CERTIFICATE COURSE IN DIGITAL LAW

BAR ASSOCIATION OF SRI LANKA

www.alexsas.net

AlexSeger SAS

Bar Association of Sri Lanka: Certificate Course in Digital Law

Module on
"Cybercrime in the digital age – Budapest Convention and new legal developments"

International legal frameworks on cybercrime: Benefits and options for Sri Lanka

Alexander Seger
former Executive Secretary, Cybercrime Convention Committee, Council of Europe

Online, 27 May 2026

Agenda

- Introduction: Problems to be addressed by international frameworks
- International treaties on cybercrime:
  - Budapest Convention & Second Protocol & benefits for Sri Lanka
  - Hanoi Convention
  - Comparing these treaties
- Conclusion and call to action

Introduction — Problems that international legal frameworks need to address

Offences

1. Offences **against** the confidentiality, integrity and availability of computer systems and data

Examples:
- Illegally accessing a computer or data ("hacking")
- Illegally intercepting computer data
- Interfering with computer data (altering, deleting, stealing data, etc. e.g. via malware)
- Interfering with computer systems (denial of service attacks, ransomware attacks, etc.)
- Development or making available of **tools** to commit such offences

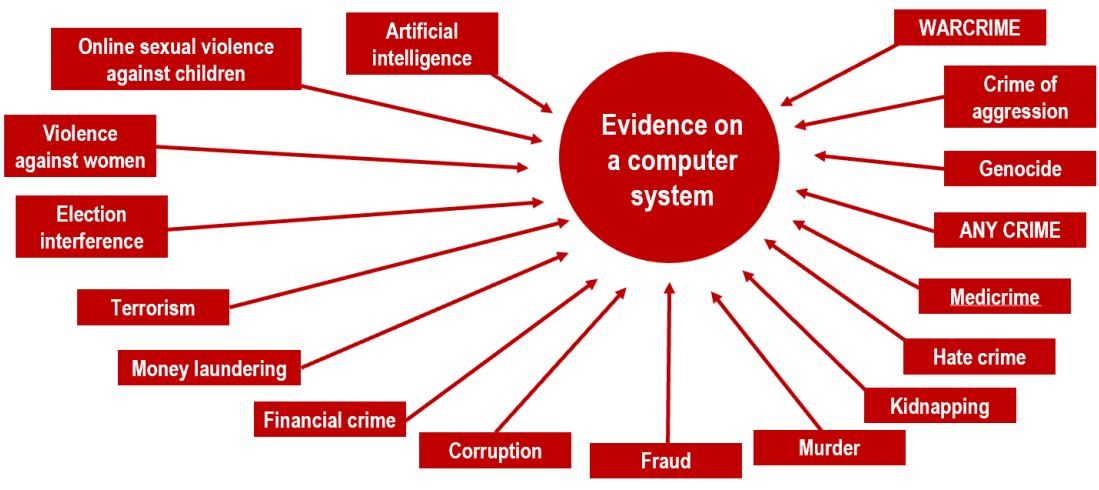
2. Offences **by means** of computer systems or data

Examples:
- Forgery (e.g. setting up a phishing website)
- Fraud (e.g. "man-in-the-middle-attack" etc. to deceive a computer system to obtain an economic benefit)
- Production, distribution, making available, possessing, accessing child sexual abuse materials ("child pornography")
- Non-consensual dissemination of intimate images (e.g. "sextortion")
- Solicitation (grooming) of children for sexual offences
- Offences related to intellectual property rights

3

Introduction — Problems that international legal frameworks need to address

Electronic evidence = evidence of any crime on a computer system

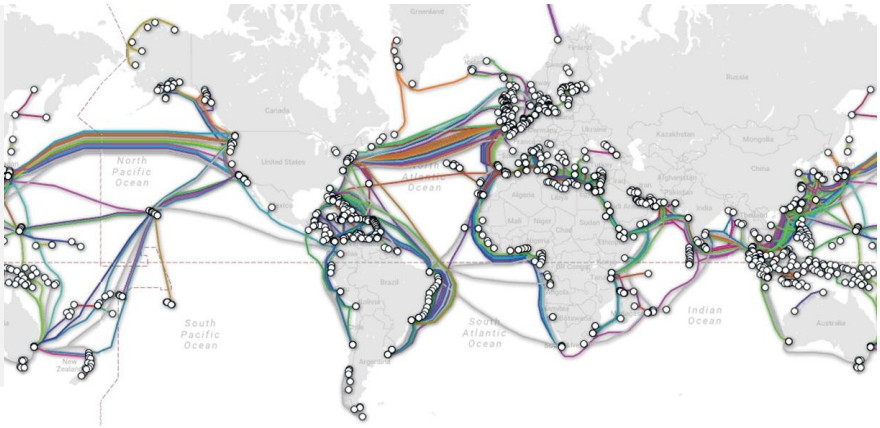


4

Introduction — Problems that international legal frameworks need to address

Electronic evidence = evidence to be obtained for use in criminal proceedings

- Where is the crime?
- Where is the data / evidence?
- Who has the data / evidence?
- What law applies?
- What boundaries for law enforcement?



