

Finalization of the United Nations Convention on Combating Cybercrime Challenges and Opportunities of overcoming them

إنهاء العمل على اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية
التحديات وفرص تجاوزها

Boudermine Mohammed

Faculty of Law, Constantine 1 - Frères Mentouri University, Algeria
Laboratory of Contracts and Business Law

mohammed.boudermine@doc.umc.edu.dz

Date of submission:06/04/2025 Date of final acceptance:13/07/2025 /Date of publication :September

Abstract:

This study explores the contextual background surrounding the drafting of the United Nations Convention on Cybercrime, positioning it within the broader framework of international efforts to standardize and enhance mechanisms for the prevention and control of cybercrime and mitigate its repercussions. It identifies the principal challenges impeding international cooperation in this area and analyzes the key aspects of their impact. The paper also offers a conceptual perspective on emerging indicators of convergence that could contribute to overcoming these challenges. The research adopts two primary methodologies: the descriptive method to present the content and objectives of the Convention, and content analysis to examine the obstacles and opportunities for its ratification. The study concludes that despite significant challenges, sustained multilateral cooperation and emphasis on consensus-building facilitated the adoption of the Convention, paving the way for its future ratification.

Keywords: United Nations Convention; Cybercrime; Combat; Challenges; Opportunities.

ملخص:

تناقش هذه الدراسة سياقات وضع اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، كجهود دولية لتوحيد وتعزيز آليات منع ومكافحة هذه الجرائم ومعالجة تداعياتها، وتهدف إلى إبراز أهم المعوقات التي تواجه هذا التعاون، وتحليل أهم جوانب تأثيرها. كما تقدم رؤية لسمات التقارب، التي قد تسهم في تجاوز تلك المعوقات. يستند العمل إلى منهجين أساسيين: المنهج الوصفي لعرض مضمون الاتفاقية وأهم أهدافها ومنهج تحليل المضمون لتحليل أهم العقبات التي جعلت الوصول إلى إيجادها بطيئا، وكذا الفرص الممكنة للتصديق عليها. وتخلص الدراسة إلى نتائج أهمها أن عملية وضع الاتفاقية واجهت تحديات كبيرة، إلا أن الرغبة في التعاون متعدد الأطراف والتركيز على القضايا التوافقية حققا اعتمادها، مما يمهد للتصديق عليها مستقبلا.

الكلمات المفتاحية: اتفاقية الأمم المتحدة؛ الجريمة السيبرانية؛ المكافحة؛ التحديات؛ الفرص.

Auteur correspondant : Boudermine Mohamme

Introduction:

In recent decades, the world has witnessed significant advancements in information and communication technologies, giving rise to a new form of crime—cybercrime. This phenomenon has emerged as a major challenge for the international community due to its transnational nature and its threat to global cybersecurity. In light of the escalating risks posed by cybercrime and the increasing sophistication of its methods, the need for a coordinated international response has become more urgent than ever.

Although some previous international efforts have resulted in regional and bilateral agreements, the absence of a comprehensive international legal framework has remained a substantial barrier to effectively addressing cybercrime. In response, the United Nations initiated efforts to develop an international legal instrument aimed at unifying efforts and enhancing global cooperation in this field.

The significance of this study lies in its examination of the contexts surrounding the formation of the Convention and in raising awareness of the legal issues it entails. The research aims to analyze the key obstacles hindering its advancement, while also highlighting certain indicators of progress that suggest the potential for overcoming these barriers and paving the way toward ratification.

Accordingly, this study addresses the central research question:

To what extent have current international cooperation efforts been effective in overcoming challenges and advancing toward a comprehensive international convention to combat cybercrime?

To achieve the objectives of the study and to answer this question, three methodological approaches were adopted:

Descriptive method – to present the content and main objectives of the Convention;
Analytical method – to examine the primary obstacles to achieving consensus on the Convention's scope and provisions, as well as to understand the reasons behind the slower-than-expected progress. This analysis also considers certain signs of convergence that suggest the potential for successful adoption; Historical method – to provide a background on the earlier negotiations that laid the groundwork for the current draft Convention.

The subject is thus explored through two main sections:

Section One: International cooperation in the development of the United Nations Convention against Cybercrime;

Section Two: Indicators of progress in the Convention and efforts to overcome key obstacles.

Section I: International Cooperation in the Development of the United Nations Convention against Cybercrime

With the rapid expansion of digital technologies and the increasing threat posed by cybercrime globally, the international community has widely acknowledged the urgent need for a comprehensive legal framework to combat this emerging form of crime. Cybercrime has evolved into a transnational security issue that demands robust international cooperation. This section examines the progression of global efforts leading to the formulation of the United Nations Convention against Cybercrime.

A) Progress of international cooperation in the elaboration of the Convention

The necessity for an international convention dedicated to combating cybercrime has been broadly recognized, given the growing urgency of the issue and the inadequacy of fragmented national responses. After sustained international deliberations, efforts culminated in the drafting of a convention under the auspices of the United Nations.

1 - Elaboration of the Convention within the United Nations

The concept of establishing an international convention on cybercrime gradually took shape within the United Nations' broader efforts to regulate transnational crime. As cybercrime emerged as a complex and evolving threat to national and international security, the need for coordinated international action became increasingly apparent.

