BUDAPEST CONVENTION ON CYBERCRIME: ASSESSMENT OF INDIA'S CONCERNS

Deepak Parashar[*]

Abstract

The Council of Europe's Convention on Cyber Crime also known as Budapest Convention is the first binding international instrument which seeks to address the global epidemic of cybercrimes in the internet age by harmonization of national laws and promotion of international cooperation in evidence collection, investigation and prosecution of such crimes. While India has a nearly two decade old, fairly robust domestic law to deal with cybercrimes, it is still not a party to the Convention due to various concerns. This paper seeks to identify and assess those concerns in light of the provisionsof the Convention on cybercrime and its working.

I Introduction

CYBERCRIME IS a *sui generis* global threat. In context of crimes having highest impact globally, cybercrime ranks third after corruption and narcotics.[1] Various reports estimate the economic impact of cybercrimes to be ranging from 172 billion[2] to 600 billion[3] USD a year, although some scholars dispute such estimates.[4] Apart from technological limitations in tackling such crimes, the borderless nature of cybercrime poses the biggest challenge for any state to tackle it on its own and requires international cooperation which has challenges of its own. Convention on Cybercrime of Council of Europe[5] is the first binding international

[*] Practicing advocate with the Supreme Court of India.

[1]The Economic Impact of Cybercrime - No Slowing Down, *available at:*https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf (last visited on Dec. 31, 2019).

[2]Norton Cyber Security Insights Report Global Results, *available at:*https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf (last visited on Nov. 1, 2019).

[3] *Supra* note 1.

[4]DineiFlorˆencio and Cormac Herley, "Sex, Lies and Cyber-crime Surveys", *available at:* https://www.microsoft.com/en-us/research/wp-content/uploads/2011/06/SexLiesandCybercrimeSurveys.pdf (last visited on Oct. 31, 2019).

[5]Convention on Cyber Crime also known as Budapest Convention, European Treaty Series No 185, *available at:*https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561(*hereinafter* referred as "Budapest Convention").

instrument which seeks to address the global epidemic of cybercrimes in the internet age by harmonization of national laws and promotion of international cooperation in evidence collection, investigation and prosecution of such crimes. According to a 2017 report by security software firm Symantec[6], India ranked third in the world,based on number of cyber threats detected, and second based on the number of targeted attacks.[7] While India has a nearly two decade old, fairly robust domestic law to deal with cybercrimes, it is still not a party to the Convention due to various concerns. This paper seeks to identify and assess those concerns in light of the provisions, specifically article 32(b) of the Convention on Cybercrime and its working.The paper is divided under five heads. The concepts involved in the discussion are explained under head II, head III covers a brief history and introduction of the Convention on Cybercrime, head IVassesses the concerns raised by India and head V covers the conclusion derived from the assessment.

II The epidemic of cybercrime

Over the last few decades connected computing has become central to our way of life. From mobile phones to connected homes powered by smart devices everything today is connected to internet. Our digital identities created in various databases owned by corporations or government have become essential part of day to day life.

This connected world has opened up new avenues for criminals also with added incentives of anonymity and global reach. From being dominated by individuals, cybercrimes now see involvement of organized crime syndicates. In 2014, a ring of Russian criminals acquired around 1.2 billion username and password combinations[8] which was huge considering there were around 3 billion internet users at the time.[9] United Nations Office on Drugs and Crime in its draft report in 2013 predicted that "In the future hyper-connected society, it is hard to imagine a 'computer crime', and perhaps any crime, that does not involve electronic evidence linked with internet protocol (IP) connectivity"[10] and that indeed has been the reality today.

[6]2018 Internet Security Threat Report, *available at*:https://www.symantec.com/security-center/threat-report (last visited on Nov. 4, 2018).
[7]An attack directed at a specific target or targets as opposed to widescale indiscriminate campaigns. See. *Id.* at 24.
[8]Sam Frizell, "Russian Crime Ring Said to Steal More Than a Billion Internet Passwords*"Time*(Aug. 5, 2014) *available at:*http://time.com/3083504/russian-hackers-passwords/ (last visited on Nov. 7, 2019).
[9] Internet users in the world, *available at:* http (last visited on Nov. 7, 2019).
[10] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime(UNODC, Vienna, 2013) at 1.*Available at:* https://www.unodc.org/documents/organized-

Till now there is no universally accepted definition of cybercrime as the definitions of cybercrime mostly depend upon the national interpretation of the term which is largely dependent upon the domestic laws. Even the Budapest Convention does not define cybercrime for the purposes of the convention. Merriam-Webster defines cybercrime as "criminal activity (such as fraud, theft, or distribution of child pornography) committed using a computer especially to illegally access, transmit, or manipulate data."[11] Although the definition may not be comprehensive to study the entire spectrum of cybercrimes but it does provide a basic understanding that use of computers is at the of the core of such crimes.

