India and the Budapest Convention: why not?

Alexander Seger, Executive Secretary Cybercrime Convention Committee, Council of Europe[1]

Contribution to CyFy 2016, New Delhi, 28 to 30 September 2016

Governments all over the world are struggling not only with increasing levels of cybercrime but also with the complexities of securing electronic evidence in relation to fraud, corruption, murder, rape, terrorism, the sexual abuse of children and, in fact, any type of crime.

If only a miniscule portion of cybercrime and other offences entailing e-evidence is investigated and adjudicated the rule of law is in question and governments may fail in their obligation to protect the rights of individuals and society against crime.

Securing e-evidence for criminal justice purposes is particularly challenging in the context of cloud computing where data is distributed over different services, providers, locations and often jurisdictions, and where mutual legal assistance is often not feasible.

These challenges are currently being addressed by the Cybercrime Convention Committee at the Council of Europe representing the Parties to the Budapest Convention on Cybercrime. Solutions to enable criminal justice access to evidence in the cloud are a priority of this Committee.

While India is confronted with the very same challenges, India is not participating in this work, is not sharing its experience and is not shaping future international solutions as it has not yet decided to join this treaty.

International agreements form an important node in a web of solutions needed to address security and the rule of law in cyberspace. However, the more cyber issues affect core national interests the more difficult it is to reach international consensus. All-inclusive solutions covering cyber warfare, terrorism and crime would not seem feasible.

With regard to "cyber" as a matter of state-to-state relations and international security, the work of the UN Group of Governmental Experts seems to be the most promising avenue at present. With regard to cybercrime and electronic evidence as a matter of criminal justice, the Budapest Convention on Cybercrime is in place and functioning.

So far, general foreign policy considerations may have prevented accession to the Budapest Convention by India. Given the surge in cybercrime and the vision of a "Digital India" it may be time for the Government of India to reconsider the benefits of joining this treaty.

Challenges

Cybercrime – that is, offences against and by means of computer systems – has been around for some 45 years and can hardly be called a new form of crime. However, with the evolution of the

[1] The views expressed here are those of the author and do not necessarily represent official positions of the Council of Europe or of Parties to the Budapest Convention on Cybercrime.

information society and its dependency on information and communication technology (ICT), the vulnerability of societies worldwide to cybercrime has increased considerably.

The current scale, nature and impact of cybercrime are such that it not only undermines confidence and trust in ICT, but that is represents a serious threat to the fundamental rights of individuals, to the rule of law in cyberspace and to democratic societies.

This is reflected, for example, in the large-scale theft of personal data that affects the right to privacy, in attacks against the dignity and integrity of individuals, in particular children, in denial of service and other attacks against media or civil society organisations affecting the freedom of expression, in attacks against governments, parliaments and other democratic institutions as well as public infrastructure, or in the misuse of ICT for xenophobia and racism or radicalisation and terrorist purposes thus threatening democratic stability. Cybercrime causes economic cost and risks to societies and undermines human development opportunities. And cybercrime is a threat to international peace and stability.

Reportedly, trillions of security incidents are noted each year and millions of attacks against computer systems and data are recorded every day. However, a rather small share of such attacks is actually reported to criminal justice authorities.

India is no exception. According to the National Crime Records Bureau, 9,622 incidents of cybercrime were recorded in 2014 under the IT Act, Indian Penal Code and State and Local Laws. Even if this represents an increase of 69% as compared to 2013, cybercrime accounted for only 0.13% of all crimes recorded in 2014.

There is, however, another aspect which is often neglected in discussions on cyber security and in policies and strategies on cyberspace and which adds another dimension, namely the question of electronic evidence. Again, India is no exception. The National Cyber Security Policy of 2013 refers to effective law enforcement capabilities for the investigation and prosecution of cybercrime, but not to the broader issue of electronic evidence.