Between the Seventh United Nations Congress on the Prevention of Crime and the Treatment of Offenders (Milan, 1985) and the Eighth Congress (Havana, 1990), a committee of experts was tasked with studying the protection of automated data processing systems and the growing phenomenon of computer-related offenses. The committee produced a comprehensive report on the subject, which was presented and debated during the 1990 Havana Congress.¹

The Congress resolution recommended that States adopt measures to prevent and combat cyber-related offenses.² Recommendations that were subsequently reaffirmed during the 1994 Congress in Riode Janeiro and the 1995 Congress in Cairo.³

In 2010, during the United Nations Congress on Crime Prevention and Criminal Justice held in Salvador, Brazil, the issue of cybercrime was once again brought to the forefront. The Commission on Crime Prevention and Criminal Justice, in accordance with item 42 of the Congress report, called upon Member States and the private sector to collaborate on multiple fronts to develop both national and international legal responses to cybercrime.⁴

Further momentum was generated during the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha, Qatar, in April 2015. At the third workshop, held under item 5 of the provisional agenda—“Strengthening Crime Prevention and Criminal Justice Responses to Evolving Forms of Cybercrime”—the Congress reaffirmed the urgent need for substantive international cooperation and practical measures to combat cybercrime effectively. In response to the growing complexity and scale of these threats, the United Nations developed and released a series of general guidance manuals—regularly updated—to raise awareness and provide clarity regarding the nature, scope, and implications of cybercrime”.⁵

The topic remained a priority for the United Nations and its Member States⁶ until 2017, when the first draft of a proposed international convention on cybercrime was officially introduced, marking a significant milestone in global efforts to establish a unified legal response to this evolving threat.

2 - Emergence of an International Convention

The development of the United Nations Convention against Cybercrime marks a pivotal moment in the evolution of international cooperation to confront the growing challenges posed by digital technologies.

The process began in October 2017, when the Russian Federation presented a preliminary draft of a proposed international convention during the Third Committee meeting of the United

Nations General Assembly. Titled the “United Nations Convention on Cooperation in Combating Cybercrime,” the draft aimed to strengthen inter-State cooperation. However, it also prompted debate over the necessity of a new convention, particularly given the existence of the 2001 Budapest Convention.

By 2019, the initiative had gained traction, culminating in the adoption of Resolution A/RES/74/247 by the General Assembly in November.⁷ The resolution laid the foundation for formal negotiations to establish a comprehensive legal framework addressing cybercrime. It was supported by 88 States, opposed by 58 (including the United States and the European Union), and 34 States abstained. This marked a significant milestone in the establishment of a negotiation platform for the Convention.

In December 2019, a special committee was established under the Third Committee to draft the Convention, with inclusive participation extended to all Member States, observer States, and non-governmental organisations. Organisational sessions began in May 2021, during which a timetable for negotiation meetings was agreed upon.⁸

The first formal negotiation sessions took place in early 2022, revealing sharp divisions among Member States. Notably, disagreements emerged over the scope and definition of cybercrime. Some countries, including Russia and China, advocated for a broad definition encompassing “content-related crimes” such as disinformation and incitement to terrorism. In contrast, Western States favoured a more technical and narrowly defined scope, focusing on offences like hacking and data theft.

In 2023, a series of consultative meetings were held to discuss a preliminary draft of the Convention. These sessions explored ways to strike a balance between enhancing cybersecurity and upholding human rights. Broad participation from civil society organisations, including Human Rights Watch, helped highlight the importance of safeguarding freedoms, particularly freedom of expression.⁹

On 9 August 2024, the draft Convention was approved without a vote during a session of the Supreme Advisory Committee, held in New York, and endorsed by the Third Committee of the General Assembly. This marked a key advancement in the negotiation process, culminating in the Convention’s unanimous adoption on 24 December 2024. The Convention is set to be opened for signature at an official ceremony hosted by Viet Nam in 2025.¹⁰ and will remain open for signature at the United Nations Headquarters in New York until 31 December 2026.¹¹

The United Nations Secretariat, through the Secretary-General, welcomed the adoption of the Convention, praising it as a major achievement and a testament to collective international will. The Convention, he noted, stands as a central United Nations mechanism for fostering international cooperation in the fight against cybercrime, while ensuring the protection of fundamental human rights in the digital sphere. He called on all Member States to support its effective implementation through collaboration with relevant stakeholders.¹²

Similarly, the United Nations Office on Drugs and Crime (UNODC), through its Executive Director, described the Convention’s adoption as a substantial step forward in enhancing global capacities to combat cybercrime and strengthen multilateral cooperation.¹³ The UNODC has been designated the lead body for overseeing the Convention’s implementation, serving as the secretariat of the committee responsible for negotiating the supplementary protocol.¹⁴

Algeria played a crucial diplomatic role throughout the negotiation process. Since its election to chair the committee in May 2021, Algerian diplomacy—led by Ambassador Fawzia

Mubarakī—spearheaded efforts to bridge divergent viewpoints among Member States. Over the course of eight rounds of negotiations held under complex geopolitical conditions, Algeria’s leadership contributed to forging consensus and ultimately securing unanimous approval of the final text. While certain contested provisions prompted requests for a vote, these did not prevent their inclusion in the adopted Convention.¹⁵

B) Main Areas of the Convention

The Convention establishes a comprehensive framework of provisions governing cybercrime, addressing multiple areas aimed at enhancing international cooperation among States and achieving fundamental objectives.

1 - Content of the Convention

The Convention is composed of nine chapters, each addressing distinct aspects of the international response to cybercrime. The general provisions set out the Convention’s objectives, key definitions, scope of application, and foundational principles. These include the reaffirmation of State sovereignty, adherence to the rule of law, and the protection of human rights as integral to the Convention’s implementation.