Evolution of cybercrimes

The use of computing devices and internet has increased exponentially since the turn of the century.[12] Today connected devices have become part of day to day lives of people are by and large unaware of the security pitfalls that come with the connected existence. The functioning of small businesses, government, corporate and individuals has become highly dependent on the computer software and systems and as a result we place huge trust in such systems. Ever sincethe large-scale adoption of these systems forprocessing and storing valuable business and personal information began, such systems have been a target for criminals too. In the 70s, criminals exploited the tone system used on phone networks. The attack was called phreaking wherein the attackers fraudulently used the networks of telephone companies to make long distance calls by reverse-engineering the tones used by such networks.[13] In 1988, world saw the first worm attack and in 1989 the first ransomware attack.[14] In 90s came web browser and penetration of internet which provided wider reach to cyber criminals and newer crimes such as phishing, viruses, malware, DDoS*etc.* With the advent of online databases and social networking in 2000s identity thefts became the "the new financial piggy bank for criminal organizations around the world."[15] While the cybercrime in the last century was mainly the work of a lone individual working who could have been "a computer nerd aiming for supremacy over the system", it was the involvement

crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf(last visited on Nov. 7, 2019) (*hereinafter* referred to as *UNODC Report)*.

[11]Definition,*available at*: https://www.merriam-webster.com/dictionary/cybercrime (last visited on Nov. 1, 2019).

[12]*Supra* note 9. There were around 400 million internet users in 2000 which has crossed 4 billion in 2018.

[13]The evolution of cybercrime, *available at:*https://hub.packtpub.com/the-evolution-cybercrime/ (last visited on Nov. 7, 2018).

[14]*Ibid.*

[15]*Ibid.*

of organized criminal syndicates around the turn of the century that established cybercrime as an industry valued at nearly $600 billion USD today.[16]

The latest evolutionary threat comes from the terror organizations resorting to technological means made available by the computer system and internet for their terrorist activities. In 2012, a United Nations report on "The Use of the Internet for Terrorist Purposes" noted that:[17]

> the benefits of Internet technology are numerous, starting with its unique suitability for sharing information and ideas, which is recognised as a fundamental human right. It must also be recognised, however, that the same technology that facilitates such communication can also be exploited for the purposes of terrorism. The use of the Internet for terrorist purposes creates both challenges and opportunities in the fight against terrorism.

The 2008 Mumbai attacks illustrated how the terrorists and their handlers based out of Pakistan, exploited Voice over Internet Protocol (VoIP) to communicate and direct the attacks.[18]

Classification of cybercrimes

Cybercrimes can be classified from the perspective of the relationship of the computer to the crime or on the basis of the act itself. On the basis of relationship of computer to the crime, cybercrimes can be categorized into four general types:[19]

i. Where computer is a target – such as information theft and use of such information for other criminal activities. Such acts are against the confidentiality, integrity and availability of computer data or systems for example hacking, virus attacks, ransomware etc.

---

[16]*Supra* note1.

[17]United Nations Office on Drugs and Crime,The Use of the Internet for Terrorist Purposes (United Nations, 2012). *Available at*:http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (last visited on Nov. 7, 2019).

[18] PTI, "VoIP used by 26/11 planners - 150 test calls made before attack"*India Today*, August 18, 2009*available at:*http://indiatoday.intoday.in/story/VOIP+used+by+26-11+planners,+150+test+calls+made+before+attack/1/57314.html (last visited on Nov 4, 2019).

