YourLawArticle

Open Access Law Journal, ISSN (O): 3049-0057

Editor-in-Chief – Prof. (Dr.) Amit Kashyap; Publisher – Reet Parihar

A Critical Study On The Adequacy Of International Law In Tackling Cross-Border Cybercrimes

Garima Sharma, LL.M (1st Year) , Lovely Professional University

Published on: 18th October 2025

Abstract

Technology has made cybercrimes a huge global concern, as offences like ransomware, financial fraud, and large-scale data theft often cross national borders. Investigating and prosecuting such crimes is challenging because domestic laws, designed for territorial offences, cannot fully address their borderless nature. This makes international law more important. This study looks at how effective international frameworks, particularly the Budapest Convention on Cybercrime and United Nations initiatives, have been in addressing challenges such as jurisdiction, evidence collection, extradition, and mutual legal assistance. The findings suggest that while these frameworks provide a foundation for cooperation, their impact is still limited. Unequal participation among states, inconsistent enforcement, and the rapid pace of technological change continue to weaken their effectiveness. The study highlights the need for stronger collaboration between countries, harmonized legal standards, and reforms that keep pace with technological advancements to create a truly effective global response to cross-border cybercrime.

Keywords: Cybercrime, International Law, Budapest Convention, Jurisdiction, Extradition, Global response

INTRODUCTION

The rise of digital technology has connected individuals, businesses, and governments like never before, but it has also created new opportunities for cybercrime. Offences such as hacking, phishing, identity theft, ransomware, and financial fraud are increasingly sophisticated and often involve perpetrators and victims in different countries. This borderless nature makes investigation and prosecution challenging, as traditional domestic laws are designed for crimes within national boundaries.

Cyberspace complicates jurisdiction, evidence collection, and enforcement. Digital data may be spread across multiple countries, requiring international cooperation that is often slow and inconsistent. Jurisdictional conflicts and varying definitions of offences further hinder effective action. International law, including the Budapest Convention on Cybercrime and UN initiatives, provides a framework for cooperation, but its impact is limited. Uneven participation, inconsistent enforcement, and rapid technological change reduce its effectiveness.

This study critically examines these frameworks, explores practical challenges, and suggests reforms to make international law more responsive and effective against cross-border cybercrime.

RESEARCH PROBLEM

The rapid growth of cyberspace has made cybercrimes like hacking, ransomware, identity theft, and data breaches increasingly global. Unlike traditional crimes, these offences often span multiple countries, involving victims, perpetrators, and evidence across different jurisdictions, which makes investigation and prosecution challenging. While international frameworks such as the Budapest Convention and UN initiatives provide guidance, their impact is limited due to uneven adoption, inconsistent enforcement, and the fast pace of technological change. This study focuses on identifying these gaps, understanding the limitations of current legal frameworks, and exploring the need for more cooperative, harmonized, and technology-aware international reforms.

RESEARCH QUESTIONS

1. How effective are international legal frameworks, such as the Budapest Convention, in addressing cross-border cybercrimes?

2. What gaps and limitations in current international law hinder the investigation and prosecution of cyber offences across jurisdictions?
3. How do jurisdictional differences and rapid technological changes affect global cooperation against cybercrime?
4. What reforms or strategies can enhance international law to make it more harmonized, technology-sensitive, and effective against cross-border cybercrimes?

RESEARCH OBJECTIVES

1. To evaluate the effectiveness of international legal frameworks, including the Budapest Convention, in addressing cross-border cybercrimes.
2. To identify the gaps and limitations in current international law that hinder the investigation, prosecution, and enforcement of cyber offences across jurisdictions.
3. To examine the impact of jurisdictional differences and rapidly evolving technology on global cooperation against cybercrime.
4. To propose reforms and strategies aimed at creating a more harmonized, technology-sensitive, and effective international legal framework for combating cross-border cybercrimes.