Criminal justice authorities need access to data for use as evidence in criminal proceedings; without data, no evidence, no justice and thus no rule of law. Increasingly, evidence in relation to any crime is stored in electronic form on computer systems. This includes serious and violent crime, such as location data in cases of murder or rape, subscriber information related to ransom e-mails sent during kidnappings, data to identify and locate victims of child abuse, or data on communications between terrorists.

It can be assumed that this is increasingly a reality in India and that a growing proportion of the more than 7 million crimes recorded entails e-evidence.

The more real-world crime involves e-evidence, the greater the chances that any law enforcement officer, prosecutor or judge will come across and need to have the skills to deal with e-evidence. Major capacity building within the criminal justice system is required and clear rules for criminal justice access to e-evidence and its admissibility in court need to be established.

Securing e-evidence related to cybercrime or other types of crime is an increasingly complex undertaking. The sheer volume of cases involving electronic evidence, the number of devices, users and victims involved, and technical complications such as encryption or anonymisers present major challenges.

The transnational nature of e-evidence – it may be stored in foreign jurisdictions even in cases that are otherwise fully domestic – combined with the transversal scope of e-evidence – in that any crime may entail such evidence – has implications on international cooperation in criminal matters. Most mutual legal assistance requests for electronic evidence are not related to cybercrime but to fraud and financial crime followed by violent and serious crimes.

Given the volatility of e-evidence, the mutual legal assistance process is rather inefficient. Response times of six to 24 months to MLA requests appear to be the norm. Many requests and thus investigations are abandoned. This adversely affects the positive obligation of governments to protect society and individuals against cybercrime and other crime involving electronic evidence.

Cloud computing further complicates the matter. Mutual legal assistance is about cooperation between authorities competent for MLA. But if evidence is less held on a specific device or in closed networks but is distributed over different services, providers, locations and often jurisdictions it is difficult to identify to which authorities to send a request.

Furthermore, law-enforcement powers are tied to the principle of territoriality, meaning that a criminal justice authority can only enforce its laws – such as ordering a service provider to produce data, or searching and seizing a computer system – on its own territory. But what principles govern the jurisdiction to enforce in a cloud context: the location of data, the nationality or location of the data owner, the location of the data controller, the headquarters of a cloud provider, the location of a subsidiary of a cloud provider or the territory where a service is offered?

The Cybercrime Convention Committee of the Council of Europe, representing the Parties to the Budapest Convention on Cybercrime, has been analysing these challenges for some time. In 2014, it adopted a set of recommendations to render mutual legal assistance more efficient. However, it also recognized that the feasibility of mutual legal assistance may be limited, in particular in the context of cloud computing. In 2015, therefore, it established a "Cloud Evidence Working Group" to identify additional solutions by the end of 2016.

These questions are not only relevant to Parties to the Budapest Convention but are equally important concerns for India. The solutions pursued within the framework of the Budapest Convention may thus also be of value for India. And other Parties would benefit from the experience of India.

International agreements

Security challenges in cyberspace require a web of responses by public and private sector stakeholders at all levels down to the individual user of a computer. International agreements are an important part of the response but – with exceptions – have been difficult to achieve.

The quest for international treaties

International efforts to address the question of cybercrime and electronic evidence as a matter of criminal justice have been pursued since the 1980s, initially by the Council of Europe and the Organisation for Economic Cooperation Development (OECD), and from the mid-1990s also within the G8. At the Council of Europe this led to the adoption of soft-law "Recommendations" providing guidance on the criminalisation of computer-related offences (1989) and six years later (1995) on law enforcement powers regarding cybercrime and electronic evidence. These

were precursors to the Budapest Convention on Cybercrime which was opened for signature in 2001.

One may argue that by 2001 the problems of cybercrime and e-evidence were sufficiently important to warrant an international treaty but that cybercrime and information technologies were not yet considered too important and not yet touching too much on the national interests and security of States to prevent consensus. The Budapest Convention was thus negotiated and agreed upon by the member States of the Council of Europe as well as Canada, Japan, South Africa and the USA. By August 2016, all of these countries, with the exception of two members of the Council of Europe, namely, the Russian Federation and San Marino, had signed the treaty.