[19]Hamid Jahankhani, A. Al-Nemrat, *et.al.* "Cybercrime classification and characteristics" in Francesca Bosco, Andrew Stanifort*het.al*., *Cyber Crime and Cyber Terrorism Investigator's Handbook* (Elsevier, Waltham, 2014) *Available at*: https://www.researchgate.net/publication/280488873_Cyber_crime_Classification_and_Characteristics (last visited on Nov. 1, 2019).

ii. Where computer is one of the primary instrumentalities of crime –such as ATM frauds, accounts frauds, credit card frauds, online hate speech, production, distribution or possession of child pornography, acts related to terrorism etc.

iii. Where use of computer is incidental –such as use of computer for record keeping or carrying out online transactions where the transaction is valid but part of bigger illegal activity.

iv. Other crimesaided by the use of computers: software piracy, counterfeiting, copyright violation of computer programs, counterfeit equipment etc.

Nature of cybercrimes

Traditional criminological understanding of crime on the basis of social, cultural and material characteristics views crimes as eventsbeing tied to a specific geographical location. This understanding of crime has characterized the crime, and the subsequent design of crime mapping and preventionmechanismsto be tailored to specific target audience. However, this characterization and associated mechanisms are not directly relatable in cases of cybercrime, because the of the inherent nature of the underlying technologies exploited by cybercrimesmakes pinpointing of such crimes to a geographic location, or distinctive social or cultural groupsextremely difficult.[20] Unlike traditional crimes, which can be located to a specific geographical territory, cybercrimes take place in cyberspace, the interconnected world that pans geographical boundaries of nations and makes it difficult for national law enforcing agencies to effectively tackle it in a specific territorial jurisdiction.

Increase in cybercrime and inability of law enforcement agencies to deal with it effectively creates a vicious circle. In the absence of appropriate measures to control and address such crimes, the confidence of such criminals is increased and results in increased incidents and at the same time it lowers the morale of general public affected by such crimes.

Cybercrime in India

According to NCRB data there were 9,622, 11,592 and 12,317 cases registered in 2014, 2015 and 2016 respectively.[21] According to the Indian Computer Emergency Response Team

[20]*Supra* note 19.

[21]National Crime Records Bureau, Crime in India 2016 (Ministry of Home Affairs, 2016).*Available at:* http://ncrb.gov.in/StatPublications/CII/CII2016/pdfs/NEWPDFs/Crime%20in%20India%20-%202016%20Complete%20PDF%20291117.pdf(last visited Nov. 4, 2018).

(CERT-In), 27,482 cases of cybercrime were reported from January to June in 2017.[22] India was the third worst hit nation by ransomware WannaCry as more than 40,000 computers were affected.[23] But these numbers do not tell the whole story as most of such cases go unreported. NCRB relies on police records and categorises a cybercrime incident only if there was a FIR under the relevant provisions of the law.[24]

III The Convention on Cybercrime

The Convention on Cybercrime of Council of Europe, also known as the Budapest Convention, is the first international treaty which addresses cybercrimes. The conventionfocuses on crimes committed through the Internet and other computer networks and contains provisions which specifically deal with computer-related fraud, copyright infringements, child pornography and breaches of network security. The main objective of the convention as provided in the preamble is "to pursue… a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation."[25] The Convention focuses on harmonization of domestic laws of member states and increasing cooperation among them.

The Convention was drawn up by the Council of Europe with the participation of its observer states Canada, Japan, Philippines, South Africa and the United States. It was adopted by the Council of Europe's Committee of Ministers at its 109th session, on November 8, 2001 and was opened for signature in Budapest on November 23, 2001. The Convention entered into force on July 1, 2004.

In most of the jurisdictions the focus of laws dealing with cybercrime has largely been on the criminalisation aspect *i.e.,*either creation of new offences or adaptation of existing provisions to address the challenges of cybercrime.[26] Most of these provisions evolved over time as per

[22]ChethanKumar,"One cybercrime in India every 10 minutes" *Times of India,* July 22, 2017, *Available at:* http://timesofindia.indiatimes.com/articleshow/59707605.cms (last accessed Nov. 4, 2019).
[23] "Wanna Cry ransomware cyber-attack: 104 countries hit, India among worst affected, US NSA attracts criticism".*Available at:* http://economictimes.indiatimes.com/articleshow/58707260.cms(last visited on Nov. 7, 2019).
[24] During the researcher's own career in IT industry spanning around a decade he came across many such incidents which were never officially reported. In February 2017, CRM application of an upcoming payments bank was hit by a ransomware which was never reported and the IT administrator instead decided to build the system again from available backups.
[25]*Supra* note 5 at 2.
[26]Jonathan Clough, "A World Of Difference: The Budapest Convention on Cybercrime And The Challenges of Harmonisation" 40(3) *Monash University Law Review* 698-736 **(**2014). *Available at:* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2615789(last visited on Nov. 8, 2018).

the local experience in each of these jurisdictions. The Convention provides the substantive and procedural provisions which need to be adopted by parties in their domestic legislations in order to bring harmonization of the laws as a precursor to effective international cooperation.

