BUDAPEST CONVENTION ON CYBER CRIME

BY: PROF. DURGAMBINI A PATEL AND ASST PROF. SANJANA BHARADWAJ
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.
The Budapest Convention provides for (i) the criminalisation of conduct, ranging from illegal access, data and systems interference to computer-related fraud and child pornography; (procedural law tools to make the investigation of cybercrime and the securing of e-evidence in relation to any crime more effective and (iii) international police and judicial cooperation on cybercrime and e-evidence.
States which participated in the negotiation of the Convention (members of the Council of Europe, Canada, Japan, South Africa and the US) can sign and ratify the treaty.

Under Article 37, any other state can become a party by ratification or accession if it is prepared to implement the convention.
INTRODUCTION

THE NUMBER OF STATES

By August 2016, 49 States were parties (those already mentioned as well as Australia, Dominican Republic, Israel, Mauritius, Panama and Sri Lanka). Another six had signed it (including South Africa) and 12 had been invited to accede (most recently Ghana; from the Asia/Pacific region these include the Philippines and Tonga).

These 67 states — together with 10 international organisations (such as the Commonwealth Secretariat, INTERPOL, International Telecommunication Union and the UN Office on Drug and Crime) participate as members or observers in the Cybercrime Convention Committee. The 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 Convention.
The Budapest Convention is backed up by capacity-building programmes. In 2014, the Council of Europe established a dedicated Programme Office on Cybercrime (C-PROC) in Bucharest Romania. In the Asia/Pacific region, the Philippines, Sri Lanka and Tonga are priority count for technical assistance given their commitment to implement the Convention. They benefit from law-enforcement and judicial training and strengthening of legislation, including rule law and human rights safeguards, of specialised institutions, public-private partnerships a international cooperation. By August 2016, C-PROC managed a portfolio of projects worth some €23 million, many being 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 dynamic framework. It helps ensure that states joining the Convention are actually able to keep improving the quality of implementation of its provisions and cooperation with other part. And it allows parties to keep the Budapest Convention up-to-date and negotiate additional solutions if necessary.
### PROVISIONS OF THE CONVENTION

<table>
<thead>
<tr>
<th>SR.NO.</th>
<th>CHAPTER NO.</th>
<th>SECTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>I- USE OF TERMS</td>
<td>ARTICLE 1</td>
</tr>
<tr>
<td>2.</td>
<td>II – MEASURES TO BE TAKEN AT THE NATIONAL LEVEL</td>
<td>ARTICLE 2 to 22</td>
</tr>
<tr>
<td>3.</td>
<td>III – INTERNATIONAL CO-OPERATION</td>
<td>ARTICLES 23 to 35</td>
</tr>
<tr>
<td>4.</td>
<td>IV – FINAL PROVISIONS</td>
<td>ARTICLES 36 to 48</td>
</tr>
</tbody>
</table>
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 Convention in case of a cybercrime (as defined under the Convention itself).
The convention covers illegal access, interference and interception of data and system networks, and the criminal misuse of devices, the computer systems related offences.

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.
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.
SPECIAL THANKS TO MS. POORVA SHARMA, STUDENT, DEPARTMENT OF LAW