Chapter two focuses on the criminalisation of specific offences. It includes provisions targeting the online sexual exploitation of children, such as soliciting or coercing minors into sexual acts through digital platforms.¹⁶ The chapter also covers core cybercrime offences, including illegal access to systems (hacking), manipulation or destruction of data, and various forms of online fraud.¹⁷ The non-consensual distribution of intimate images is likewise addressed. Moreover, it introduces mechanisms for holding legal entities accountable, while simultaneously safeguarding the procedural rights of individuals facing prosecution.¹⁸

Recognising the inherently transnational dimension of cybercrime, the Convention establishes jurisdictional rules aimed at closing legal loopholes that offenders might exploit. States may exercise jurisdiction over crimes committed within their territory, against their nationals, or by their nationals abroad. Additionally, where extradition is not possible, States are empowered to prosecute offences committed by individuals within their jurisdiction. In scenarios involving multiple jurisdictions, States are encouraged to consult with one another to determine the most appropriate response.¹⁹

To enhance international cooperation, the Convention includes detailed provisions on extradition, mutual legal assistance, and the sharing of digital evidence. While encouraging collaboration, it also allows States to withhold cooperation on specific grounds—such as violations of data protection standards, concerns related to non-discrimination, or matters affecting sovereignty and public order.

The chapter on procedural measures grants States the authority to conduct investigative actions such as tracing, preserving, and confiscating electronic data. It also provides for the interception of communications, subject to strict safeguards. These include judicial oversight, clear legal justification, the preservation of the integrity of digital evidence, and full respect for human rights and civil liberties.²⁰

The Convention further establishes a global framework to support investigations, prosecutions, and various judicial proceedings, including asset recovery, extradition, joint investigations, and the facilitation of access to electronic evidence. This is achieved through

measures for data preservation, access, and interception, coordinated via a network of contact points operating continuously, 24 hours a day, seven days a week.²¹

The chapter on technical assistance and information exchange provides for enhancing States' capacities in the enforcement process, with particular emphasis on developing countries. It underscores the exchange of necessary tools for detecting cybercrimes, as well as expertise in handling electronic evidence, forensic analysis, and tracing the proceeds of such crimes. Furthermore, the chapter promotes partnerships among governments, non-governmental organisations, academia, financial institutions, and the private sector to effectively address the evolving and expanding threats posed by cybercrime.²²

While the chapter on the implementation mechanism recommends the establishment of a Conference of States Parties to oversee the implementation of the Convention. Through this framework, States Parties are required to submit reports on the measures undertaken to implement the Convention, enabling periodic reviews and the formulation of recommendations to enhance effectiveness. The Conference further facilitates the exchange of information on legal, political, and technological advancements in this field and has the authority to adopt complementary protocols or strengthen cooperation with relevant stakeholders, including intergovernmental and non-governmental organisations, as well as the private sector. The inaugural Conference will take place within the first year of the Convention's entry into force, with the United Nations Office on Drugs and Crime (UNODC) serving as its secretariat.²³

The chapter on final provisions outlines the procedures governing accession to or withdrawal from the Convention, as well as the provisions related to its entry into force and legal effects. It further affirms that any disputes concerning the interpretation or implementation of the Convention shall be resolved through negotiations or other peaceful means of international dispute settlement.²⁴

In addition, the chapter provides for the possibility of amending the Convention or adopting supplementary protocols. It also stipulates that States may withdraw from the Convention by submitting written notification, which shall take effect one year after its submission.²⁵

2 - Objectives of the Convention

The Convention pursues multiple objectives, with particular emphasis on key areas such as international cooperation, capacity-building, prevention, victim support, and child protection.

2.1 Promotion of International Cooperation

In line with the general principles of cooperation, the Convention designates investigations, legal proceedings, and prosecution as the primary areas of international collaboration,²⁶ this encompasses a range of law enforcement measures, including the freezing, seizure, confiscation, and return of the proceeds of crime, as well as all procedures related to the collection and exchange of electronic evidence. While the Convention underscores the importance of international cooperation, it mandates that States transfer personal data in compliance with their national laws or applicable data protection regulations under international law. Furthermore, where a mechanism for the transfer of personal data to a third party is established, prior authorisation from the transferring State of origin is required.²⁷

With regard to extradition, the Convention stipulates that the act in question must constitute an offence under the national laws of both States concerned.²⁸ A State Party may refuse extradition if there are substantial grounds to believe that the request is intended to prosecute a person on racial

grounds.²⁹ In cases involving multiple jurisdictions, States may, by mutual agreement, transfer criminal proceedings to ensure effective prosecution.³⁰

To facilitate and expedite the processing of mutual legal assistance (MLA) requests, each Party shall designate a central authority responsible for receiving and executing such requests, without prejudice to existing mechanisms. Additionally, a State may exercise its discretion to refuse MLA on the grounds of sovereignty, national security, or public order.³¹

The Convention mandates Parties to establish a continuous 24/7 network to provide immediate assistance for investigations and prosecutions, as well as to facilitate measures such as technical advice, the preservation of stored electronic data, the collection of evidence, and related activities.³² Furthermore, it encourages Parties to conclude bilateral or multilateral agreements or to use the Convention as a common framework for such cooperation.³³

2.2 Capacity Building

The Convention provides a structured framework for the exchange of expertise, technical assistance, and technology transfer between developed and developing States. This initiative aims to support the development of strategic policies and legislative frameworks by leveraging technical resources. Additionally, it promotes the exchange of modern law enforcement strategies and advanced technological tools, ensuring that all States have access to the necessary means to combat cybercrime effectively.