At the level of the United Nations, it has not been possible to reach consensus so far as to whether an international treaty on cybercrime was necessary and feasible and what it would possibly comprise. The matter of "combating the criminal misuse of information technologies" was the subject of a resolution at the United Nations Congress on Crime Prevention and Criminal Justice in Havana, Cuba, in 1990. It referred to the work of the OECD and the Council of Europe, but no follow up was given within the UN. In 2001 and 2002, it was taken up once more in UN General Assembly Resolutions but at that point the Convention on Cybercrime of the Council of Europe had been opened for signature in Budapest.

Subsequently, the question was on the agendas of UN Crime Congresses (in 2005, 2010 and 2015) and annual UN Crime Commissions without much progress. The Intergovernmental Group of Experts on Cybercrime, established at the Salvador Crime Congress in 2010, "in view of examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime", noted in the conclusions of its most recent meeting in 2013 "broad support for capacity-building and technical assistance" and "diverse views" with respect to options of new international instruments.

It would seem that from around 2001 onwards, the focus within the UN had shifted from cybercrime as a matter of criminal justice to the protection of critical information infrastructure and towards cyber or information security as a matter of international security. From 2004, Groups of Governmental Experts (GGEs) have been meeting to examine "existing and potential threats from the cyber-sphere and possible cooperative measures to address them". Progress at the UN towards norms, rules or principles of "responsible State behaviour" in cyberspace is slow but is considered the most relevant forum on state-to-state relations concerning cybersecurity.

These observations are meant to illustrate the following:

- International consensus on rules for cyberspace will remain difficult to achieve given strong and often diverging (national) interests.
- An all-inclusive international agreement encompassing cyber (or information) warfare, terrorism and crime as proposed by some States, would hardly be feasible.
- Separating the issues into more manageable portions would seem a wiser approach. With regard to "cyber" as a matter of state-to-state relations and international security, the work of the UN Group of Governmental Experts seems to be the most promising avenue at present, complemented, for example, by confidence building measures agreed upon by the Organisation for Security and Cooperation in Europe, bi-lateral "cyber diplomacy" or initiatives such as the "London process".
- With regard to cybercrime as a matter of criminal justice, not much progress has been achieved within the UN since 1990, while the Budapest Convention on Cybercrime is in place and functioning.

The Budapest Convention on Cybercrime

The Budapest Convention is a criminal justice treaty which provides for (i) the criminalisation of conduct, ranging from illegal access, data and systems interference to computer-related fraud and child pornography; (ii) procedural law tools to make the investigation of cybercrime and the securing of electronic evidence in relation to any crime more effective, and (iii) international police and judicial cooperation on cybercrime and e-evidence.

It was opened for signature in Budapest in 2001. States which participated in the negotiation of the Convention (members of the Council of Europe, Canada, Japan, South Africa and USA) can sign and ratify the treaty. Under Article 37 any other State can become a Party by "accession" if the State is prepared to implement this treaty. Whether becoming a Party through ratification or accession, the end-result is the same.

By August 2016, 49 States were Parties (European countries as well as Australia, Canada, Dominican Republic, Israel, Japan, Mauritius, Panama, Sri Lanka and the USA). Another six had signed it (including South Africa) and another 12 had been invited to accede (most recently Ghana. From the Asia/Pacific region these include the Philippines and Tonga).

These currently 67 States – together with ten international organisations (such as the Commonwealth Secretariat, INTERPOL, the International Telecommunication Union, the UN Office on Drugs and Crime and others) participate as members or observers in the Cybercrime Convention Committee. This Committee among other things assesses implementation of the Convention by the Parties, adopts Guidance Notes or prepares additional legal instruments such as draft Protocols to the Budapest Convention.

