

Item 10: Update on the United Nations treaty process



Background:

- UNGA initiative by Russia ► Dec 2019: UNGA Resolution 74/247 ► Decision to establish an Ad Hoc Committee (AHC) to elaborate “a comprehensive international convention on countering the use of information and communications technologies for criminal purposes”.
- Feb 2022 – Aug 2024: 8 formal sessions and numerous informal and intersessional meetings of the AHC
- 8 Aug 2024: Agreement by AHC on the draft text of a UN treaty and a draft resolution
- 11 Nov 2024: Agreement by UNGA 3rd Committee
- Adoption by UNGA expected by December 2024
- Opening for signature in Vietnam in 2025 [tbc]

Result:

Draft “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”

AHC agreement on draft UN treaty:

- Major political success considering history and current international context.
- A narrow criminal justice treaty.
- Largely consistent with BC.
- Draft UN treaty is broader in some (crime proceeds) and narrower in other (scope of international cooperation) respects than BC.
- With minimum safeguards necessary for international cooperation.
- Maximum achievable and agreeable result.
- Will benefit cooperation between and with States that are not Parties to the BC.
- Will take some years until it be in force and operational.
- Protocol negotiations to commence two years after adoption by UNGA

Core concepts and measures of the draft treaty

- are 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)
- ▶ **confirms the timeless quality and relevance of the BC**

Example:

Art.	Budapest Convention		Draft 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

New in draft 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 draft UN treaty:

None of the measures of the Second Protocol to the BC on enhanced cooperation and disclosure of electronic evidence (2022):

- ▶ Article 6 on “Requests for domain name registration information” directly to a registrar or a similar entity in another Party.
- ▶ Article 7 on orders for the “Disclosure of subscriber information” directly to a service provider in another entity.
- ▶ Article 8 on “Giving effect to orders from another Party for the expedited production of subscriber information and traffic data”.
- ▶ Article 9 on “Expedited disclosure of stored computer data in an emergency”.
- ▶ Article 10 on “Emergency mutual assistance”.

Safeguards beyond UNTOC and UNCAC:

- Article 6 on “respect for human rights” with its important paragraph 2;
- 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;
- Article 40.22 on non-discrimination within the context of mutual legal assistance.

Risks/concerns:

- Risk that some States will not respect human rights and rule of law conditions*. Conference of States Parties (COSP) unlikely to review compliance.
- Risk of targeting assets of individuals, private sector organisations, media or civil society organisations through combination of provisions on fraud, money laundering, corporate liability, participation and attempt, and crime proceeds.
- Risk of supplementary criminalisation through a protocol (negotiations to commence two years after adoption of the convention as per draft UNGA resolution).
- ▶ Concerns raised by governments, civil society and industry stakeholders during the AHC process remain valid.
- ▶ Governments to decide on signature and ratification.

*See results of voting and disagreement expressed by some States during AHC

Implications for the Convention on Cybercrime (Budapest Convention):

- BC with its Protocols will remain the more relevant framework in the foreseeable future.
- Synergies between both treaties feasible (▶ including capacity building with a focus on safeguards)
- More States may seek accession to the BC (based on experience during AHC process) because:
 - the political obstacle of BC being considered as preventing a UN treaty has been removed;
 - countries learned much about the BC during the AHC process;
 - the provisions of the BC form the backbone also of the draft UN treaty,
 - the advanced tools of the Second Protocol on electronic evidence are only available to Parties to the BC;
 - Governments need to act on cybercrime now and may not want await more years before the UN treaty becomes operational.
- A clear commitment to meeting human rights and rule of law conditions will be necessary when governments are seeking accession to the Budapest Convention on Cybercrime.