In addition to technical assistance, capacity-building measures encompass the development of human resources. The Convention emphasizes the importance of equipping personnel with essential skills, such as language training, drafting and processing mutual legal assistance requests, and implementing methods to protect victims and witnesses. To ensure the sustainability of efforts to assist developing countries, the Convention encourages Member States to provide financial support through voluntary contributions.³⁴

2.3 Prevention

Prevention is a fundamental priority, and to this end, the Convention underscores that cooperation and capacity-building should not be confined solely to addressing crimes but should also aim to prevent their occurrence from the outset. Accordingly, the Convention highlights the importance of harmonising policies and best practices across jurisdictions, with the active involvement of multiple stakeholders, to ensure the implementation of preventive measures that effectively address both the prevention and suppression of offences criminalised under the Convention.³⁵

The Convention also encourages the role of service providers in strengthening the security of their customers' products, services, and data within Member States. Furthermore, it recognises the pivotal contribution of the legitimate activities of security researchers in enhancing overall cybersecurity.³⁶

Notably, the Convention calls for the strengthening of measures aimed at preventing individuals from engaging in criminal activities and, where such engagement occurs, encourages States to facilitate their reintegration into society.³⁷ The Convention does not establish a specific mechanism for implementing these measures, as they are understood to fall within the scope of national prevention and rehabilitation policies. Consequently, States will need to assess their national laws and strategies to ensure their alignment with the evolving nature of these crimes.

2.4 Victims support

As part of its protective framework, the Convention establishes measures to assist and safeguard victims of cybercrime, particularly those affected by violent offences. It calls upon States Parties to develop initiatives that ensure access to compensation and restitution proportionate to the gravity of the crime. For instance, the Convention highlights the importance of providing medical and psychological care for victims of online child sexual exploitation and individuals subjected to the non-consensual dissemination of intimate images, while considering the specific needs of victims based on their age and circumstances.³⁸

2.5 Protection of children

The Convention emphasises the need to strengthen cooperation among Member States to combat cybercrime, particularly sexual offences against children. It mandates Parties to adopt national legislation and other necessary measures to criminalise all forms of online child sexual abuse. This includes the production, possession, sale, dissemination, management, or financing of child sexual abuse material, as well as any form of exploitation involving such material stored or transmitted through information and communications technology (ICT) systems³⁹. The Convention calls for the adoption of appropriate legislation and measures to criminalise all acts involving the solicitation or inducement of children online for the purpose of committing a sexual offence.⁴⁰

The Convention notably expands the scope of criminalisation to encompass all acts that may impact children, thereby extending legal responsibility to a broader range of actors. This includes service providers, who may be held accountable as intermediaries in the transmission of such material, potentially subjecting them to criminal liability.

Section II: Progress in the Convention and Overcoming Obstacles

The Member States of the United Nations have reached a significant milestone by agreeing on the first draft of the Organisation's international convention against cybercrime. While this achievement marks a crucial step forward, it remains subject to challenges that continue to be debated among the negotiating States (the Parties). In this context, this section examines the obstacles encountered in finalising the Convention and the points of convergence that contribute to advancing consensus towards its ratification.

A) Obstacles to the Progress of the Convention

The adoption of the United Nations Convention against Cybercrime has faced significant challenges, primarily due to differing international perspectives on its provisions, reflecting each Party's distinct priorities. Additionally, the Convention has been met with widespread concerns and criticism on several key issues.

1 - Divergence of International Perspectives

In May 2021, the United Nations General Assembly adopted a regulatory resolution to initiate the drafting of a treaty aimed at combating cybercrime⁴¹. The negotiations were marked by sharp disagreements among Member States regarding the working mechanisms. Russia viewed the Convention as a means to bridge the technological gap between developed and developing countries and potentially as an alternative to the Budapest Convention on Cybercrime. It proposed that negotiations take place in New York under the auspices of the General Assembly, where decisions are adopted by an absolute majority vote. In contrast, Western countries, supported by Latin American States, advocated for negotiations to be conducted in Vienna within the Commission on

Crime Prevention and Criminal Justice (CCPCJ), adhering to a consensus-based decision-making mechanism.⁴²

During the first meeting, held from 10 to 12 May 2021, States failed to reach an agreement. Russia advocated for the inclusion of a comprehensive list of additional crimes, such as terrorism, extremism, and online drug trafficking, among others, and proposed the development of an additional protocol to the Convention should these crimes not be incorporated. In contrast, the United States, before the commencement of the drafting process, suggested that each issue be addressed separately within the Convention to ensure a more focused approach⁴³ It further urged Member States not to classify traditional crimes as cybercrimes solely on the basis that computer systems were used as a means to perpetrate them.⁴⁴

During the final informal discussions on the Convention's scope, Canada, representing fifty States and the European Union, proposed to the Ad Hoc Committee on Cybercrime (AHC) that no provision should be interpreted as enabling the suppression of freedom of expression, conscience,

opinion, belief, peaceful assembly, or association, nor as permitting discrimination or persecution based on individual characteristics. This proposal sought to establish common ground, build trust, and strengthen international cooperation while ensuring the Convention aligns with Member States' obligations under the UN Charter and other relevant international instruments.⁴⁵

