Cyber-Case Plattform, Bern, Switzerland, 21 November 2025

Transborder "access" to data:

What is available within the framework of the (Budapest) Convention on Cybercrime?

Alexander Seger, Strasbourg, France

1. Intro, background, terminology
2. Measures for transborder access / disclosure of data
   - CCC: Art 18.1.b, Art 19, Art 32
   - 2nd Protocol: Art 7-9
3. Summary / conclusion
4. Epilogue: What to expect from the "Hanoi Convention" of the United Nations?

Version 21 Nov 2025

Alex.cyber@protonmail.com (Until Sep. 2025 Head of Cybercrime Division, Council of Europe)

1

Summary/conclusion

Summary: Toolbox to obtain electronic evidence from other Parties without MLA within the framework of the Convention on Cybercrime (CCC)

- **Article 18.1.b CCC**: Legal justification for requests for subscriber information to service providers offering a service in your territory [difficult to enforce but see Yahoo/Belgium; does not cover disclosure of content in an emergency]
- **Article 19.2 CCC**: Extending a search from a computer system in your territory to a connected system in your territory [In practice: authorities of most States are able to extend a search beyond their territory under varying conditions]
- **Article 32.a CCC**: Access for use as evidence of publicly available data from anywhere [possibly also useful for public blockchain-related evidence]
- **Article 32.b CCC**: Limited scope according to T-CY Guidance Note [can a service provider voluntarily consent?] but frequently used by some State ("other situations are neither authorised, nor precluded")

► The **Second Protocol** provides additional tools and closes some gaps:

- **Article 7**: Solid framework with safeguards for orders for subscriber information directly to service providers
- **Article 8**: More efficient tool to obtain traffic data (and enforcement mechanism for Article 7)
- **Article 9**: Flexible/discretionary tool to obtain the disclosure of content in an emergency via 24/7 network
- **Article 10**: Tool for expeditious MLA

2

2004: Nicolai Seitz: Transborder Search: A new perspective in law enforcement?

The question remains of what influence and to what application range the Convention on Cybercrime has on the situation of international law …
the high number of signatory states, the importance of the signatory states (in which a large part of the infrastructure of the Internet, including storage capacity, is located), as well as the fact that thus far, **no caveats regarding Article 32 (b) have been expressed by non-signatory states.** Considering the mentioned factors, it can thus be assumed that **Article 32 (b) is the result of (newly emerged) international customary law.**

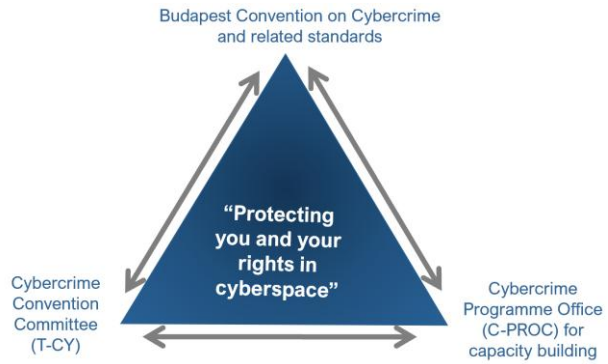
3

The framework of the Convention on Cybercrime

- **Convention on Cybercrime** (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** e.g. articles 32, 18.1.b)

www.coe.int/cybercrime

October 2025: **81 Parties, 2 Signatories, 15 Invited to accede**



Link to booklet with Convention, Protocols and Guidance Notes

4

Terminology

Computer Data:

- Subscriber information (Bestandesdaten) – Art. 18.3 CCC
- Traffic data (Verkehrsdaten / Randdaten) – Art. 1.d CCC
- Content data (Inhaltsdaten)

Access (Zugriff)
v. Production (Herausgabe)
v. Disclosure (Offenlegung)

Art. 18 CCC: to order to submit

Art. 19 CCC: to search or similarly access

Art. 32 CCC: to access or receive

Art. 7 2AP: to obtain the disclosure of subscriber information

Art. 8 2AP: compelling a provider to produce subscriber information or traffic data

5

Terminology > Subscriber information

- Subscriber information (Bestandesdaten) – Art. 18.3 CCC

- Less sensitive
- Most often needed
- Question of dynamic vs static IP addresses
- CJEU: retention and access permitted

Second Protocol – Explanatory Report:

92. Subscriber information is the most often sought information in criminal investigations relating to cybercrime and other types of crime for which electronic evidence is needed …
… It does not allow precise conclusions concerning the private lives and daily habits of individuals concerned, meaning that its disclosure may be of a lower degree of intrusiveness compared to the disclosure of other categories of data.