The Budapest Convention is furthermore backed up by capacity building programmes. Given the need for and the broad international consensus on capacity building and technical assistance, the Council of Europe in 2014 established a dedicated Programme Office on Cybercrime (C-PROC) which is located in Bucharest, Romania. In the Asia/Pacific region, the Philippines, Sri Lanka and Tonga are priority countries for technical assistance given their commitment to implement the Budapest Convention. They benefit from law enforcement and judicial training, and the strengthening of legislation including rule of law and human rights safeguards, of specialised institutions, public/private partnerships and international cooperation. By August 2016, C-PROC managed a portfolio of projects with a volume of some EUR 23 million. Several of these were joint projects with the European Union.

This triangle of common standards (Budapest Convention), follow up and assessments (Cybercrime Convention Committee) and capacity building (C-PROC) represents a rather dynamic framework. It helps ensure that States joining this treaty are actually able to implement its provisions and to cooperate with other Parties. It keeps improving the quality of implementation by States that are Parties already. And it allows Parties to keep the Budapest Convention up to date and to negotiate additional solutions if necessary.

Access to evidence in the cloud

Obviously, defining the conduct that constitutes cybercrime in criminal law is essential. In the Budapest Convention this is reflected in Articles 2 (illegal access to a computer system) to 12 (corporate liability). In recent years, the Cybercrime Convention Committee has adopted a series of Guidance Notes to show how these provisions cover phenomena such as botnets, distributed

denial of service attacks, identity theft or other types of conduct that did not exist as such when the Convention was adopted. And the Committee is currently assessing to what extent Parties have adopted sanctions and other measures that are effective, proportionate and dissuasive as foreseen in Article 13. With respect to substantive criminal law the Budapest Convention remains up to date.

The question of procedural law powers to secure electronic evidence and, by extension, the question of efficient access to evidence in a transnational and cloud context is a more complicated challenge, given the limitations of the mutual legal assistance process which is normally designed to protect the rights of individuals as well as the interests of States in which evidence is located.

The Cybercrime Convention Committee has, therefore, been focusing in recent years on the question of:

- how to ensure effective access to evidence on servers stored on, or distributed or moving between servers in foreign, multiple or unknown jurisdictions, and
- how to reconcile the need for efficient law-enforcement access to data with the need to respect rule-of-law and human-rights requirements, and thus how to avoid the trap of undermining the rule of law through actions meant to protect it.

A number of options have been proposed by the "Cloud Evidence Group" of the Cybercrime Convention Committee and are currently under discussion:

- Rendering the mutual legal assistance process more efficient. Specific recommendations to this effect have already been adopted by the Committee and relate, for example, to resource allocation in Parties, the role of 24/7 points of contact for urgent cooperation, or streamlining of MLA procedures.

- Specific and lighter domestic rules and procedures for production orders for subscriber information in line with Article 18 Budapest Convention given that subscriber information is the most often sought information in domestic and international criminal investigations. Subscriber information is less privacy sensitive than traffic or content data and production orders are less intrusive than search, seizure or interception powers. A lower threshold for the disclosure of such information would thus be justified.

- A Guidance Note on Article 18 Budapest Convention on production orders for subscriber information to clarify the scope of this provision. It would require service providers located in or "offering a service in the territory" of a Party – under certain conditions – to disclose subscriber information irrespective of the actual location of such data.

- A clearer (legal) and more predictable basis for the current practice of voluntary disclosure of subscriber information by service providers directly to foreign criminal justice authorities. For example, in 2015, Parties to the Budapest Convention other than the USA sent some 140,000 requests to six major US providers and received data in 60% of the cases on average. (Incidentally, India sent about 20,000 to the same providers – of which more than half to Facebook – with a response rate of 48% in 2015.) It is yet to be confirmed whether Article 18 Budapest Convention can serve as the legal basis for such direct cooperation or whether a Protocol to the Convention would be needed.

- An additional Protocol to the Budapest to cover, for example, a simplified regime for mutual legal assistance requests for subscriber information and/or international production orders; direct cooperation between judicial authorities; joint investigations; emergency procedures; direct cooperation with providers in foreign jurisdictions; a clearer framework and safeguards for transborder access to data; and data protection rules and other safeguards.

