ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep1436

The Evolving Role of International Conventions in Regulating Cyberspace and Combating Cybercrime

Kamallini G.[1]

[1]School of Low, Hindustan Institute of Technology and Science

Publication Date: 2025/10/07

Abstract: International conventions are the backbone of our global effort to make cyberspace safer. The internet connects us all, but it also creates avenues for cybercrime, from fraud and hacking to more insidious threats like child exploitation and the spread of harmful misinformation. International conventions play a critical yet complex role in the evolving regulation of cyberspace. Facing a borderless and rapidly advancing digital domain, these agreements strive to establish common legal frameworks, foster international cooperation, and address transnational cyber threats. A foundational paradigm for many states, treaties such as the Council of Europe's Budapest Convention on Cybercrime have greatly standardized national cybercrime legislation and enabled reciprocal legal aid. The UN Convention against Cybercrime, that was recently adopted, represents an international attempt to create a more thorough and widely recognized framework that would close current loopholes and improve the exchange of evidence across borders.

The ever-changing nature of cyber technology, conflicting national interests regarding sovereignty and data governance, the difficulty of attribution of cyberattacks, and the substantial involvement of non-state actors all pose challenges to the efficacy of these conventions. While these instruments provide essential norms for responsible state behavior, promote capacity building, and criminalize a range of malicious cyber activities, their implementation often faces hurdles such as slow ratification, broad definitions, and the need to balance security imperatives with human rights protections. Ultimately, international conventions serve as crucial, albeit imperfect, mechanisms for building consensus and legal predictability in a domain that defies traditional geographical and legal boundaries. To sum it up in simpler words it is the shared rulebooks nations create to tackle online threats that transcending the borders.

Keywords: *International Conventions, Cyber Security, Cyber Space, Treaties.*

How to Cite: Kamallini G. (2025) The Evolving Role of International Conventions in Regulating Cyberspace and Combating Cybercrime. *International Journal of Innovative Science and Research Technology*, 10(9), 2623-2627. https://doi.org/10.38124/ijisrt/25sep1436

I. INTRODUCTION -THE IMPERATIVE FOR INTERNATIONAL CYBER GOVERNANCE

The digital realm, commonly referred to as cyberspace, has rapidly evolved from a mere communication medium into a critical domain impacting global sustainability agendas and even national security[1]. Due to this change, worldwide legal frameworks have had to be established in order to regulate behavior in this particular setting and to counter the constant threat of cybercrime. International conventions play a crucial role in cyberspace by fostering cooperation, setting norms, and establishing legal frameworks to address global challenges like cybercrime, national security, and human rights in the digital realm. These conventions aim to harmonize national laws, facilitate information sharing, and promote a stable and secure cyberspace for all[2]. International

[1] ESIL Reflection: Regulation of Cyberspace by International Law Vol 7, Issue 1
Editorial board: Samantha Besson, Jean d'Aspremont (Editor-in-Chief), Jan Klabbers and Christian Tams available at https://esil-sedi.eu/fr/esil-reflection-regulation-of-cyberspace-by-international-law/ (last accessed on 28th July 2025)

[2] International Cooperation on Cyber Space: India's role. Amb (Retd) Asoke Mukerji
Venue: National Academy Of Customs, Indirect Taxes And Narcotics (NACIN), Faridabad available at https://www.mea.gov.in/distinguished-lectures-detail.htm?743#:~:text=These%20include%20norms%20for%20ensuring,ensure%20the%20security%20of%20cyberspace. (last accessed on 28th July 2025)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep1436

