INDIA AND THE BUDAPEST CONVENTION

TO SIGN OR NOT? CONSIDERATIONS FOR INDIAN STAKEHOLDERS

DR. ANJA **KOVACS**
INTERNET DEMOCRACY PROJECT

In 2001, the Convention on Cybercrime of the Council of Europe, also known as the Cybercrime Convention or the Budapest Convention, became the first binding international instrument to foster a common criminal policy and international cooperation to battle cybercrime in signatory States.*

The Convention lays out a range of changes each signatory State is expected to make to its substantive criminal law – touching on crimes as diverse as data interference, over computer-related fraud, to child pornography. It also includes legislative and other measures that each Party needs to take to establish specific 'powers and procedures' for the purpose of 'criminal investigations or proceedings' and jurisdiction regarding the substantive crimes that come under the purview of the Convention. Finally, the Convention includes a number of principles and procedures to facilitate international cooperation to further investigations or proceedings and the collection of electronic evidence concerning criminal offences within the purview of the Convention.[1] In 2006, an additional protocol entered into force, which further extended the scope of the Convention to also include offences of racist or xenophobic propaganda for those states who had ratified the protocol.

Although invited to consider accession,[2] India has so far not signed the Convention and has, in fact, on several occasions explicitly expressed grave hesitations to do so.[3] At first sight, India's hesitations might seem surprising. After all, concerns around cybersecurity, as has been repeatedly argued elsewhere,[4] have been central drivers of India's overall global Internet governance policy. Jurisdictional issues, in particular, have posed a great challenge for India's cybersecurity establishment when trying to tackle anything from cyberfraud to terrorism in the digital age. While the Mutual Legal Assistance Treaty (MLAT) system is supposed to address these, seeing that response times reportedly average three years and four months it has clearly failed to do so adequately.[5] The Budapest Convention aims to establish an alternative framework to resolve exactly the same issue, including through the establishment of a 24/7 'points of contact network'.

* The author would like to thank Rajat Rai Handa for his valuable research assistance.

• 1. Convention on Cybercrime. Council of Europe European Treaty Series No. 185, Budapest, 23 November 2011, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (articles quoted in the text throughout this paper refer to this document).

• 2. PTI (2009). Council of Europe Asks India to Join Convention on Cybercrime. *Economic Times*, 30 March, http://articles.economictimes.indiatimes.com/2009-03-30/news/28401922_1_cyber-terrorism-cybercrime-convention.

• 3. As, for example, on 22 October 2015, during the second Government Preparatory Meeting for the WSIS+10 Review, in New York, which the author also attended.

• 4. Datta, Saikat (2016). *Cybersecurity, Internet Governance and India's Foreign Policy: Historical Antecedents*. New Delhi: Internet Democracy Project, https://internetdemocracy.in/reports/cybersecurity-ig-ifp-saikat-datta/; Kovacs, Anja (2014). Is a Reconciliation of Multistakeholderism and Multilateralism in Internet Governance Possible? India at NETmundial. In Lea Kaspar (ed.), *NETmundial: Reflections from Brazil, India and Kenya*. London: Global Partners Digital, http://www.gp-digital.org/wp-content/uploads/pubs/Netmundial%20-%20Reflections%20from%20Brazil%20India%20and%20Kenya.pdf.

• 5. Mathai, Anahita (2015). The Budapest Convention and Cyber Cooperation. *ORF Cyber Monitor,* 3(3), http://cyfy.org/the-budapest-convention-and-cyber-cooperation/.

Moreover, despite its hesitations to sign the Convention, India has brought its legal framework largely in line with the provisions of the Convention: when India amended its Information Technology Act (IT Act) in 2008, this was one of the big outcomes.[6]

If at first sight, India's needs seem to align so closely with the goals of the Budapest Convention, why then this reluctance to sign? In this paper, I will critically assess the major strengths and weaknesses of the Budapest Convention with regard to five areas of particular importance to India: the fight against terrorism; the protection of sovereignty; the promotion of human rights; copyright related matters; and the general effectiveness of the Convention. What this analysis will show is that the question of whether or not India should sign the Budapest Convention is not one that can be answered in a straightforward manner as yet. At the moment, as this paper will make clear, the tactical value of signing the Budapest Convention might well be greater than the practical value. At the same time, however, doing so would also bring with it a number of tactical and practical drawbacks. What is, therefore, required before any decision is taken, is a thorough and detailed cost benefit analysis from a long-term perspective on each of the different aspects discussed here. For this analysis to be effective, it is essential that it is made by all stakeholders in India together.

Before looking into these areas in more depth, let us, however, first look at one of the most common criticisms of the Budapest Convention often heard in international gatherings, and raised by India as well as others: is the Budapest Convention faulty by default simply because it wasn't drafted in a sufficiently inclusive manner?

The origins and development of the Budapest Convention – Inclusion and exclusion?