5

Introduction — Problems that international legal frameworks need to address

Summary: Challenges to be addressed by international treaties on cybercrime and electronic evidence

- **Criminalizing** offences **against and by means** of computer systems and data
- **Procedural powers to collect electronic evidence** not only in relation to these offences but e-evidence of any offence
- **Obtaining volatile e-evidence** that may be somewhere "in the cloud" or in multiple or shifting jurisdictions
  - Government-to-government cooperation?
  - Direct access to computer systems in other jurisdictions?
  - Direct cooperation with service providers in other jurisdictions?
  - Protection of sovereignty?
  - Protection of rights of individuals?
  - Different types of data/evidence with different levels of sensitivity/protection?

6

Key international treaties on cybercrime and electronic evidence

- **Convention on Cybercrime** of the Council of Europe ("Budapest Convention") of 2001 with protocols (2003 & 2022)
- Convention against cybercrime of the United Nations ("Hanoi Convention") of 2025
  - Official title: "**United Nations convention against cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes**"

7

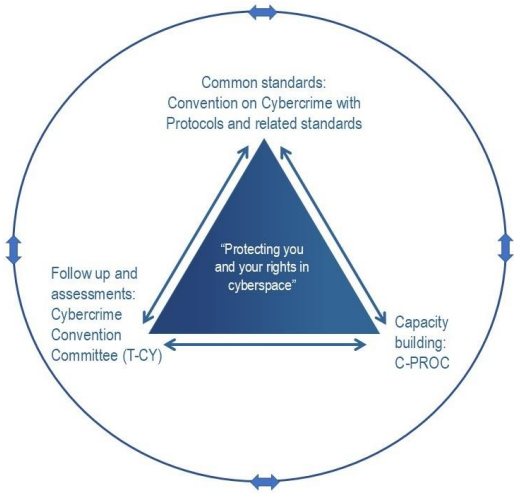
The framework of the Budapest Convention

- **Convention** on Cybercrime (Budapest, 2001)
  1. Specific offences
  2. Procedural powers
  3. International cooperation
- **1st Protocol** on Xenophobia and Racism via Computer Systems (2003)
- **2nd Protocol** on enhanced cooperation and disclosure of electronic evidence (2022)
- **Guidance Notes**

NB: Cybercrime & e-evidence!

As of May 2026:

82 Parties and 16 "Observer States"



8

Content of the Budapest Convention

Criminalising conduct
- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

Procedural tools
- Expedited preservation
- Production orders
- Search and seizure
- Interception of computer data