India also made additional contributions, proposing that the negligent protection of personal data or information be classified as a criminal offence, including the failure of data-owning institutions to maintain and implement adequate security measures. Furthermore, India incorporated the concept of cyberterrorism into its draft and advocated for a data-oriented jurisdictional approach rather than a territorially based jurisdiction.⁴⁶

Another area of contention was the balance between the scope of the Convention and the obligation to cooperate, particularly in determining whether this obligation should be restricted to the offences explicitly covered by the Convention or extend to all types of crimes, while ensuring full adherence to human rights principles.⁴⁷

Despite the unanimous adoption of the final resolution, some States characterised it as "fragile, hasty, and uncoordinated", citing the persistence of fundamental disagreements among Member States, which could signal a complex and challenging path for future negotiations⁴⁸. Concerns were further exacerbated by the fact that the resolution was introduced abruptly following informal meetings, raising doubts about the inclusivity and transparency of the process.

2 - Concerns and Criticisms

The Convention has faced concerns and criticisms from States, human rights organisations, and privacy advocates due to the absence of explicit safeguards to regulate intrusive surveillance, as well as the lack of fundamental human rights principles. This critical issue has implications for the overall scope of criminalisation and the potential for future agreements between States.⁴⁹

While discussions have largely centered on offences such as child sexual abuse material and the sharing of images produced by children, these provisions may have broader human rights implications. The call for an additional protocol to criminalize further acts listed in paragraph 5 of the draft resolution—provisions that themselves lack procedural safeguards—suggests that the Convention remains incomplete in its current form. Moreover, the potential inclusion of offences like terrorism and extremism in the future, which have historically been used to justify restrictions on freedom of expression, raises further human rights concerns.

Similarly, the framework for international cooperation remains a point of contention, particularly in relation to Articles 45 and 46, which faced objections during negotiations. A proposal was made to replace the term "shall" with "may" to grant Parties greater discretion in providing mutual legal assistance for the collection of real-time traffic data. This measure is particularly sensitive, as it could impose an obligation on States to cooperate in data exchange, potentially conflicting with their duty to uphold privacy rights.⁵⁰

On the other hand, the confidentiality requirements imposed by the Convention have been criticised for undermining transparency and due process by granting governments unrestricted powers over censorship while preventing individuals from being informed of or objecting to surveillance measures. Such provisions could be exploited by authoritarian governments to legitimise censorship practices and suppress political dissent, thereby threatening fundamental rights, particularly the right to privacy and freedom of expression.

The provisions on cross-border data sharing and law enforcement cooperation agreements have raised concerns that, without strong safeguards, data exchanges between States could increase the risk of personal information misuse. These risks are particularly alarming in cases of judicial abuse and due process violations.

Moreover, the Convention's broad restrictive measures could inadvertently criminalize the legitimate work of security researchers conducting forensic cybersecurity investigations⁵¹. This could hinder critical research, ultimately weakening efforts to enhance cybersecurity and protect privacy—both of which are core objectives of the Convention.

B) Manifestations of overcoming contentious issues

Despite the numerous unresolved issues⁵² and the concerns that have complicated the adoption of a comprehensive convention against cybercrime, there are promising prospects for overcoming these challenges. The progress achieved in developing the Convention suggests a pathway toward resolution. For instance, while consensus has yet to be reached on paragraph 2 of Article 7 (unauthorized access) and Article 8 (unauthorized interception), the Convention allows States the flexibility to introduce specific requirements, adapting provisions to their legal frameworks.

1 - Willingness of Parties to Cooperate

Since the adoption of Resolution 74/247 by the United Nations General Assembly in December 2019, which established a Special Committee to negotiate and draft the Convention, States have shown a willingness to engage in the process despite their differing perspectives. Many actively participated in organizational meetings and follow-up consultations, including States Parties to the Budapest Convention. These States, despite existing challenges, saw their involvement as a commitment to multilateralism and an opportunity to create a cooperative framework with countries unable to accede to the Budapest Convention due to political considerations or non-compliance with its requirements.⁵³

Additionally, the inclusion of non-governmental stakeholders in the negotiations, along with their limited right to intervene, marked a positive step, given the value of their contributions. These stakeholders underscored the Convention's significance as a legal mechanism for cybercrime investigations, particularly in cases involving cross-border jurisdiction. While European States Parties to the Budapest Convention benefit from established cooperation frameworks, many other States lack equivalent standards—a gap the Convention seeks to bridge.⁵⁴

2 - Manifestation of Convergence Factors and Overcoming Contentious Issues

In addition to its substantive positive aspects, the Convention contributes to the maintenance of international peace and security through the various advantages it offers as a United Nations framework for cooperation in criminal investigations, the collection of electronic evidence, access to and exchange of data, and prosecution. Furthermore, it enhances responses to victims' needs and strengthens preventive mechanisms⁵⁵. Notably, the factors promoting convergence of State interests towards the Convention outweigh adherence to contentious issues, fostering broader acceptance and reinforcing its role as a comprehensive multilateral instrument.

Progress in international negotiations resulting from flexible positions and stakeholder engagement has added a practical dimension to the solutions put forward and contributed to a partial consensus that is a first step towards a broader consensus.

Previous successful experiences in international cooperation combat organized crime have contributed to the possibility of making use of them to facilitate the adoption of a cybercrime-like agreement. The growing economic and political implications of cyberattacks also put pressure on States to accelerate the search for common solutions.