The Budapest Convention was negotiated by the Council of Europe (CoE) Member States as well as Canada, Japan, South Africa and the United States. It was adopted by the CoE's Committee of Ministers at its 109th session, on 8 November 2001, opened for signature in Budapest less than two weeks later, on 23 November 2001,[7] and entered into force on 1 July 2004. As of March 2016, 48 states have ratified the Convention. An additional six states have signed, but not ratified it – this includes South Africa, one of the original negotiators. In addition, Russia and San Marino, though Council of Europe member states, neither signed nor ratified.[8]

• 6. Bhaumik, Anirban (2012). India, Allies to Combat Cybercrime. *Deccan Herald*, 16 May, http://www.deccanherald.com/content/249937/india-allies-combat-cybercrime.html.

• 7. Explanatory Report to the Convention on Cybercrime, Council of Europe European Treaty Series No. 185, Budapest, 23 November 2001, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b (henceforth Explanatory Report).

• 8. The full list of signatures and ratifications of the Convention can be found here: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

The fact that the Convention was drafted without extensive input from developing countries has been flagged by India repeatedly,[9] and is indeed correct. But if this criticism has nevertheless often left observers baffled,[10] this is arguably with reason. For instance, as recently as 2012, and only two years after it became possible for non-member states to do so, India signed and ratified the Convention on Mutual Administrative Assistance in Tax Matters, jointly developed by the CoE and the OECD.[11] The treaty first came into force in 1995. India had not had any hand in its negotiation.

If India, thus, does not a priori refuse to sign a treaty merely because it has not been party to the negotiations of its provisions, then why make this criticism with regard to the Budapest Convention? The problem lies in the way in which the geographical imbalance has shaped the scope, focus and content of the Convention. It has been argued that, if the Cybercrime Convention includes only a limited number of offences in its section on substantive law, this is simply because on other offences, a minimum consensus could not be reached.[12] But India as well as others have raised concerns both about what is included and what is excluded: India's priorities simply do not find sufficient reflection in the Budapest Convention as it stands right now.[13] Rather than being taken at face value, the criticisms of the treaty's limited origins thus should be seen as a short-hand for these more complex points.

Terrorism and the Internet

It is to these complex substantive issues that we will turn our attention now. As Saikat Datta has shown, among the most pressing cybersecurity issues for the Indian government has been the question of how cyberspace has changed terrorism – so much so even that terrorism has become the overarching paradigm within which cybersecurity dialogues are frequently conducted.[14] The extent to which the Budapest Convention actually manages to address India's concerns on this issue in particular is a matter of debate.

For one thing, the Budapest Convention's sections on substantive criminal law do not address the issue of terrorism at all (the Council of Europe has a separate convention on the prevention of terrorism). However, according to the United Nations Office on Drugs and Crime (UNODC),[15] the procedural provisions of the

• 9. See, for example, Singh, Pratap Vikram (2013). India Won't Sign Budapest Pact on Cybersecurity. *Governance Now,* 15 October, http://www.governancenow.com/news/regular-story/india-wont-sign-budapest-pact-cyber-security.
• 10. See, for an example, Grigsby, Alex (2014). Coming Soon: Another Country to Ratify the Budapest Convention. *Council on Foreign Relations*, 11 December, http://blogs.cfr.org/cyber/2014/12/11/coming-soon-another-country-to-ratify-to-the-budapest-convention/.
• 11. The full list of signatures and ratifications of this treaty can be found here: http://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/127/signatures?p_auth=ETTd160N.
• 12. Explanatory Report, p. 7.
• 13. With thanks to Dr. Cherian Samuel, Associate Fellow, Institute for Defence Studies and Analyses, for this valuable insight, shared in a conversation at Delhi, 2 March 2016.
• 14. Datta, *Op. Cit.*
• 15. United Nations Office on Drugs and Crime (2012). *The Use of the Internet for Terrorist Purposes*. Vienna: United Nations Office, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

Cybercrime Convention may have considerable value in the fight against terrorism. These provisions apply to any criminal offence committed by means of a computer and the collection of evidence in electronic form for such an offence (art 14(2) b and c of the Convention), and could, thus, 'facilitate investigations and evidence-gathering in connection with acts of terrorism involving use of the Internet'.[16]

And so one question for India is: could the Convention be genuinely helpful in its fight against terrorism? For example, as one of the countries that with section 66F actually has a domestic provision regarding cyberterrorism, could India ask for another country's assistance under the Convention on the basis of this section?

The answer is a somewhat complex one. As a general principle, the Convention encourages signatory States to cooperate 'to the widest extent possible' (art. 23 and 25) and with regard to both criminal offences related to computer systems and data and the collection of evidence in electronic form of a criminal offence (as provided for in art. 14). Though it makes some exceptions, the Convention itself, thus, does not put into place a generic, default dual criminality requirement, and in some cases (such as article 29, on expedited preservation of stored computer data) even explicitly argues against it.