Limited by safeguards

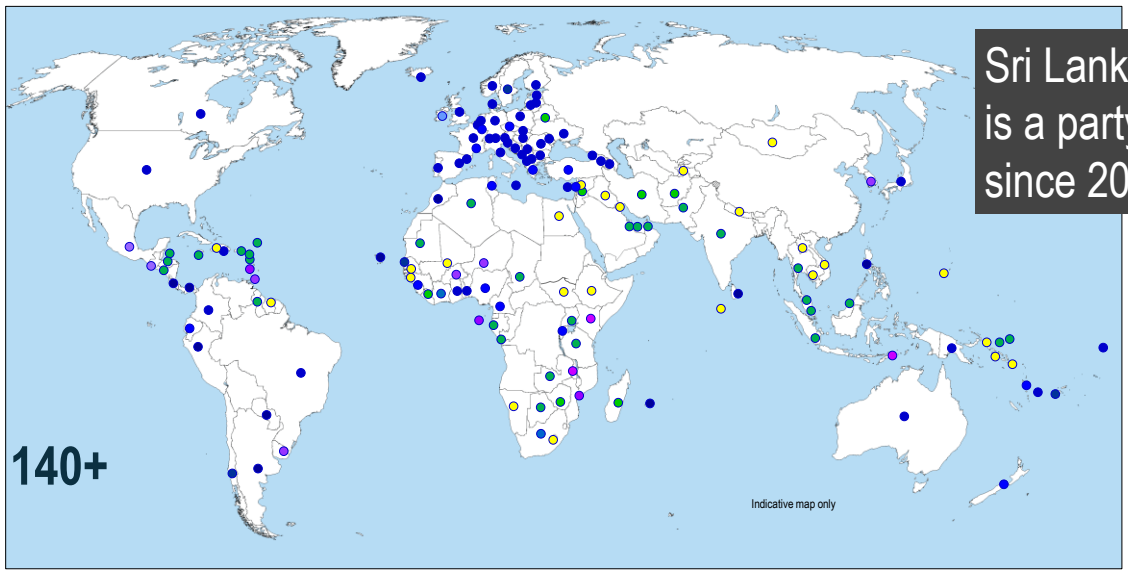
+

International cooperation
- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Cybercrime and e-evidence:
Procedural powers and international cooperation for any criminal offence involving evidence on a computer system!

9

Reach of the Budapest Convention



10

Joining the Budapest Convention: Benefits for Sri Lanka

- [Further] strengthening and harmonization of legislation (Computer Crime Act of 2007 aligned with Budapest Convention; MLA Amendment Act 2018; Personal Data Protection Act No. 9 of 2022; etc.)
- Capacity building for judiciary, Attorney General's Department, CID Units
- Strengthening institutional frameworks (CERT established, Police Cybercrime Investigation Department and 24/7 point of contact)
- Public/private cooperation
- South-South cooperation
- Criminal investigations and proceedings on cybercrime and e-evidence

Sri Lanka is a party since 2015

11

Second Protocol to the Budapest Convention on e-evidence

Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence

- Opened for signature May 2022
- As of May 2026: 52 signatories (Costa, Rica, Hungary, Japan and Serbia have ratified it)

Sri Lanka participated in negotiations and **signed** in November 2022

12

Second Protocol to the Budapest Convention on e-evidence

Chapter II: Measures for enhanced cooperation

Article 6	Request for domain name registration information	→ Public-2-Private
Article 7	Disclosure of subscriber information	→ Public-2-Private
Article 8	Giving effect to orders from another party for expedited production of subscriber information and traffic data	→ Public-2-Public
Article 9	Expedited disclosure of stored computer data in an emergency	→ Public-2-Public
Article 10	Emergency mutual assistance	→ Public-2-Public
Article 11	Video conferencing	→ Public-2-Public
Article 12	Joint investigation teams and joint investigations	→ Public-2-Public

Subject to safeguards, including for the protection of personal data (Article 14)

13

Second Protocol to the Budapest Convention on e-evidence

DAILY MIRROR ONLINE

Over 5,400 cybercrime cases in 2025; CID warns of job, investment scams Cybercrime rises in Sri Lanka

26 July 2025 12:04 am Views - 567 2 Bookmark Google News

The majority of cases involve social media platforms such as Facebook, WhatsApp, Instagram, Snapchat, and TikTok, with nearly 90% linked to Facebook. A significant number also involve misuse of artificial intelligence (AI) tools.

Asia

Sri Lanka arrests more than 260 foreigners cyberscams

Authorities have arrested hundreds of foreign nationals in recent months as Sri Lanka intensifies a sweeping crackdown on suspected cyber scam operations.

09 May 2

Call to action:

Reform domestic legislation for **ratification of the Second Protocol** to permit on a clear legal basis:

- Direct cooperation with multi-national service providers across borders
- Disclosure of content cross-border in emergency situations across borders

14

T-CY Guidance Notes

Guidance Notes:

- Common understanding between the Parties
- Adopted by consensus
- Keeping the Convention up-to-date and adapting to evolving technology, techniques and forms of crime

15

Current work by the Cybercrime Convention Committee (T-CY)

Ongoing: **Mapping study on virtual assets and relevance of the Convention on Cybercrime** (January 2025 – 2026?)

Ongoing: **Working Group on artificial intelligence** (January 2025 – 2026?)

To prepare a mapping study on cybercrime, electronic evidence and artificial intelligence (AI), including options and recommendations for further action by the T-CY.

The mapping study shall focus on the specific links between cybercrime, electronic evidence and artificial intelligence, and address issues such as:

- Offences committed against and by means of AI systems[3], and applicability of current criminal law, including the Convention on Cybercrime and its First Protocol on Xenophobia and Racism.
- The use of AI systems for the prevention, detection, investigation and prosecution of offences, for the collection of electronic evidence and for international cooperation, and the applicability of current criminal law and agreements, including the Convention on Cybercrime and its Second Protocol.
- The applicability of human rights and rule of law safeguards, chain of custody, territoriality and jurisdiction, and other conditions and principles in this regard.

