Convention on Cybercrime

Nilupul Gunawardena*

November 2018

*Nilupul Gunawardena is a Research Fellow at the Lakshman Kadirgamar Institute of International Relations and Strategic Studies (LKI). The opinions expressed in this article are the author’s own views. They are not the institutional views of LKI, and do not necessarily represent or reflect the position of any other institution or individual with which the author is affiliated.
About the *LKI Explainers*
LKI Explainers examine an agreement or another aspect of Sri Lanka’s international relations. They summarise key points and developments, with up-to-date information, facts, and figures.

**Terms of use**
LKI is not responsible for errors or any consequences arising from the use of information contained herein. The views expressed in a LKI Explainer are those of the author(s). They are not the institutional views of LKI and do not necessarily reflect the position of any other institution or individual with which an author is affiliated.
Contents

1. What are Cybercrimes?.................................................................1
2. What is Cybersecurity and why is it important................................1
3. What is the Budapest Convention on Cybercrime?....................1
4. What are the key features of the Convention?.............................2
5. What are the objectives and priorities of this Convention?..............3
6. What are the responsibilities & obligations incumbent upon the State Parties to this Convention?..................................................................................................................4
7. Benefits and drawbacks of the Convention .............................4
8. Implementations of the Convention in Sri Lanka..........................4
9. Key Readings.............................................................................5
## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLA</td>
<td>Mutual Legal Assistance</td>
</tr>
<tr>
<td>ICTA</td>
<td>Information and Communication Technology Agency</td>
</tr>
</tbody>
</table>
1. What are Cybercrimes?

- Cybercrimes are defined as crimes committed through the internet using a computer. This includes a wide range of offences against computer data and systems (such as ‘hacking’), computer-related forgery and fraud (such as ‘phishing’), content offences (such as disseminating child pornography), and copyright offences (such as the dissemination of pirated content).¹

2. What is Cybersecurity and why is it important?

- Cybersecurity is the protection of computer networks, programs and other internet connected systems from cyberattacks.

- Cyberattacks could do irreparable and irreversible damage to businesses and persons. This includes the misuse of personal information such as email addresses and credit card information, or huge financial losses to multinational organisations. For instance, the Bangladeshi Central Bank was recently hacked and millions of dollars were transferred to dubious NGOs registered in Sri Lanka.²

- With Sri Lanka’s ambition to make Colombo a Global Financial Centre, strengthening of cybersecurity is imperative to enable a safer, reliable and more conducive environment for persons and organisations. Sri Lanka also has a rapidly growing Information Technology market amounting to $900mn worth exports and employing over 85,000.³

- Key priorities include increasing awareness, and developing related skills for law enforcement personnel, stakeholders and the general public.

3. What is the Budapest Convention on Cybercrime?

- The Convention on Cybercrime (also known as the Budapest Convention) is the first international convention⁴ out to pursue a common criminal policy against cybercrime. It promotes the harmonisation of national laws, capacity building, and the fostering of international cooperation.

- The Convention was drafted by the Council of Europe and was opened for signatures on 23 November 2001. It entered into force on 1 July 2004.⁵
4. What are the key features of the Convention?

- The Convention facilitates the detection, investigation and prosecution of crimes committed via the internet and other computer systems. This includes aiding or abetting the commission of an offence.

Source - Alexander Seger⁶

*MLA - Mutual Legal Assistance - is an agreement between two or more states to gather and exchange information in an effort to enforce criminal law.
• The Convention broadly operates on three dimensions. First, it criminalises conduct such as illegal access and data interference. Second, it provides the procedural tools for states to follow, this includes search and seizure of computers and other devices used in the criminal activity. Finally, it places upon States an obligation for mutual cooperation in assisting with the investigations.

• The Budapest Convention is further supplemented by an Additional Protocol adopted in 2003, which makes using computer networks to publish xenophobic and racist propaganda, a punishable offence.

5. What are the objectives and priorities of the Convention?

• The Convention aims to:
  o Pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime;
  o Build the capacity of countries to combat cybercrime; and
  o Function as a mutual information sharing channel in order to facilitate better law enforcement.

• The Preamble of the Convention emphasises the importance of maintaining a proper balance between the interest of law enforcement and respect for fundamental human rights, specifically the right to hold opinions without interference, freedom of expression and the rights concerning the respect for privacy.

6. What are the responsibilities and obligations incumbent upon the State Parties to the Convention?

• Each party is required to adopt legislative and other measures to establish the offences listed in Convention as criminal offences under its domestic law.

• Parties are primarily required to:
  o Provide mutual assistance to states investigating crimes under the Convention;
  o Allow search and seizure of stored computer data for investigations;
  o Extradite those charged with cybercrimes or prosecute them domestically;
  o Real-time collection of internet traffic data including IP addresses and email header information; and
  o Preserve computer data for up to 90 days.
7. Benefits and Drawbacks of the Convention

Benefits of the Convention:

- The Convention sets a normative standard within the international legal framework, acknowledging the need to pursue a common criminal policy and procedural law in relation to cybercrimes.
- It contains provisions concerning mutual assistance as well as extradition rules to further facilitate and enhance international cooperation.\(^\text{10}\)
- It promotes cooperation between State parties and the private sector.

Drawbacks of the Convention:

- It does not cover a wide range of cybercrimes including identity theft, sexual grooming of children, and unsolicited emails and spam.
- Mutual legal assistance facilitated by the Convention is too complex and lengthy, rendering it inefficient in practice.\(^\text{11}\)
- Enforcement of the Convention is limited since over two thirds of States have not ratified the treaty.

8. Implementation of the Convention in Sri Lanka

- Sri Lanka ratified the convention in May 2015, becoming the first South Asian country and the second Asian Country (after Japan) to ratify the Convention.
- Preparation towards ratifying the Convention was carried out over several years under the “e-Sri Lanka Development Initiative.”\(^\text{12}\) This included regulatory reforms through the adoption of relevant legislation and capacity building.
- In June 2006, the Sri Lanka Computer Emergency Readiness Team Coordination Centre (Sri Lanka CERT) was established in collaboration with the Information and Communication Technology Agency (ICTA) of Sri Lanka. It acts as the focal point for cybersecurity in Sri Lanka.\(^\text{13}\)
Key Readings


Notes


5 Ibid.


7 Ibid.


