MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

The UN Cybercrime Convention: Key Features and Global Stances

Rohit Kumar Sharma

January 20, 2025

Summary

The participation of multiple stakeholders in the adoption of the UN Convention against Cybercrime highlights the effectiveness of inclusive decision-making involving not just states but also civil society organisations. Despite mixed reactions, the convention offers a timely legal framework for information sharing and improved coordination among law enforcement agencies globally.

While 2024 saw a marked rise in ransomware incidents,[1] financial fraud[2] and the proliferation of 'cyber scam compounds',[3] the year also ended with a breakthrough as the global community reached a consensus on a comprehensive legal instrument to address cybercrime. On 24 December 2024, the United Nations General Assembly (UNGA) adopted the UN Convention against Cybercrime, the first global legally binding instrument addressing cybercrime.[4]

The development marks a significant milestone, as the document reflects the values of multiple stakeholders, encompassing civil society, academic institutions and the private sector. It also provides states with a cooperative mechanism to address the growing challenge of transnational cybercrime activities collectively. The convention, set to open for signature in Hanoi in 2025, will not override any "existing international instruments and efforts at national, regional, and international levels".[5] Instead, it aims to complement and strengthen these initiatives.

The convention seeks to criminalise acts as detailed in Articles 7 to 21 of the document. The broad range of offences attracting criminal liability includes illegal access, unlawful interception, interference with electronic data and the misuse of devices. Malicious intent is a crucial element in invoking criminal liability for these acts. The term 'device' encompasses programs specifically designed to commit offences outlined in the convention.[6] Acts such as obtaining, producing, selling, procuring for use, or distributing such programs are also criminalised.[7] This provision could be interpreted as targeting ransomware-as-a-service (RaaS) operations, where affiliates purchase malware or similar programs to conduct their attacks.

Background

As the adoption of information and communications technologies (ICT) became widespread, threat actors evolved new methods to target victims. Realising the increasing threats and potential risks associated with emerging technologies, the UNGA, in 2019, decided to establish an Ad Hoc committee of experts, with

[1] Tom Spring, **"Ransomware 2024: A Year of Tricks, Traps, Wins and Losses"**, *SC Media*, 31 December 2024.

[2] Anubhav Mukherjee, **"Bank Fraud Cases Rise 27% YoY in 2024; Scams Worth ₹21,367 Crore Logged in H1FY25: RBI Data"**, *Livemint,* 26 December 2024.

[3] **"Billion-dollar Cyberfraud Industry Expands in Southeast Asia as Criminals Adopt New Technologies"**, United Nations Office on Drugs and Crime (UNODC), 7 October 2024.

[4] **"United Nations: Member States Finalize a New Cybercrime Convention"**, UNODC, 9 August 2024.

[5] **"United Nations Convention Against Cybercrime"**, UN Doc. A/79/460, United Nations, 27 November 2024.

[6] Article 11 (1) (a) (i), **"United Nations Convention Against Cybercrime"**, United Nations, 27 November 2024.

[7] Ibid.

representation from all regions, to draft a comprehensive convention to combat the use of ICT for criminal purposes.[8] In 2021, the UNGA adopted a resolution setting a timeline for the committee to complete its work and submit a draft convention to the assembly during its seventy-eighth session.[9] This led to the onset of deliberative sessions that shaped the contours of the UN Convention against Cybercrime.

Salient Features

The convention aims to promote and enhance preventive measures, foster international cooperation, and facilitate technical assistance and capacity-building support to prevent and combat cybercrime.[10] Recognising the shared nature of cyberspace, the convention places particular emphasis on promoting technical assistance and capacity-building initiatives to benefit the developing world. It is pertinent to examine the convention in light of its broader goals, with a particular focus on key areas it seeks to address: issues relating to cooperation, capacity building, prevention, victim support and child protection.

International Cooperation

The convention outlines general principles of cooperation and identifies key areas for collaboration in investigations, prosecution and judicial proceedings.[11] This includes a range of law enforcement activities, including the freezing, seizing, confiscating and returning proceeds of crimes, as well as actions related to collecting and sharing electronic evidence. The convention also maintains a fine balance between enhancing international cooperation while recognising the sanctity of the national sovereignty principle.