RESEARCH METHODOLOGY

This study adopts a doctrinal and analytical approach to examine the adequacy of international law in addressing cross-border cybercrimes. It involves a qualitative analysis of international legal instruments, including the Budapest Convention, UN resolutions, national legislations, and scholarly articles. Comparative analysis is used to identify gaps in enforcement, jurisdictional challenges, and differences in state participation. Selected case studies of notable cybercrime incidents are examined to highlight practical difficulties in investigation, prosecution, and international cooperation. The methodology aims to critically evaluate existing frameworks and propose reforms for a more harmonized, technology-sensitive, and effective international legal response to cybercrime.

LITERATURE REVIEW

Cross-border cybercrimes have quickly become one of the toughest challenges for international law today. Crimes like ransomware, identity theft, and large-scale data breaches do not stop at national borders, yet laws are still tied to territorial boundaries. Scholars like Smith (2022) point out that

differences in jurisdiction, vague legal definitions, and weak cooperation between states make it difficult to respond effectively.

The Budapest Convention is often seen as the cornerstone of international cyber law. While Lee and Patel (2021) acknowledge its role in setting common standards, they argue that unclear rules on active cyber defense and inconsistent enforcement limit its effectiveness. Johnson (2020) adds that the fragmented nature of laws and the uneven participation of states weaken collective action.

Chen (2019) highlights another key issue: technology evolves much faster than law. Even when frameworks exist, their adoption and application are uneven, giving cybercriminals room to exploit gaps. The Council of Europe (2001) notes that the Budapest Convention relies heavily on voluntary compliance, while recent UN initiatives (2024) struggle with limited adoption.

As Davis (2023) and Miller (2022) show, without harmonization and stronger cooperation, cybercriminals will continue to take advantage of loopholes, making reforms urgently necessary.

RESEARCH GAP

Despite significant research on cross-border cybercrimes and international law, gaps remain in understanding practical enforcement. Most studies focus on legal frameworks like the Budapest Convention and UN initiatives but rarely assess how jurisdictional differences, evidence sharing, and technological advances affect implementation. Literature also underexplores emerging UN efforts and regional cooperation. This study aims to address these gaps by evaluating the strengths and limitations of international law, its enforcement challenges, and proposing reforms for a more harmonized and effective global response to cross-border cybercrime.

CHAPTER 1: EVALUATION OF INTERNATIONALl LEGAL FRAMEWORKS

The rapid proliferation of cross-border cybercrimes has highlighted the need for robust international legal frameworks.[1]The Budapest Convention on Cybercrime, adopted in 2001 by the Council of Europe, is the first international treaty aimed at harmonizing national laws and promoting international cooperation in combating cybercrime.[2] In addition, the United Nations has initiated efforts to develop a

[1] Council of Europe, About the Convention - Cybercrime (n.d.) https://www.coe.int/en/web/cybercrime/the-budapest-convention accessed 29 September 2025
[2] Ibid

global cybercrime treaty to address the evolving digital threat landscape.[3] This chapter critically evaluates these frameworks, focusing on their effectiveness, challenges, and areas for reform.

The Budapest Convention on Cybercrime

The Budapest Convention seeks to standardize national cybercrime laws, enhance international cooperation, and facilitate lawful collection of electronic evidence.[4] According to the Council of Europe, the Convention has influenced domestic legislation in multiple countries, leading to the enactment of cybercrime laws globally.[5] It has also fostered international collaboration, allowing law enforcement agencies to share information and coordinate operations against cybercriminals.[6] The Cybercrime Convention Committee reports that the Convention has been instrumental in facilitating emergency cooperation and mutual legal assistance among parties.[7]

United Nations Initiatives

In response to global cyber threats, the United Nations has worked toward establishing a comprehensive international legal framework to combat cybercrime.[8] The UN's efforts culminated in the proposed United Nations Convention Against Cybercrime, aimed at providing a universal legal instrument for the prevention and prosecution of cybercrimes while safeguarding human rights.[9] The treaty promotes the use of Mutual Legal Assistance Treaties to facilitate cross-border data requests, enhancing international cooperation without compromising individual rights.[10]

Effectiveness and Challenges

While both the Budapest Convention and UN initiatives have made progress, challenges remain. Lack of harmonized national laws and standardized evidentiary requirements pose significant obstacles to

