Page 885 - 894

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 4

2026

The United Nations Cybercrime Convention: A Critical Analysis of the Tectonic Issues of the Contemporary Cybersecurity Deliberations

UDIT SHARMA*

ABSTRACT

This paper offers a critical analysis of the United Nations Convention against Cybercrime, 2025, and its capacity to serve as a truly global framework for combating cybercrime through international cooperation. It traces the evolution of cybercrime instruments from the Budapest Convention and subsequent regional conventions to the present treaty, and provides a provisional summary of the Convention's substantive offences, procedural measures and mechanisms for international cooperation. The paper then identifies a series of structural or 'tectonic' issues within the text, including the absence of any definition of cybercrime, a loose definition of serious offences, ambiguity regarding the nature of electronic evidence, an exhaustive conception of personal data that excludes corporate data, uncertainty over the nature of shared data, and the want of an oversight mechanism. It argues that these gaps risk reducing the Convention to a mere text open to misuse, particularly by States with a weak commitment to the rule of law, and concludes with suggestions for definitional clarity, adaptation to technological developments such as artificial intelligence, stronger data-protection safeguards and an effective oversight mechanism.

Keywords: *cybercrime, United Nations Cybercrime Convention, international cooperation, electronic evidence, personal data protection, cybersecurity, right to privacy*

I. INTRODUCTION

Information and Communications Technology (ICT) has become a bedrock of modern global social and economic infrastructure, with every activity of the contemporary globalised order running on ICT systems. The expansion of the global economic order has seen a parallel development in the ICT systems that have grown to facilitate it. An interconnection of the ICT systems across the globe, also known as 'cyberspace', has modelled itself into a novel space

* Author is a Ph.D. Research Scholar at Himachal Pradesh National Law University, Shimla, Himachal Pradesh, India.

 [ISSN 2581-5369]

where the world interacts and transacts. Cyberspace has thereby grown with the growth in ICT, and is expanding with each passing day.

However, the development in cyberspace has also seen a rise in another facet of the ICT systems, which is connected to the delinquent activities undertaken with their assistance. Such activities use cyberspace to target individuals and institutions, including government institutions, to cause economic and security-related damages, and are collectively known as cybercrimes.

Cybercrimes can be defined as illicit acts undertaken through the use of a computer device or a related system. A cybercrime is an unlawful act which uses a computer, a communication device or a computer network to commit or facilitate the commission of a crime. It can also be defined as "any crime that is facilitated or committed using a computer, network, or hardware device."[1] Cybercrime is, therefore, a delinquent act facilitated through the use of ICT systems.

An important aspect related to cybercrimes is that such crimes are not territorial in their operation and effect. These may have an effect on a particular computer system or an individual while originating in a completely different location or a different country altogether. It is their cross-border interoperability that makes these crimes hard to resolve by a single entity or a single country.

In light of such cross-border impact of cybercrimes, the Convention on Cybercrime, or the Budapest Convention, was signed on 23 November 2001 and enacted on 1 July 2004. The Convention was the first international treaty which addressed the risks regarding the use of computer networks and electronic information for committing criminal offences.[2]

The Convention was prepared by the Council of Europe, but its operation was also expanded to non-European nations (in the capacity of observers), such as Canada, South Africa and other countries that expressed their intention to be a signatory to the Convention. It was focused on addressing and safeguarding human rights in the perceived "new reality"[3] of the ICT systems. It focused on safeguarding the rights of the individuals affected by cybercrimes within the European borders.

It was followed by several regional conventions addressing cybercrimes, such as the "Arab Convention on Combating Information Technology Offences"[4] in 2010 and the "African Union

[1] Sarah Gordon & Richard Ford, *On the Definition and Classification of Cybercrime*, 2 J. COMPUTER VIROLOGY 13, 14 (2006).
[2] Convention on Cybercrime, Nov. 23, 2001, E.T.S. 185.
[3] Armando A. Cottim, *Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime*, 2 EUR. J. LEGAL STUD., Winter 2010, at 56.
[4] LEAGUE OF ARAB STATES, Arab Convention on Combating Information Technology Offences (Dec. 2010), https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf.