The Convention provides for four broad categories of substantive offence:

1. Offences against the confidentiality, integrity and availability of computer data and systems[27]
2. Computer-related offences[28]
3. Content-related offences[29]
4. Infringements of copyright and related rights.[30]

The Convention includes substantive provisions for criminalization of attempt and aiding or abetting[31] and corporate liability.[32]

The procedural law provisions cover

1. Expedited preservation of stored computer data[33]
2. Production Orders[34]
3. Search and seizure of stored computer data[35]
4. Real-time collection of computer data[36]

The Convention also provides for provisions for establishment of jurisdiction[37] and for international cooperation.[38] Chapter III of the Convention establishes a legal framework for fostering international cooperation among the member states with both general and specific measures such as imposition ofobligation upon member states to cooperate to the "widest extent possible", to take urgent and immediate measures to preserve data related to offences

[27]*Supra* note 5.Budapest Convention, chapter II, section 1, title 1, arts. 2-6 include offences such as illegal access, illegal interception, data interference, system interference and misuse of devices.
[28]*Id.*chapter II, s. 1, title 2, arts. 7 (computer-related forgery) and 8 (computer-related fraud).
[29]*Id.*chapter II, s. 1, title 3, art. 9 - Offences related to child pornography.
[30]*Id.*chapter II, s. 1, title 4, art. 10 - Offences related to infringements of copyright and related rights.
[31]*Id.*chapter II, s. 1, title 5, art. 11 - Attempt and aiding or abetting.
[32]*Id.*chapter II, s. 1, title 5, art. 12 - Corporate liability.
[33]*Id.*chapter II, s. 2, title 2, art. 16-17 - Expedited preservation of stored computer data and preservation and partial disclosure of traffic data.
[34]*Id.*chapter II, s. 2, title 3, art. 18 – Production order.
[35]*Id.*chapter II, s 2, title 4, art. 19 -21.
[36]*Id.*chapter II, s. 2, title 3, art. 20-21.
[37]*Id.*chapter II, s. 3, art. 22 - Jurisdiction.
[38]*Id.*chapter III – International co-operation.

and to extend efficient mutual legal assistance.[39]The Convention seeks to establish important channels of cooperation by leveraging the I-24/7 global communication system of Interpol as well as the existing network already established by Interpol which includes designated investigators working in national computer crime units in more than 120 countries, also known as National Central Reference Points.[40]In 2006, an additional protocol[41] came into force which provides for adoption of legislative measures to recognize and prosecute offences of racist or xenophobic propaganda by the parties adopting the protocol.

IV Convention on cybercrime: Why is India not a party?

Despite facing challenges in tackling the cybercrimes due to territorial jurisdictional issues India is still not a party to the Budapest Convention. Although there has been no official statement as to why India is not a party to the Convention, but it can be gathered that there aresome concerns about the convention itself. Based on the limited information available in the public domain, are the contentions raised by India in relation to being a party to the convention can be broadly categorised into following heads

i. Not being a party to drafting of the convention
ii. Participation in future development of convention/protocols
iii. Article 32 of the Convention*vis-à-vis* sovereignty
iv. Effectiveness of the legal assistance provisions

Not a party to drafting

Recently at an event[42] a senior government official remarked "They are asking us to join the Budapest Convention. Let us join that but when we ask them kindly clarify the concept, European Union is not coming forward to do that."[43] The remark has to be seen in the light of the historical perspective of "*developed versus developing countries"*battle at multilateral forumsthat India has found itself since the 1980s. India's foreign policy since 1980s has been