93. …. Information needed for the purpose of identifying a subscriber of a service may include certain Internet Protocol (IP) address information – for example, the IP address used at the time when an account was created, the most recent log-on IP address or the log-on IP addresses used at a specific time…

Cybercrime Convention Committee (T-CY) 2018: Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses (discussion paper)

Court of Justice (EU) decisions 2020, 2024:
Possible to require providers to **retain, generally and indiscriminately, data relating to the civil identity of users** (pure identification data). This is permitted for safeguarding national/public security **and for combating crime in general –** it is not limited to "serious crime"

6

History

Council of Europe 1989, 1990, 1995:

The question of unilateral direct access by law enforcement authorities to data stored on a computer abroad or compelling a person to submit such data, require an urgent international solution….

7

G8 meeting of Ministers of Justice and Interior (Moscow, October 1999): Principles on Transborder Access to Stored Computer Data

"Notwithstanding anything in these Principles, a State need not obtain authorization from another State when it is acting in accordance with its national law for the purpose of:

accessing publicly available (open source) data, regardless of where the data is geographically located

accessing, searching, copying, or seizing data stored in a computer system located in another State, if acting in accordance with the lawful and voluntary consent of a person who has the lawful authority to disclose to it that data. The searching State should consider notifying the searched State, if such notification is permitted by national law and the data reveals a violation of criminal law or otherwise appears to be of interest to the searched State."

- Reproduced in Article 32 CCC (without "notification") of Nov 2001

Case of Alexey Ivanov / Vasiliy Gorshkov (US / Russia)
(2000/2001)

https://www.justice.gov/archive/criminal/cybercrime/press-releases/2001/gorshkovconvict.htm

8

CCC (November 2001)

Article 32 CCC – Trans-border access to stored computer data with consent or where publicly available

A Party may, **without the authorisation of another Party:**

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, **if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system**.

(See Guidance Note on Article 32)

9

What solutions beyond Art. 32 CCC?

- T-CY Transborder Group (2012 – 2014)
  - ✓ Guidance Note Art. 32
  - ~~✓ Protocol on transborder access~~
- T-CY Cloud Evidence Group (2015 – 2017)
  - ✓ Guidance Note Art. 18
- Negotiation of the 2. Protocol (2017 – 2021)
- T-CY Working Group on undercover investigation and extension of searches (2022)

Snowden June 2013!

Options considered:

- transborder access with consent but without the limitation to date stored "in another Party"
- transborder access without consent but with lawfully obtained credentials;
- extending a search from the original computer to connected systems without the limitation "in its territory" (Art. 19)
- the power of disposal as connecting legal factor

(T-CY 2014: "Avoid "jungle" scenario and rogue assertion of jurisdiction")

10

Questions?

Transborder access / production / disclosure of data

- ► Options and measures within the framework of the CCC
  - CCC: Articles 18.1.b, 19, 32
  - Second Protocol: Articles 7 – 9

Article 18 – Production order and Guidance Note

Challenge: How to obtain subscriber information needed to identify a person (owner of an email/social media account, user of an Internet Protocol address)

13

Obtaining data / subscriber information from multi-national providers

► Practice of voluntary disclosure

Example

Meta: Direct government requests for data (Jul-Dec 2024)

County	Total	User accounts	Emergency disclosure	Response rate
All countries	322,062	600,341		78%
Switzerland	**574**	**793**	**94**	**70%**
France	16,341	19,017	9,410	84%
Germany	20,643	32,071	874	78%

(USG position: go directly to providers for subscriber information!)

14

Obtaining data / subscriber information from multi-national providers ► Practice of voluntary disclosure ► Issues

- Large number of government requests to major US providers
- Disclosure of subscriber or traffic data (ca. 65-80 %)
- Providers decide whether or not to respond to lawful requests and whether to notify customers
- Provider policies/practices volatile
- Data protection concerns
- No disclosure by European providers
- No admissibility of data received in some States

► Clearer / more stable framework required

Article 18.1.b CCC
(according to Guidance Note)

Partial solution (legal justification for ordering production of subscriber information)

(Article 7 Second Protocol: complete solution)

15

Article 18 – Production order

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer data storage medium; and

b. **a service provider offering its services in the territory of the Party to submit subscriber information** relating to such services in that service provider's possession or control.