However, while the above is relevant for the forms of mutual assistance explicitly addressed in the Convention (especially in articles 29 to 34), with regard to which the Convention takes precedence, this is not the complete story. According to article 25(4), which lays out the general principle on this issue, mutual assistance in all other situations 'shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse cooperation'. Many mutual assistance treaties do have a requirement of dual criminality in place.

Moreover, if the two Parties involved in a request for mutual assistance do not yet have any agreements in place between them to govern this request, article 27 of the Convention comes into play, according to which mutual assistance requests 'shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party' [emphasis mine]. In addition, article 27(4) states that the requested Party can also refuse cooperation where it considers the offence concerned a political offence or when it believes that providing assistance would 'prejudice its sovereignty, security, ordre public or other essential interests'. These same qualifications also apply to several specific provisions, such as on the expedited preservation of stored computer data (art. 29) and on expedited disclosure of preserved traffic data (art. 30).

The Convention's Explanatory Report states explicitly, in the context of article 27(4):

> grounds for refusal established by a requested Party should be narrow and exercised with restraint. They may not be so expansive as to create the potential for assistance to be categorically denied, or subjected to onerous conditions, with respect to broad categories of evidence or information.[17]

• 16. *Ibid.*, p. 20.
• 17. Explanatory Report, p. 48.

But if the Report had to state this so clearly, this is precisely because it is easy to see how these paragraphs could be invoked to refuse assistance, even if this goes against the spirit of the Convention – and this may be a risk especially where relations between States are tense or interpretations of what constitutes terrorism vary widely.

In fact, when concerns were expressed in the US that the ratification of the Convention would mean that US law enforcement would now be forced to cooperate with request that arguably entailed human rights violations, including regarding acts that are actually legal on US soil, the US Department of Justice noted that '"essential interests" would allow the US to refuse any request that would violate the Constitution'.[18] For India, the promise of cooperation held out by the Budapest Convention might, thus, simply not be firm enough.[19]

There is an additional important issue to take into consideration when discussing the issue of terrorism. The Convention's approach is also restrictive because it focuses only on crime, and thus on private actors. This makes it impossible to impose any measures, such as sanctions, on states, even where terrorist actions or other cyberattacks for political purposes can be traced back to a government.

Whether or not a comprehensive international treaty is needed that can encompass both crime and state behaviour in cyberspace is one of the big cybersecurity questions that the international system is currently grappling with.[20] Some have argued that it is at the moment simply impossible to negotiate even a treaty with the restricted scope of the Cybercrime Convention at the global level – the differences in opinions on what constitute appropriate global standards are simply too big, it is argued, making it particularly difficult to scale up procedural and cooperation commitments to a global level.[21] At the same time, however, if harmonisation is crucial to the effectiveness of the battle against cybercrime, as promoters of the Budapest Convention will also argue, it is legitimate to ask whether we really have a choice in the matter of whether a new treaty should be attempted: what value does the Cybercrime Convention really have if some of the countries from whose territory a considerable amount of such crime is believed to emanate, such as Russia and China, will never sign up?[22]

Whatever its reasons, India for one has, over the past few years, started to plead more and more vocally for a new cyberjurisprudence to deal with challenges of cybercrime and cybersecurity within the UN system. In

• 18. Anderson, Nate (2006). 'World's Worst Internet Law' Ratified by Senate. *Ars Technica*, 4 August, http://arstechnica.com/uncategorized/2006/08/7421/.
• 19. See also Singh, *Op. Cit.*
• 20. For more on this debate, especially in the context of India's global cybersecurity concerns, see Kovacs, Anja (2015). *Addressing India's Global Cybersecurity Concerns: Norm Development, Regulatory Challenges, Alternative Approaches*. New Delhi: Internet Democracy Project, https://internetdemocracy.in/reports/addressing-indias-global-cybersecurity-concerns/.
• 21. Harley, Brian (2010). A Global Convention on Cybercrime? *Columbia Science and Law Tech Review*, 23 March, http://stlr.org/2010/03/23/a-global-convention-on-cybercrime/.
• 22. Such concerns about the impact of fragmentation on the fight against cybercrime have also been raised, for example, in United Nations Office on Drugs and Crime (2013). *Comprehensive Study on Cybercrime – Draft.* Vienna: United Nations Office on Drugs and Crime, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

2015, it put forward this demand, for example, at the UN Commission on Science and Technology for Development (CSTD)[23] and at various points during the WSIS+10 Review.[24] In addition, this point was included in the BRICS Ufa Declaration of July 2015, which called explicitly for a 'universal regulatory binding instrument on combating the criminal use of ICTs under the UN auspices'. [25]

Clearly, the question that India is already asking itself is how prudent a choice it is, in this context, to already sign a treaty that does not sufficiently reflect the country's priorities. Would the Budapest Convention be able to evolve over time in a direction that would be more responsive to India's needs? If one of India's long term goals is to see these issues addressed within the UN system, would signing the Convention mean that India would inadvertently contribute to the stalling of any such UN-centric efforts? The answers for the moment are not yet so clear.