While emphasising cooperation, the convention requires states to transfer personal data in compliance with their domestic laws or applicable international data protection regulations.[12] It also provides a mechanism to transfer personal data to a third party, with due authorisation from the original transferring state.[13]

For extradition, however, parties are required to adhere to the principle of dual criminality, meaning the act in question must be recognised as a criminal offence under the domestic laws of both parties involved.[14] States can also refuse extradition if they have reasonable grounds to believe the request is intended to punish an

[8] **"Resolution Adopted by the General Assembly on 27 December 2019"**, UN Doc. A/RES/74/247, 20 January 2020.

[9] **"Resolution Adopted by the General Assembly on 26 May 2021"**, UN Doc. A/RES/75/282, 1 June 2021.

[10] Article 1, **"United Nations Convention Against Cybercrime"**, United Nations, 27 November 2024.

[11] Ibid., Article 35.

[12] Ibid., Article 36 (1)(a).

[13] Ibid., Article 36 (3).

[14] Ibid., Article 37 (1).

individual based on their sex, race, language, religion, nationality, ethnic origin or political opinions.[15] In crimes involving several jurisdictions, states can seek transfer of criminal proceedings with mutual agreement.[16]

To ensure seamless and prompt processing of mutual legal assistance requests, each party will designate a central authority responsible for receiving and executing such requests without affecting existing mechanisms.[17]A state may exercise its discretionary power to refuse mutual legal assistance on grounds of sovereignty, security or public order.

The convention mandates states to establish a 24/7 network to provide immediate assistance for investigations and prosecutions, as well as to facilitate measures such as technical advice, preservation of stored electronic data, evidence collection and related activities.[18] It also encourages states to strengthen cooperation by entering into bilateral or multilateral agreements or by using the convention as a legal basis for such collaboration.[19] The international cooperation sought to be enhanced by the convention will adhere to the jurisdictional rules outlined in the legal instrument.

Capacity Building

In recent years, cybercrime has evolved into a transnational issue driven by the interconnectedness of the modern world. Some states are better equipped to address threats, while others remain highly vulnerable. To bridge this glaring gap, particularly considering the interests and needs of the developing world, the convention provides a mechanism for knowledge sharing between countries, including technical assistance, expertise exchange and transfer of technology.[20] This also includes sharing insights to help countries formulate strategic policies and relevant legislation to prevent and combat cybercrime. Technical assistance also includes providing modern law enforcement equipments to states that lack adequate resources.[21]

Capacity building measures are not merely limited to technical assistance. The convention also emphasises imparting human resources with skills, including language training, drafting and handling of mutual legal assistance requests, and other relevant responsibilities.[22] To strengthen efforts in assisting developing countries, the convention encourages member states to make financial contributions towards achieving the goals.

[15] Ibid., Article 37 (15).

[16] Ibid., Article 39.

[17] Ibid., Article 40 (12).

[18] Ibid., Article 41.

[19] Ibid., Article 47 (2).

[20] Ibid., Article 54 (1).

[21] Ibid., Article 54 (3) (d).

[22] Ibid., Article 54 (7).

Prevention

For any individual or organisation, prevention remains the key priority. The convention emphasises that cooperation and capacity building should focus not only on responding to crime but also on preventing it from occurring in the first place. To that end, the convention underlines the importance of harmonising policies and best practices across different jurisdictions.[23] It equally stresses the utility of involving multiple stakeholders, including the private sector, academia, civil society and the general public, to ensure robust preventive measures. Connecting and strengthening cooperation between these stakeholders and law enforcement agencies is considered a crucial step in preventing cybercrime.[24]

Recognising their critical role in prevention, the convention also encourages service providers to enhance the security of their products, services and customer data. It also recognises the essential role of "legitimate activities of security researcher" to strengthen overall security.[25] This validates the work done by security researchers, penetration testers and ethical hackers without inviting any criminal liability on these professionals.