……..

(See Guidance Note on Article 18 on the production of subscriber information)

16

2 Measures

The production of subscriber information under Article 18 Budapest Convention could be ordered if the following criteria are met in a specific criminal investigation and with regard to specified subscribers

IF

The criminal justice authority has jurisdiction over the offence;

AND IF

the service provider is in possession or control of the subscriber information;

AND IF

Article 18.1.a The person (service provider) is in the territory of the Party.	OR	Article 18.1.b A Party considers that a service provider is "offering its services in the territory of the Party" when, for example: – the service provider enables persons in the territory of the Party to subscribe to its services (and does not, for example, block access to such services); and – the service provider has established a real and substantial connection to a Party. Relevant factors include the extent to which a service provider orients its activities toward such subscribers (for example, by providing local advertising or advertising in the language of the territory of the Party), makes use of the subscriber information (or associated traffic data) in the course of its activities, interacts with subscribers in the Party, and may otherwise be considered established in the territory of a Party.

17

2 Measures

Article 19 – Search and seizure of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a. b. a computer system or part of it and computer data stored therein; and a computer-data storage medium in which computer data may be stored in its territory.

2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of **it in its territory**, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously **extend the search or similar accessing to the other system**.

(For implementation of Article 19, see T-CY Assessment Report)

18

Article 19.2 Extending a search in practice (According to T-CY Assessment Report)

Question: Could a search be extended to a computer system in another territory?

Affirmative requirement in domestic law that the connected system must be in the territory of the State executing the measure: Armenia, Bosnia and Herzegovina, Bulgaria, Costa Rica, Latvia, Paraguay, [USA].

However, many other States may extend the measure to access data from a computer in its territory to computer systems possibly located abroad. Different conditions may apply (e.g. unknown location or location concealed). For example:

- **France:** in case of a cloud - if the computer equipment allows a connection to a remote service, the investigators will in principle be able to access it. If data stored abroad, authorities use Article 32 of the Convention on Cybercrime.
- **Germany:** in cases of cloud computing when it cannot be determined where the data are located.
- **Switzerland:** if the access credentials are acquired lawfully and the conditions for a search are met, a remote access is generally possible if conducted from Switzerland.

19

Article 19.2 Extending a search in practice

Note:

The T-CY Cloud Evidence Group "looked into the long-arm doctrine of EU anti-trust law (Cases ICI 48/69; Woodpulp 89/85) and noted that the European Commission recommends that competition authorities within the European Union obtain access to servers anywhere in the world to gather evidence in anti-trust proceedings (CEG report of September 2016)

See: European Competition Network "RECOMMENDATION ON THE POWER TO COLLECT DIGITAL EVIDENCE, INCLUDING BY FORENSIC MEANS" :

"… To have effective powers to gather digital evidence, it is important that the Authorities can in the exercise of their inspection powers gather digital information which is accessible to the undertaking or person whose premises are being **inspected irrespective of where it is stored, including on servers or other storage media located outside the territory of the respective national competition authority or outside the European Union**."

20

Article 32 CCC – Trans-border access to stored computer data with consent or where publicly available

A Party may, **without the authorisation of another Party:**

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, **if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system**.

(See Guidance Note on Article 32)

21

Article 32 CCC – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically;
……..

Question regarding the use of Article 32.a:

- This provision may permit to validate for use as evidence, for example, domain name registration information obtained via publicly available WHOIS records.
- Could Article 32.a also give jurisdiction to obtain – and a legal justification to use as evidence - publicly available data related to blockchain data without a specific location (transaction records, wallet addresses, network metadata etc.)?

22

T-CY Guidance Note on Transborder Access to Data (Article 32)

Regarding Article 32b, typical situations may include:

"A suspected drug trafficker is lawfully arrested while his/her mailbox - possibly with evidence of a crime - is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another Party, police may access the data under Article 32b."

23

Guidance Note on Article 32

General considerations: Article 32b is a measure to be applied in specific criminal investigations and proceedings within the scope of Article 14.