Sovereignty

Perhaps the most controversial provision of the Budapest Convention as it stands is Article 32, on transborder access to stored computer data with consent or where publicly available. The article reads as follows:

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.

It is paragraph (b) from this article in particular that has been cause for concern; for Russia, this clause has in fact been the main reason for its decision not to sign the treaty, as it believes that it violates the country's sovereignty. Thus, at India's 2013 CyFy Conference, Boris Vasiliev from the Office of the Special Coordinator for International Information of Russia's Ministry of Foreign Affairs argued: 'According to the Budapest

• 23. Statement made by India on Agenda Item 3, 'Progress made in the Implementation of and follow-up to the outcomes of the World Summit on the Information Society at the Regional and International Levels', at the 18th Session of the UN Commission on Science & Technology for Development (CSTD), Geneva, 4-8 May 2015, http://www.pmindiaun.org/pages.php?id=1106.
• 24. Inputs for the United Nations General Assembly Review of Tunis Agenda for the Information Society. Submitted by the Government of India as part of the preparatory process for the WSIS+10 United nations General Assembly High Level Meeting, July 2015, http://workspace.unpan.org/sites/Internet/Documents/UNPAN95026.pdf; Comments and Views on WSIS+10 Review: Non-Paper. Submitted by the Government of India as part of the preparatory process for the WSIS+10 United Nations General Assembly High Level Meeting, September 2015, http://workspace.unpan.org/sites/Internet/Documents/UNPAN95307.pdf; Statement by Mr. J.S. Deepak, Secretary, Department of Electronics and Information Technology, Government of India, at the United Nations General Assembly High Level Meeting on WSIS+10 Review, New York, 15 December 2015, https://www.pminewyork.org/pages.php?id=2340.
• 25. BRICS Ufa Declaration, Ufa, 9 July 2015, http://www.brics.utoronto.ca/docs/150709-ufa-declaration_en.html.

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 processing'.[26] He then proceeded to explain how, in his country's reading, this had contributed to the practices of mass-surveillance by the NSA and its counterparts in the remaining Five Eyes. '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', he had stated at the meeting.

But since then, the Cybercrime Convention Committee of the Council of Europe has issued a Guidance Note on how Article 32 is to be read that explicitly contradicts this reading, on two important points in particular. First, the Guidance Note clarifies explicitly that service providers generally cannot provide access or disclose data under this provision:

> Service providers are unlikely to be able to consent validly and voluntarily to disclosure of their users' data under Article 32. Normally, service providers will only be holders of such data; they will not control or own the data, and they will, therefore, not be in a position validly to consent.[27]

Second, the Guidance Note states explicitly that the article is 'not relevant to domestic production orders or similar lawful requests internal to a Party'.[28] Even in those rare cases where a service provider might be able to give access or disclose data, this provision can, thus, not be mobilised if the data is stored by the service provider in the territory of the requesting state.

Though Russia's reading might thus be a misinterpretation, a simple use-case can make clear that problems remain even after the clarifications that the Guidance Note provides. 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.[29]

Indeed, as the Guidance Note repeatedly notes, 'it is presumed that the Parties to the Convention form a community of trust'. But while such an assumption might work well among the relatively homogeneous originators of the Convention, it doesn't necessarily in the world at large. For India, Article 32(b) might not pose much of a concern as long as the other Parties to the Convention are states with whom relations are friendly. Once that changes – for example because a state with which India traditionally has more strained relations joins the treaty – India might well have justified cause for concern.

• 26. Vasiliev, Boris (2013). Sovereignty, International Cooperation and Cybersecurity – A Treaty Dialogue. Transcript from speech at CYFY13, New Delhi, 14 October, http://cyfy.org/speaker/boris-vasiliev/.
• 27. Cybercrime Convention Committee (2014). T-CY Guidance Note No. 3: Transborder Access to Data (Article 32). Strasbourg, Council of Europe, 3 December, p. 7, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY%282013%297REV_GN3_transborder_V12adopted.pdf (henceforth Guidance Note No. 3).
• 28. *Ibid*.
• 29. With thanks to Dr. Cherian Samuel for this insight and example, shared in a conversation at Delhi, 2 March 2016.

It is true that, according to article 37 of the Convention, the 'unanimous consent' of all Parties to the convention is required to invite any new Parties to join, and so India would be able to veto any such invitation if it believes this to be in its interest. But the question then is: to what extent is a Convention that can only ever extend to part of the world be really beneficial if it is to address an issue that is as inherently transnational as cybercrime?