Interestingly, the convention calls for "developing, facilitating and promoting" activities and measures aimed at discouraging those at risk of engaging in cybercrime from becoming offenders.[26] This provision, though commendable, lacks a clear roadmap as to how member states intend to put this into practice. Furthermore, it also asks states to promote the reintegration of offenders into society, demonstrating the reformative aspect of the convention. However, whether competent authorities will consider the severity of crime before reintegration remains uncertain. States will also have to initiate periodic assessments of their national strategies and legal framework to align them with the evolving nature of threats.

Victim Support

Recognising the urgent need to support victims of crimes, Article 34 outlines measures for their assistance and protection. It asks states to initiate measures to provide access to compensation and restitution for the victims.[27] Measures will be commensurate with the severity of the crime. For instance, in cases involving online child sexual abuse, grooming a child for sexual exploitation, or victims of non-consensual dissemination of intimate images, states are required to take steps to ensure both the physical and psychological recovery of the victims.

[23] Ibid., Article 53 (1).

[24] Ibid., Article 53 (3) (a).

[25] Ibid., Article 53 (3) (e).

[26] Ibid., Article 53 (3) (f).

[27] Ibid., Article 34 (2).

Child Protection

The convention classifies the selling, buying and possessing of material related to child sexual abuse as criminal offences. Expanding its scope, it also recognises the production, offering, selling, distribution and possession of such material through the use of ICTs as criminal activities. The criminalisation of "possessing" and "controlling" such materials could significantly impact service providers and intermediaries, as merely acting as a conduit might expose them to criminal liability. The article not only covers the 'visual material' but also includes written or audio content.[28] Similarly, the convention criminalises acts of intentionally communicating, soliciting, grooming or making arrangements through ICT for sexual exploitation.[29]

The obstacle-strewn path to the Convention

The convention, in its current form, is the culmination of five years of sessional and intersessional consultations, during which UN member states deliberated and contributed to the draft. During these sessions, stakeholders, including states, members of civil society, and non-governmental organisations, shared position papers outlining their views on the scope, objectives and structure of the new convention. At a later stage of the negotiations, when the draft convention was under discussion, participants shared their respective draft texts, reflecting their perspectives and opinions on the proposed document. While some were critical of the progress, others advocated for incremental changes.

For instance, during the first session of the Ad Hoc committee, the US submitted its views on the convention's structure before the drafting process commenced among member states. It cautioned the members against addressing every cyber-related issue within the convention to ensure more focus.[30] Furthermore, the US appealed to participants not to treat conventional crimes as "cybercrime" merely because of the involvement of computer systems in planning and execution.[31] The US also shared its support for the convention without undermining the existing instruments and ongoing international cooperation in the fight against cybercrime.[32] At the reconvened concluding session of the Ad Hoc Committee, the US welcomed the adoption of the convention with the caveat that the trade language related to the "transfer of technology" held no relevance to its trade policy.[33]

---

[28] Ibid., Article 14 (2).

[29] Ibid., Article 15.

[30] **"First Session of the Ad Hoc Committee"**, UNODC, New York, 28 February to 11 March 2022.

[31] Ibid., p. 5.

[32] Ibid., p. 9.

[33] **"Reconvened Concluding Session of the Ad Hoc Committee"**, UN, 29 July to 9 August 2024, New York.

The European Union (EU) recognised the convention's crucial role in eliminating potential "safe havens" for criminals.[34] In its proposal during the first session, the EU advocated excluding certain matters from the scope of the convention, including issues related to or regulating national security or state behaviour and matters concerning internet governance.[35] It also made a proposal arguing against directly imposing obligations upon non-governmental organisations under the convention.

