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

MP-IDSA
Issue Brief

United Nations Cybercrime Convention: A Milestone in Digital Governance?

Rajeesh Kumar

January 06, 2025

Summary

The adoption of the UN Cybercrime Convention underscores the ability of multilateralism to navigate complex global challenges. There are concerns, though, about the treaty's broad provisions, particularly around data sharing and cross-border law enforcement, which could undermine privacy, freedom of expression, and be used for political repression.

On 24 December 2024, the United Nations General Assembly (UNGA) adopted the UN Convention against Cybercrime, marking a significant milestone in the global fight against cybercrime.[1] This treaty, the first legally binding UN instrument addressing cyber issues, establishes a crucial framework for international cooperation in the prevention, investigation and prosecution of cybercrimes. As cyber threats grow in scale and complexity, the convention aims to prevent and combat cybercrime, enhance international cooperation and promote technical assistance and capacity-building, particularly for developing countries.[2] The Convention will be open for signature at a formal ceremony in Hanoi, Vietnam in 2025, and will enter into force 90 days after ratification by the 40th signatory.

The adoption of the Convention underscores the ability of multilateralism to navigate complex global challenges. It also reflects the collective determination of UN Member States to strengthen global cooperation in combating cybercrime. However, the treaty has faced criticism from human rights groups and privacy advocates who warn it could be misused by authoritarian regimes to justify surveillance, monitor citizens' online activities and censor speech under the guise of combating cybercrime.[3] Critics are concerned that the treaty's broad provisions, particularly around data sharing and cross-border law enforcement, could undermine privacy, freedom of expression and be used for political repression.[4] This Brief explores the treaty's potential to shape digital governance while examining the criticisms surrounding its implementation and impact.

Background

The rapid growth of digital technologies has brought significant benefits but has also led to a rise in cyber threats. Cybercrime encompasses a wide range of activities, from hacking and identity theft to financial fraud and ransomware attacks. These crimes often span multiple jurisdictions, exploiting legal differences to evade justice, making cybercrime a global issue that requires a coordinated international response. While national and regional frameworks, such as the Council of Europe's Budapest Convention (2001), have been valuable, they are insufficient in tackling the transnational nature of cybercrime.[5]

[1] **"UN General Assembly Adopts Milestone Cybercrime Treaty"**, United Nations, 24 December 2024.

[2] "Draft United Nations Convention Against Cybercrime", UN Doc. A/AC.291/L.15, United Nations, 7 August 2024.

[3] **"Joint Statement on the Proposed Cybercrime Treaty Ahead of the Concluding Session"**, *Human Rights Watch*, 23 January 2024.

[4] **"New UN Cybercrime Treaty Primed for Abuse"**, *Human Rights Watch*, 30 December 2024.

[5] **"Convention on Cybercrime"**, European Treaty Series-185, Council of Europe, Budapest, 23 November 2001.

The UN Convention against Cybercrime was formed after extensive negotiations that began in the late 2010s. In December 2019, the UNGA established an ad hoc committee to draft a global cybercrime treaty in response to the growing threats posed by cybercrime.[6] On 26 May 2021, the General Assembly adopted Resolution 75/282, which requested the Ad Hoc Committee to present a draft convention to the Assembly at its seventy-eighth session.[7] From 2022 to 2024, the Committee held six negotiating sessions, a concluding session and five intersessional consultations to advance the development of the convention.[8] In the concluding session, the Committee approved the draft text for the convention for the adoption of General Assembly.[9]

Key Features of the UN Convention

The UN Convention aims to enhance the prevention and effective combating of cybercrime, strengthen international cooperation and support technical assistance and capacity-building, particularly for developing countries.[10] It comprises nine chapters: General Provisions, Criminalization, Jurisdiction, Procedural Measures and Law Enforcement, International Cooperation, Preventive Measures, Technical Assistance and Information Exchange, Mechanism of Implementation and Final Provisions.

The chapter on General Provisions addresses the statement of purpose, definitions, scope and key issues such as the protection of sovereignty and the respect for human rights. The second chapter examines the Convention's role in establishing a comprehensive framework to combat cybercrimes, including hacking, online fraud and child exploitation, with a particular emphasis on cross-border cooperation and capacity-building. A key provision in the criminalization chapter addresses child abuse, encompassing offenses such as online child sexual abuse, the distribution of exploitation material and the solicitation or grooming of a child for the purpose of committing a sexual offence.[11] It underscores the requirement to criminalise cyber-

[6] "Countering the Use of Information and Communications Technologies for Criminal Purposes", UN Doc. A/RES/74/247, General Assembly Resolution, 27 December 2019.