Moreover, parallel to the development of the Guidance Note, a process to explore the possibility of extending article 32(b) beyond its current remit was, interestingly, also taking place. In an assessment of the mutual legal assistance provisions of the Convention by the Council of Europe's Cybercrime Convention Committee (T-CY), it was found that many signatories of the Convention in practice used production orders to get foreign service providers who have a legal representation in the signatory's territory, even if the data requested is stored abroad. Sometimes, authorities also have agreements with foreign service providers.[30] In other words, whatever the intended meaning of article 32(b), State practice clearly does not remain within the limits of what is laid out there as permissible, and takes a wide variety of forms, even if data thus obtained often cannot be used in court proceedings before being formalised through a subsequent mutual assistance request.[31]

In response, T-CY put forward five proposals to extend the provisions on transborder access to data through a draft additional protocol, relaxing the current restrictions.[32] If these proposals had been accepted, this might again have heightened Russia's concerns regarding the violations of sovereignty that the Convention might make possible. In addition, when the Council of Europe held a hearing, on 3 June 2013 in Strasbourg, 'to collect views from civil society and the private sector on its plans', the responses were negative almost across the board as well. A central bone of contention at this event was the way in which the proposals would undermine privacy and data protection.[33] It seems that even Parties to the Budapest Convention could not come to an agreement, however. As the report of the Ad-hoc Subgroup on Transborder Access noted, among other things:

> within many governments, some ministries may oppose transborder access to data if the data is located within their jurisdiction, while ignoring or tolerating that their own authorities access data in other jurisdictions.[34]

For the moment, the proposal to add an additional protocol has been stalled.

• 30. Cybercrime Convention Committee (2014). T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime. Strasbourg, Council of Europe, 3 December, p. 88, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY%282013%2917_Assess_report_v50adopted.pdf (henceforth MLA Assessment Report).
• 31. *Ibid.*
• 32. Cybercrime Convention Committee (2013). (Draft) Elements of an Additional Protocol to the Budapest Convention on Cybercrime Regarding Transborder Access to Data. Proposal Prepared by the Ad-hoc Subgroup on Transborder Access. Strasbourg, Council of Europe, 9 April, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY%282013%2914transb_elements_protocol_V2.pdf.
• 33. Marzouki, Meryem (2013). Transborder Data Access: Strong Critics on Plans to Extend CoE Cybercrime Treaty. *EDRI*, 5 June, https://edri.org/edrigramnumber11-11transborder-data-access-cybercrime-treaty/.
• 34. Cybercrime Convention Committee (2014). Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY. Report prepared by the Ad-hoc Subgroup on Transborder Access and Jurisdiction. Strasbourg, Council of Europe, 3 December, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf.

Human Rights and the Rule of Law

To what extent the Cybercrime Convention strengthens or weakens human rights has been an issue of concern from the time of its development.[35]

Article 15 of the Budapest Convention requires each party to provide conditions and safeguards to ensure the 'adequate protection of human rights and liberties', including the principle of proportionality. These conditions and safeguards should include 'judicial or other independent supervisions, grounds justifying application, and limitation of the scope and the duration of such power or procedure', as appropriate. 'To the extent that it is consistent with the public interest, in particular the sound administration of justice,' the article further reads, 'each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties'.

More concrete guidance on how to ensure human rights are adequately protected while fighting crime in cyberspace is provided for a limited number of specific sections. For example, article 21, on interception of content data, specifies that it should apply specifically in relation to serious offences, though what those offences are is left to domestic law to determine. In some cases, the Explanatory Report also provides further guidance, e.g. when it stresses under article 4, on data interference that:

> The modification of traffic data for the purpose of facilitating anonymous communications (e.g., the activities of anonymous remailer systems), or the modification of data for the purpose of secure communications (e.g. encryption), should in principle be considered a legitimate protection of privacy and, therefore, be considered as being undertaken with right.[36]

On the whole, however, the Convention is thin on instructions as to how to translate the advice contained in Article 15 into a reality on the ground. As the Convention's Explanatory Report explains: 'As the Convention applies to Parties of many different legal systems and cultures, it is not possible to specify in detail the applicable conditions and safeguards for each power or procedure'.[37] Rather, as the Guidance Note on Article 32 says, the Budapest Convention presumes 'that rule of law and human rights principles are respected in line with Article 15 Budapest Convention' in each Party.[38]

That assumption might not always be correct. For example, the Convention accepts as a 'competent authority' for all the procedural law provisions in Chapter II, Section 2 any 'judicial, administrative or other law enforcement authority that is empowered by domestic law to order, authorise or undertake the execution of

• 35. Marzouki, Meryem (2007). Enditorial: The 2001 CoE Cybercrime Convention More Dangerous than Ever. *EDRI*, 20 June, https://edri.org/edrigramnumber5-12cybercrime-convention-dangerous/.
• 36. Explanatory Report, p. 11.
• 37. Explanatory Report, p. 23.
• 38. Guidance Note No. 3, p. 5.

procedural measures for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings'.[39] The assumption here is that the 'competent authority' in its constitution and practice by definition upholds the minimum safeguards for human rights provided for under international law. Where, for example, the right to privacy is concerned, this is, however, currently under considerable debate in India. Many have argued that the checks and balances necessary in the digital age at present are simply not in place.[40]