On the notion of "access without the authorisation of another Party": Article 32b does not require mutual assistance, and the Budapest Convention does not require a notification of the other Party. At the same time, the Budapest Convention does not exclude notification. Parties may notify the other Party if they deem it appropriate.

On the applicable law: In all cases, law enforcement authorities must apply the same legal standards under Article 32b as they would domestically. If access or disclosure would not be permitted domestically it would also not be permitted under Article 32b.

24

Guidance Note on Article 32

On the person who can provide access or disclose data: Service providers are unlikely to be able to consent validly and voluntarily to disclosure of their users' data under Article 32.

Domestic lawful requests versus Article 32b: Article 32b is not relevant to domestic production orders or similar lawful requests internal to a Party.

On the location of the person consenting to provide access or disclose data: The standard hypothesis is that the person providing access is physically located in the territory of the requesting Party. However, multiple situations are possible.

= The possibilities under Article 32 are very limited.

Regarding service providers:

3.6 On the person who can provide access or disclose data

As to "who" is the person who is "lawfully authorised" to disclose the data, this may vary depending on the circumstances, laws and regulations applicable.

For example, it may be a physical individual person, providing access to his email account or other data that he stored abroad.

It may also be a legal person.

Service providers are unlikely to be able to consent validly and voluntarily to disclosure of their users's data under Article 32. Normally, service providers will only be holders of such data; they will not control or own the data, and they will, therefore, not be in a position validly to consent.

Q: If a VASP is not considered a service provider but is in possession or control of subscriber information, could Art. 32b be used to request submission of subscriber info?

25

Observation on direct access to stored data on computer systems abroad via Articles 32 and 19.2 CCC:

- While the scope of Article 32.b CCC is limited, many States (ie most Parties to the CCC) are able to extend a search from a computer system in their own territory to a computer system abroad under varying conditions (loss of location, lawfully acquired access credentials etc.)
  - ► De facto: Article 19.2 CCC without the limitation of "in its territory".
- Since solutions via protocols to the CCC have not been feasible to date, this remains precarious under international law.

NB:
Article 39 – Effects of the Convention
- 3. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.
- Explanatory report (para 293): "other situations are neither authorised, nor precluded."

26

2. Measures: Second Protocol

Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence

Opened for signature in May 2022

By November 2025:

- 52 signatures of which 2 ratifications (Japan and Serbia)
- Switzerland has not yet signed it

For EU member States: link to "E-evidence Regulation"

5 ratifications needed for entry into force

27

2. Measures: Second Protocol

Negotiating the Second Protocol (2017 – 2021) ► Specific issues:

► How to obtain subscriber information efficiently?

► How to cooperate directly with a service provider in another Party?

► How to obtain WHOIS data (domain name registration information) from registrars?

► How to obtain stored data, including content, in an emergency situation?

► How to make mutual assistance more effective?

► Solutions for transborder access beyond Article 32?

► How to reconcile efficient and effective measures with rule of law and data protection requirements?

28

2. Measures: Second Protocol

29

2. Measures: Second Protocol

Efficiency with safeguards

- Article 2 – scope of Protocol: specific criminal investigations or proceedings related to cybercrime and e-evidence
- Article 13 incorporates Article 15 of the Convention to ensure the adequate protection of human rights and liberties and that provides for the principle of proportionality
- **Article 14 provides for detailed data protection safeguards that are unique for a criminal justice treaty**
- Articles specify types of data to be disclosed
- Articles specify information to be included to permit application of domestic safeguards
- Reservations and declarations to permit domestic safeguards and limit information to be provided

Article 14 – Protection of personal data

1. Scope
2. Purpose and use
3. Quality and integrity
4. Sensitive data
5. Retention periods
6. Automated decisions
7. Data security and security incidents
8. Maintaining records
9. Onward sharing within a Party
10. Onward transfer to another State or international organisation
11. Transparency and notice
12. Access and rectification
13. Judicial and non-judicial remedies
14. Oversight
15. Consultation and suspension

30

Tools of the Second Protocol:

Chapter II: Measures for enhanced cooperation

Article 6	Request for domain name registration information ►**Public2Private**
Article 7	Disclosure of subscriber information ►**Public2Private**
Article 8	Giving effect to orders from another party for expedited production of subscriber information and traffic data ►Public2Public
Article 9	Expedited disclosure of stored computer data in an emergency ►Public2Public (via 24/7 network)
Article 10	Emergency mutual assistance ►Public2Public
Article 11	Video conferencing ►Public2Public
Article 12	Joint investigation teams and joint investigations ►Public2Public

31

Article 7 – Disclosure of subscriber information

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities **to issue an order to be submitted directly to a service provider in the territory of another Party**, in order to obtain the disclosure of specified, stored subscriber information in that service provider's possession or control, where the subscriber information is needed for the issuing Party's specific criminal investigations or proceedings.