[7] "Countering the Use of Information and Communications Technologies for Criminal Purposes", UN Doc. A/RES/75/282, General Assembly Resolution, 26 May 2021.

[8] **"Meetings of the Ad Hoc Committee"**, UNDOC, United Nations.

[9] **"Report of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes on its Reconvened Concluding Session"**, United Nations, 19 August 2024.

[10] Article 1, **"Draft United Nations Convention Against Cybercrime"**, United Nations, 9 August 2024.

[11] Ibid., Article 14.

dependent offenses, such as unauthorised hacking and data interference,[12] alongside cyber-enabled crimes, including online fraud and the non-consensual dissemination of intimate images.[13] Furthermore, it addresses the accountability of legal entities while ensuring procedural safeguards for accused individuals.[14]

Given the transnational nature of cybercrime, the Convention establishes jurisdictional rules to prevent criminals from exploiting legal gaps. States must claim jurisdiction over offences committed on their territory or affecting their nationals, with provisions for action against offenders within their borders if extradition is not possible.[15] When jurisdictions overlap, States are required to consult with each other.[16] The Convention also mandates cooperation in investigations, including extradition, evidence sharing and mutual legal assistance for electronic data. However, States may refuse cooperation on grounds of sovereignty, public order or non-compliance with data protection or anti-discrimination principles.

The chapter on procedural measures equips States with tools to effectively secure and collect electronic evidence, adapting traditional methods to the ICT environment[17] while protecting human rights.[18] It empowers States to preserve, search, seize and produce electronic data, as well as intercept data in transit, to combat cybercrimes efficiently.[19] These powers are governed by safeguards such as judicial oversight, clear justifications, limited scope and access to remedies, ensuring evidence integrity and the protection of rights.

The Convention also establishes a global framework to assist in investigations, prosecutions and judicial proceedings, including extradition, joint investigations and asset recovery.[20] It facilitates cross-border access to electronic evidence through measures like data preservation, access and interception, supported by a 24/7 contact point network for rapid response.[21] It outlines the general principles and procedures for mutual legal assistance, stating that States Parties shall provide each other with the widest possible support in investigations, prosecutions and judicial proceedings.[22] The provisions on international cooperation require States to work

[12] Ibid., Articles 11 & 12.
[13] Ibid., Article 16.
[14] Ibid., Article 21.
[15] Ibid., Article 22 (d) 4.
[16] Ibid., Article 22 (d) 5.
[17] Ibid., Article 23.
[18] Ibid., Article 24.
[19] Ibid., Articles 28, 29 and 30.
[20] Ibid., Chapter V, 'International Cooperation'.
[21] Ibid., Article 41.
[22] Ibid., Article 40.

closely together, in line with their respective domestic legal and administrative systems, to enhance the effectiveness of law enforcement in combating these offences.[23]

The Convention promotes collaboration between law enforcement and stakeholders, public awareness campaigns, training for justice officials and the use of security researchers' expertise. It emphasises protecting vulnerable groups, preventing gender-based violence, safeguarding children and supporting victims and offender reintegration.[24] States are required to evaluate their legal frameworks, ensure accessible reporting mechanisms and designate authorities for international preventive collaboration, creating a global network to address evolving cybercrime threats.[25]

The chapter on technical assistance and information exchange focuses on strengthening global capacity to combat cybercrime, particularly in developing countries. It emphasises sharing knowledge and resources for preventing, detecting, investigating and prosecuting cybercrime, including handling electronic evidence, forensic analysis and tracking cybercrime proceeds.[26]

The Convention emphasises providing financial and technical assistance to developing countries to help them prevent and combat the offences covered. States Parties are encouraged to make regular voluntary contributions to a United Nations funding mechanism to support the implementation of the Convention in these countries.[27] The chapter also fosters partnerships between governments, NGOs, academia, financial institutions and the private sector to address the growing threat of cybercrime.[28]

The chapter on the Mechanism of Implementation establishes the Conference of States Parties, responsible for overseeing the Convention's implementation. States parties must submit reports on their implementation measures for periodic reviews, with the Conference offering recommendations to improve effectiveness.[29] The Conference facilitates information exchange on legal, policy and technological developments, and may adopt supplementary protocols. It can also collaborate with stakeholders, including international organisations, NGOs and the private sector. The first Conference will be convened by the UN Secretary-General within a year of