Similarly, while the Explanatory Report recognises the important information that even metadata can reveal about a person,[41] the Convention nevertheless continues to leave the circumstances under which such data can be intercepted in real time completely up to domestic law to determine. The only qualification that it makes (and with that, it does provide an important protection that Indian law doesn't extend) is that traffic data cannot be intercepted in an indiscriminate manner; it has to be associated with specified communications. Similarly, while the interception of content data is only legitimate under the Convention 'in relation to serious offences', what constitutes a serious offence is, as mentioned, again left to be established by domestic law. Moreover, except under conditions explicitly set out in article 28 of the Convention, 'a broad, categorical or systematic application of data protection principles to refuse cooperation is […] precluded'.[42]

It has also been argued that aspects such as the absence of a consistent dual criminality requirement in the Budapest Convention actually undermine human rights – as mentioned before, this was one of the concerns raised by local civil society when the US government ratified the Convention. While this may be helpful for governments focused on the fight against terrorism, it is detrimental to the values that that fight is supposed to support in the first place.

Finally, by not providing clearer guidance, the Cybercrime Convention may contribute to the legitimisation of government practice on a whole range of issues that are not yet widely recognised as human rights violations, yet deserve further consideration from that perspective. For example, the Cybercrime Convention allows for a wide approach that criminalises all forms of hacking under Article 2, on illegal access, of the Convention; consideration of qualifying elements such as the intent to obtain computer data, is completely optional.[43] The possibility that hacking could, under certain conditions, be a legitimate form of political protest in the digital age is not even considered. Similarly, the Convention leaves it to domestic law to decide whether or not someone whose data has been seized should be notified. As the Explanatory Report recognises, seizure

• 39. Explanatory Report, p. 22.
• 40. For a detailed analysis of privacy and surveillance in India, see Centre for Internet and Society and Privacy International (2016). State of Surveillance: India. London: Privacy International, https://privacyinternational.org/node/738. To get a sense of the challenges in a nutshell, see Kovacs, Anja (2013). No Getting Away from the Gaze of the State. Hindustan Times, 3 July, http://www.hindustantimes.com/india/no-getting-away-from-the-gaze-of-the-state/story-mMS8ZSJACTVymAvD91LVnL.html.
• 41. Explanatory Report, p. 39.
• 42. Explanatory Report, p. 48.
• 43. Explanatory Report, p. 9.

would almost always be noticed by the suspect in the offline world, as in those cases, 'seized objects will be physically missing'.[44] If offline rights apply online, it deserves to be asked whether an obligation to notify should not exist with regard to online seizures as well.

For stakeholders from India (and elsewhere), it deserves serious consideration, therefore, whether this general reference to the need to protect human rights in the Budapest Convention is sufficient. The application of human rights in the digital age remains an intensely-debated and contentious topic, perhaps even more so now than when the Budapest Convention was first formulated. While some regions, including Europe and the Americas, have strong regional human rights mechanisms, making possible both challenges to domestic law that is believed to violate human rights and work on standards development regionally, this is absent in South Asia. As a consequence, decisions by India's Supreme Court that strike down any challenges to legal provisions deemed, e.g. disproportionate, cannot be challenged further. At the same time, engagement by the Indian judiciary with global human rights standards development specifically for the digital age remains restricted.

In these circumstances, it is a legitimate question whether a cybercrime treaty should perhaps give greater direction on how exactly to safeguard human rights in cyberspace than the Budapest Convention does at the moment, possibly through the inclusion of an oversight or complaints mechanism as well. As the implementation of human rights stands for challenges never met before, and consensus on what minimum safeguards for human rights seems further away than ever, the presumption that safeguards and conditions to protect human rights are in place can do more harm than good.

Even more, while the task of building safeguards into a new treaty might indeed be difficult,[45] in an age where even democratic countries consequently are all too often seen to violate human rights, it can be questioned whether this can really be altogether ignored. In doing so, we are sending a signal that the fight against cybercrime is more important than the protection of human rights – a signal that is both misplaced and dangerous. Moreover, we will also likely be setting a precedent for a long time to come. If the concrete application of human rights in the digital age will not be addressed in the context of a treaty on cybercrime, when will this get the detailed attention that it deserves, leading to a binding outcome?

It is encouraging that where India has pitched for a global treaty to address cybercrime, it has at times brought human rights concerns directly within its remit. For example, at the eighteenth session of the UN Commission on Science and Technology for Development (CSTD) in Geneva, in May 2015, India appealed to start the 'development of an international legal framework for online privacy and data protection, including issues like

• 44. Explanatory Report, p. 34.
• 45. For one critic who argues that attempting to integrate protection of privacy in particular in a treaty would set it up for failure, see Clough, Jonathan (2014). A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation. *Monash University Law Review*, 40(3): 698-736, https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf.

human rights, trade standardisation and security perspectives'.[46] Though the domestic legal framework can be strengthened considerably where human rights protections are concerned, it deserves consideration on the part of human rights activists whether this perhaps provides an opportunity for a new alliance with the government.

