Published in Journal of Cyber Policy [1]
6 October 2025
Contact: alex.cyber@protonmail.com

The 'Hanoi Convention' against cybercrime: managing risks

Alexander Seger, 6 October 2025

Abstract:

In October 2025, the new United Nations convention against cybercrime will be opened for signature in Hanoi, Vietnam. This is a major political achievement given that for more than 30 years agreement on such a treaty was not feasible at the level of the United Nations. The primary reason for this delay had been the perception by most democratic countries that such a United Nations treaty would entail major risks to human rights, the rule of law and a free and open internet. The question now is whether such risks have been sufficiently addressed in the final text of the new 'Hanoi Convention' and how remaining risks could be managed in the future.

On 24 December 2024, the United Nations General Assembly (UNGA) formally adopted a new international treaty on cybercrime which is to be opened for signature in Hanoi, Vietnam in October 2025. The official title is rather bulky: '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'. The 'UNCAC' acronym is already taken by the UN Convention against Corruption and thus the new treaty will probably be known as the 'Hanoi Convention'.

Agreement on the text of this treaty is a major political achievement, given the current fractured international context, and an indication that multilateralism still has a chance.

It has taken more than three decades to come to this point. The first reflections on a UN treaty on 'computer crime' date back to 1990. But while the Council of Europe moved ahead with soft-law instruments in the 1990s and then with the 'Budapest Convention' on Cybercrime in 2001, agreement on a UN treaty was not feasible until 2024.

The primary reason was the perception by most democratic states that the risks caused by such a treaty on this topic at the level of the United Nations would outweigh the benefits. The question now is whether such risks have been sufficiently addressed in the final text of the Hanoi Convention and how remaining risks could be managed in the future.

---

[1] To cite this article: Alexander Seger (06 Oct 2025): The 'Hanoi Convention' against cybercrime: managing risks, Journal of Cyber Policy, DOI: 10.1080/23738871.2025.2567922 To link to this article: https://doi.org/10.1080/23738871.2025.2567922

This question is relevant given that states currently not only make decisions on whether to sign the Hanoi Convention but are now also engaging in the preparation of the rules of procedure of the future Conference of States Parties (COSP), and from 2027 onwards will, in principle, be negotiating an additional protocol to the Hanoi Convention.

Risks preventing agreement in the past

Early proposals to prepare a UN treaty on computer crime were discussed at the UN Crime Congress in Cuba in 1990 but failed to gain traction. The same was true when the issue came up at the UN Crime Congress in Bangkok, Thailand in 2005. By that time, the Budapest Convention was in place and had entered into force. At the UN Crime Congress from 12 to 19 April 2010 in Salvador de Bahia (Brazil), Brazil, Russia and South Africa pushed for a decision to launch treaty negotiations, but again there was no consensus.[2]

The UN Intergovernmental Expert Group on Cybercrime that was established as a compromise further to the 'Salvador Declaration' and that met seven times between 2011 and 2021, again reached no agreement on the need and feasibility of a UN treaty on cybercrime. Neither did it achieve its task of preparing an agreed version of a 'comprehensive study on the problem of cybercrime and responses to it'.

This is why Russia decided to take the question directly to UNGA, where in December 2019 a relative majority of UN member states voted in favour of Resolution A/RES/74/247 that established the treaty process in the form of an 'Ad Hoc Committee' (AHC) tasked to negotiate the draft text of a convention.[3]

Those opposing a UN Convention, not only in December 2019 but in recent decades, were concerned that such a treaty risked:

- leading to greater international polarization, including that Russia, China and others would use a new treaty to create their own 'club' of countries opposing those adhering to the Budapest Convention;
- exacerbating fragmentation and the digital divide in which 'developed' countries are making use of the more advanced framework of the Budapest Convention while countries of the Global South would have to rely on a 'weaker' UN treaty;
- being aimed at the control of information instead of at crime online;
- comprising a wide range of offences with risks to the freedom of expression and other rights;
- comprising intrusive powers without safeguards, causing risks to privacy and other rights; and
- feeding into attempts to redesign the architecture of internet governance by replacing the multi-stakeholder model of a free, open and global internet with an internet or internets under the control of states.

The fact that Resolution 74/247 had been introduced by Russia 'also on behalf of Belarus, Cambodia, China, the Democratic People's Republic of Korea, Myanmar, Nicaragua and Venezuela (Bolivarian Republic of)', and that it was adopted via a

[2] Note: The 2nd BRIC Summit took place in Brazil in the same week, and later that year, South Africa joined what then became the 'BRICS' group of countries.
[3] Because of the COVID pandemic, treaty negotiations only started in February 2022.

contested vote by a relative majority (79 states in favour, 60 against, 33 abstentions), did nothing to alleviate these concerns.