conventions help create a baseline of legal standards for cybercrime, data protection, and other digital issues, making it easier for countries to cooperate and prosecute offenders. Conventions provide universally agreed-upon definitions for cybercrimes like hacking, online fraud, and child exploitation, reducing ambiguity and facilitating cross-border investigations[3]. Some conventions focus on establishing norms for state behavior[4] in cyberspace, addressing issues like responsibility for cyber-attacks originating from their territory, and the protection of critical infrastructure[5]. Treaties like the Budapest Convention establish mechanisms for countries to share digital evidence and cooperate in investigations of cybercrimes. Many conventions include provisions for capacity building, particularly for developing countries, to enhance their ability to combat cybercrime and participate effectively in international efforts[6]. Some conventions address the use of cyberspace for terrorist activities, facilitating information sharing and cooperation between countries to counter these threats[7].International agreements seek to strike a balance between the defense of basic human rights like privacy and freedom of speech and the requirements of law enforcement and national security. Vulnerable people are shielded from online abuse and exploitation by conventions such as those that address child exploitation online. Conventions can aid in the establishment of guidelines and standards that discourage malevolent online behavior, fostering a more safe and stable online environment. International efforts aim to protect critical infrastructure, such as communication networks and energy grids, from cyber attacks that could disrupt essential services. As states give increased attention to the governance of cyberspace, the role of international law in the cyber context has gained increasing prominence[8].

II. ANALYSIS OF INTERNATIONAL CONVENTIONS

➢ *The Budapest Convention (2001)[9]*

The Budapest Convention[10], The first and most extensive international agreement addressing cybercrime is the Budapest Convention, officially known as the Convention on Cybercrime. It was created by the Council of Europe and offers a framework for: Improving international cooperation, improving investigative methods, and harmonizing cybercrime laws across countries. The treaty, which has more than 60 signatories, including non-European countries like the US, Japan, and Australia, covers crimes like online fraud, data breaches, and illegal access. Among the difficulties are:

- Major powers like China and India have not participated.
- Attacked for being antiquated and Eurocentric in its handling of changing cyberthreats.

➢ *The Malabo Convention (2014)[11]*

Adopted by the African Union, the Malabo Convention focuses on cybercrime and data protection[12]. The Malabo Convention, which was ratified by the African Union, addresses data protection and cybercrime. It creates clauses for the Budapest Convention on Cybercrime (ETS No. 185) and its Protocols.

- Combating online fraud
- Safeguarding private information
- Promoting awareness and capacity building.

Few African nations have ratified the agreement, and even fewer have put its principles into practice.

➢ *The UN Cybercrime Treaty (Adopted November 2023)*

The UN Cybercrime Treaty[13] An important turning point in international attempts to combat cybercrime is the UN Cybercrime Treaty. This treaty, which was approved by the UN General Assembly in November 2023, attempts to create a thorough framework to prevent the use of ICT (information and communication technologies) for illegal activities. The treaty's provisions include

- Key cybercrime offenses, such as hacking, online fraud, child exploitation, and the use of ICT for terrorism, are defined by the treaty in a way that is widely accepted.
- It creates efficient procedures for sharing digital evidence and collaborating across borders.

[3] A Brief Primer on International Law and Cyberspace by Duncan B. Hollis Published on June 14, 2021available at https://carnegieendowment.org/posts/2021/06/a-brief-primer-on-international-law-and-cyberspace?lang=en (last accessed on 28th July 2025)

[4] UNICAF https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf

[5] International Cybercrime Treaties and Case Laws: An Overview (Till December 2024) Advocate (Dr.) Prashant Mali , International Cyber & Privacy Lawyer available at https://www.cyberlawconsulting.com/global_cybersecurity_sco_framework.php (last accessed on 28th July 2025)

[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 available at https://www.unodc.org/unodc/en/cybercrime/convention/home.html#:~:text=The%20Convention%20is%20the%20first,electronic%20evidence%20for%20serious%20crimes. (last accessed on 28th July 2025)

[7] *Supra 1*

[8] *Supra 1*

[9] International Cybercrime Treaties and Case Laws: An Overview (Till December 2024) - Cyber Law Consulting | Advocates & Attorneys

[10] The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols

[11] International Cybercrime Treaties and Case Laws: An Overview (Till December 2024) - Cyber Law Consulting | Advocates & Attorneys

[12] African Union Convention on Cyber Security and Personal Data Protection 2014

[13] *Supra 2*

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep1436

- In order to ensure that underdeveloped countries can effectively tackle cybercrime, the convention places a strong emphasis on capacity building.
- It addresses concerns about overreach by including measures to strike a balance between privacy and freedom of expression and state surveillance.