[39]"International Cooperation against Cybercrime",*available at:*https://www.coe.int/en/web/cybercrime/international-cooperation(last visited onNovember8, 2018).
[40]*Ibid.*
[41] Council of Europe, "Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems".*available at:*http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008160f (last visited on Nov. 8, 2019).
[42]Annual 11th India Security Summit organised by ASSOCHAM on Aug. 31, 2018.
[43] IANS, "India can't be guest member of EU Budapest Convention: Dr Gulshan Rai" *Business Standard,* Aug. 31, 2018.*Available at:* https://www.business-standard.com/article/news-ians/india-can-t-be-guest-member-of-eu-budapest-convention-dr-gulshan-rai-118083100671_1.html(last visited on Nov. 4, 2019).

shaped around the deep rooted suspicions that originate from the technology denials related to cryogenic rocket engines for India's space program as a fallout of India's 1974 nuclear tests and later the sanctions imposed by US in aftermath of 1998 nuclear tests.[44] Various technology denial regimes like the Non Proliferation Treaty (NPT), the Comprehensive Test Ban Treaty (CTBT), or the Missile Technology Control Regime (MTCR) have consistently been labelled by India as "discriminatory", and have been consistently described as an "unequal treaty"by India.[45]India has always viewed these technology denial regimes as instrumentality of creating technology "haves and have-nots" in the world.

In 2013, the list of export restricted technologies under theWassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologiesyear was amended and expanded to include the latest technologies such as intrusion software, IP Surveillance Software *etc.,* critical for any nation to create both defensive and offensive capabilities in cyberspace.India strongly conveyed its objections to the legitimacy of these multilateral regimes as long as India was not a party to them and reiterated its demand to be treated as an equal.[46]

India's experience with such existing international multilateral regimes that had imposed unilateral restrictions in the pastwhichhave dealt huge blow to the technological development of the country has probably taught it to take the claims of international cooperation, peace, advancement by such regimes with a pinch of salt.But, the case of Budapest Convention is one that has to be viewed from a fresh perspective for two reasons, firstly, India has recentlyratified two CoEconventionsin which India had not had any hand in the negotiations.[47] For one in 2012, India signed and ratified the Convention on Mutual Administrative Assistance in Tax Matters[48] which was developed by the Council of Europe and the Organisation for Economic Co-operation and Development (OECD) The treaty first came into force in 1995 and it was in 2010 that it was opened for other state to be a party to it by invitation. More recently in February 2018, India acceded to Convention on the Transfer

[44]*Supra* note 12.
[45]*Ibid.*
[46]*Ibid.*
[47] Council of Europe, Treaty list for a specific state – India (Status as of 05/11/2018), *available at:* https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/country/IND?p_auth=Y0NGIZXO (last visited on Nov. 5, 2019). The Convention on the Transfer of Sentenced Persons and the Convention on Mutual Administrative Assistance in Tax Matters. These conventions came into force in 1983 and 1988 respectively and India ratified this in 2018 and 2012 respectively.
[48] "India Signs Multilateral Convention on Mutual Administrative Assistance in Tax Matters",*available at:* http://pib.nic.in/newsite/PrintRelease.aspx?relid=79915 (last visited on Nov. 4, 2019)

of Sentenced Persons.[49]Secondly, the considerations of national interest which have been the basis accession to these treaties should also be applicable in the case of Budapest Convention on the similar grounds of national interest.

Participation in development of convention/protocols

At an event[50]Gulshan Rai noted that,"They [Council of Europe] are the founder members, they will make the law and they will change the law. We can become a member but we cannot participate in making or changing the law."[51] Although this may be true to a limited extent that the final decision to adopt or not rests with the Committee of Ministers[52] of Council of Europe but that should not be a major cause of concern. Article 44 provides for amendments and reads as under:[53]

> Article 44 – Amendments
>
> 1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.
>
> 2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.
>
> 3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.
>
> 4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

---

[49] "India accedes to Convention on the Transfer of Sentenced Persons",*available at:* https://www.coe.int/en/web/transnational-criminal-justice-pcoc/-/india-accedes-to-the-convention-on-the-transfer-of-sentenced-persons (last visited Nov. 4, 2018)

[50]*Supra* note 42.

[51]*Supra* note 43.

[52]The Committee of Ministers is the Council of Europe's statutory decision-making body. Its role and functions are broadly defined in Chapter IV of the Statute. It is made up of the Ministers for Foreign Affairs of member States of Council of Europe. *See,*About the Committee of Ministers, *available at:*https://www.coe.int/en/web/cm/about-cm (last visited on Nov. 4, 2019).

[53]*Supra* note 5 at 24.

