

International cooperation on cybercrime and electronic evidence: New tools, old debates?

Alexander Seger, Head of Cybercrime Division, Council of Europe

Cyber Crime Conference, Roma, 11-12 maggio 2023

1

Intro/purpose

► Update on UN treaty process

(UN “Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes”)

- Risks v. chances of success
- Impact on Budapest Convention on Cybercrime
- Potential benefits

► Déjà-vu / old debates

- UN Convention on Transnational Organised Crime (UNTOC 2000)
- UN Convention on Corruption (UNCAC 2003)
- Budapest Convention on Cybercrime (2001)

► New tools:

- Second Additional Protocol to the Budapest Convention on enhanced cooperation and disclosure of electronic evidence (May, 2022)

2

2

Buda Convention and Second Protocol: tools

Budapest Convention (2001):

1. Offences (articles 2-12)
 - CIA offences (illegal access, data/system interference etc.), forgery and fraud, "child pornography", IPR
2. Procedural powers to investigate cybercrime and collect e-evidence in relation to **any** offence (articles 14-21)
 - Expedited preservation, production orders, search and seizure, interception, safeguards
3. International cooperation on cybercrime and e-evidence
 - General provisions, expedited preservation, MLA, 24/7 network

Second Protocol on enhanced cooperation and disclosure of e-evidence (2022):

- Scope: criminal investigations and proceedings related to computer systems and data and collection of e-evidence re **any** criminal offence
- Direct cooperation with service providers and registrars in other Parties
- Giving effect to production orders from other Parties
- Expedited cooperation in emergencies
- Video conferencing
- Joint investigation teams and joint investigations
- Data protection and other safeguards

3

3

Buda Convention and Second Protocol: reach

Budapest Convention (2001):

By April 2023:

- ▶ Parties: 68 (European, Argentina, Australia, Canada, Chile, Costa Rica, Ghana, Japan, Mauritius, Nigeria, Senegal, Sri Lanka, Tonga, USA etc.)
- ▶ Signatories: 2 (Ireland, South Africa)
- ▶ Invited to accede: 18 (Cameroon, Fiji, Kazakhstan, New Zealand, Uruguay, Vanuatu etc.)
- ▶ 130+ States have legislation aligned with BC

Second Protocol on enhanced cooperation and disclosure of e-evidence (2022):

By April 2023:

- ▶ Signed: 36 States (European (incl. Italy), Argentina, Japan, Sri Lanka, USA etc.)
- ▶ Ratified: 1 (Serbia)

(5 ratifications needed for entry into force)

4

4

UN treaty process: (troubled) history

- ▶ 1990: UN Crime Congress (Cuba): no agreement to develop a treaty; capacity building instead
- ▶ 2005: UN Crime Congress (Bangkok): no agreement to develop a treaty; capacity building instead
- ▶ 2010: UN Crime Congress (Salvador, Brazil): no agreement to develop a treaty. Intergovernmental Expert Group (UNIEG) to study the matter instead
- ▶ 2011 – 2021 UNIEG: no agreement to develop a treaty but broad agreement on capacity building
- ▶ 2019: UN General Assembly Resolution 74/247 proposed by Russia: Established AHC by contested vote (79 yes / 60 no / 54 abst)
- ▶ 2021: Modalities agreed: consensus or 2/3 majority required
- ▶ First session of AHC: 28 February 2022

Concerns:

- Greater international polarization, divisions
- Greater digital divide
- Control of information/society instead of crime
- Broad scope of criminalization with risks to freedom of expression and other rights
- Procedural powers without safeguards with risks to privacy and other rights
- Re-design architecture of Internet governance: sovereign internets under control of states vs. free, open and global Internet with multi-stakeholder governance

5

5

UN treaty process: motivation of Russia

Russia and cybercrime:

- ▶ Major source of cybercrime, disinformation and other cyberoperations for 20+ years
- ▶ Limited intentions to cooperate
- ▶ Operating like a criminal organization: State and non-state actors under the same “roof”
- ▶ FSB/GRU/SVR [and other State institutions]:
 - Commit cybercrime, carry out cyber operations
 - Recruit/employ criminals
 - Outsource activities to cybercriminal organisations
 - Tolerate/give protection to cybercriminal organisations acting in the interest of the regime

Why would Russia promote an international treaty?

- Origin in “Doctrine of Information Security” (2000/2016)
 - Spin off: “Fundamentals of the State Policy ... on international information security” (2013): Create a system of international information security.
 - ▶ Promote UN treaty on combating information crime
- UN treaty: part of effort to re-design architecture of Internet governance
- International treaty to legitimize domestic control (“successful” domestic information control already)

6

6

UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

1st Meeting ✓	New York, 28 Feb – 11 March 2022	Objectives, scope and structure of the convention and the mode of work of the AHC
2nd Meeting ✓	Vienna, 30 May – 10 June 2022	First reading of the provisions on criminalization, the general provisions and the provisions on procedural measures and law enforcement
3rd Meeting ✓	New York, 29 Aug – 9 Sep 2022	First reading of the provisions on international cooperation, technical assistance, preventive measures and the mechanism of implementation, the final provisions and the preamble
4th Meeting ✓	Vienna, 9 – 20 Jan 2023	Second reading of the preamble, the general provisions and the provisions on criminalization and procedural measures and law enforcement
5th Meeting ✓	Vienna, 11 – 21 Apr 2023	Second reading of the provisions on international cooperation, preventive measures, technical assistance and the mechanism of implementation, and the final provisions
6th Meeting	New York, 21 Aug – 1 Sep 2023	Third reading of the draft text of the convention
Concluding session	New York, 29 Jan – 9 Feb 2024	Finalization and approval of the draft text of the convention; discussion and approval of a draft resolution to which the text of the draft convention will be annexed, for consideration and adoption by the General Assembly at its seventy-eighth session, in 2024

7

7

UN AHC: Current proposals

Structure of the future treaty

Preamble

1. General provisions
2. Criminalization
3. Procedural measures and law enforcement
4. International cooperation
5. Technical assistance, including exchange of experience
6. Preventive measures
7. Mechanism of implementation
8. Final provisions

Types of provisions

... likely to find consensus:

- ▶ General provisions aligned with UNTOC and UNCAC
- ▶ Specific provisions aligned with Budapest Convention
- ▶ [Basic safeguards]

... unlikely to find consensus:

- ▶ Any content-related offence other than child sexual abuse materials (CSAM)
- ▶ Provisions on direct and expedited means of cooperation (of Second Protocol to BC)
- ▶ Strong safeguards (data protection)

8

8

Conclusions

Re current treaty process:

- Engagement in UN process needed
- Process so far confirms validity of provisions of Budapest Convention
- New tools of Second Protocol to BC not feasible in UN treaty
- UN treaty process triggers much interest in BC (numerous requests for accession)

Re is a UN treaty feasible?

- ▶ Treaty combining provisions of UNTOC + UNCAC + Buda Convention may be feasible
 - = Useful framework for cooperation
- ▶ February 2024 timeline not realistic but perhaps some time in 2024/25, if difficult decisions are made. Voting (2/3)?

Not excluded that:

- ▶ Process may drag on for years
- ▶ Some States may hinder the process if they cannot get their way

Re UN treaty vs Budapest Convention:

- ▶ BC in place and functioning
- ▶ Agreeable UN treaty likely to serve as bridge to BC
- ▶ As process drags on: More countries seek to join BC + Protocols

9

Alexander Seger

Alexander.seger@coe.int

www.coe.int/cybercrime

10