[3] United Nations, Basic Facts about the Global Cybercrime Treaty (2024) https://www.un.org/en/peace-and-security/basic-facts-about-global-cybercrime-treaty accessed 29 September 2025
[4] Council of Europe (n 1)
[5] Council of Europe, The Budapest Convention on Cybercrime: Benefits and Impact in Practice (2020) https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac accessed 29 September 2025
[6] Ibid
[7] Ibid
[8] United Nations (n 3)
[9] Ibid
[10] U.S. Chamber of Commerce, UN Cybercrimes Treaty: A Well-Intentioned but Flawed Approach (n.d.) https://www.uschamber.com/security/cybersecurity/un-cybercrimes-treaty-a-well-intentioned-but-flawed-approach accessed 29 September 2025

effective investigations and prosecutions.[11]Rapid technological developments, including ransomware and state-sponsored cyberattacks, have outpaced existing legal frameworks, creating a gap between theory and practice.[12] The voluntary nature of the Budapest Convention's implementation and varying commitment levels among signatory states lead to inconsistent enforcement and cooperation.[13]

Thus, international legal frameworks such as the Budapest Convention and UN initiatives have laid important groundwork for combating cross-border cybercrime, but their effectiveness is limited by inconsistent implementation, technological advancements, and jurisdictional disparities.[14] Addressing these issues requires harmonization of national laws, standardization of evidentiary requirements, and adaptation of legal frameworks to keep pace with technology.[15]

CHAPTER 2: GAPS AND LIMITATIONS IN CURRENT INTERNATIONAL LAW

Despite the progress made by international frameworks such as the Budapest Convention and emerging United Nations initiatives, significant gaps continue to impede effective cross-border cybercrime enforcement. These challenges arise from jurisdictional differences, technological evolution, procedural delays, and uneven commitment by states, limiting the practical utility of existing legal instruments. This chapter critically examines these gaps to provide a foundation for proposing reforms.

1. Jurisdictional Conflicts and Legal Fragmentation

Cybercrimes frequently span multiple jurisdictions, creating conflicts between national laws. Differences in legal definitions, criminalization standards, and procedural rules complicate investigations and prosecutions. For instance, an act considered illegal in one country may not be recognized as a crime in another, which often delays or prevents cross-border cooperation.[16]

[11] United Nations Office on Drugs and Crime (UNODC), Obstacles to Cybercrime Investigations (n.d.) https://www.unodc.org/e4j/zh/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html accessed 29 September 2025
[12] Ibid
[13] Council of Europe (n 5)
[14] United Nations (n 3); Council of Europe (n 1)
[15] Council of Europe (n 5); UNODC (n 11)
[16] Leppard Law, 'Jurisdictional Challenges in Cross-Border Cybercrime' (2025) https://leppardlaw.com/federal/computer-crimes/jurisdictional-challenges-in-cross-border-federal-cybercrimes/ accessed 29 September 2025

The Budapest Convention encourages harmonization of laws among signatory states; however, compliance is voluntary, and enforcement mechanisms are decentralized.[17] This leads to inconsistencies in interpretation and application, leaving gaps that cybercriminals can exploit.[18]

2. Inadequate Mutual Legal Assistance Mechanisms

Mutual Legal Assistance Treaties are vital for sharing evidence and coordinating investigations across borders. Yet, traditional MLAT processes are often slow, bureaucratic, and ill-equipped for real-time cybercrime investigations.[19] Even under the Budapest Convention, mutual assistance depends on voluntary state cooperation, which can lead to delays in gathering electronic evidence critical for prosecution.[20]These procedural inefficiencies reduce the ability of law enforcement agencies to respond swiftly to cyber threats.[21]

3. Technological Advancements Outpacing Legal Frameworks

The rapid evolution of technology has outstripped existing international legal instruments. New platforms such as cloud computing, cryptocurrencies, the Internet of Things, and AI-driven malware present challenges that older frameworks like the Budapest Convention were not specifically designed to address.[22]Cybercriminals can exploit these technological gaps, while law enforcement struggles to adapt legal procedures in time.[23]