 [ISSN 2581-5369]

Convention on Cyber Security and Personal Data Protection" in 2014. The conventions, though they addressed cyber-oriented criminal offences, were localised in their operation. This meant that while they catered to the cross-border issues of cybercrimes, they were restricted by the borders of the operable region, such as the countries of the Arab States or the members of the African Union.

Thus, there existed a void within the international framework that aimed to address cybercrimes at a cross-border level. It was felt by the international community that there was a need for an all-encompassing, truly global treaty that catered to cybercrimes and the various facets related to it, such as cybercrime investigation and emerging issues such as money laundering through the use of ICT systems.

Thereby, in order to establish a universal outline for digital cooperation and dealing with cybercrimes and allied investigation, 2,514 delegates from 119 countries gathered in the Vietnamese capital, Hanoi, to strengthen the global defence against cybercrime.[5] This led to the formation of the United Nations Convention against Cybercrime, 2025, which has been envisioned to be a global framework of digital cooperation for a safer cyberspace.

II. The Cybercrime Convention: A Provisional Summary

The United Nations Convention against Cybercrime, 2025 is centred around the acknowledgement of the adverse impact of cybercrimes on countries and individuals, and aims to address them at a global scale. The Convention addresses cybercrimes as an increasing threat, especially in the context of their cross-border impact and the scale at which such crimes are being operated, and thereby stresses coordination and cooperation between the States.

The Convention, under Chapter II, elaborates on aspects that the States should incorporate within their domestic laws to deal with cybercrimes. It provides for the criminalisation of offences such as illegal access[6] and illegal interception[7] of an ICT system. Further, it calls upon States to frame laws regarding the manipulation of electronic data and interference with the ICT system[8], in addition to ensuring that devices enabling cybercrimes are restricted in terms of their sale or distribution.[9]

---

[5] United Nations Office on Drugs and Crime, *Seventy-two Nations Sign First UN Treaty to Fight Cybercrime, in Milestone for Digital Cooperation*, https://www.unodc.org/unodc/frontpage/2025/October/seventy-two-nations-sign-first-un-treaty-to-fight-cybercrime--in-milestone-for-digital-cooperation.html.

[6] 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 art. 7, Dec. 24, 2024, C.N.196.2025.TREATIES-XVIII.16.

[7] *Id.* at art. 8.

[8] *Supra* note 6, at art. 10.

[9] *Id.* at art. 11(3).

 [ISSN 2581-5369]

It further covers specific cyber offences such as online theft or fraud,[10] online CSAM (Child Sexual Abuse Material),[11] dissemination of intimate images without consent[12] and money laundering.[13] The Convention, through Chapter II, details the criminal liability principles and includes the scope of tackling cybercrimes by bringing abetting and aiding within the criminal liability framework. The Convention stresses upon the States the need to include these within their domestic cybersecurity framework, including the process regarding prosecution and sanctions[14], in line with their respective legal principles and national laws.

In addition to these substantive provisions, the Convention details certain procedural measures within Chapter IV that the respective States shall adopt within their municipal framework for investigation and further proceedings.[15] This includes having adequate safeguards and procedural justiciability[16] and provisions such as the preservation of stored data[17] and disclosure of site traffic data.[18]

Further, the Convention also elucidates the general procedural aspects such as search and seizure[19], collection of data,[20] seizure and confiscation of criminal proceeds[21] and taking measures to ensure the establishment of a criminal record detailing any previous conviction of the accused.[22] Thus, the Convention pursues an effective cybercrime investigation in accordance with the general principles of law and justice.

A running theme across the Convention, in fact the foundation on which the Convention is based, is international cooperation. The Convention relies heavily on international collaboration to realise its preambular objectives. These include establishing the basic principles of such cooperation and dealing with specific international criminal law issues such as extradition,[23] mutual legal assistance,[24] joint investigations and the sharing of cross-border information.

[10] *Supra* note 6, at art. 13.
[11] *Id.* at art. 14.
[12] *Supra* note 6, at art. 16.
[13] *Id.* at art. 17.
[14] *Supra* note 6, at art. 21.
[15] *Id.* at art. 23.
[16] *Supra* note 6, at art. 24(2).
[17] *Id.* at art. 25.
[18] *Supra* note 6, at art. 26.
[19] *Id.* at art. 28.
[20] *Supra* note 6, at art. 29.
[21] *Id.* at art. 31.
[22] *Supra* note 6, at art. 32.
[23] *Id.* at art. 37.
[24] *Supra* note 6, at art. 40.