2. a. Each Party shall adopt such legislative and other measures as may be **necessary for a service provider in its territory to disclose subscriber information** in response to an order under paragraph 1.

…..

Features:

- Optional notification regime
- Reservations
- Declarations
- Enforcement via Article 8

32

Article 8 – Giving effect to orders from another Party for expedited production of subscriber information and traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted as part of a request to another Party for the purpose of compelling a service provider in the requested Party's territory to produce specified and stored

a) subscriber information, and
b) traffic data

in that service provider's possession or control which is needed for the Party's specific criminal investigations or proceedings

2. Each Party shall adopt such legislative and other measures as may be necessary to give effect to an order under paragraph 1 submitted by a requesting Party.

Aim:
expeditious production of subscriber information and traffic data to another Party

Purpose:
- complementary to mutual legal assistance mechanisms
- more streamlined and efficient, due to less data required and an easier process of formulating the order to a foreign service provider

Scope:
- production of stored **subscriber information** or **traffic data**
- specific enforcement mechanism for **orders issued under Article 7**

33

Article 9 – Expedited disclosure of stored computer data in an emergency

1 a. Each Party shall adopt such legislative and other measures as may be necessary, in an emergency, **for its point of contact for the 24/7 Network** referenced in Article 35 of the Convention ("point of contact") to transmit a request to and receive a request from a point of contact in another Party **seeking immediate assistance in obtaining from a service provider** in the territory of that Party the expedited disclosure of specified, stored computer data in that service provider's possession or control, without a request for mutual assistance.

2 Each Party shall adopt such legislative and other measures as may be necessary to enable, pursuant to paragraph 1:

a) its authorities **to seek data from a service provider** in its territory following a request under paragraph 1;
b) a service provider in its territory to disclose the requested data to its authorities in response to a request under paragraph 2.a; and
c) its authorities **to provide the requested data** to the requesting Party.

Aim:

- Expedited disclosure of stored computer data in emergency situations (Def. see Art. 3.2c 2AP)

Means:

- Relies on 24/7 Network of point of contacts (Art. 35 BC) for transmission and receiving requests

34

2. Measures: Second Protocol

Second Protocol:

- Proposals for provisions that did not find consensus:
  - Undercover investigations
  - Extension of searches

35

3. Summary/conclusion

Summary: Toolbox to obtain electronic evidence from other Parties without MLA under the framework of the Convention on Cybercrime

- **Article 18.1.b** CCC: Legal justification for requests for subscriber information to service providers offering a service in your territory [difficult to enforce but see Yahoo/Belgium; does not cover disclosure of content in an emergency]
- **Article 19.2** CCC: Extending a search from a computer system in your territory to a connected system in your territory [In practice: authorities of most States are able to extend a search beyond their territory under varying conditions]
- **Article 32.a** CCC: Access for use as evidence of publicly available data from anywhere [possibly also useful for public blockchain-related evidence]
- **Article 32.b** CCC: Limited scope according to T-CY Guidance Note (can a service provider voluntarily consent?) but frequently used by some State ("other situations are neither authorised, nor precluded").

- The **Second Protocol** provides additional tools and resolves some issues:
  - **Article 7**: Solid framework with safeguards for orders for subscriber information directly to service providers
  - **Article 8**: More efficient tool to obtain traffic data (and enforcement mechanism for Article 7)
  - **Article 9**: Flexible tool to obtain the disclosure of content in an emergency via 24/7 network
  - **Article 10**: Tool for expeditious MLA