The Cybercrime Convention Committee – with its 67 Parties and observer States – will continue consideration of these proposals in November 2016 in view of deciding on the further course of action.

These issues are also of relevance to India as reflected, for example, in questions 15 and 17 of the "Consultation Paper on Cloud Computing" circulated by the Telecommunication Regulatory Authority of India in June 2016.

So far, however, India remains uninvolved in the deliberations of the Cybercrime Convention Committee.

India and the Budapest Convention: why not?

In 2007 and 2008, the authorities of India and the Council of Europe cooperated in the reform of the Information Technology Act. These reforms brought the legislation of India broadly in line with the Budapest Convention.

While membership in the Budapest Convention more than doubled since then, the authorities of India have not yet come to a decision whether or not to join this treaty. The reasons are not entirely clear. Concerns voiced by different stakeholders over time include:

- That India did not participate in the negotiation of the Budapest Convention and should thus not sign up to it. Obviously, participation by India in the negotiation of the original treaty would have been preferable. This concern is not unique to India. Other States, however, have come to the conclusion that the interest and benefits of joining the Budapest outweigh such concerns. They are now in a position to participate in the further evolution of the treaty, including the possible negotiation of additional protocols. India has come to a similar conclusion with respect to two other Council of Europe treaties which India did not negotiate, namely on international cooperation in tax matters (India became a Party in 2012) and on the transfer of sentenced persons (India requested accession and was invited to accede in 2016).

- That the Budapest Convention – through its Article 32b – allows for transborder access to data and thus infringes on national sovereignty. The Cybercrime Convention Committee has studied this provision in detail and confirmed the very limited scope of Article 32b in a Guidance Note in 2014. This then led some counterparts in the Government of India to criticise that Article 32 was too limited and that additional options would be needed.

- That the MLA regime of the Budapest Convention is not effective, "the promise of cooperation not firm enough", or that there are grounds for refusal to cooperate. It is true that the Cybercrime Convention Committee in its own assessment of the functioning of MLA has come to the conclusion that while the level of mutual legal assistance keeps increasing between Parties, the MLA process needs to be made more

efficient overall. This matter is being addressed through follow up to a set of recommendations adopted in 2014 and the proposals made by the Cloud Evidence Group. The "algorithm" of the Budapest Convention, that is, the triangle of standards, follow up and capacity building, allows to address possible shortcomings. However, one should remain realistic and not expect one treaty to resolve all possible problems. India would certainly not expect this from other international treaties to which it is a Party.

- That it is a criminal justice treaty and thus does not cover state actors or that some of the States from which most attacks affecting India emanate have not signed up to the Budapest Convention. Indeed, it is a criminal justice treaty and the question of state-to-state relations would need to be addressed in other fora such as the UN Governmental Group of Experts (GGE).

- That India should promote a treaty at the level of the United Nations. This proposal seems to be favoured in the context of BRICS but the intended scope remains unclear – is it meant to be a criminal justice treaty, or to focus on terrorism, or to address state-to-state relations and matters of international security, or all in one? Taking into account experience since 1990, it is unlikely that a binding treaty at the UN level will become available in the coming years. Meanwhile, cybercrime keeps growing day by day.

Overall, it would seem that the question of India joining this treaty has so far primarily been a question of diplomacy and foreign policy considerations and less of actual criminal justice cooperation on cybercrime and electronic evidence. From the latter perspective,

- the challenges currently being addressed by the Parties to the Budapest Convention through the Cybercrime Convention Committee are highly relevant also for India;
- the Budapest Convention offers a legal basis and practical framework for police to police and judicial cooperation on cybercrime and electronic evidence with an increasing number of other Parties. This framework is constantly under review by the Parties to make it more effective;
- as the Budapest Convention evolves, India would be able to contribute to shaping future solutions if it were a Party;
- India would become a priority country for capacity building.

Given Prime Minister Narendra Modi's vision of a Digital India and given the surge in cybercrime, why would it not be beneficial for India to join this treaty?