Copyright

While protection for human rights in the Budapest Convention might leave much to be desired, the reverse is arguably true for copyright and related rights: here, the extent of protection might be too extensive. Article 10 requires each Party to establish as criminal offences under its domestic law the infringement of copyright and related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under a range of international instruments. In addition to the widely signed and ratified Bern Convention, Rome Convention and Agreement on Trade-Related Aspects of Intellectual Property Rights, the list includes the WIPO Copyright and the WIPO Performances and Phonograms Treaty – jointly known as the WIPO Internet Treaties. Unlike the earlier named conventions, the WIPO Internet Treaties have been signed by only about half of all countries in the world, and although India, in 2012, brought its own Copyright Act in line with the WIPO Internet Treaties 'to the extent considered necessary and desirable',[47] it is not among them.

It is important to realise that if India does become a signatory to the Budapest Convention, it is 'not bound to apply agreements cited to which it is not a Party'.[48] At the same time, it is worth considering to what extent the inclusion of the WIPO Internet Treaties here perhaps contributes to them further being established as soft law standards. Brazil has reportedly objected to the Budapest Convention on this ground,[49] among other things, and has cited the fact that the Convention's intellectual property-crime provisions were not compatible with Brazil's developing and emerging market as one reason not to sign.[50] In the case of India, the same concern deserve serious and in-depth consideration.

• 46. Statement made by India on Agenda Item 3, 'Progress made in the Implementation of and follow-up to the outcomes of the World Summit on the Information Society at the Regional and International Levels', at the 18th Session of the UN Commission on Science & Technology for Development (CSTD), Geneva, 4-8 May 2015, http://www.pmindiaun.org/pages.php?id=1106.
• 47. Warrier, Vishnu S. (2012). Impact of Coypright (Amendment) Act, 2012 in the Digital Era. *Lex Warrier*, 31 July, http://lex-warrier.in/2012/07/impact-of-copyright-amendment-act-2012-in-the-digital-era/.
• 48. Explanatory Report, p. 18.
• 49. Mizukami, Pedro N., Oona Castro, Luiz F. Moncau, and Ronaldo Lemos (2011). Brazil. In Joe Karaganis (ed.). *Media Piracy in Emerging Economies*. Brooklyn: Social Science Research Council, piracy.americanassembly.org/wp-content/uploads/2011/06/MPEE-PDF-Ch5-Brazil.pdf.
• 50. Wakefield, Megan (2012). International Criminal Tribunal for Cybercrime and Human Rights. Human Rights Brief, Center for Human Rights and Humanitarian Law, 10 December, http://hrbrief.org/2012/12/international-criminal-tribunal-for-cybercrime-and-human-rights/.

Ineffective, out of date?

A final set of arguments that need to be considered are those regarding to the effectiveness of the Convention. We already briefly considered some related arguments earlier in the paper. Does the Convention really have the potential to become a truly global treaty, and what will be the impact in either case? Is the absence of a comprehensive dual criminality requirement a bane or a boon? There are, however, two additional contentions that are often made and that speak directly to the question of effectiveness. One is that there is no evidence of the Convention's effectiveness. The second is that the Convention is a static one, and some would also argue out-dated, and therefore of limited value.

The point that there is no evidence of the Convention's effectiveness seems to unfortunately be on rather firm ground. In fact, the Council of Europe's own documentation on the Convention indicates that Parties continue to face important road blocks in international cooperation around cybersecurity. Thus, an Assessment Report on the mutual legal assistance provisions of the Budapest Convention, adopted by the Cybercrime Convention Committee in December 2014, found:

> MLA [mutual legal assistance] is considered too complex, lengthy and resource-intensive to obtain electronic evidence, and thus often not pursued. Law enforcement authorities tend to attempt to obtain information through police-to-police cooperation to avoid MLA, even though the information thus obtained in most cases cannot be used in criminal proceedings. Frequently, authorities contact foreign (in particular USA-based) service providers directly to obtain subscriber or traffic data. Often investigations are abandoned.[51]

Elsewhere, the Assessment Report refers to the MLA process as 'inefficient', and notes that 'response times to requests of six to 24 months appear to be the norm'.[52]

It has been argued that one of the core challenges in international cooperation on cybercrime is that there is less harmonisation with regard to cybercrime investigative powers than with regard to substantive law on cybercrime.[53] If one of the core aims of the Cybercrime Convention was precisely the former, its success so far clearly has been limited.

There are two important issues to keep in mind here though. The first is that the Assessment Report also notes that

> Parties appear not to make full use of the opportunities offered by the Budapest Convention on Cybercrime and other agreements for the purposes of effective mutual legal assistance related to cybercrime and electronic evidence.[54]

- 51. MLA Assessment Report, p. 7.
- 52. MLA Assessment Report, p. 123.
- 53. UNODC, *Comprehensive study on Cybercrime – Draft*.
- 54. MLA Assessment Report, p. 123.