4. Uneven Implementation and Enforcement

[17] Council of Europe, About the Convention - Cybercrime (n.d.) https://www.coe.int/en/web/cybercrime/the-budapest-convention accessed 29 September 2025
[18] Council of Europe, The Budapest Convention on Cybercrime: Benefits and Impact in Practice (2020) https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac accessed 29 September 2025
[19] United Nations Office on Drugs and Crime (UNODC), 'Obstacles to Cybercrime Investigations' (n.d.) https://www.unodc.org/e4j/zh/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html accessed 29 September 2025
[20] Cross-Border Data Forum, 'The Budapest Convention: What Is It and How Is It Being Updated?' (2024) https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/ accessed 29 September 2025
[21] Ibid
[22] Europol, Common Challenges in Cybercrime 2024 (2024) https://www.europol.europa.eu/cms/sites/default/files/documents/Common_Challenges_in_Cybercrime_2024.pdf accessed 29 September 2025
[23] Council of Europe, 'Key Facts - Cybercrime' (2025) https://www.coe.int/en/web/cybercrime/key-facts accessed 29 September 2025

Implementation of international cybercrime laws is inconsistent among states. Variations in domestic legislation, technical expertise, infrastructure, and politics will create uneven enforcement.[24]Some jurisdictions may serve as "safe havens" for cybercriminals due to weak regulatory frameworks, undermining global cooperation.[25]

5. Human Rights and Privacy Concerns

Balancing enforcement with human rights protection remains a significant challenge. Provisions enabling surveillance, data interception, or cross-border data transfers can threaten privacy if not carefully regulated.[26]While the Budapest Convention includes safeguards, their application varies, and enforcement practices in some states raise concerns about potential overreach.[27]

So, International legal frameworks have laid an important foundation for combating cross-border cybercrime. However, challenges persist in the form of jurisdictional conflicts, inadequate mutual assistance, outdated technological provisions, uneven enforcement, and human rights concerns. Addressing these gaps requires legal reforms, harmonization of domestic laws, technology-sensitive policies, and strengthened international cooperation.

CHAPTER 3: IMPACT OF JURISDICTIONAL DIFFERENCES AND TECHNOLOGICAL EVOLUTION ON GLOBAL COOPERATION AGAINST CYBERCRIME

Cybercrime is inherently transnational, often involving perpetrators, victims, and evidence across multiple jurisdictions.[28]This global nature presents significant challenges to international cooperation, primarily due to jurisdictional differences and the rapid evolution of technology.[29] These factors complicate the enforcement of existing legal frameworks and hinder effective collaboration among states.

[24] ScienceDirect, 'Cybercrime and International Law Enforcement: A Global Perspective' (2020) https://www.sciencedirect.com/science/article/abs/pii/S0267364920301266 accessed 29 September 2025
[25] Lawfare, 'Confusion and Contradiction in the UN Cybercrime Convention' (2021) https://www.lawfaremedia.org/article/confusion---contradiction-in-the-un--cybercrime--convention accessed 29 September 2025
[26] Chicago Journal of International Law, 'Evaluating Active Cyber Defense Measures Under the Budapest Convention' (2019) https://cjil.uchicago.edu/print-archive/when-cyber-defense-crime-evaluating-active-cyber-defense-measures-under-budapest accessed 29 September 2025
[27] Ibid
[28] Europol, 'AI is Turbocharging Organized Crime, EU Police Agency Warns' (2025) https://apnews.com/article/846847536f6feb2bbb423943fd96e1f1 accessed 29 September 2025
[29] United Nations Office on Drugs and Crime (UNODC), 'Cybercrime Module 7 Key Issues: Sovereignty and Jurisdiction' (n.d.) https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/sovereignty-and-jurisdiction.html accessed 29 September 2025

1. Jurisdictional Challenges in Cybercrime Enforcement

Jurisdictional issues are a primary obstacle in cross-border cybercrime investigations.[30]Traditional legal principles, such as territoriality and nationality, often fail to address the complexities of cybercrimes that transcend national borders.[31] For instance, an offense committed in one country may have its impact felt in another, or the data related to the crime may be stored in a third country.[32]This disparity can lead to conflicts of law, delays in legal processes, and difficulties in obtaining evidence or securing extradition of suspects.[33]