36

4. Epilogue: What to expect from the UN Hanoi Convention

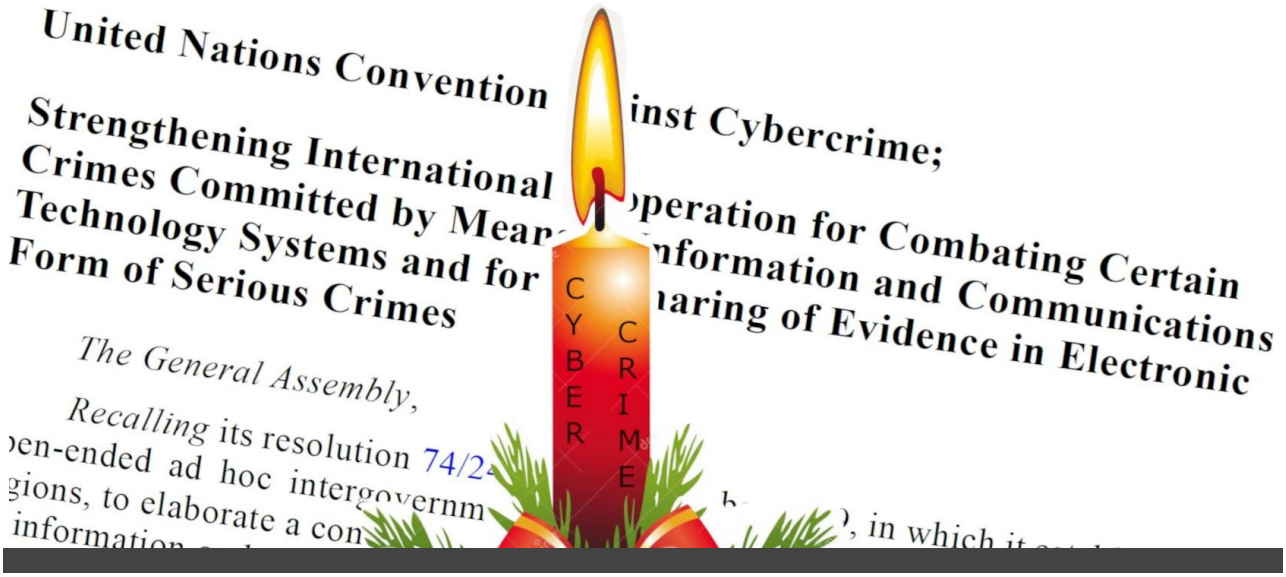
The framework of the Convention on Cybercrime (Budapest Convention)

?

Hanoi Convention
"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"

37

4. Epilogue: What to expect from the UN Hanoi Convention



38

4. Epilogue: What to expect from the UN Hanoi Convention

"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"

- Adopted by UNGA: 24 Dec 2024
- Opened for signature: Hanoi, Vietnam, October 2025

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

39

4. Epilogue: What to expect from the UN Hanoi Convention

Core concepts and measures of the Hanoi Convention:

- are drawn from the Convention on Cybercrime (2001)
- complemented by provisions adapted from the UN Conventions on Transnational Organised Crime (UNTOC, 2000) and Corruption (UNCAC, 2003)

► confirms the timeless quality and relevance of the Convention on Cybercrime

Examples:

Art.	Convention on Cybercrime	Art.	UN treaty
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

40

New in Hanoi Convention:

- 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 Hanoi Convention:

- Article 10 CCC on IPR
- **Article 32 CCC on transborder access to data**

None of the provisions of the Convention on Cybercrime's:

- First Protocol on Xenophobia and Racism (2003)
- **Second Protocol** on enhanced cooperation and disclosure of electronic evidence (2022), e.g.:
  - Direct cooperation with service providers and registrars in other Parties (articles 6 and 7)
  - Expedited cooperation in emergency situations (articles 9 and 10)

41

Budapest Convention v Hanoi Convention: Synergies?

- Both treaties seem largely consistent or complementary. No obvious contradictions.
- UN treaty offers a framework for cooperation primarily between and with States not able to join the Convention on Cybercrime.
- Adherence to human rights and rule of law requirements essential to create the necessary trust for cooperation.
- The Budapest Convention with its Protocols, T-CY and capacity building (C-PROC) will remain the more relevant framework for practitioners in the future.
- Synergies and cooperation between the United Nations and the Council of Europe may take the form of joint, coordinated or complementary capacity building activities by the UN Office on Drugs and Crime (UNODC) and the Council of Europe's Cybercrime Programme Office (C-PROC).

42

Q & A

Alex.cyber@protonmail.com

43