16

The Hanoi Convention of the United Nations

"United Nations convention against cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes"

- Opened for signature in Hanoi, Vietnam, in October 2025 ► "Hanoi Convention"
- As of May 2026:
  - 73 signatories (**including Sri Lanka**)
  - 3 parties (Azerbaijan, Qatar, Vietnam)

17

The Hanoi Convention of the United Nations: Structure

- Chapter I: General provisions
- Chapter II: Criminalisation
- Chapter III: Jurisdiction
- Chapter IV: Procedural measures and law enforcement
- Chapter V: International cooperation
- Chapters VI–IX: Preventive measures, Technical assistance, Mechanism of implementation, Final provisions

18

The Hanoi Convention of the United Nations: Safeguards

- Article 6 on “respect for human rights”
- Article 21.4 with procedural guarantees
- Article 24 on conditions and safeguards, which is similar to Article 15 BC, and with the addition of paragraph 4
- Article 36 on the protection of personal data [de facto a ground for refusal]
- Article 40.22 on non-discrimination within the context of mutual legal assistance [grounds for refusal]

19

Comparing Hanoi and Budapest conventions

Example: Offences

Art.	Budapest Convention	Art.	Hanoi Convention
2	Illegal access	7	Illegal access
3	Illegal interception	8	Illegal interception
4	Data interference	9	Interference with electronic data
5	System interference	10	Interference with an information and communications technology system
6	Misuse of devices	11	Misuse of devices
7	Computer-related forgery	12	Information and communications technology system-related forgery
8	Computer-related fraud	13	Information and communications technology system-related theft or fraud
9	Child pornography	14	Offences related to online child sexual abuse or child sexual exploitation material
10	Copyright infringements	-	
-		15	Solicitation or grooming for the purpose of committing a sexual offence against a child
-		16	Non-consensual dissemination of intimate images
-		17	Laundering of proceeds of crime

20

Comparing Hanoi and Budapest conventions

Core concepts and measures:

- Drawn from the BC on Cybercrime (2001)
- Complemented by provisions adapted from the UN Conventions on Transnational Organised Crime (UNTOC, 2000) and Corruption (UNCAC, 2003)

► **Consistency**

New in UN treaty:

- Solicitation or grooming of children for sexual offences (Article 15)
- Non-consensual dissemination of intimate images (Article 16)
- Adapted from UNTOC and UNCAC: measures on money laundering and crime proceeds

NOT in UN treaty:

- IPR offences
- Art. 32 on transborder access to data
- Xenophobia and racism (First Protocol to BC)
- None of the measures of the Second Protocol to the BC on enhanced cooperation and disclosure of electronic evidence (2022):
  - Direct cooperation with service providers and registrars in other Parties (articles 6 and 7)
  - Expedited cooperation in emergency situations (articles 9 and 10)

21

Comparing Hanoi and Budapest conventions

Reservations and declarations:

- Budapest Convention: Limited to specific provisions. Article 42: "No other reservations may be made".
- Hanoi Convention: Open-ended, only limited by object and purpose test.

► **Risk of uneven, ambiguous or deferred implementation by parties to the Hanoi Convention**

► **Preventing effective international cooperation**

Hanoi Convention: **Examples of reservations** made upon ratification

Qatar: Reservation to child abuse articles

(1) The State of Qatar does not consider itself bound by the provisions of Articles (16), (15), and (14) of the Convention, as they contradict the provisions of Islamic Sharia, national legislation, and the social and cultural values of the State of Qatar.

Vietnam

1. The Socialist Republic of Viet Nam declares that the provisions of the United Nations Convention against Cybercrime are non-self-executing. The implementation of provisions of this Convention shall be in accordance with constitutional principles and substantive law of the Socialist Republic of Viet Nam, on the basis of bilateral or multilateral cooperative agreements with other States and the principle of reciprocity.

22

Conclusion

- Adoption of the Hanoi Convention by the United Nations is an important political achievement given the current fractured international context
- The Hanoi Convention is broadly consistent with the Budapest Convention, no obvious contradictions ► States (like Sri Lanka) may join also the Hanoi Convention (TBC: Probably only limited changes to laws of Sri Lanka needed)
- For Parties to the Budapest Convention (such as Sri Lanka) the Hanoi Convention offers additional options for cooperation with States that are not parties to the Budapest Convention
- For criminal justice practitioners, the Budapest Convention will remain the more relevant framework in the years to come
- The tools of the Second Protocol on e-evidence have NOT beenincorporated in the Hanoi Convention
- Sri Lanka is a signatory to the Second Protocol. Data protection safeguards are already in place
- **Call to action:** Sri Lanka is encouraged to undertake the necessary reforms of legislation prior to ratification of this Protocol

23

Discussion

Q & A

www.alexsas.net

24