> 5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

As may be observed from the provisions

a. The amendments may be proposed by any party to the convention and the same shall be communicated to both member and non-member states to the convention.
b. The Committee of Ministers shall consider the proposed amendment and while considering the adoption it will have consultation with the non-member states.
c. Even after the adoption of the amendment by Council of Ministers the same has to be accepted by all the parties to the convention and the amendment would come into force only after all parties have accepted it.

Moreover, para 323 of the explanatory report[54] to the Convention on Cybercrime provides that[55]

> The amendment procedure is mostly thought to be for relatively minor changes of a procedural and technical character. The drafters considered that major changes to the Convention could be made in the form of additional protocols.

The first additional protocol[56] to the Budapest Convention was adopted in 2003 and a second protocol[57] is under consideration. United States has conveyed its reservations to the first additional protocol because of the concerns that it was not compatible with its Constitutional guarantees.[58]

It may be that India, or any party for that matter, may not be able to push any amendment of any new protocol without the adoption by Committee of Ministers and further by acceptance

[54] Council of Europe,"Explanatory Reportto the Convention on Cybercrime" European Treaty Series - No. 185, *available at:*https://rm.coe.int/16800cce5b (last visited on November 2, 2018). The text of the explanatory report does not constitute an instrument providing an authoritative interpretation of the Convention, although it might be of such a nature as to facilitate the application of the provisions contained therein.
[55]*Id.* para 323 at 59.
[56]*Supra* note 41.
[57]Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime approved by Council of Europe on June 8, 2017 at the 17th Plenary of the Cybercrime Convention Committee (T-CY). *See,*Council of Europe Ponders a New Treaty on Cloud Evidence, *available at:*https://ccdcoe.org/council-europe-ponders-new-treaty-cloud-evidence.html (last visited on Nov. 4, 2019).
[58]Michael A. Vatis, "The Council of Europe Convention on Cybercrime", *Proceedings of a Workshop on Deterring Cyberattacks:Informing Strategies and Developing Options for US Policy*207-223 (The National Academies Press, Washington, 2010) at 210, *available at:*https://www.nap.edu/catalog/12997/ (last visited on Nov. 5, 2019).

of all the parties to the Convention but similar is the case with any multilateral treaty. Hence saying that India will not be able to participate in making or changing the law will not be the correct reading of the provisions of the Convention.

Article 32 *vis-à-vis*sovereignty

Article 32 of the Budapest Convention, which provides for "Trans-border access to stored computer data with consent or where publicly available", has been the centre of a lot of controversy and has turned out to be a major concern for India. Article 32 of Budapest Convention provides that[59]

> Article 32 – Trans-border access to stored computer data with consent or where publicly available
>
> 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.

The Explanatory Report[60] to the Budapest Convention remarks that "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"[61] and that "[t]he drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area."[62]

This article addresses two situations - first, where the data being accessed is publicly available, and second, where the party has accesses or receives the data located outside of its territory through a computer system in its territory after obtaining the lawful and voluntary

[59] *Supra* note5 at 20.
[60] *Supra* note 54.
[61] *Id.,* para 293 at 53.
[62] *Ibid.*

consent of the person who has lawful authority to disclose the data to the party through that system.[63]

In first case the law enforcement agencies can access any data that is available to general public even if the data is in another party without the authorization of the that party.

India's concerns echoed by Russia[64] relate to the key phrase "without the authorization of another party" with respect to clause (b) which gives rise to apprehensions of violation of sovereignty. Russia despite being the member of Council of Europe has not even signed the treaty as it believes that it would lead to violation of sovereignty. As noted by the assessment report[65]

In 2013, a representative from the Office of the Special Coordinator for International Information of Russia's Ministry of Foreign Affairs, at a conference in India, argued that,[66]"According to the Convention, the only requirement for the access to data of citizens of other states is a permission of service provider of any other company involved in that processingwhich has contributed to the practices of mass-surveillance by the NSA and its counterparts" and expressed his belief that "Such permission allows the intelligence agencies to view and analyse Internet history in mails and track users' files and transfer both in the territory of the United States and abroad."[67]

Subsequently in March 2017, a guidance note[68] was issued by Cybercrime Convention Committee (T-CY) of Council of Europe which seeks torepresent "the common

---

[63]*Supra* note 54. *Explanatory report* clause 294 at 53.