 [ISSN 2581-5369]

It also highlights the various facets under which States shall provide mutual technical assistance and facilitate the sharing of information.[25] It plans capacity-building initiatives such as training and assistance, particularly focusing on developing countries. The text, therefore, tries to establish the basic parameters on which the principles and policies shall be effectuated at an international level, and in a manner that is coherent with the foundational parameters of international law.

In order to realise such effectuation, the Convention, under Chapter VIII, establishes a Conference of the States Parties[26] to be convened by the United Nations Secretary-General. Such a conference shall be held at regular intervals in accordance with the rules and procedures established in this regard by the conference. Such a conference has been envisioned to assist in collaboration and support amongst the States by sharing best practices, as highlighted under Chapter VI of the Convention.

The United Nations Cybercrime Convention is, therefore, an effort towards establishing a coherent cross-border mechanism to tackle cybercrimes. The Convention proposes the coming together of the international community towards an emerging and expanding threat of ICT-oriented crimes. The textual interpretation of the Convention significantly points out its quest for a global mechanism to arrest cybercrime.

III. Structural Issues within the Convention

While the textual content of the Convention tries to address cybercrime in letter, there exist certain issues within the textual ambit of the same that lead the objectives to fall short of the desired effect. These issues relate to the provisions of the Convention, especially within the terminological aspects, which restrict the scope of the application of the Convention and make it exhaustive in nature.

A. No Definition of Cybercrime

The Convention is centred around the prevention and combating of cybercrimes; however, it falls short in providing a comprehensive definition of the same. The scope of the Convention is, therefore, related to a concept which is an abstract notion at best. With no common consensual definition of cybercrime at the international forum in general, and in the present Convention in particular, the effectiveness of the Convention in achieving the desired objective of combating cybercrime seems a difficult task.

[25] *Id.* at ch. VII.
[26] *Supra* note 6, at art. 57(1).

 [ISSN 2581-5369]

The lack of definition further raises the possibility of an inept implementation of the Convention, since the chief point of discussion, that is, cybercrime, has been reduced to being a subjective entity rather than a consensus-driven objective concept. With each State possibly defining cybercrime differently, it could hamper the implementation of important aspects of the Convention, especially in relation to international cooperation.

B. Loose Definition of Serious Offences

'Serious crime', as defined under Article 2(h) of the Convention, refers to an offence for which the maximum amount of imprisonment (termed 'deprivation of liberty' under the text) amounts to four years.[27] Under the Convention, the collecting of evidence and cross-country sharing of the same is to be done specifically for serious crimes. The textual interpretation of the provision points out certain flaws regarding the overall effectiveness of the document.

The Convention does not provide an exhaustive list or a criterion to categorise what nature of offences could be included within the definition of serious crime. It rather includes under its ambit such offences as are applicable under any other Convention or protocol of the United Nations.[28] While *prima facie* this expands the scope of the Convention, it also opens the possibility of the provisions of the Convention being misapplied to offences which would not fall under the ambit of cybercrimes in normal parlance.

This could also lead to certain governments, particularly with a deficiency of the rule of law, using the Convention to legitimise their unjustified actions at the international level. Further, with no minimum cap on the punishment, the State is at liberty to term even a minor offence as a serious crime, which could further accentuate the issues with the rule of law and could act as a tool to gain global legitimacy for stifling human rights such as the freedom of speech and expression.[29]

C. Ambiguity Regarding the Nature of Electronic Evidence

The scope of the Convention includes "collecting, obtaining, preserving and sharing of evidence in electronic form"[30] amongst the States. It is one of the core principles towards international cooperation in combating cybercrimes under the Convention.[31] Electronic evidence is,

[27] *Supra* note 6, at art. 2(h).
[28] *Supra* note 6, at art. 35(c).
[29] Universal Declaration of Human Rights art. 19, Dec. 10, 1948, G.A. Res. 217 (III) A ("Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.").
[30] *Supra* note 6, at art. 3(b).
[31] *Id.* at art. 35(1)(b).

