (and potential recommendations for the same) are listed below:

Weakness and Delays in Mutual Assistance: In practice it has been found that though States refuse requests on a number of grounds,[66] some states even refuse cooperation in the event that the case is minor but requires an excessive burden on the requested state. Further, the delays associated with the mutual assistance process are another major hurdle, and are perhaps the reason by police-to-police cooperation for the sharing of data related to cybercrime and e-evidence is much more frequent than mutual legal assistance.[67] The lack of regulatory and legal awareness often leads to procedural lapses due to which requests do not meet legal thresholds. More training, more information on requirements to be met and standardised and multilingual templates for requests may be a useful tool to address this concern.

Access to data stored outside the territory: Access to data located in another country without consent of the authorities in that country poses another challenge. The age of cloud computing with processes of data duplication and delocalisation of data have added a new

[63] Council of Europe, *Convention on Cybercrime*, 23 November 2001, Article 35.

[64] Council of Europe, Explanatory Report to the Convention on Cybercrime, Para 304, https://rm.coe.int/16800cce5b, para 298.

[65] Council of Europe, *Cybercrime Convention Committee assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime*, December 2014, pg. 86.

[66] Some of the grounds listed by Parties for refusal are: (i) grounds listed in Article 27 of the Convention, (ii) the request does not meet formal or other requirements, (iii) the request is motivated by race, religion, sexual orientation, political opinion or similar, (iv) the request concerns a political or military offence, (v) Cooperation may lead to torture or death penalty, (vi) Granting the request would prejudice sovereignty, security, public order or national interest or other essential interests, (vii) the person has already been punished or acquitted or pardoned for the same offence "*Ne bis in idem*", (viii) the investigation would impose an excessive burden on the requested State or create practical difficulties, (ix) Granting the request would interfere in an ongoing investigation (in which case the execution of the request may be postponed). Council of Europe, *Cybercrime Convention Committee assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime*, December 2014, pg. 34.

[67] Council of Europe, *Cybercrime Convention Committee assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime*, December 2014, pg. 7.

dimension to this problem.[68] It is precisely for that reason that the Cybercrime Committee has suggested alternatives to the existing mechanism such as granting access to data without consent in certain specific emergency situations;[69] or access to data stored in another country through a computer in its own territory provided the credentials for such access are obtained through lawful investigative activities.[70] Another option suggested by the Cybercrime Committee is to look beyond the principle of territoriality and look at a connecting legal factor as an alternative such as the "power of disposal".

Language of requests: Language of requests create a number of problems such as delays due to translations, cost of translations, quality of translations, etc. Due to these problems, the Cybercrime Convention Committee has already released for public comment, a provisional draft Additional Protocol to address the issue.[71]

Bypassing of 24/7 points of contact: Although 24/7 points have been set up in most States, it has been found that there is often a disconnect between the 24/7 point of contact and the MLA request authorities leading to situations where the contact points may not be informed about whether preservation requests are followed up by MLA authorities or not.[72]

India and the Budapest Convention

Although countries outside the European Union have the option on signing the Budapest Convention and getting onboard the international cooperation mechanism envisaged therein, India has so far refrained from signing the Budapest Convention. The reasons for this refusal appear to be as follows:

- India did not participate in the drafting of the treaty and therefore should not sign. This concern, while valid is not a consistent foreign policy stand that India has taken for all treaties, since India has signed other treaties, where it had no hand in the initial drafting and negotiations.[73]
- Article 32(b) of the Budapest Convention involves tricky issues of national sovereignty since it allows for cross border access to data without the consent of the other party. Although, as discussed above, the Guidance Note on Article 32 clarified this issue to an extent, it appears that arguments have been raised in some quarters of

[68] Giovanni Buttarelli, *Fundamental Legal Principles for a Balanced Approach*, Selected papers and contributions from the International Conference on "Cybercrime: Global Phenomenon and its Challenges", Courmayeur Mont Blanc, Italy available at ispac.cnpds.org/download.php?fld=pub_files&f=ispacottobre2012bassa.pdf

[69] Situations such as preventions of imminent danger, physical harm, the escape of a suspect or similar situations including risk of destruction of relevant evidence.

[70] Council of Europe, Cybercrime Convention Committee, Subgroup on Transborder Access, (Draft) Elements of an Additional Protocol to the Budapest Convention on Cybercrime Regarding Transborder Access to Data, April 2013, pg. 49.

[71] https://www.coe.int/en/web/cybercrime/-/towards-a-protocol-to-the-budapest-convention-further-consultatio-1

[72] Council of Europe, *Cybercrime Convention Committee assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime*, December 2014, pg. 86.

[73] Dr. Anja Kovaks, *India and the Budapest Convention - To Sign or not? Considerations for Indian Stakeholders*, available at https://internetdemocracy.in/reports/india-and-the-budapest-convention-to-sign-or-not-considerations-for-indian-stakeholders/

the government that the options provided by Article 32 are too limited and additional means may be needed to deal with cross border data access.[74]

- The mutual legal assistance framework under the Convention is not effective enough and the promise of cooperation is not firm enough since States can refuse to cooperate on a number of grounds.[75]
- It is a criminal justice treaty and does not cover state actors; further the states from which most attacks affecting India are likely to emanate are not signatories to the Convention either.[76]
- Instead of joining the Budapest Convention, India should work for and promote a treaty at the UN level.[77]

Although in January 2018 there were a number of news reports indicating that India is seriously considering signing the Budapest Convention and joining the international cooperation mechanism under it, there have been no updates on the status of this proposal.[78]

Conclusion

The Budapest Convention has faced a number of challenges over the years as far as provisions regarding international cooperation are concerned. These include delays in getting responses from other states, requests not being responded to due to various reasons (language, costs, etc.), requests being overridden by mutual agreements, etc. The only other alternative which is the MLAT system is no better due to delays in providing access to requested data.[79] This however does not mean that international cooperation through the Budapest Convention is always late and inefficient, as was evident from the example of the Norwegian bank robber-murderer given above. There is no doubt that the current mechanisms are woefully inadequate to deal with the challenges of cyber crime and even regular crimes (specially in the financial sector) which may involve examination of electronic evidence. However that does not mean the end of the road for the Budapest Convention, one has to recognize the fact that it is the pre-eminent document on international cooperation on electronic evidence with 62 State Parties as well as another 10 Observer States. Any mechanism which offers a solution to the thorny issues of international cooperation in the field of cyber crime would require most of the nations of the world to sign up to it; till such time that happens, expanding the scope of the Budapest Convention to address atleast some of the issues discussed above by leveraging the work already done by the Cybercrime Committee through various reports and Guidance Notes (some of which have been referenced in this paper itself) may be a good option as this could be an incentive for non signatories to

---

[74] Alexander Seger, *India and the Budapest Convention: Why not?*, Digital Debates: The CyFy Journal, Vol III, available at https://www.orfonline.org/expert-speak/india-and-the-budapest-convention-why-not/

[75] *Id.*

[76] *Id.*

[77] *Id.*

[78] https://indianexpress.com/article/india/home-ministry-pitches-for-budapest-convention-on-cyber-security-rajnath-singh-5029314/

[79] Elonnai Hickok and Vipul Kharbanda, *Cross Border Cooperation on Criminal Matters - A perspective from India*, available at https://cis-india.org/internet-governance/blog/cross-border-cooperation-on-criminal-matters

become parties to a better and more efficient Budapest Convention providing a more robust international cooperation regime.