The United Nations Office on Drugs and Crime (UNODC) highlights that jurisdiction in cybercrime cases is primarily determined by the location of offenders, victims, and the impacts of the crime.[34]However, the global nature of the internet often makes it challenging to apply these traditional jurisdictional principles effectively.[35]

2. Technological Evolution Outpacing Legal Frameworks

The rapid advancement of technology has introduced new challenges in combating cybercrime.[36]Emerging technologies such as artificial intelligence, blockchain, and the Internet of Things (IoT) have created new avenues for cybercriminals.[37] These technologies can be exploited to conduct sophisticated attacks, often leaving traditional legal frameworks ill-equipped to address such threats.[38]

For example, the use of AI in cybercrime has enabled more precise and devastating attacks targeting governments, businesses, and individuals.[39]Europol has issued warnings about the significant enhancement of organized crime through AI, which poses severe threats to societal foundations.[40]

[30] Ibid
[31] Ibid
[32] Ibid
[33] Ibid
[34] Ibid
[35] Ibid
[36] Europol, 'Common Challenges in Cybercrime 2024' (2024) https://www.europol.europa.eu/cms/sites/default/files/documents/Common_Challenges_in_Cybercrime_2024.pdf accessed 29 September 2025
[37] Ibid
[38] Council of Europe, 'Key Facts - Cybercrime' (2025) https://www.coe.int/en/web/cybercrime/key-facts accessed 29 September 2025
[39] Europol (n 1).
[40] Ibid

Moreover, the proliferation of cloud computing has complicated issues related to data sovereignty and access.[41]Data stored in multiple jurisdictions can be subject to varying national laws, creating conflicts and delays in accessing critical evidence for investigations.[42]

3. Inconsistent Implementation of International Agreements

While international agreements like the Budapest Convention aim to harmonize laws and facilitate cooperation, their implementation varies significantly among signatory states.[43]Differences in legal traditions, levels of technological advancement, and political will can lead to inconsistent application of these agreements.[44]

Some countries may have robust legal frameworks and technological infrastructure to combat cybercrime, while others may lack the necessary resources or political commitment.[45] This disparity can create safe havens for cybercriminals and undermine global efforts to combat cybercrime.[46]

4. Case Studies Illustrating Jurisdictional &Technological Challenges

Recent operations have highlighted the impact of jurisdictional differences and technological evolution on cybercrime enforcement:

Operation Contender 3.0: Conducted across 14 African countries, this operation resulted in the arrest of over 250 individuals involved in online romance and extortion scams.[47]The operation highlighted the challenges of coordinating efforts across jurisdictions with varying legal frameworks and technological capabilities.

[41] Ibid
[42] Ibid
[43] Council of Europe, About the Convention - Cybercrime (n.d.) https://www.coe.int/en/web/cybercrime/the-budapest-convention accessed 29 September 2025
[44] ScienceDirect, 'Cybercrime and International Law Enforcement: A Global Perspective' (2020) https://www.sciencedirect.com/science/article/abs/pii/S0267364920301266 accessed 29 September 2025
[45] Ibid
[46] Lawfare, 'Confusion and Contradiction in the UN Cybercrime Convention' (2021) https://www.lawfaremedia.org/article/confusion---contradiction-in-the-un--cybercrime--convention accessed 29 September 2025
[47] Interpol, 'Interpol Arrests Hundreds in Africa-Wide Sextortion Crackdown' (2025) https://theweek.com/world-news/africa-interpol-sting-cybercrime-sextortion accessed 29 September 2025

Operation Serengeti 2.0: A large-scale cybercrime crackdown across 18 African nations and the United Kingdom led to the arrest of 1,209 individuals and the recovery of nearly $97.4 million.[48] The operation targeted cybercrimes such as inheritance scams, ransomware, and business email compromise, underscoring the need for enhanced international cooperation and standardized legal procedures.