 [ISSN 2581-5369]

therefore, important towards effectuating and implementing the Convention and consolidating its scope.

However, the scope of electronic evidence under the Convention is unclear. The Convention does not define what constitutes electronic evidence. This leaves room for ambiguity regarding the sharing of electronic information. The nature of electronic information such as a digital footprint is not certain, as to whether it would constitute electronic evidence for the purpose of the international convention and *ipso facto* for cross-border cooperation against cybercrimes.

Further, with the constant expansion of AI and its extensive use in almost every sector of the global trade and communication system, it is imperative to include its impact on cyber systems in general and its (mis)use for the purpose of cybercrimes in particular. However, the Convention does not reflect on these issues and thus leaves a huge gap within the cybersecurity framework and the desired objective to address cybercrimes.

D. The Exhaustive Scope of Personal Data Provisions

One of the major contentions for any cyber-oriented legal issue is the handling of personal data. The Cybercrime Convention provides for the States to take respective measures in the sharing of personal data for the purpose of addressing cybercrimes.[32] However, the scope of personal data is slender when perceived against the overall objective of the Convention.

Article 2(g) of the Convention defines personal data as information belonging to "an identified or identifiable natural person."[33] While, on the surface, the provision provides for dealing with the personal information of an individual with sensitivity, especially in relation to cross-border sharing of such information, the definition leaves room for ambiguity and possible misuse of the sharing provision under Article 36 of the Convention.

It is an established legal principle that the scope of a natural person is restricted only to individuals or humans. Any other entity, such as a company, is not a natural person. Such an exhaustive approach towards natural personhood establishes an issue within the new cybersecurity deliberation. With personal data being restricted to information pertaining to a natural person, corporate data is left out of the ambit of establishing a coherent protocol regarding the sharing of information.

This means that while States are to take precautions regarding the sharing of data related to an individual, no such caution is mandated against the sharing of corporate data. Such data could include the personal information of its customers, especially if the primary commercial base of

[32] *Supra* note 6, at art. 36.
[33] *Id.* at art. 2(g).

 [ISSN 2581-5369]

the company is individuals, such as in the case of companies offering services as a product. Thus, it bypasses the very framework which has been envisaged under the Convention to protect individual information.

This ultimately has the cascading effect of infringement of privacy and violation of the associated human right. The breach of privacy by the State could be legitimised under such provisions and can have detrimental effects, especially in cases where the State using this loophole has a history of undermining human rights.

E. Uncertainty on the Nature of Shared Data

Another issue which correlates to the nature of the data being shared amongst the States is its blurred definition (or a lack of it). The Convention treats data as an umbrella term without specifying the nature or categories of data. On one hand, such clubbing could seem to be productive to the objectives, as the sharing of any data with the potential to be misused can be restricted under the global Convention.

However, the flip side of the coin could also lead to any data being shared by a State, citing the lack of protection for the specific category of data under the Convention. For instance, the Convention is silent regarding whether encrypted data can be requested to be made available by the State from the data fiduciary in the case of a serious offence. Since the definition of serious offence is already blurred, a State can ask for private data of its citizens, which, again, could hamper the person's right to privacy. In the absence of a legal safeguard for the shared data, a State can use the provision to gain access to confidential information of its citizens, which could ultimately lead to the curbing of dissent and the conduct of other human rights violations.[34]

Further, the Convention is silent on the duration for which a State can retain data for the purpose of addressing cybercrime. With no limit on data retention, it can be used as a tool for targeted access to individuals under the garb of preventing cybercrimes, which, as already established, could be one of the measures to curb human rights and silence dissidents, particularly within the States falling on the lower end of the democratic spectrum.

F. Dearth of an Oversight Mechanism

The greatest structural deficit within the Cybercrime Convention can be said to be the lack of an oversight mechanism. The Convention is heavily reliant upon a bona fide pretext, whereby it is assumed that the signatory States would abide by the Articles of the Convention and forward

[34] Marshall Green, NORTH ATLANTIC POLICY FORUM, *Dangers of Ambiguity in the UN Cybercrime Treaty* (Aug. 4, 2025), https://www.napforum.org/policy-briefs/dangers-of-ambiguity-in-the-un-cybercrime-treaty.