[23] Ibid., Article 47.
[24] Ibid., Article 53 (3) h & i.
[25] Ibid., Article 53 (4).
[26] Ibid., Article 54 (3) c.
[27] Ibid., Article 56.
[28] Ibid., Article 54 (4).
[29] Ibid., Article 57.

the Convention's entry into force, with the United Nations Office on Drugs and Crime (UNODC) serving as its secretariat.[30]

The chapter on final provisions outlines the procedures for States to become parties to or withdraw from the Convention, as well as the rules governing its entry into force and its legal effects. It also covers the settlement of disputes related to the interpretation or application of the Convention, emphasising that such disputes should be resolved primarily through negotiations or other peaceful means, including arbitration. If necessary, the International Court of Justice may be called upon to settle disputes at the request of the parties involved.[31] Furthermore, the chapter provides for the potential amendment of the Convention and the addition of supplementary protocols. States may withdraw from the Convention through written denunciation, with the withdrawal taking effect one year after the notification is made.[32]

Contrasting the UN and Budapest Conventions

The Budapest Convention on Cybercrime, adopted in 2001, was the first international treaty focused on combating cybercrime and strengthening cross-border cooperation. While both the Budapest and UN Conventions seek to combat cybercrime, their scopes differ significantly. The Budapest Convention focuses on criminalising specific offences, establishing procedural measures and facilitating cross-border access to electronic evidence.[33] In contrast, the UN Convention adopts a broader approach, emphasising prevention, capacity-building and technical assistance, with particular attention to supporting developing countries.[34] Additionally, the UN Convention offers a global framework for cooperation on serious cybercrimes and incorporates provisions related to state sovereignty and prevention, expanding its scope beyond the Budapest Convention's emphasis on criminalisation and procedural mechanisms.

The definitions in the UN Convention largely align with those in the Budapest Convention, with key differences that reflect the broader scope of the UN Convention. Notably, the UN Convention adopts the terms "ICT" and "ICT systems" instead of the "computer" and "computer systems" terminology used in the Budapest Convention,

[30] Ibid., Article 58.

[31] Ibid., Article 63.

[32] Ibid., Article 67.

[33] **"Convention on Cybercrime"**, European Treaty Series-185, Council of Europe, Budapest, 23 November 2001.

[34] **"Draft United Nations Convention Against Cybercrime"**, United Nations, 9 August 2024.

reflecting the evolving nature of technology and the increasing reliance on information and communication technologies.[35]

While both conventions criminalise offences such as illegal access to systems, the UN Convention extends its focus to include additional crimes, such as money laundering, and places greater emphasis on child sexual abuse. For example, while the Budapest Convention criminalises the possession and distribution of child abuse material,[36] the UN Convention also targets preparatory offences, including grooming and solicitation, thus broadening its approach to combating such crimes.[37] Furthermore, the procedural powers in the UN Convention are broader than those in the Budapest Convention. For instance, the UN Convention includes measures for the confiscation of proceeds from crime[38] and the protection of witnesses,[39] which are not addressed in the Budapest Convention.

Criticisms and Concerns

The UN Cybercrime Convention has been the subject of significant criticism from human rights organisations and privacy advocates, particularly due to its potential for misuse by authoritarian regimes.[40] Critics contend that such regimes could exploit the Convention's provisions to legitimise heightened surveillance, censorship and the suppression of political dissent, thereby posing serious risks to fundamental rights, including privacy and freedom of expression.[41] A key concern with the Convention is its lack of explicit safeguards to regulate intrusive surveillance, leaving it vulnerable to misuse. The absence of core human rights principles such as legality, necessity and non-discrimination exacerbates the risk of abuse. Without clear legal definitions, limits on surveillance and protection against discriminatory practices, the Convention risks undermining fundamental rights and enabling unchecked surveillance measures.[42]

---

[35] **"Comparative Analysis: The Budapest Convention vs the UN Convention Against Cybercrime"**, *digwatch*, 22 October 2024.

[36] Article 9, Budapest Convention.

[37] Article 15, Draft United Nations Convention Against Cybercrime.

[38] Ibid., Article 31.

[39] Ibid., Article 33.

[40] **"Written Testimony of David Kaye Before a Hearing of the Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy"**, 24 September 2024.