A universal instrument containing human rights guarantees - and, if considered inadequate by the parties - developed incrementally, is likely to add significant value to international cooperation.⁵⁶

The basic concepts and definitions adopted in the draft convention, such as the list of crimes, procedural powers, and specific provisions on international cooperation, are consistent with those contained in the Budapest Convention, albeit with different names for political reasons, which avoids complicating the negotiation process and could be positively reflected in the possibility for the parties to the Budapest Convention to vote on the future United Nations convention.⁵⁷

On the other hand, States want to see some sort of result from their intensive efforts over the course of three years, or at least not be seen as trying to derail or damage the process⁵⁸. This is reflected in the consensus on amendments to each part of the Convention, particularly in the field of human rights, which was proposed by the President.⁵⁹

Several provisions of the United Nations Cybercrime Convention were also adopted through a referendum, including full articles and specific paragraphs that regulate the criminalisation of certain acts, reflecting varying levels of acceptance among the drafters of the Convention.

What unifies all these elements is the adoption of the final text of the Convention by the General Assembly on 24 December 2024, which can be interpreted as an expression of the collective will of States and their general acceptance of the agreement. The remaining challenge is to resolve the outstanding disputed issues. Therefore, it appears advisable to accept the treaty with some reservations, as rejecting it may pave the way for "digital authoritarianism" and undermine efforts to achieve cybersecurity.⁶⁰

The Convention represents a rare opportunity to enhance cybersecurity, promote international cooperation, and bridge regulatory gaps between nations. However, if it deepens divisions and its adoption sparks widespread concerns, the final decision will rest on the official ratification ceremony hosted by Vietnam this year. Should it secure 40 votes, the Convention will enter into force within 90 days, as stipulated in Article 65, marking the first legally binding multilateral United Nations Convention against Cybercrime. Otherwise, its adoption will be postponed until full consensus is reached on unresolved issues.

Nevertheless, ensuring the Convention's effectiveness requires ongoing monitoring of its implementation. If audits reveal that its enforcement compromises human rights and data protection, States should reconsider their participation or explore alternative frameworks, such as the Budapest Convention, which remains in effect as a fallback option.

Conclusion:

This study has demonstrated that the adoption of the United Nations Convention on Cybercrime by the General Assembly marks the culmination of extensive, collaborative efforts and represents a significant milestone in enhancing international cooperation to address the mounting challenges in cyberspace.

Although the journey to this achievement has been marked by numerous hurdles, the gradual progress made reflects a growing momentum toward consensus and eventual ratification.

Results:

- Inclusive cooperation, involving stakeholders from both the public and private sectors alongside governments, played a vital role in enriching the negotiation process and ensuring the Convention's eventual adoption.
- The pressing need and strong political will of States to combat cybercrime reinforced their commitment to establishing a common legal framework—albeit a relatively balanced one—that accommodates differing national interests while addressing the risks of inaction.
- Despite the complex challenges encountered throughout the drafting process, several factors enabled a convergence of views among States, paving the way for broader international consensus.
- The Convention sets out a binding international legal framework that fosters cross-border cooperation and contributes to strengthening global cybersecurity efforts.
- The ultimate success of the Convention will depend on States' effective implementation of its provisions and their ongoing commitment to upholding human rights and data protection standards. Should implementation prove difficult, States may need to reassess their engagement with the Convention or explore alternative instruments, such as the Budapest Convention, which continues to serve as an existing international standard.

Suggestions:

- Enhance coordination and cooperation: States should promote coordinated efforts in the implementation of the Convention by facilitating the exchange of information, best practices, and experiences. This will help ensure the equitable and consistent application of its provisions across jurisdictions.
- Conduct regular reviews: Periodic assessments should be undertaken to evaluate the Convention's alignment with evolving technological landscapes and emerging cyber threats. These reviews should aim to maintain a balanced approach between prevention, enforcement, the protection of personal data, and the respect for human rights.
- Broaden stakeholder engagement: It is crucial to expand the involvement of all relevant

stakeholders—including government entities, the private sector, and civil society organisations—to ensure that the Convention is implemented in a practical, inclusive, and balanced manner. This approach will strengthen both its effectiveness and its legitimacy on the international stage.

1- United Nations (1990), "Crime Prevention and Criminal Justice in the Context of Development: Realities and Perspectives of International Co-operation", Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, A/CONF.144/5, P03.

2- Ibid, P31-36.

3- Council of Europe (1995), Report on the International Conference on Population and Development (Cairo, 5-13 September 1994): Follow-up by the Council of Europe and its Member States, Doc. 7208, Strasbourg : Council of Europe. PP 02–14.

4- United Nations (2010), Twelfth United Nations Congress on Crime Prevention and Criminal Justice: Fact Sheet 8 – Too Little International Cooperation Allows Cybercriminals an Easy Getaway, Salvador, Brazil: United Nations. PP18.

5- Nations, U (2015), Strengthening Crime Prevention and Criminal Justice Responses to Evolving Forms of Crime, Such as Cybercrime and Trafficking in Cultural Property, Including Lessons Learned and International Cooperation, A/CONF.222/12, Qatar: United Nations. PP02-14.

6- United Nations (2024), 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, A/RES/79/243, New York: United Nations. P04.

7- Nations, U (2019), Countering the Use of Information and Communications Technologies for Criminal Purposes, A/RES/74/247, United Nations.

8- Gullo Karen, a. Katitza (2023), UN Cybercrime Draft Treaty Timeline, Electronic Frontier Foundation, Visited: 27/01/2025, <https://www.eff.org/deeplinks/2023/04/un-cybercrime-treaty-timeline/>

9- Ibid.