[64]Keir Giles "Russia's Public Stance on Cyberspace Issues" in C. Czosseck, R. Ottis*et.al.* (eds.)*4th International Conference on Cyber Conflict* 63-75 (NATO CCD COE Publications, 2012) at 67.
The key phrase which prompts Russian objections is "without the authorisation of another Party". In the Russian view, this is an intolerable infringement on the principle of sovereignty as described above. In addition, the range of options covered by "the person who has the lawful authority to disclose the data" is a source of concern, including as it may organisations other than the State. Russian concerns over practical application of the Budapest convention are illustrated by a report in the official government newspaper which highlighted the "dubious provision for foreign special services to invade our cyberspace and carry out their special operations without notifying our intelligence services", *available at:*
https://ia902702.us.archive.org/33/items/CyconBookCombineallpapers/CyCon_book.pdf (last visited on Nov. 4, 2018).

[65]*Supra* note 54.

[66] As quoted by Anja Kovacs, "India and the Budapest Convention: To sign or not? Considerations for Indian stakeholders" *Internet Democracy Project* 2016, *available at:*https://www.academia.edu/36672078/India_and_the_Budapest_Convention_To_sign_or_not_Considerations_for_Indian_stakeholders(last visited on Nov. 4, 2018).

[67]*Id.* at 7.

[68]Cybercrime Convention Committee, T-CY Guidance Note # 3 Transborder access to data (Art. 32), (December 2014), a*vailable*

understanding of the parties to the treaty regarding the use of certain provisions of the Convention". Guidance note addresses the issue of trans border access to data under article 32 of Budapest Convention.

The concerns of India (and Russia) are due to the fact that most of the service providers are located in US or other developed countries and this factor may be exploited by the western states to compel disclosure of the data by service providers under article 32. Guidance Note explicitly states that service providers being only the holders of their users' data and not the controllers or owners of data, are unlikely to be able to validly and voluntarily consent to the disclosure of such data.[69] Regarding "consent" Guidance Note provides that "Article 32b stipulates that consent must be lawful and voluntary which means that the person providing access or agreeing to disclose data may not be forced or deceived."[70]

Regarding the "location" of the data the guidance note clarifies that the article 32b may be resorted to only when it is known where the data is located[71] and further clarifies thata "party may not use article 32b where it is uncertain where the data is located or where the data is stored locally in the within the territorial jurisdiction of the party".[72] It recommends that "in situations where it is unknown whether, or not certain that, data are 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."[73]

It can be observed from the provision of article 32b and the guidance note that even in the rare cases where a service provider might be able to give access or disclose data, article 32bcannot be resorted to, if the data is stored by the service provider in the territory of the requesting state.[74]

---

*at:*https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a(last visited on Nov. 5, 2018).

[69]*Id.* at 13.

[70]*Id.* at 12.

[71]*Ibid*."Article 32b refers to 'stored computer data located in another Party'. This implies that Article 32b may be made use of if it is known where the data are located.".

[72]*Ibid.* "The Article 32b would not cover situations where the data are not stored in another Party or where it is uncertain where the data are located. A party may not use article 32b to obtain disclosure of data that is stored domestically".

[73]*Id.* at 12.

[74]*Supra* note 66.

As example of application of article 32b, the guidance note considers two typical situations,[75] while reiterating that other situations are neither authorised nor precluded.[76] In first situation the person, whose data is stored in another country, retrieves it and with "lawful authority" voluntarily discloses the data to law enforcement[77] whereas in the second situation, the person voluntarily consents that the police access the data through a system present in that country and if the police are sure that the data is located in another country, policemay access the data under article 32b.[78]The broader questionssuch as whether such an action would amount to violation of right against self-incrimination or the admissibility of such data in judicial proceedings will depend upon the domestic laws of such country. In some cases, it may require resorting to mutual legal assistance treaties ("MLATs") for ensuring admissibility of such evidence.

Anja Kovacspoints out that despite the clarifications in the guidance notes problems remain by highlighting the following situation:[79]

> What if a country hostile to India claims that a computer in India has been used for a crime in that country and that its law enforcement agencies have the computer owner's consent to access the computer and its files in India? Such a case would fall within the parameters set out by the Guidance Note, and thus not require Indian law enforcement to be notified. [*assuming that in this hypothetical case the computer owner is present in the other country*]

---

[75]*Supra* note 68 at 10.