[41] **"New UN Cybercrime Treaty Primed for Abuse"**, *Human Rights Watch*, 30 December 2024.

[42] **"The UN Cybercrime Convention: Analyzing the Risks to Human Rights and Global Privacy"**, *Just Security*, 27 August 2024.

The Convention's provisions for monitoring online activities are perceived as a threat to digital rights, enabling intrusive oversight that could erode individual privacy.[43] Its strict secrecy requirements have been criticised for undermining transparency and due process. These provisions grant authorities unchecked power, limiting oversight and restricting individuals' ability to know about or challenge surveillance, thereby eroding trust and threatening fundamental rights such as privacy and due process.[44]

Furthermore, its provisions on data-sharing agreements and cross-border law enforcement cooperation raise significant apprehensions. The facilitation of inter-state data exchange, without robust protective mechanisms, heightens the potential for the misuse of personal information. For instance, under the treaty's passive personality jurisdiction, State A could request State B to surveil or extradite a citizen of State C, located in State B, for reporting a data breach involving State A. Such scenarios raise critical issues regarding jurisdictional overreach and due process.[45]

The Convention's provisions also risk impeding the activities of legitimate security researchers. Its overly broad and restrictive measures could inadvertently discourage or criminalise research endeavours vital to identifying vulnerabilities and enhancing cybersecurity frameworks.[46] These restrictions not only curtail critical research but also undermine global efforts to strengthen cybersecurity and safeguard privacy, thereby compromising the Convention's overarching objectives.[47]

Challenges

One of the major challenges in implementing the Convention is the lack of harmonised legal frameworks among member states. Countries have significant differences in their legal systems, cybersecurity laws and enforcement capacities, making it difficult to develop a unified approach to addressing cybercrime. These differences include variations in how cybercrime is defined, the methods used for investigation, and the penalties imposed, leading to inconsistencies in applying the

[43] **"The UN General Assembly and the Fight Against the Cybercrime Treaty"**, Electronic Frontier Foundation, 26 September 2024.

[44] **"The UN Cybercrime Convention: Analyzing the Risks to Human Rights and Global Privacy"**, *Just Security*, 27 August 2024.

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

[46] **"HackerOne Urges U.S. to Advocate for Research Protections in UN Cybercrime Treaty"**, *Cyberscoop*, 14 November 2024.

[47] US Senator Roy Wyden's Letter to Antony Blinken, Secretary of the State, 29 October 2024.

Convention. For example, an act considered a cybercrime in one country might not be recognised as such in another, creating conflicts and enforcement gaps.

The uneven levels of technological development and institutional capacity among countries add to the challenge. While developed nations may have sophisticated systems to address cybercrime, many developing countries lack the necessary infrastructure, expertise and resources to implement effective cybersecurity measures. This inequality could lead to a fragmented global response, with some countries successfully addressing cybercrime while others remain vulnerable or become safe havens for cybercriminals.

The greatest challenge, however, lies in the potential misuse of the convention's provisions for political purposes. Without adequate safeguards, governments may use the convention to suppress free speech, privacy rights and political dissent. Additionally, disagreements over the definition of cybercrime and concerns about sovereignty could hinder global adoption and consistent application. To maintain its legitimacy, the convention must balance international cooperation with human rights protections, ensure transparency and adapt to evolving cyber threats.

Addressing these challenges requires capacity-building initiatives, technical assistance and strong international cooperation to ensure all member states can effectively implement the Convention.

Conclusion

The adoption of UN Cybercrime Convention marks a significant milestone in addressing global cybercrime challenges, offering a comprehensive framework for prevention, cooperation and capacity-building. It exemplifies how multilateralism can foster global solidarity and provide a collective response to transnational issues. By bringing together a wide range of stakeholders—including states, international organisations, the private sector and civil society—this initiative exemplifies the power of collective action in addressing issues that transcend national borders.

Its success, however, depends on Member States overcoming several challenges. These include safeguarding human rights, ensuring that provisions are not misused for political or surveillance purposes, and promoting equitable access to resources for developing nations to strengthen their cybersecurity capabilities. Moreover, the Convention must remain adaptable to rapidly evolving cyber threats and emerging technologies. With a balanced, inclusive approach, the Convention has the potential to not only combat cybercrime but also create a secure and resilient digital ecosystem globally.

About the Author

Dr. Rajeesh Kumar is Research Fellow 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