10- General Assembly (2024), adopts landmark convention on cybercrime, United Nations Libya, New York, Visited: 30/01/2024, <https://libya.un.org/en/286533-un-general-assembly-adopts-landmark-convention-cybercrime>

11- See Article 64, Paragraph 01, (2024), draft resolution:Countering the Use of Information and Communications Technologies for Criminal Purpose- A/79/460, Strengthening International Cooperation for Combating Certain, United Nations.

12- Vision (2024), The United Nations Adopts a Historic Convention Related to Cybercrime, Visited: 15/01/2025, <https://alroya.om/post/357804/>

13- Ibid.

14- Youm7 (2024), The United Nations Adopts a Convention Against Cybercrime, Youm7, Visited: 20/01/2025, <https://www.youm7.com/story/2024/>

15- Algerian (2024), Adoption of a Convention Against Cybercrime... Another Gain in the Record of Algerian Diplomacy Efforts Led by the President of the Republic, Algerian Radio, Visited: 10/01//2025, <http://news.radioalgerie.dz/ar/node/50035/>

16- See Article 11-12, draft resolution- A/79/460, op.cit.

17- Ibid, Article 16.

18- Ibid, Article 21.

19- Ibid, Paragraph 04-05, Article 22.

20- Ibid, Article 24.

21- Ibid, Article 41.

22- Ibid, Article 54.

23- Ibid, Article 57.

24- Ibid, Article 63.

25- Ibid, Article 62-67.

26- Ibid, Article 35.

27- Ibid, Paragraph 03, Article 36.

28- Ibid, Paragraph 01, Article 37.

29- Ibid, Paragraph 15.

30- Ibid, Article 39.

31- Ibid, Paragraph 12-21, Article 40.

32- Ibid, Article 41.

33- Ibid, Paragraph 02, Article 47.

34- Ibid, Article 54.

35- Ibid, Paragraph 01-03, Article 35.

36- Ibid, Paragraph 03, Article 53.

37- Ibid.

38- Ibid, Article 34.

39- Ibid, Article 14.

40- Ibid, Article 15.

41- Council, Security (2024), Security Council Report, Meeting, No. S/PV.9779, United Nations, New York, p02.

42- Walker, Summer (2021), UN Cybercrime Resolution Stumbles Out of the Gate, Global Initiative, Visited: 2/01/2025, <https://globalinitiative.net/analysis/un-cybercrime-resolution/>

43- Office. Drugs and Crime (2022), First Session of the Ad Hoc Committee, United Nations, P01, Visited: 30/01/2025, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html/

44- Ibid, p05.

45- Office. Drugs and Crime (2024), Proposal by Canada on Behalf of a Group of 50 States and the European Union to the Ad Hoc Committee on Cybercrime (AHC) to Further Define the Scope of the Draft Convention, United Nations, P01.

46- Assembly, General (2022), Second Session of the Ad Hoc Committee, A/AC.291/9/Add.3, United Nations, pp05-14.

47- Anastasiya, Kazakova (2024), UN Cybercrime Convention: Will States Give in Disagreements for the Sake of a Global Common Threat?, Geneva Internet Platform, Visited: 02/01/2025, <https://www.dig.watch/updates/un-cybercrime-convention-will-states-give-in-disagreements-for-the-sake-of-a-global-common-threat/>

48- Walker, Summer, op.cit.

49- Rajeesh, Kumar (2025), United Nations Cybercrime Convention : A Milestone in Digital Governance?, Institute for Defense Studies and Analyses, Visited: 04/02/2025, https://www.idsa.in/publisher/issue-brief/united-nations-cybercrime-convention-a-milestone-in-digital-governance/#footnoteref40_iycl6nr/

50- Crime, O. T (2024), Cyber Convention Check-in, Global Initiative Against Transnational Organized Crime, Visited: 26/02/2025, <https://globalinitiative.net/announcements/cyber-convention-check-in/>

51- Greg, Otto (2024), HackerOne Urges U.S. to Advocate for Research Protections in UN Cybercrime Treaty, Cyberscoop, Visited: 26/01/2025, <https://cyberscoop.com/un-cybercrime-treaty-hackerone-letter-security-research/>

52- (E.P.). for example, no agreement has yet been reached on Article 7, paragraph 2, concerning unlawful access, or Article 8, regarding unlawful interception, both of which allow States to introduce specific requirements that may vary from one article to another.

53- Anastasiya, Kazakova (2024), op.cit.

54- Ibid.

55- Office. Drugs and Crime (2024), Five Reasons Why the New Cybercrime Convention Matters, Visited: 02/02/2025, <https://www.unodc.org/unodc/frontpage/2024/December/five-reasons-why-the-new-cybercrime-convention-matters.html>

⁵⁶- Anastasiya, Kazakova (2024), op.cit.

⁵⁷- Ibid.

⁵⁸- Nations, U Nd (2024), Global Cybercrime Treaty: A Delicate Balance between Security and Human Rights, Law and Crime Prevention, United Nations, Visited: 02/02/2025, <https://news.un.org/en/interview/2024/02/1146772/>

⁵⁹- Office. Drugs and Crime (2024), Explanatory Notes on the Updated Draft Text of the Convention and the Revised Draft General Assembly Resolution, United Nations, PP03-06.