Risks addressed in the Hanoi Convention

Following the adoption of Resolution 74/247, the 'like-minded countries' that had opposed it – most of them parties to the Budapest Convention – decided to engage in the UN treaty process, also in the spirit of multilateralism, with the following objectives:

- to ensure consistency of the future treaty with the Budapest Convention on Cybercrime;
- to ensure the inclusion of human rights and rule of law safeguards, and to avoid overbroad criminalization; and
- to prevent Russia and its allies from controlling the process.

These objectives were to help mitigate the above risks, and they were largely achieved:

- The Hanoi Convention is broadly consistent with the Budapest Convention on Cybercrime.[4] The backbone of the Hanoi Convention – that is, the list of offences, the procedural powers to investigate and collect electronic evidence, and the international cooperation provisions that are specific to cybercrime and electronic evidence – has been more or less copied from the Budapest Convention. A new and important addition in the UN treaty is the non-consensual dissemination of intimate images (NCDII). Some of the definitions (Article 2, Use of terms) appear different but they are not (for example, in order to satisfy Russia, what is a 'computer system' in the Budapest Convention is called an 'information and communication technology system' in the Hanoi Convention, but while this choice of terminology is likely to cause confusion, the underlying text is identical). Overall, there seem to be no major contradictions between both treaties. Given this consistency, those 130 or more states that have adopted domestic legislation based on the Budapest Convention will not have to modify their existing laws.

- At the same time, the more advanced tools of the Second Protocol to the Budapest Convention on 'enhanced cooperation and disclosure of electronic evidence', including its provisions on direct cooperation with service providers or the disclosure of content in emergency situations, have not been incorporated into the Hanoi Convention. The reason is that the level of safeguards needed would not have been achievable at the UN level. This will render the effectiveness of the Hanoi Convention more limited in practice. For example, subscriber information held by service providers in other jurisdictions is what criminal justice authorities need most often in their investigations. While the Second Protocol to the Budapest Convention provides for the competent authorities of one state to order a service provider in another state directly – and subject to conditions and safeguards – to produce such subscriber information, this tool is not available in the Hanoi Convention. However, the omission of this and other provisions does not create conflicts between both treaties.

[4] See https://rm.coe.int/conventions-on-cybercrime-the-budapest-convention-and-the-draft-un-tre/1680b1631a
For a comparative table see https://rm.coe.int/un-ahc-treaty-compare-table-v2-aug-2024-/1680b159ea

- The Hanoi Convention comprises important human rights and rule of law safeguards. Key provisions in this respect are Article 6 (Respect for human rights), Article 24 (Conditions and safeguards), Article 36 (Protection of personal data) and Article 40, paragraph 22 (on non-discrimination within the context of mutual assistance). Article 14 on child sexual abuse material and Article 16 on NCDII strike a careful balance so that states are not obliged to criminalize children for legitimate sexual conduct. Insertion of these safeguards was possible because of the insistence by a coalition of democratic countries (comprising most parties to the Budapest Convention) and because of the pressure exercised by civil society and industry stakeholders participating in the process.

- The list of offences in the Hanoi Convention (articles 6 to 17) remains fairly limited (so far). It consists of those of the Budapest Convention minus offences related to intellectual property rights but plus the grooming of children, NCDII, fraud in general and money-laundering. Prior to and during the UN treaty process, Russia insisted on a range of other offences. For example, in December 2023, a few weeks before what was supposed to be the concluding session in January 2024, they submitted a list of 19 additional offences to be included ('incitement to subversive or armed activities', 'extremism-related offences', etc.). While these were not taken into account, the following compromise was agreed upon: the UNGA resolution of 24 December 2024 adopting the Hanoi Convention also comprises the decision to launch negotiation of 'a draft protocol supplementary to the Convention, addressing, *inter alia*, additional criminal offences as appropriate' two years after the adoption of the Convention.

- While the treaty process was launched because of Russia, and while Russian representatives kept underlining that the process was their 'baby', Russia did not control the process. On the contrary, the text resulting from it was agreed upon in spite of Russia. The Hanoi Convention is certainly not the treaty that it wanted. It was not only negotiated in 'the world of the Budapest Convention' (as one senior representative of the UN phrased it) but also confirmed the continued relevance of the Budapest Convention which Russia had opposed and criticized as 'outdated' for years. The UN treaty process was a major advertisement for the Budapest Convention and led to a steep increase in accessions and requests for accession to it between 2022 and 2024.

