Lecture- 25

European Convention on cybercrime

India voted in favour of a cybercrime resolution led by Russia in a committee of the United Nations General Assembly. The resolution seeks to set up new cyber norms considered as counter alternative to the US backed Budapest Accord. A final General Assembly vote to adopt the resolution will be held in December, 2019.

Budapest Convention

The Council of Europe's (CoE) Cybercrime Convention is also known as the Budapest Convention. It was open for signature in 2001 and came into force in 2004. The convention is the sole legally binding international multilateral treaty on cybercrime. It coordinates cybercrime investigations between nation-states and criminalizes certain cybercrime conduct.

It serves as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between state parties to this treaty.

The Budapest Convention is supplemented by a Protocol on Xenophobia and Racism committed through computer systems.

The Convention on Cybercrime or Budapest Convention is the only binding multilateral treaty instrument aimed at combating cybercrime. It was drafted by the Council of Europe with active participation from its observer states in 2001. The Convention provides a framework for international cooperation between state parties to the treaty. It is open for ratification even to

states that are not members of the Council of Europe. The Convention is the only substantive multilateral agreement with a stated objective of addressing cybercrime with convergent, harmonized legislation and capability building. Therefore, it is widely recognized as a decisive document on international best practice and enjoys compliance even from non-signatory states. Most model legislation and attempts at drafting a new international instrument on cybercrime have also relied on the principles expounded in this Convention. The Budapest Convention is also supplemented by an Additional Protocol to the Convention which was adopted in 2003.

Offences under the Convention

The Budapest Convention broadly attempts to cover crimes of illegal access, interference and interception of data and system networks, and the criminal misuse of devices. Additionally, offences perpetrated by means of computer systems such as computer-related fraud, production, distribution and transmission of child pornography and copyright offences are addressed by provisions of the Convention. The substantive offences under the Convention can broadly be classified into

1. offences against the confidentiality, integrity and availability of computer data and systems;
2. computer-related offences;
3. content-related offences; and
4. criminal copyright infringement.

The Additional Protocol makes the act of using computer networks to publish xenophobic and racist propaganda, a punishable offence. However, the full range of cybercrimes are not covered under the Budapest Convention. These include cybercrimes such as identity theft, sexual grooming of children and unsolicited spam and emails.

Provisions of the Convention

The treaty functions on a mutual information sharing and formal assistance model in order to facilitate better law enforcement and lays down procedure to seek and receive such assistance. Article 23 of the Convention outlines the general principles under which international cooperation can be sought, as follows:

"Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."

It is clear then that assistance facilitated by the Convention relies on pre-existing cooperative agreements between the parties. Thus, as also stated in Article 39 of the Convention, the provisions only serve to supplement multilateral and bilateral treaties already effective between parties. In addition, mutual legal assistance (MLA) between parties where no such mutual arrangements exists, can be facilitated through procedures laid down under Article 27. Principles and procedures related to extradition for criminal offences under the Convention is also detailed in Article 24 of the Budapest Convention. These sections primarily aid formal legal assistance between signatory parties to the Convention in case of a cybercrime (as defined under the Convention itself).

The Convention itself does not demand 'dual criminality' per se. However, the adoption of the Convention demands harmonization of national legislations and results in reciprocal

criminalization. This is crucial as the Convention has mutual assistance and extradition provisions, both easier to process when dual criminality is established between the requesting and assisting parties.

The Cybercrime Convention Committee (T-CY) was setup to represent the interests of and foresee regular consultations between state parties to the Convention. The biannual plenaries conducted by the T-CY and working groups discuss developments, shortcomings, grievances and possible amendments of the Budapest Convention.

Significant Drawbacks of the Convention

The Convention on Cybercrime has also come under severe criticism for both its specific provisions that fail to protect rights of individuals and states, and its general inadequacy in sufficing to ensure a cyberspace free of criminal activity.

The 12th Plenary of the T-CY (at page 123) concluded that the mutual legal assistance facilitated by the Convention was too complex and lengthy, rendering it inefficient in practice. The outdated nature of provisions of the Convention clearly fail to cater to the needs of modern investigation.

The provisions of the Convention have been critiqued for supposedly infringing on state sovereignty. In particular, Article 32 has been contentious as it allows local police to access servers located in another country's jurisdiction, even without seeking sanction from authorities of the country. In order to enable quick securing of electronic evidence, it allows trans-border access to stored computer data either with permission from the system owner (or service provider) or where publically available. As Russia finds this provision to be an intolerable infringement of its sovereignty (amongst other things),[3] it has categorically refused to sign the Convention in its current state. However, it is important to note that the claim that provisions

infringe on sovereignty has been addressed and countered by the T-CY in its guidance note on Article 32

Russia's displeasure with the existing multilateral instrument was evidenced by the introduction of a Russia-backed proposal for an international cyberspace treaty. The proposal, specifically for a convention or protocol on cybersecurity and cybercrime was considered and rejected at the 12th UN Congress on Crime Prevention and Criminal Justice. US and EU refused to countenance a new cybercrime treaty, opining that the Budapest Convention sufficed and efforts should be directed at capacity building.

Regardless, Brazil and China which have expressed displeasure at the primarily-European treaty, have refused to adopt the Convention for the same reason. India also continues to remain a non-signatory to the inequitable Convention, having categorically declined to adopt the Convention which was drafted without its participation. India's statements also reflect its belief that the Budapest Convention in its present form is insufficient in tackling cybercrimes. This may hold especially true as India routinely faces cyber-attacks from China. This is a problem that will not be resolved by mere ratification of the Budapest Convention as China is a non-signatory to the treaty. With multiple countries remaining a non-signatory, with little scope for change in their positions, the reach of the Convention is certainly limited. There is a demonstrable need for a unique, equitable and all-encompassing instrument that governs cybercrime. To ensure maximum consensus and compliance, this instrument must necessarily be negotiated with active participation from all states.