⁶⁰- Jakobi Anja P, Lena Herbst (2024), Between a Rock and a Hard Place: The UN Cybercrime Convention, The Peace Research Institute, Frankfurt, P04.

Bibliography :

A- International Legal and Institutional Documents

- United Nations (1990), "Crime Prevention and Criminal Justice in the Context of Development: Realities and Perspectives of International Co-operation", Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, A/CONF.144/5, P03.
- Council of Europe (1995), Report on the International Conference on Population and Development (Cairo, 5-13 September 1994): Follow-up by the Council of Europe and its Member States, Doc. 7208, Strasbourg: Council of Europe. PP 02–14.
- United Nations (2010), Twelfth United Nations Congress on Crime Prevention and Criminal Justice: Fact Sheet 8 – Too Little International Cooperation Allows Cybercriminals an Easy Getaway, Salvador, Brazil: United Nations, P18.
- Nations, U (2015), Strengthening Crime Prevention and Criminal Justice Responses to Evolving Forms of Crime, Such as Cybercrime and Trafficking in Cultural Property, Including Lessons Learned and International Cooperation, A/CONF.222/12, Qatar: United Nations. PP02-14.
- United Nations (2024), 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, A/RES/79/243, New York: United Nations. P04.
- Nations, U (2019), Countering the Use of Information and Communications Technologies for Criminal Purposes, A/RES/74/247, United Nations.
- United Nations (2024), draft resolution:Countering the Use of Information and Communications Technologies for Criminal Purpose- A/79/460, Strengthening International Cooperation for Combating Certain, United Nations.
- Council, Security (2024), Security Council Report, Meeting, No. S/PV.9779, United Nations, New York, p02.
- Office. Drugs and Crime (2022), First Session of the Ad Hoc Committee, United Nations, P01, Visited:30/01/2025, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html/

- Office. Drugs and Crime (2024), Proposal by Canada on Behalf of a Group of 50 States and the European Union to the Ad Hoc Committee on Cybercrime (AHC) to Further Define the Scope of the Draft Convention, United Nations, P01.
- Assembly, General (2022), Second Session of the Ad Hoc Committee, A/AC.291/9/Add.3, United Nations, pp05-14.
- Office. Drugs and Crime (2024), Explanatory Notes on the Updated Draft Text of the Convention and the Revised Draft General Assembly Resolution, United Nations, PP03-06.
- UNODC (2024), Five Reasons Why the New Cybercrime Convention Matters, Accessed: 02/02/2025, <https://www.unodc.org/unodc/frontpage/2024/December/five-reasons-why-the-new-cybercrime-convention-matters.html>
- General Assembly (2024), adopts landmark convention on cybercrime, United Nations Libya, New York, Visited: 30/01/2024, <https://libya.un.org/en/286533-un-general-assembly-adopts-landmark-convention-cybercrime>

B- Online Articles & Online Reports

- Gullo Karen, a. Katitza (2023), UN Cybercrime Draft Treaty Timeline, Electronic Frontier Foundation, Visited: 27/01/2025, <https://www.eff.org/deeplinks/2023/04/un-cybercrime-treaty-timeline/>
- Walker, Summer (2021), UN Cybercrime Resolution Stumbles Out of the Gate, Global Initiative, Visited: 2/01/2025, <https://globalinitiative.net/analysis/un-cybercrime-resolution/>
- Anastasiya, Kazakova (2024), UN Cybercrime Convention: Will States Give in Disagreements for the Sake of a Global Common Threat?, Geneva Internet Platform, Visited: 02/01/2025, <https://www.dig.watch/updates/un-cybercrime-convention-will-states-give-in-disagreements-for-the-sake-of-a-global-common-threat/>
- Rajeesh, Kumar (2025), United Nations Cybercrime Convention : A Milestone in Digital Governance?, Institute for Defense Studies and Analyses, Visited: 04/02/2025, https://www.idsa.in/publisher/issue-brief/united-nations-cybercrime-convention-a-milestone-in-digital-governance/#footnoteref40_iycl6nr/
- Crime, O. T (2024), Cyber Convention Check-in, Global Initiative Against Transnational Organized Crime, Visited: 26/02/2025, <https://globalinitiative.net/announcements/cyber-convention-check-in/>
- Jakobi Anja P, Lena Herbst (2024), Between a Rock and a Hard Place: The UN Cybercrime Convention, The Peace Research Institute, Frankfurt, P04.

C- Web Articles & Media Reports

- Algerian (2024), Adoption of a Convention Against Cybercrime... Another Gain in the Record of Algerian Diplomacy Efforts Led by the President of the Republic, Algerian Radio, Visited: 10/01/2025, <http://news.radioalgerie.dz/ar/node/50035/>

- Greg, Otto (2024), HackerOne Urges U.S. to Advocate for Research Protections in UN Cybercrime Treaty, Cyberscoop, Visited: 26/01/2025, <https://cyberscoop.com/un-cybercrime-treaty-hackerone-letter-security-research/>
- Nations, U Nd (2024), Global Cybercrime Treaty: A Delicate Balance between Security and Human Rights, Law and Crime Prevention, United Nations, Visited: 02/02/2025, <https://news.un.org/en/interview/2024/02/1146772/>
- Vision (2024), The United Nations Adopts a Historic Convention Related to Cybercrime, Visited: 15/01/2025, <https://alroya.om/post/357804/>
- Youm7 (2024), The United Nations Adopts a Convention Against Cybercrime, Youm7, Visited: 20/01/2025, <https://www.youm7.com/story/2024/>