- The risk of a digital divide between 'developed' countries applying the framework of the Budapest Convention and countries of the Global South relying on a 'weaker' UN treaty has become less pertinent in recent years. By September 2025, the number of parties to the Budapest Convention had increased to 81 states of which 30 were from Africa, Asia-Pacific, Latin America and the Caribbean. And another 15 countries from these regions had signed it (South Africa) or been invited to accede. For some states, experience gained with the implementation of the Hanoi Convention may facilitate subsequent accession to the framework of the Budapest Convention.

Risks remaining

While the outcome of the treaty process is satisfactory and while it will provide a framework for cooperation by and with states that are not part of the Budapest Convention, risks remain:

- Non-compliance by some states with the provisions on conditions and safeguards of the Hanoi Convention is the main concern. The final draft text of the treaty, as formally adopted by UNGA on 24 December 2024, had been agreed upon by the AHC during the 'Reconvened concluding session' held from 29 July to 9 August 2024 in New York. Towards the end of that session, on 8 August, Iran requested voting on proposals to delete safeguards contained in seven articles of the draft text. A large majority of the states participating in the AHC rejected these proposals in seven rounds of voting. The draft text was then agreed by the AHC without a vote 'by consensus'. Subsequent oral and written statements and 'explanations of vote and position' during that AHC session suggested that some states will disregard the conditions and safeguards of the new convention and that they would not permit any external oversight over their domestic application of the convention.

- In some states – Russia, for example – seizing assets is a primary means to target political opponents, media, civil society organizations or businesses and to restrict fundamental rights. During the negotiations, Russian representatives repeatedly referred to the activities of multinational service providers as a form of 'neo-colonialism'. Provisions of the Hanoi Convention on money-laundering and asset forfeiture in combination with articles on fraud, the liability of legal persons, participation and attempt, jurisdiction and other things may permit abusive criminalization, investigations or the seizure of assets. For example, the combination of broad jurisdiction (Article 22 and Article 17.2.c) with low thresholds for liability of legal persons (Article 18) or low threshold and intent standards for participation and attempt (Article 19) could elevate non-criminal and unintentional conduct by service providers to a predicate offence and lead to the freezing of assets. Or for political reasons, individuals and organizations may be targeted for fraud (Article 13.c) and their assets may then be confiscated domestically or via international cooperation.

- Other concerns raised by stakeholders during the treaty process, to some extent, also remain valid.

Implementation of the Hanoi Convention: monitoring risks

The question is how such risks can be monitored and addressed once states begin their implementation of the Hanoi Convention.

According to Article 57 of this treaty, a Conference of the States Parties (COSP) will be established to promote and review its implementation. In theory, the COSP could provide an accountability mechanism for compliance with the convention including its safeguards, for cooperation or non-cooperation on cybercrime in general or even for 'state-sponsored cybercrime'.

The preparation of the rules of procedure for the COSP has commenced. The objective is to have the draft rules finalized by a meeting of the AHC from 26 to 30 January 2026 in Vienna as per UNGA Resolution A/79/243. Once the Hanoi Convention enters into force – that is, after 40 ratifications – the first meeting of the COSP would then adopt these rules.

It remains to be seen to what extent the COSP will be able to review compliance by parties with the convention, including its safeguards, and monitor possible abuses.

The effectiveness of the COSP as a review body will also depend on the role that stakeholders will be able to play. Article 57 of the convention reads, for example, that 'inputs received [by the conference] from representatives of relevant non-governmental organizations, civil society organizations, academic institutions and private sector entities, duly accredited in accordance with procedures to be decided upon by the conference, may also be considered'. The details of such stakeholder participation will need to be defined in the rules of procedure.

A good number of initial submissions by states regarding the rules of procedure already underline that the COSP should 'enable the inclusive, transparent, and open participation of civil society, the private sector, and other stakeholders'.

However, it is very possible that the future COSP will be a rather formalistic governance mechanism that is subject to political considerations and that meets once every two or three years. Stakeholders may sit in on plenary sessions while actual deliberations are conducted in so-called 'informals' by governments only. A detailed review of compliance and a calling out of violations is difficult to achieve in such a setting.

Creative thinking is needed. The experience of stakeholder participation during the treaty process from February 2022 to August 2024 may serve as a starting point: the coherence of positions developed by stakeholders and the persistence with which they were presented throughout the process was remarkable.

The question, therefore: Is it conceivable to translate this experience into some sort of stable mechanism by which stakeholders independently and continuously follow the implementation of the convention, receive, analyse and call out reports of abuses, and then feed their findings into the COSP?