Jurisdictional differences and technological evolution present significant challenges to global cooperation against cybercrime.[49]To enhance international collaboration, there is a need for:

Harmonization of legal frameworks to address jurisdictional issues effectively.
Development of adaptable legal instruments that can keep pace with technological advancements.
Strengthening international cooperation through mutual legal assistance treaties and capacity-building initiatives.
Addressing these challenges is crucial for creating a cohesive and effective global response to the growing threat of cybercrime.[50]

CHAPTER 4: PROPOSED REFORMS AND STRATEGIES FOR AN EFFECTIVE INTERNATIONAL FRAMEWORK AGAINST CROSS BORDER CYBERCRIME

Cross-border cybercrime has revealed serious gaps in the effectiveness of international law. Frameworks like the Budapest Convention were once groundbreaking, but today they often fail to meet the needs of a rapidly changing digital world. Many developing countries struggle to keep pace due to limited resources, while criminals take advantage of loopholes and uneven enforcement. For reforms to be meaningful, they must move beyond theory and create practical, flexible, and inclusive strategies.

1. Building Trust and Political Will

   One of the strongest lessons learned is that cybercrime cannot be solved by treaties alone. Even when legal tools exist, cooperation is often blocked by politics, sovereignty concerns, or lack of trust. Countries sometimes hesitate to share evidence or extradite offenders, which slows down investigations.

[48] Interpol, 'Large Interpol Cybercrime Crackdown in Africa Leads to the Arrest of Over 1,200 Suspects' (2025) https://apnews.com/article/057fee9214a008eb2829a672b10e69b0 accessed 29 September 2025
[49] Europol (n 9)
[50] UNODC (n 2)

To overcome this, reforms must encourage confidence-building measures. Regional cyber task forces, joint training programs, and neutral coordination platforms under organizations like the UN or INTERPOL could make states more willing to collaborate. Unless political will and genuine trust are developed, even the best-drafted treaties will remain ineffective.

2. **Making Laws Flexible and Technology-Sensitive**

Technology is moving faster than law. Cybercriminals constantly innovate through AI-driven attacks, ransomware, and cryptocurrency scams, while international frameworks remain rigid and slow to adapt. If legal instruments cannot evolve quickly, they will always be one step behind.

A practical solution is to include review clauses in treaties or create standing cyber committees that can update protocols regularly. This would allow international law to respond dynamically to emerging threats, rather than waiting years for renegotiations. A flexible, technology-sensitive approach is key to keeping pace with cybercriminals.

3. **Addressing the Global Digital Divide**

Not all countries have equal capacity to deal with cybercrime. Many developing nations lack advanced forensic tools, trained specialists, or reliable digital infrastructure. This imbalance creates safe havens for criminals and weakens global security.

Reforms must therefore focus on capacity-building. This could include providing technical training for investigators, setting up regional forensic labs, and offering financial or technological support to resource-limited states. Global cooperation will only succeed if every country has the tools to contribute.

4. Involving Non-State Actors

Cybercrime affects not only governments but also individuals, businesses, and tech firms. In fact, private companies and civil society groups often detect threats much earlier than states. Excluding them from global responses limits effectiveness.

Future reforms should build public-private partnerships that allow real-time data sharing and coordinated responses. At the same time, victims—who are often ignored in international discussions—must be

given proper recognition. Accessible reporting systems, mechanisms for compensation, and faster redressal processes would make responses more inclusive and humane.

5. Strengthening Global and Regional Cooperation

A balance is needed between universal conventions and regional initiatives. While frameworks like the Budapest Convention provide a common standard, regional agreements—such as those by the African Union or ASEAN—offer context-specific solutions. Linking these regional approaches with global efforts can create a stronger, multilayered system of cooperation.

CONCLUSION

Cross-border cybercrime is not just a legal or technological challenge—it is also political and human. A stronger international framework must focus on trust-building, flexible laws, capacity-building, partnerships with non-state actors, and regional cooperation, while protecting victims and human rights. Only by adopting these inclusive and practical reforms can states create a legal system that evolves as quickly as the threats it seeks to defeat. A united, adaptable, and cooperative framework is the best way forward for ensuring a safer digital world.