Clearly, some of the problems that the Convention faces are challenges of implementation, rather than framing,[55] and the Assessment Report thus makes a number of recommendations that fall primarily under the responsibility of domestic authorities.

In addition, moreover, there seem to be a range of efforts underway to try and strengthen the Convention itself – and this brings us to the second argument, that the Convention is static and even out-dated.

The Assessment Report on the Convention's mutual legal assistance provisions also makes recommendations which might require a new additional protocol to the Convention. An Additional Protocol on Criminalisation of Acts of a Racist and Xenophobic Nature already entered into force in 2006. Moreover, the Cybercrime Convention Committee's Transborder Group is currently working on an instrument 'to further regulate the transborder access to data and data flows, as well as the use of transborder investigative measures on the Internet and related issues',[56] while the Cloud Evidence Group is exploring additional 'solutions on criminal justice access to evidence stored on servers in the cloud and in foreign jurisdictions'.[57] Although these discussions may not have yielded results yet, as long as no other instruments have been agreed to, the context of the Budapest Convention for now is the one in which they have the greatest chance of actually doing so at some point.

In fact, the Convention explicitly makes provision for the Parties to consult periodically to facilitate its 'effective use and implementation', the exchange of information and 'consideration of possible supplementation or amendment of the Convention' (art. 46). In addition, any Party may propose an amendment to the Convention.

To describe the Convention as a static document therefore seems incorrect. Unfortunately, despite the supposedly global ambitions of the Convention initiators, the decision making structures of the Cybercrime Convention through which such changes would need to be approved ultimately remain solidly focused on the CoE, however: whether an amendment is adopted is ultimately a decision of the CoE's Committee of Ministers, taking into account the opinion of the CoE's European Committee on Crime Problems and following consultation with non-member state Parties (art. 44). This does give cause for pause.

Irrespective of, or perhaps in addition to, the current practical value of the Budapest Convention, it is then important for India to ask itself: what are the costs and benefits both of being part of these conversations, and of remaining on the side lines of them? Even if agreements cannot unite all countries in the world, regional instruments can have 'significant potential for positive progress towards greater sufficiency and

• 55. The Assessment Report on Preservation similarly found considerable problems in implementation, undermining the usefulness of the Convention to Parties. See Cybercrime Convention Committee (2015). Assessment Report: Implementation of the Preservation Provisions of the Budapest Convention on Cybercrime – Supplementary Report. Strasbourg, Council of Europe, June, p. 4, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168044be2b.
• 56. See the website of the Transborder Group: http://www.coe.int/en/web/cybercrime/tb.
• 57. See the website of the Cloud Evidence Group: http://www.coe.int/en/web/cybercrime/ceg.

harmonisation of national laws and in the long run enhanced international cooperation against a global challenge'.[58] India will have to ask itself whether it can really help push and shape such progress while standing on the side lines. At the same time, it is also important to ask: how much influence will India really be able to wield if decision making procedures with regard to the future of the Convention are not organised in a more democratic manner?

Conclusion and the Way Forward

Should India sign the Budapest Convention or not? While the issue comes up in intergovernmental meetings and at conferences on cybersecurity issues on a regular basis, the time might not be right for any straightforward answer to that question yet.

As discussed in this paper, at present the tactical value of signing the Budapest Convention might well be greater than the practical value. At the same time, as this paper has shown, doing so would also bring with it a number of tactical and practical drawbacks. Indeed, there are several areas in which the Budapest Convention displays significant weaknesses that matter to India and Indian people; yet whether better outcomes can be achieved elsewhere, and within what timeline, isn't yet clear.

In this context, what might be the best way forward is for the Indian government to make a more comprehensive analysis of its concerns and the current situation in collaboration with all stakeholder groups in the country, and to use that analysis to push for either reform of the Cybercrime Convention and/or for a new treaty elsewhere. At the moment, what India wants exactly, and why it believes the Cybercrime Convention might not be able to deliver, isn't always clear to other governments and stakeholders. The formulation of a stronger, more detailed case can go considerable length in helping India achieve its foreign policy objectives on this issue and to make the most of any opportunities that arise or are created, including over and above those mentioned here.

In order to do so, the questions raised in this paper will need to be considered in all their complexity. As there are so many variables involved in each of them, firm answers at this time will likely be difficult to come by. It is for this reason, though, that it is so important that the government draw on the widest possible number of perspectives from within the country: only then will the government be able to construct the truly comprehensive picture that it will need to make a sound judgement on how to move forward successfully on this issue. Among other things, such a picture will not pit cybersecurity against human rights, but will see human rights and cybersecurity as integral to one another. If cybercrime victimisation rates are considerably higher than for other forms of crime, this is particularly the case in developing countries.[59] Seeing the gravity of this complex issue, such consultations can, therefore, not start soon enough.

• 58. UNODC, *Comprehensive study on Cybercrime – Draft*, p. 76.
• 59. UNODC, *Comprehensive study on Cybercrime – Draft.*

March 2016