It is anticipated that the treaty will improve international cooperation, particularly for those nations that have not ratified the Budapest Convention. It encourages more legal uniformity, which lessens jurisdictional disputes in cybercrime investigations. During discussions, disagreements arose over the pact; Western countries supported the Budapest Convention, while China, Russia, and certain developing countries supported the UN-led agreement. Significant conformity between domestic laws and treaty provisions will be necessary for implementation.

➢ *The UN Convention Against Cybercrime*

The UN Convention Against Cybercrime[14] adopted on December 24, 2024, is the first global treaty focused on combating cybercrime. Originating from a 2019 proposal led by Russia, the Convention aims to strengthen international cooperation, modernize digital crime-fighting tools, and promote human rights in cyberspace. It opens for signature on October 25, 2025, and enters into force after 40 ratifications. The key objectives & provisions include

- Enhances global coordination on cybercrime investigations.
- Criminalizes core cyber-dependent crimes (e.g., hacking, data interference, online fraud) and some cyber-enabled crimes like child exploitation.
- Promotes capacity-building for developing countries and cross-border data-sharing.
- Uses tech-neutral language to remain future-proof.
- Requires states to bolster digital law enforcement.

The challenges are

- Western states preferred a narrower treaty; Russia, China, and others pushed for broader control, including criminalizing disinformation.
- Critics say safeguards are vague, defer to national laws, and could allow abuse by authoritarian regimes.
- The treaty lacks strong oversight, data protection standards, and provisions to limit misuse of surveillance powers.

While a major step toward global cybercrime cooperation, the Convention faces criticism over rights protections, scope, and enforceability, raising concerns about potential misuse and uneven implementation.

➢ *Russia-China Bilateral Agreement on Cybersecurity (2015)*

In 2015,[15]China and Russia inked a bilateral agreement to work together to ensure global information security. The following are the main points of this agreement:

- Both countries committed to working together to prevent cybercrimes, such as hacking and the use of the internet for destabilizing and terrorist purposes.
- The agreement places a strong emphasis on the idea that states have the sovereign right to control their own domestic internet free from outside intervention.
- It also contains pledges to stop technology from being used to threaten political stability in either nation.
- Mutual Assistance: The two countries agreed to support one another in the event of cybersecurity attacks and incidents that come from or target their respective countries.

➢ *The Russia-China Proposal at the UN[16]*

In line with their ideas of cyber sovereignty, Russia and China have also been outspoken in drafting an international cyber treaty supported by the UN. This was included in their 2011 and 2015 revisions of the "International Code of Conduct for Information Security," which they proposed at the UN.

- Supporting a state's ability to regulate information inside its borders in order to preserve public order and national security is one of the main goals.
- Stressing that information created inside a country's boundaries ought to be governed by its laws.
- Outlining policies to stop hostile uses of cyberspace, such as cyberwarfare or political manipulation.

The plan is in line with China's and Russia's domestic internet regulations, which support strict censorship and restriction. Western governments and democratic states argue that the idea might justify internet censorship under the pretext of "cybersecurity," weakening internet freedom and free expression.

➢ *Russia-China Alignment on the UN Cybercrime Treaty[17]*

China and Russia were key players in influencing the UN Cybercrime Treaty negotiations, which were adopted in 2023.

- Treaty centered on sovereign authority over domestic cyberspace was what they pushed for.
- International organizations' involvement in national cyber regulations should be less invasive.
- Clauses prohibiting ICT usage for "subversive purposes," which detractors claim might excuse government censorship.

[14] The United Nations Convention against Cybercrime 2024 - resolution 79/243.
[15] The Russia-China Bilateral Agreement on Cyber security , 2015
[16] *Supra 2*
[17] *Supra 2*

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep1436

Many other nations, especially in the Global South, who are also concerned about Western domination in global internet governance, backed their efforts.

- *The Shanghai Cooperation Organization (SCO) Cyber Security Framework*

A regional strategy for cyber security is also supported by the Shanghai Cooperation Organization (SCO), which is headed by China and Russia. SCO member nations working together to combat cybercrime is one of the main elements. Disseminating cyber security infrastructure best practices Bringing member nations' legal systems into line with cyber sovereignty concepts.