 [ISSN 2581-5369]

its objectives. However, it has been observed that such bona fide assumptions under international law are seldom efficacious.

A lack of an oversight body or institution, and a void of general penal provisions for the infringing States or parties in a mutual data-sharing agreement, makes the Convention lose its value. It is reduced to a standard text, something that the States are obligated to follow but with no consequent effect of non-compliance. With no oversight, there is always an inherent risk of the States twisting the interpretation of the text and exploiting the aforementioned structural deficits of the Convention.

Furthermore, the Convention establishes certain basic principles and puts the burden on the domestic laws of the States. With the municipal laws doing the heavy lifting, the effectiveness of the Convention on an international scale seems uncertain. Unless a collated and unified approach towards implementation is undertaken at the municipal level by all the States, the Convention, as pointed out earlier, is reduced to a standard text and a bunch of guidelines.

It would not be wrong to state that, since the Convention is still in the early stages of its conception, these structural issues can be remedied. However, for such resolution and patching of these deficits, a collaborative approach is required, whereby the international body, that is, the United Nations, perceives the Convention as more than a mere document for addressing cybercrimes, and rather perceives it as a possible solution to tackle it at an international level.

IV. Conclusion and Suggestions

The United Nations Convention against Cybercrime, 2025 is a quest for universal action against cybercrimes, based on international cooperation and a smooth cross-border criminal investigation. Based on the premise that cybercrimes are ever-evolving and thereby require a proactive approach at the international scale, the Convention focuses on the substantive and procedural aspects of addressing them through international cooperation. However, the Convention has certain structural or tectonic issues rooted in the overall framework of the text.

These issues stem from the open-ended outline of the Convention, which, in its quest for being an agreeable framework, leaves several unplugged gaps that may render the Convention a mere text with no significant consensus on addressing cybercrimes. It therefore requires structural amendments, or at the least deliberations upon them, for streamlining cross-border cybercrime investigation.

Firstly, the parties to the Convention must move to set a definition of important aspects of the Convention, such as 'cybercrimes' and 'serious offences'. With a certain definition at hand, it

 [ISSN 2581-5369]

would be easier for parties to frame their municipal laws and, in fact, effectuate cooperation with other States regarding ICT activities that may fall within the nature and scope of cybercrimes. Further, with an exhaustive list of serious offences, either in the form of an Annexure to the Convention or through a mutual consensus within the definition part of the Convention, it would be easier for States and the international community as a whole to rapidly act on cyber threats and build a proactive mechanism to deal with definite cybercrimes.

Secondly, the Convention must incorporate the contemporary developments in cyberspace, especially related to criminal investigation. The scope of electronic evidence is ambiguous within the framework, and this hampers the overall process of handling cybercrimes. The Convention must elaborate upon the categories of electronic evidence and the circumstances whereby these shall be admissible in cross-border investigations. Further, the assistance of industry experts can be taken to ascertain the definitiveness of artificial intelligence (AI), especially where such AI tools have been used for committing cyber offences.

Thirdly, emphasis on data protection, especially data shared by individuals or States for the purpose of investigation, must be made. The personal data of citizens is significant, for it determines the protection of the right to privacy of the individual. Specific protocols must be put in place within the Convention which highlight the purposes for which such data could be collected by the State and the conditions under which such information could be shared with the other (investigating) country. Furthermore, the duration of retention of such personal data must be defined within the text, which could assist in a smooth investigative mechanism.

Lastly, the Convention cannot be an achievement without an oversight provision for its implementation. While trust in State capabilities for cooperation and resolution is a positive sign for the international legal order, history shows that it has seldom been achieved. Abandoning over-reliance on the municipal laws of the respective States, and rather establishing a mechanism whereby States are obligated to abide by the principles of the Convention, can be a better approach to handle cybercrime investigation at a global scale.

However, ultimately, the effectiveness of the Convention, like any other international deliberation, lies with the will of the States. The States need to establish a cooperative and accommodative stance to ensure that cybercrimes are effectively dealt with, and that the Convention presents itself as a definitive text on efficacious cybersecurity deliberation.

*****

 [ISSN 2581-5369]