[76]*Supra* note 54.Explanatory report clause 293. "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 further experience has been gathered and further discussions may be held in light thereof. In this regard, Article 39, paragraph 3 provides that other situations are neither authorised, nor precluded."

[77] A person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the article.

[78] A suspected drug trafficker is lawfully arrested while his/her mailbox – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another party, police may access the data under article 32b

[79]*Supra* note 66.

At the moment it seems that the faith is entirely on the presumption "that the Parties to the Convention form a community of trust and that rule of law and human rights principles are respected in line with Article 15 Budapest Convention."

Effectiveness of the legal assistance provisions

Another concern raised in respect of the Convention is the effectiveness of its mutual legal assistance ("MLA") provisions.

Article 31 of the Convention provides that[80]

> Article 31 - Mutual assistance regarding accessing of stored computer data
>
> i. A Party may request another Party 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.
> ii. The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.
> iii. The request shall be responded to on an expedited basis where:
> a. there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
> b. the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Assessment report on the mutual legal assistance provisions of the Budapest Convention on cybercrime[81] noted that given the,"transnational and volatile nature of electronic evidence"[82]MLA is one of the most important,"condition for effective measures against cybercrime" but "in practice, however, current mutual legal assistance procedures are considered too complex, lengthy and resource intensive, and thus too inefficient."[83] The assessment report concluded that though detailed data or statistics on MLA are not

[80]*Supra* note 5, Budapest Convention, arts. 31 at 19.
[81]Cybercrime Convention Committee, T-CY assessment report: The mutual legal assistance provisions of theBudapest Convention on Cybercrime (Dec. 2014), a*vailable at*: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c (last visited on Nov. 6, 2019).
[82]*Id.,*s. 5 at 123.
[83]*Ibid.*

available[84] but based on replies from participating and observer states it concluded that response times generally appeared to range from 6 to 24 months resulting in many requests and thus investigations being abandoned.[85] It also noted that the parties were not making full use of the provisions of the Budapest Convention for MLA related to cybercrime and electronic evidence.[86]

V Conclusion

As can be seen from the preceding discussion, the answer to the question whether India should be a party to the Budapest Convention or not is not be a straightforward one. Despite raising the issue of international mechanism to address the issue of cybercrime at various international forums, India is still not a party to the only binding international instrument which currently occupies the field. There a number of issues raised by Indian authorities which impede India's acceptance of the Budapest Convention.

The Indian foreign policy, shaped by the various domestic events during early years of the republic, economic crisis of early 90s and international exclusionary politics during 80s and 90s, has evolved its own approach to international diplomacy and has been successful in carving out a unique space for itself in global arena. The challenges related to regulations in cyberspace and threat of cybercrime are areas which are still at developing and the response of international community has been considerably slow. In light of this, a wait and watch policy cannot be easily faulted altogether. On the other hand, the Indian experience also shows that the epidemic of cybercrimes is on the rise and the efforts of achieving greater digital inclusion on the domestic policy front may further result in the increased threats of cybercrimes.

While the concerns addressed in this paper cannot at any rate be discounted as insubstantial but the evaluation of those concerns has to be in the realistic context. With large part of internet resources currently hosted in the developed western countries India the investigation of such crimes inevitably requires cooperation from other countries and India is mostly a requesting party. At the moment this cooperation is facilitated by the diplomatic efforts which are taken up case by case basis. The outcome of such interactions is highly unpredictable and is based on the diplomatic dynamics prevalent at the time with the requested party. Based on mutuality, these diplomatic channels may also limit India's options in case of an assistance

[84] *Id.* conclusion 3 s. 5.1.1 at 123.
[85] *Id.* conclusion 1 s. 5.1.1 at 123.
[86] *Id.* conclusion 2 s. 5.1.1 at 123.

request from these countries as India may not be in a position to decline such request in consideration of maintenance of mutual relationship.

Even if the party status to the convention may not be of much practical advantage (as even the assessment report confirms that despite the provisions of the conventions, the parties to the Convention resort to other channels of communication) it may provide a tactical advantage. It will provide India with the moral authority with the backing of the convention to request assistance from the countries and also allow room for declining any request falling outside the bounds of the convention. In light of the above discussion it is submitted that India should consider being a party to the Budapest Convention.