- *Other International Instruments*

Beyond broad cybercrime conventions, specialized international instruments play a vital role in regulating specific aspects of cyberspace[18]. The WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonogram Treaty (WPPT), collectively known as the "Internet Treaties," are prime examples[19].

Administered by the World Intellectual Property Organization (WIPO), these treaties establish international norms aimed at preventing unauthorized access to and use of creative works disseminated over the Internet or other digital networks. Their purpose is to update and supplement major existing WIPO treaties on copyright and related rights (such as the Berne Convention and Rome Convention)[20] to address the profound technological advancements and marketplace changes of recent decades.

The WCT specifically deals with the protection of authors[21] of literary and artistic works (e.g., writings, computer programs, original databases, musical works, audiovisual works, fine art, photographs), while the WPPT focuses on the rights of performers and producers of phonograms. These treaties clarify that existing rights continue to apply in the digital environment and also create new online rights. To maintain a fair balance, they allow countries reasonable flexibility in establishing exceptions or limitations to these rights for public interest uses, such as non-profit educational and research purposes. Crucially, they require countries to provide legal protection against the "circumvention of technological measures" (anti-circumvention provisions, addressing "hacking") used by rightholders to protect their works, and to prohibit the deliberate alteration or deletion of electronic "rights management information[22]".

III. LANDMARK INTERNATIONAL CYBER CASE LAWS

- *Microsoft v. United States (2018)[23]*

The question in this case was whether the held Communications Act (SCA) allowed U.S. law enforcement to access material that was held abroad. After the CLOUD Act was passed, the U.S. Supreme Court finally declared the matter moot, enabling U.S. authorities to access data kept overseas through agreements with other nations. The Impact promoted the creation of bilateral data-sharing agreements and brought attention to the difficulties associated with data sovereignty.

- *Schrems II (2020)[24]*

The EU-U.S. Privacy Shield framework was declared illegal by the Court of Justice of the European Union because it did not adequately protect the data of EU citizens under U.S. surveillance laws. Standard Contractual Clauses (SCCs) for data transfers were mandated by the case. This cleared the path for the 2023 introduction of the EU-US Data Privacy Framework.

- *BEC Scams and Extradition Cases[25]*

International efforts to tackle cybercrime through extradition treaties are highlighted by a number of Business Email Compromise (BEC) instances, including the Hushpuppi extradition from the United Arab Emirates to the United States. In addition to encouraging additional nations to ratify mutual legal assistance treaties (MLATs), it improved international cooperation in the prosecution of cybercriminals.

IV. TREATIES IN THE PIPELINE[26]

- *The ASEAN Cooperation Agreement on Cybersecurity*

To improve cooperation among member governments, the Association of Southeast Asian Nations (ASEAN) is

[18] Science and Technology in International Economic Law Balancing Competing Interests Edited ByBryan Mercurio, Kuei-Jung Ni

[19]COPYRIGHT ISSUES IN ELECTRONIC GAMES: A COMPARATIVE STUDY
Abhinaya Ramesh Vol. 18 No. 2 (2023) | https://www.acgpublishing.com/ | ISSN - 1071-8443

[20] The localization of IP infringements in the online environment: from Web 2.0 to Web 3.0 and the Metaverse Open Access
Eleonora Rosati Author Notes
Journal of Intellectual Property Law & Practice, Volume 18, Issue 10, October 2023, Pages 720–742, https://doi.org/10.1093/jiplp/jpad077
Published: 08 September 2023

[21] https://www.legalservicesindia.com/law/article/939/7/Intellectual-Property-Law-and-Internet

[22] https://assets.vmou.ac.in/PGDCL02.pdf

[23] Microsoft Corp. v. United States, 584 U.S. ___, 138 S. Ct. 1186 (2018).

[24] Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (Case C-311/18).

[25] 74 Arrested in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes available at https://www.justice.gov/archives/opa/pr/74-arrested-coordinated-international-enforcement-operation-targeting-hundreds-individuals (last accessed on 28th July 2025)

[26] *Supra 2*

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep1436

pursuing a cyber security pact for the whole region. It is anticipated that this pact will:

- Promote information exchange.
- Help smaller countries develop their cybersecurity capabilities.
- Deal with local cyberthreats, such as phishing scams and ransomware attacks.

➢ *India's BRICS Cyber Treaty Push To combat cyberthreats within the group, India is pushing for a cybercrime framework tailored to the BRICS. This project consists of:*

- Creating common standards and procedures
- Promoting cooperation in the development of capacity.
- Dealing with international concerns such as data sharing and digital forensics.

V. SUGGESTIONS AND RECOMMENDATIONS FOR STRENGTHENING INTERNATIONAL CYBER GOVERNANCE

To navigate the complex landscape of cyber governance and enhance the effectiveness of international conventions, a multi-faceted and adaptive approach is imperative.

- Human Rights Protections: Move beyond vague language by enforcing specific safeguards—judicial oversight, proportionality, and mandatory refusal of cooperation where rights are at risk.
- Cross-Border Cooperation: Develop secure, standardized, and rights-respecting mechanisms for data sharing and legal assistance.
- Technological Adaptability: Use technology-neutral language and create expert bodies to regularly update legal frameworks in response to emerging threats like AI and IoT.
- Public-Private Partnerships: Institutionalize multi-stakeholder involvement (including tech companies and civil society) across all phases of cyber governance.

VI. CONCLUSION

As cyberspace continues to expand and evolve, the role of international conventions in regulating digital activity and combating cybercrime becomes increasingly vital. From foundational treaties like the Budapest Convention to the more recent and globally inclusive UN Convention Against Cybercrime, these instruments reflect a growing consensus on the need for cross-border legal harmonization, cooperation, and shared cyber norms.

However, existing frameworks face serious limitations: geopolitical divides, insufficient human rights protections, slow adaptation to technological change, and the exclusion of key global stakeholders. Initiatives driven by regional blocs or specific states, such as the Russia-China cybersecurity agreements or the Malabo Convention, further highlight the fragmented nature of current governance models.

To address these challenges, international cyber governance must shift from reactive treaty-making to proactive, inclusive, and flexible frameworks. This means embedding strong human rights safeguards, establishing trusted and secure data-sharing systems, and designing legal instruments with built-in mechanisms for technological adaptability. In sum, creating a secure, stable, and rights-respecting cyberspace will require continuous dialogue, global cooperation, and innovative legal thinking. Rather than relying on a single, comprehensive treaty, the international community must embrace a layered and collaborative approach, combining broad conventions with targeted instruments that can evolve alongside the digital threats they seek to address. Only through such a balanced and inclusive strategy can we build a safer digital future for all.

REFERENCES

➢ *Websites*

[1]. https://esil-sedi.eu/fr/esil-reflection-regulation-of-cyberspace-by-international-law/
[2]. https://djilp.org/international-legal-frameworks-on-cybersecurity-and-data-protection-law/
[3]. https://www.researchgate.net/publication/385089998_The_need_for_cybercrime_regulation_on_a_global_scale_by_the_international_law_and_cyber_convention
[4]. https://www.un.org/en/peace-and-security/basic-facts-about-global-cybercrime-treaty
[5]. https://www.unodc.org/unodc/cybercrime/convention/home.html
[6]. https://www.unodc.org/unodc/en/frontpage/2024/August/united-nations_-member-states-finalize-a-new-cybercrime-convention.html
[7]. https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=2294&context=facpub
[8]. https://ejurnal.unisri.ac.id/index.php/proictss/article/view/10254/5431

➢ *Case laws*

[9]. Microsoft Corp. v. United States, 584 U.S. ___, 138 S. Ct. 1186 (2018).
[10]. Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (Case C-311/18).

➢ *Books referred*

[11]. Cyber law – Dr.Bhagyashree A.Deshpande

➢ *Publications*

[12]. Role of international organizations in prevention of cyber-crimes: an analysis by Neethu N - NALSAR University of law hyderabad