India also played a proactive role during the Ad hoc committee sessions. India proposed that failure or negligence in protecting 'sensitive' personal data or information should be recognised as a criminal act.[36] This includes negligence in maintaining and implementing reasonable security practices by a corporate body in possession of sensitive data. India also included the aspect of 'cyber terrorism' in its draft and proposed a 'data-oriented jurisdiction' rather than a 'territorial-based jurisdiction'.[37] Data-oriented jurisdiction would mean that states could claim broader jurisdiction based on where their citizens' data is stored/processed/screened/ federated rather than solely relying on where data is physically located. The proposal encapsulates India's approach to asserting control over its citizens' data, regardless of location. It also reflects the perennial challenge that Indian law enforcement agencies have faced over the years, particularly its inability to access cross-border data through existing Mutual Legal Assistance Treaties (MLAT).[38] India also stressed the need to combat phishing effectively, proposing the use of a 24/7 network to render phishing links inaccessible swiftly.

The INTERPOL in 2022 emphasised the need to foster information sharing between national agencies as well as cooperation between law enforcement and the private sector.[39] It also underlined the significance of existing mechanisms like the INTERPOL National Central Bureau (NCB), which serves as the liaison point between INTERPOL and various departments and agencies within the country. The existing mechanisms would, therefore, assist in the operationalisation of the convention.

There has been a fair bit of criticism as well, raised mainly by human rights organisations and the private sector. Human Rights Watch (HRW) criticised the convention for establishing "expansive electronic surveillance power to investigate

[34] **"EU Explanation of Position - UN General Assembly 3rd Committee: Adoption of the United Nations Convention against Cybercrime"**, The European External Action Service (EEAS), 11 November 2024.

[35] **"First Session of the Ad Hoc Committee"**, no. 30.

[36] **"Second Session of the Ad Hoc Committee"**, UNODC, Vienna, 30 May to 10 June 2022.

[37] Ibid.

[38] Aarathi Ganesan, **"India Proposes 'Data-Oriented Jurisdiction' at the UN to Assert Control Over Citizens' Data Abroad"**, *Medianama,* 12 October 2022.

[39] **"INTERPOL's Contribution to the Comprehensive International Convention on Countering the Use of Information Communications Technologies for Criminal Purposes"**, UNODC, December 2022.

and cooperate", even for crimes that do not involve an ICT system.[40] Also, according to the HRW, the convention in its current form risks overstretching the MLAT system, leading to unwarranted delays. Mainly focusing on Article 14 dealing with child sexual abuse, it underlines the risks of even criminalisation of material that has "evidentiary, scientific, or artistic value".[41] Concerns have been raised about the convention's potential to introduce a jurisdictional shift by broadly legitimising "passive personality jurisdiction".[42] This principle allows states to assert jurisdiction over extraterritorial actions that impact their citizens. Similarly, the private sector has raised the alarm over the convention's potential to "…erode data privacy, threaten digital sovereignty, and undermine online rights and freedoms globally".[43]

Conclusion

The adoption of the UN Convention against Cybercrime is a welcome step that illustrates the willingness of states to address the rising threat in digital space collectively. The participation of multiple stakeholders in the negotiation towards a draft is also suggestive of how decision-making to address the threats could not be limited to states. Despite both the optimism and misgivings raised by various stakeholders, the convention comes at an opportune moment. It provides a legal framework for information sharing along with avenues to enable coordination between law enforcement agencies of different states.

However, the effectiveness of the cybercrime convention can only be assessed once it is fully operationalised. The emphasis on leveraging existing mechanisms without undermining them risks falling back to the inefficiencies that initially necessitated such a convention. It will also be interesting to see how the EU and the US operationalise data sharing and law enforcement mechanisms, given the stringent regulations currently governing such matters and the majority of tech companies located in their jurisdiction.

[40] **"Human Rights Watch's Comments on the Updated Draft Text of the UN Cybercrime Convention (Rev 3)"**, UNODC, July 2024.

[41] Ibid., p. 8.

[42] Eli Scher-Zagier, **"The New UN Cybercrime Treaty is a Bigger Deal Than Even Its Critics Realize"**, Lawfare, 2 October 2024.

[43] **"Microsoft's Submission to the Seventh Reconvened Session"**, UNODC.

About the Author

Mr. Rohit Kumar Sharma is Research Analyst at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses