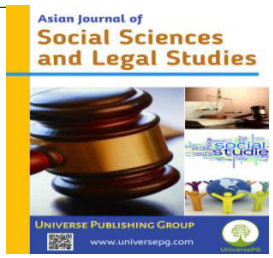
Publisher homepage: www.universepg.com, eISSN: 2707-4668

Asian Journal of Social Sciences and Legal Studies

Journal homepage: www.universepg.com/journal/ajssls



OPEN ACCESS | Research Article

Cybercrime Prosecution in Cross-Border Jurisdictions: Legal Challenges and Paths to Harmonization

Md. Mutasim Billah Kandaker*

Department of Law, Green University of Bangladesh

*Correspondence: mustasim@law.green.edu.bd (Md. Mutasim Billah Kandaker, Lecturer, Department of Law, Green University of Bangladesh).

Received Date: 18 December 2026 Accepted Date: 20 January 2026 Published Date: 3 February 2026

Abstract

The global rise of cybercrime presents unprecedented challenges to national legal systems, particularly where offences transcend territorial boundaries. Cybercriminals commonly take advantage of fragmented jurisdictional frameworks, disparate legal standards, and cumbersome mutual legal assistance procedures, all of which hamper effective prosecution. This paper analyses the legal and procedural challenges involved in prosecuting transnational cybercrime, with Bangladesh as its primary jurisdiction of focus. Through a doctrinal and comparative legal analysis, the study examines substantive and procedural cybercrime laws in Bangladesh as well as in selected jurisdictions such as the United States and the European Union, while also assessing international mechanisms including Mutual Legal Assistance Treaties (MLATs) and the Budapest Convention on Cybercrime. The findings reveal significant discrepancies among jurisdictions in cybercrime definitions, jurisdictional rules, standards for digital evidence, and procedures for accessing data stored abroad, which together constitute institutional barriers to effective law enforcement. Comparative analysis further demonstrates that the United States and the European Union have developed sophisticated and convergent frameworks such as the CLOUD Act, the European Investigation Order (EIO), and emerging e-Evidence mechanisms to facilitate expedited cross-border data access and coordinated prosecution. By contrast, Bangladesh continues to face substantial techno-legislative constraints, limited treaty networks, and outdated procedural mechanisms, resulting in investigative delays and prosecutorial inefficiencies. The study proposes a harmonization-oriented model emphasizing unified cybercrime definitions, streamlined MLAT procedures, reforms in digital evidence law, institutional capacity-building, and accession to key international conventions. It concludes that, without substantive legal harmonization and enhanced international cooperation, Bangladesh and similarly situated developing states will remain vulnerable to transnational cyber threats, thereby undermining national security and global cyber governance.

Keywords: Cybercrime, Cross-border jurisdiction, Digital evidence, Harmonization and Bangladesh.

1. Introduction

The rapid expansion of digital tools has altered the daily social and economic interactions and communications in Bangladesh and across the world. As more people can access the internet, mobile financial platforms can be used, and the dependence on digital services increased, cybercrime became a national and international problem that is demanding more and

more attention. Bangladesh is not an exception, as reported incidents of cyber-crime has seen increase of enormous scale mainly due to strengthening digital connectivity, widespread of social media usage, and low efficiency of the existing national cyber security regulation (Rana, 2023). The country is also at risk of sophisticated, transnational cyberthreats, as evidenced by high-profile incidents like the Bangladesh Bank heist of 2016. Documented manipulations of Facebook and other forms of operations highlight the growing complexity and dynamism in the forms of cyber threats targeting people and institutions.

Amid these advancements, our existing laws, including the Information and Communication Technology Act 2006, and more recently the Cyber Security Ordinance, 2025, have not been able to address modern-day cyber issues appropriately. Nevertheless, such laws are still plagued by vagueness, ambiguity of definition and application, violating the spirit of free speech, but do not effectively mitigate transnational cybercrime (Momtaz, 2024). Due to deficiencies in investigation, lack of technological knowledge and expertise and lack of digital forensic capabilities, Bangladesh lacks an adequate capacity to prosecute a cybercrime. Paragraph Description: The absence of sophisticated technological infrastructure dedicated to the management and display of digital evidence poses major challenges for lawyers and forensic investigators in the collection, preservation, and presentation of such evidence (Rahman, 2023). The problems are exacerbated by the fact that, due to Bangladesh's lack of a proper framework of extradition treaties, low level mechanism of inter-national cooperation, and low use of Mutual Legal Assistance Treaties (MLAT) (Momtaz, 2024), internet-based offences committed by individuals or groups, especially in countries that have the basis of a legal effect, make it a major challenge for domestic law enforcement agencies to investigate.

These challenges are not unique to Bangladesh. Cross-border jurisdictional disputes, ambiguities in cybercrime definitions, and variations in digital evidence standards across jurisdictions are well-documented issues in international scholarship (Phillips, 2022). In addition, the use of encryption, the storage of data outside of state borders, and the transnational nature of cybercrime (Bruce, 2024) further complicate the investigation and prosecution of cybercrime. A growing academic consensus has also acknowledged that the conventional approaches to policing and enforcement are not well-suited to respond to technologically progressed cybercrimes creating the need for new governance regimes, harmonized legal frameworks and greater international collaboration (Kandaker MMB., 2025). Although the literature on the legal institutions and regulatory framework on cybercrime in Bangladesh is growing, very few studies have measured the status of Bangladesh against international standards or best practices; or how international instruments such as the Budapest Convention on Cybercrime can help Bangladesh respond more consistently and effectively to cross-border cybercrime. There is also a lack of discussion of how to reform things like specialized cyber courts, MLAT procedures, and the digital forensic capacities. In light of these gaps, this study examines the legal and procedural challenges associated with prosecuting cross-border cybercrime in Bangladesh and compares them with international approaches adopted in jurisdictions such as the United States and the European Union. It seeks to provide a harmonization-facilitating model that has the potential to bolster Bangladesh legal capacity, facilitate trans-border collaboration, and ameliorate cybercrime prosecutions in an ever-connected cyber landscape.

2. Review of Literature

A growing body of scholarship suggests that cybercrime in Bangladesh has increased as access to digital tools and the internet has expanded. According to a study, enhanced internet penetration, prevalent use of social media and continuous existence of any security gaps contributes a lot to the rise in number of incidents and crimes in the cyber landscape. Even the most cyber-professional countries plagued by high-profile cyberattacks (e.g., the famed 2016 Bangladesh Bank heist) remain vulnerable to cyberattacks on their national systems. Use of social media - particularly Facebook - as a vehicle to promote numerous types of cybercrime and spread disinformation remains misused (Rana, 2023). The author goes on to claim that despite many laws being enacted in Bangladesh (ICT Act 2006, Cyber Security Ordinance, 2025), they

still fall short and lacks on effectiveness. Yet, these laws have been heavily criticized for being abused against dissent and ineffective against transnational cybercrime. These deficiencies are further compounded by jurisdictional obstacles, limited extradition treaties, weak institutional capacity, shortages of technical skills and forensic infrastructure, that allow offenders to escape accountability. In the same vein, another author observes that Bangladesh lawyers, most precisely from Rajshahi, face serious challenges in dealing with cybercrime (Rahman, 2023). The collection, preservation and presentation of digital evidence continue to pose a challenge as there is limited, if any, technological capability among investigators and advocates. Transnational offences compound these challenges, while also raising complex issues of admissibility, jurisdiction and compliance with procedures. Rahman also draws attention to the fact that scarcity of resources, such as lack of modern technological equipment to counter terrorism, lack of skilled manpower, lack of a proper forensic laboratory has caused a barrier in a successful prosecution process.

At the same time, Human Rights Watch (2024) and Hossain *et al.* Contend that the condition of the international nature of cybercrime has not been properly embodied in Bangladesh judicial practice (Hossain, 2024). Some specific laws, such as the Cyber Security Ordinance, 2025 and relevant legislative instruments do exist, but vague statutory definitions and weak enforcement mechanisms greatly limit the effect of deterrence. The lack of an efficient and prevalent framework for international cooperation or clear and operational guidelines for mutual legal assistance complicates matters further in cross-border investigations; in the Bangladesh Bank cyber heist for instance, investigators were faced with this daunting task. This involves the development of specialized cyber courts, enhancements to forensic capacity and collaboration at an international level, as stressed by these studies. They too lists conflicting jurisdictional assertions, failure of an appropriate legal framework and lack of global cooperation, as significant factors inhibiting the prosecution of cross-border cyber-crime in Bangladesh (Ehsan, 2024). It says ambiguities created due to overlaps between the Digital Security Act 2018 and the Cyber Security Act 2023 make the legal interpretation difficult and raises concerns about freedom of expression and privacy. Furthermore, insufficient mechanisms for obtaining digital evidence and low technical capability make the vast majority of cross-border crimes virtually impossible to investigate. Abstract of their analysis also states that Bangladesh uses very few available MLATs and regional tools and it causes delay in getting evidence based that is preserved in foreign lands.

In line with this, another study provides that the escalation of cyber-crime into more and more cross-border activity represents one of the most appealing enforcement challenges for Bangladesh (Momtaz, 2024). This is particularly the case where perpetrators, victims, servers, and facilitators are located in different jurisdictions and domestic courts are often ill-equipped to try such offences. In addition, the small number of treaties dealing with cybercrime, both bilateral and multilateral, can also present obstacles in the collection and taking evidence, extradition and enforcement of judgments. The literature routinely emphasizes the need for legal clarity, forensic capacity and international cooperation in Bangladesh to deal with such cases since they often cross borders. These national challenges echo what has been identified in international scholarship as persistent global matters. As a study points out jurisdictional clashes between states commonly interfere with international investigation of cybercrime worldwide (Ashurov, 2024). The World Cybercrime Index (Bruce, 2024) shows that criminal activity by cybercriminals is geographically uneven, requiring coordinated responses from the global community. It has been claimed that the inconsistency of definitions and types of cybercrime across jurisdictions as an obstacle to efficient international cooperation on this problem (Phillips, 2022). According to another study, encryption is a double-edged sword, a necessary measure to protect individual privacy but also one that creates obstacles to legitimate access to digital evidence (Van Daalen, 2023). In the context of Bangladesh, works of Chowdhury and Fahim and Mahmud *et al.* reiterate poor law enforcement capacity, low inter-institutional coordination, and

poor updating of legal and technological frameworks (Chowdhury, 2020).

Recent scholarship highlights ongoing lacunas in applicable laws dealing with cybercrime and data protection in Bangladesh - in particular, when it comes to cross-border processing and privacy protections. Some scholars widen the lens, focusing on under-researched populations and viewpoints in cybercrime studies (Ahmed, 2025), developing criminological theories for framing new cyber risks (Onwuadiamu, 2025), and calling for more robust worldwide institutions able to contend with technology-enabled crimes (Furger, 2024). Some of the earlier foundational work on global governance also emphasised the challenges in aligning legal regimes across jurisdictions (Alam, 2019).

In summary, the literature suggests that Bangladesh is experiencing increasing cyber risks without corresponding harmonized legal frameworks, contemporary investigative resources, dependable forensic capacity and robust international collaboration. Though challenges in prosecuting cyber-crimes in Bangladesh in a timely manner have been identified by previous studies, none contextualizes the needs within a best-practice framework nor examine the potential adoption or adaptation of international instruments such as the Budapest Convention on Cybercrime with a view to enable more effective cross-border prosecution of cyber-crimes affecting Bangladesh. Additionally, the potential for pragmatic reforms such as specialization of cyber courts, simplified mechanisms for MLAT, and consistent capacity-building for investigators, has not yet been explored in depth. To fill these gaps, this study correlates Bangladesh-specific challenges with comparative international perspectives and identifies realistic harmonization strategies that can be recommended to strengthen cross-border cybercrime prosecution.

Research Questions

1) What legal, jurisdictional, and procedural inconsistencies between Bangladesh and other jurisdictions constrain the effective prosecution of cross-border cybercrime?
2) What legal guidelines and collaborative mechanisms are required for Bangladesh to overcome these limitations and strengthen its capacity to prosecute transnational cybercriminal activities?

Research Objectives

1) To analyse the existing legal and jurisdictional framework of Bangladesh to suppress the cross border cybercrime.
2) To identify procedural and technical obstacles with respect to the access to, collection of and use of digital evidence which is stored abroad.
3) To Identify the types of Cybercrime prosecution mechanisms that exist in Bangladesh as compared to those in the United States and European Union.
4) To assess the effectiveness of existing international cooperation instruments, including Mutual Legal Assistance Treaties (MLATs) and the Budapest Convention on Cybercrime.
5) To propose harmonization-oriented legal and institutional reforms aimed at strengthening the prosecution of cross-border cybercrime in Bangladesh.

3. Methodology

This study adopts a doctrinal and comparative legal research methodology to examine the challenges of prosecuting cross-border cybercrime and to identify harmonization measures relevant to the Bangladeshi context. The study uses doctrinal evaluation of the statute provisions, case laws, International and institutional frameworks on cybercrime prosecution, digital evidence, jurisdiction and mutual legal assistance. This method enables a necessary review of the pros and cons of the current Bangladeshi legal system, focusing especially on the Information and Communication Technology Act 2006, and more recently the Cyber Security Ordinance, 2025. The study further employs a comparative legal approach by analyzing how advanced jurisdictions, notably the United States and the European Union, address cross-border cybercrime through instruments such as the CLOUD Act, the European Investigation Order (EIO), and the emerging e-Evidence framework. This comparison is designed to highlight practices from which Bangladesh may learn or adapt in building its prosecutorial capacity. The analysis relies mainly on secondary material such as the academic literature, policy reports, and recent academic works, which

provide background information as well as analysis. In addition, the methodology incorporates a prescriptive dimension, drawing on international legal standards to formulate recommendations for legal reform and harmonization. These recommendations also acknowledge the existing lack of institutional capacity and the limited treaty networks and old procedural mechanisms within which Bangladesh currently operates. The research is qualitative because of the purpose of this study to interpret legal instruments, do comparative legal analysis and make policy oriented recommendations.

Theoretical Framework

Through jurisdictional theory, transnational crime theory, legal harmonization theory and network governance theory, this study provides an account of the unique jurisdictional challenges that Bangladesh faces when prosecuting horizontal or cross-border cybercrime (Phillips, 2022). Jurisdictional theory shows that the traditional principles of criminal jurisdiction based on territoriality and nationality fail when the crime occurs in artificial environments like the web, a website or online service. When dealing with cybercrime layered across foreign jurisdictions, the point of the crime is often divided among numerous national authorities as criminals use technological infrastructures that exceed the boundaries of sovereign jurisdictions. Thus, cyber-crimes may seem to resemble conventional crimes while in fact they entail dispersed phases of action, and proof in multiple jurisdictions, making it more complex to investigate and punish. Transnational crime theory conceptualizes cybercrime as an inherently transnational crime that flourishes in the absence of comparably-legal regimes (Siddiqua, 2024). Cybercrime is not global in the sense that it transcends national borders, but rather due to the fragmentation of jurisdiction, pervasive global financial networks, and (transnational) digital infrastructure, no one state can hope to investigate or prosecute a crime perpetrated on foreign servers or involving foreign actors without the cooperation of other states. As crimes of global reach, this theoretical lens highlights the need for coordinated responses, as otherwise, unilateral enforcement mechanisms are largely ineffective against this transnational crime. Legal harmonization theory directly addresses these challenges and underscores the need for substantive and procedural laws to be aligned across jurisdictions. The aim of legal harmonization is to minimize disparities in definitions of cybercrime, jurisdictional rules, and standards of evidence which impede effective investigation and prosecution (Furger, 2024). Harmonization encourages compatible legal frame-works, which in turn provide for more seamless mutual legal assistance, quicker access to foreign stored data and interoperable enforcement mechanisms. This approach has been operationalized through international instruments such as the Budapest Convention on Cybercrime, the CLOUD Act, and the e-Evidence framework of the European Union. On this note, network governance theory who holds that the best governance of cybercrime is not monolithic and has both state and non-state actors (especially private tech companies and international service providers) - also mystifies the complexity of the cybercrime landscape and our global response to it. The relevance of this dimension is particularly notable in the context of Bangladesh, where access to key pieces of digital evidence is often in the hands of foreign-based platforms operating within different legal regimes. Network governance emphasizes cross-sectoral collaboration among states, non-state actors and international institutions on cybercrime. These theoretical frameworks give justifications for comprehending the systemic, legal, and institutional barriers that Bangladesh faces in its ability to investigate and prosecute cybercrime of cross-border relevance. They also contribute to the analysis of international best practices and assist in creating harmonization-related recommendations that are relevant to the context of Bangladesh both from a legal and institutional perspective.

Legal Frameworks of Relevant Countries and International Instruments

Bangladesh's Legal Framework

For more than two decades now, the trajectory of the law relating to cybercrime has evolved in Bangladesh, yet the existing legal regime is not sufficient for substantive addressable of offences with extra-territorial dimensions (Rana, 2023). The first official attempt to address cybercrime in Bangladesh was the

Information and Communication Technology (ICT) Act 2006 which criminalized acts like hacking, unauthorized access and electronic fraud. Although the Act was groundbreaking, it unfortunately received broad condemnation for poorly defined offences, major procedural deficiencies and most importantly for the over-broad application of Section 57, which severely limited existing freedoms of expression. The Digital Security Act (DSA) 2018 was passed with aim of updating the cybercrime regime, including a wider scope of cyber offences, dedicated cyber tribunals, and investigative powers of digital forensics. However, the DSA was heavily questioned for its heavy emphasis on content-based crimes and little room for complex and transnational cybercrimes. Based on continued domestic and international criticism, the DSA 2018 was repealed and replaced by Cyber Security Act (CSA) 2023. Yet the CSA still faced criticism for lack of clarity in specific definitions, opacity or vagueness in procedures that followed, and inconsistency with international norms of dealing with cybercrime. Currently, Bangladesh has the Cyber Security Ordinance 2025, which repealed the Cyber Security Act 2023, under which of course, it regulates cyber-crimes. While the Ordinance is an attempt to strike a new balance, preliminary analysis suggests that it recycles many of the systemic failures of its forebears, especially in cross-border cybercrime cases. This includes a restricted framework for extraterritorial jurisdiction, opaque processes for cooperation, and the lack of expedient and effective means for the access of foreign stored computer data.

Bangladesh lacks many of the key legal tools needed to meaningfully prosecute cybercrime, especially clear and operational means to secure digital evidence from abroad. While USA has the CLOUD Act and the EU has access to the e-Evidence framework and European Investigation Orders for cross-border accessing data or electronic evidence, Bangladesh continues to be an MLAT or heavy user. This process is considered slow, bureaucratic, and wrong type of mechanism for cybersecurity investigative speed. Bangladesh has initiated only a few bilateral MLATs and lacks direct data-sharing pacts with all major global service providers like Meta, Google, Apple etc. As a result, access to logs, references (IP address) as well as subscriber information and communication data stored abroad may take a long time for investigators or at worst, the evidence may be tampered with, deleted, and cannot be presented in court.

Additionally, there is no comprehensive evidentiary structure for the investigation of Digital Forensics in Bangladesh. While the Evidence Act 1872 has been amended to recognize electronic records, the legislation fails to address some fundamental issues such as lack of chain-of-custody requirements; the absence of specifications regarding metadata preservation; lack of uniformity in encryption standards; or lack of standards related to digital forensic authentication. OVERVIEW Cyber tribunals are often burdened by case backlogs, while judges, prosecutors and investigators often have little experience handling digital evidence. These limitations directly undermine the perceived evidential worth of cybercrime cases and therefore, the prosecution of this activity, especially when foreign offenders or transnational crime groups are implicated. At the institutional level, the regulation of cybercrime remains fragmented across various organizations - Bangladesh Telecommunication Regulatory Commission (BTRC), Digital Security Agency, different law enforcement cyber roles, and intelligence agencies. It has led to duplication of mandates, ambiguity over accountability structures, poor inter-agency coordination, and lack of a coherent national cyber governance framework. Along with little to no forensic laboratory capacity or even a lack of proper technological infrastructure and lack of training of enforcement weaponry, prosecution of cybercrime in Bangladesh remains ill-suited to the cross-border cyber-crime it faces.

On the whole, though the mechanisms to handle domestic cyber offences in Bangladesh may be at least sporadically functional, they are simply not fit for handling the sophisticated nature of transnational cybercrime. Unhelpful statutory silence upon the substantive or territorial jurisdictional triggers on cross-jurisdictional implicated crimes, expedited cross-border extract-guide procedures, and material procedural and enforcement guide unification with existing cybercrime international standards steadily preserve physical postures to effective prosecution. Such limitations highlight the importance of deep and

all-encompassing legal modernization, procedural consistency and bilateral and regional cooperation to bolster Bangladesh's capacity to fight against cross-border cybercrime.

United States Legal Framework

The United States has one of the most sophisticated legal framework on cybercrime control, founded by statutes like the Computer Fraud and Abuse Act (the "CFAA"), and the Clarifying Lawful Overseas Use of Data (the "CLOUD") Act. The CFAA also has wide jurisdiction to prosecute unauthorized access and related offences, irrespective of the physical location of the offender within or out of the United States. This is especially important in the context of international cooperation because the CLOUD Act permits U.S. authorities to order U.S. providers - e.g., Facebook, Google, Microsoft - to disclose data stored on any server, anywhere in the world. The latter also allows the foreign governments, through the executive agreements, to request electronic records from U.S. companies without the need of the traditional MLATs. Such legal framework positions the United States as a necessary forum for cross-border digital evidence retrieval and establishes a gold standard for rapid access to data around the world.

European Union Legal Framework

Within the European Union (EU), however, there has emerged a harmonized regional model for examining and prosecuting cybercrime across its Member States, enabling this cross-border crime to be properly addressed. One of the most important tools is the European Investigation Order (EIO), which enables law enforcement to obtain evidence from any EU state in a rapid and standardized manner. This is alongside the e-Evidence Regulation, which allows authorities in one EU country to quickly, and via mandatory short deadlines, request electronic evidence like subscriber information, IP logs, and communication records from service providers located in another Member Country. These frameworks further a less MLAT-dependent world and are exemplars of legal harmonization. The combination of the (largely) equal implementation of the Budapest Convention and the joint and comprehensive data protection rules under the GDPR contribute to an overall better coordinated cyber governance in the EU.

Mutual Legal Assistance Treaties (MLATs)

Mutual Legal Assistance Treaties (MLATs) represent the conventional channels shining light on ways that countries ask foreign countries for help in obtaining evidence, freezing proceeds of crime or locating suspects. While MLATs are vital in international co-operation they are notorious for their bureaucratic nature and slowness, which often contrasts with the speed that cyber criminality can occur at. The processing times average several months and in some cases, years, and result in the loss of volatile digital evidence. As for a country like Bangladesh, where specific bilateral agreement(s) and regional mechanism(s) are absent, MLAT is the only weapon in combating foreign stashed data; hence, arresting the perpetrators of cross-border cybercrime increases complexity.

Budapest Convention on Cybercrime

The Budapest Convention is the first and most significant international treaty to address cybercrime. It facilitates uniformity in definitions of cybercrime, standardization of investigation procedures and expeditious cooperation between nations are concerned. With its 24/7 Network signatory countries can call to each other to request urgent data preservation and assistance from other member states. The Convention considerably enhances international enforcement powers by establishing clear frameworks for jurisdiction, evidence sharing and procedural alignment. Bangladesh, on the other hand, is not a signatory yet, meaning that its access to these rugged cooperation mechanisms is limited and, to an extent, it finds itself unable to prosecute individuals involved in cybercrimes that have cross-border elements.

4. Results and Discussion

Comparative Analysis of Cross-Border Cybercrime Legal Frameworks

An analysis of the cybercrime laws adopted by Bangladesh, the USA, the EU, and some important global instruments shows very remarkable differences in prosecuting transborder crimes (Ashurov, 2024; Phillips *et al.,* 2022). These differences are what can explain a lack of Bangladesh's progress on this area compared to much more progressive jurisdictions that are able to react more cohesively and stronger against transnational cybercrime (Momtaz, 2024). The general legal domain surrounding this issue in Bangladesh

(ICT Act 2006, and Cyber Security Ordinance, 2025) is almost completely domestic, with few provisions for extraterritorial jurisdiction or expedited cooperation for digital evidence stored abroad. This is due to its dependence on slow Mutual Legal Assistance Treaties (MLATs), the lack of special bilateral treaties and that it is not a member of the well-known Budapest Convention, which very much limits its easy access to evidence from foreign technology giants such as Meta, Google or Apple.

The combination of these factors renders it almost powerless against techno-intelligent jurisdictions, while institutional constraints–limited forensic capacity, fractionalization among law enforcement, lack of judicial specialization - further entrains its subservient status. And as opposed, the U.S. has created a comprehensive and sweeping legal regime to prosecute these crimes. Extraterritorial application of the CFAA is quite expansive when U.S. systems or people are impacted. But, the most transformative provision is the provision known as the CLOUD Act, which allows U.S. law enforcement and partner governments to directly request digital evidence from U.S. service providers no matter where the data is stored in the physical world. It avoids longstanding MLAT logjams and forms a rapid access route for evidence - something Bangladesh would never be able to access, as none, and there are no bilateral CLOUD Act agreements either. Elite cyber teams from U.S. federal agencies also make investigations more efficient. The European Union, therefore, offers an even more intertwined and harmonized model. In this regard, the European Investigation Order (EIO) and the e-Evidence Regulation provide well established mechanisms to allow fast-paced and harmonized cross-border access to electronic evidence on the basis of mutual recognition. The protection of cross-border evidence requests within tight deadlines from EU service providers provides the region with unequaled procedural uniformity. In addition, Athens would show how legislative harmonization can respect human rights as the EU enforces the Budapest Convention with strong data protection safeguards in the GDPR (Council of Europe, 2001; Van Daalen, 2023). This is in stark contrast to Bangladesh's piecemeal and slower approach. As far as international cooperation frameworks are concerned, MLATs represent the minimal method for the sharing of evidence. Nevertheless, the three jurisdictions - Bangladesh, the U.S., and the EU - are quite different in their MLAT dependence. While Bangladesh relies almost entirely on MLATs for obtaining foreign data, the U.S. and EU are increasingly adopting direct access mechanisms that minimize delays and enhance investigative results.

Beyond strengthening cooperation, the Budapest Convention makes cybercrime definitions, procedural rules, and jurisdictional principles more uniform among signatories (Council of Europe, 2001). The rapid channel of cooperation directly benefits the United States and EU Member States while putting Bangladesh who has yet to sign at a disadvantage. In general, the comparison shows that Bangladesh works in a localhost, domestic, and process-oriented way that cannot facilitate the nature of transnational cybercrime. On the other hand, the US and the EU use more up-to-date, streamlined, technology-responsive systems that allow for time-sensitive evidence retrievals and cross-border investigations. These gaps between the constitution as well as the existing systems reflect the necessity for Bangladesh to rationalize its legal framework, institute harmonization policies, build institutional capacity, and penetrate into the depth of international cooperation tools to prosecute cross-border cyber-crimes.

Key Findings

The analysis of Bangladesh's cross-border cybercrime prosecution framework, compared with the legal systems of the United States, the European Union, and key international mechanisms, reveals the following major findings:

Bangladesh's jurisdictional framework is inadequate for cross-border cybercrime

The challenge for cybercrime prosecution however comes from the fact that hardly any of the cybercrime laws in Bangladesh are territorial in nature. Unlike the United States - which claims sweeping extraterritorial jurisdiction via the CFAA - and the European Union, which has codified harmonized jurisdictional rules, Bangladesh has no clear legislative power to prosecute cybercriminals residing in other countries. This

shortcoming gives rise to geographical loopholes available to offenders to evade enforcement.

Accessing foreign-stored digital evidence remains one of Bangladesh's most significant challenges

The inability to directly address the major service provides such as Meta, Google, Apple - which mostly fall under U.S. and/or EU jurisdiction - leads Bangladesh to go through the sluggish Mutual Legal Assistance Treaty (MLAT) process to collect pertinent evidence like IP logs, metadata, and subscriber information. On the contrary, US CLOUD Act and EU e-Evidence Regulation propose quick and straightforward access tools to skip MLAT delays. No such agreements exist for Bangladesh, leading to significant loss of evidence and delays in investigation.

Bangladesh's institutional and forensic capacity is insufficient to meet the demands of modern cybercrime investigation

There are insufficient digital forensic laboratories in the country, few cyber investigation units, and law enforcement forces capable of dealing with sophisticated cyber offences. Depending on agency, eg, BTRC, Digital Security Agency, police cyber units; there are overlapping mandates and weak coordination due to fragmentation. By contrast, the U.S. (FBI, CISA) and EU (Europol, ENISA) have dedicated and highly sophisticated cybercrime infrastructures.

Bangladesh's procedural laws are not harmonized with international cybercrime standards

Furthermore, being outside the Budapest Convention denies Bangladesh the use of standardized investigative measures, expedited channels for requesting assistance, preservation of evidentiary data on an emergency basis, and harmonized definitions of cybercrime. At the same time, the harmonized nature of these explorations allows the U.S. and the EU to conduct timely, collaborative cross-border inquiries.

Reliance on traditional MLATs makes Bangladesh's cross-border investigations slow and ineffective

MLATs also have a very bureaucratic and slow nature, frequently taking months if not many years to go through. Since cyber evidence is a volatile type of evidence that can be altered or deleted in no time, delays in the collection of digital data to preserve evidentiary value is a major drawback. Getting around the delays they can face under their MLATS, the U.S. and EU are looking for ever more ways to work directly, such as with the CLOUD Act and EIO, leaving Bangladesh comparatively behind.

Private technology companies play a critical role that Bangladesh cannot currently leverage effectively

Since service providers gate a good portion of digital evidence, network governance theory demonstrates that cybercrime enforcement is contingent not only on governments. Though countries like the U.S. or the EU already have such frameworks that legally obligate service providers to cooperate, the same is not true for Bangladesh, which lacks any such mechanism with its international partners. In result, cooperation with foreign companies is sporadic and often takes time.

Bangladesh's cyber laws focus more on domestic content regulation than sophisticated transnational threats

For instance, while the ICT Act, 2006, and the Cyber Security Ordinance, 2025 drag crimes related to speech and online content, more intricate types of crimes (like transnational hacking, financial malware and ransomware, or international fraud networks) are left unmentioned and unregulated. The difference in laws limits the application of criminal codes to international cybercrime trends, making these criminal codes less effective for prosecutors.

There is a significant gap between Bangladesh's legal framework and international best practices

Commentary analysis indicates the design of U.S. and EU systems as modern, efficient, and harmonized to facilitate rapid access to evidence, cross-border cooperation, and cyber investigations. In comparison, Bangladesh has no such extraterritorial jurisdiction, speed and ease of evidence-sharing, forensic capacity, harmonized legal standards and treaty networks needed to pursue effective cross-border prosecutions.

Bangladesh must adopt harmonization strategies to improve cross-border cybercrime prosecution

The results demonstrate the need for Bangladesh to update its laws, including adapting definitions of

cybercrime to match those found in the rest of the world, implementing speedier methods for evidence-sharing, joining international conventions like the Budapest Convention, enhancing institutional capacities and establishing bilateral data-sharing deals with crucial jurisdictions such as the US.

5. Conclusion and Recommendations

This study highlights that Bangladesh's rapidly increasing dependence on digital technologies has not been matched by an effective legal, procedural, or institutional framework capable of addressing cross-border cybercrime. The findings reveal significant shortcomings in investigative capacity, evidentiary mechanisms, and international cooperation, particularly in cases involving foreign servers, digital platforms, and transnational criminal networks. Existing procedures for obtaining electronic evidence from abroad are slow and inefficient, resulting in delays, evidentiary gaps, and weak prosecution outcomes. Moreover, Bangladesh's current legal framework remains largely inward-focused, emphasizing content regulation rather than effectively addressing transnational cyber offenses such as digital extortion, fraud, and coordinated foreign cyberattacks.

The absence of clear extraterritorial jurisdiction, simplified mechanisms for accessing overseas data, and harmonization with international cybercrime instruments has allowed cybercriminals to exploit jurisdictional loopholes. In contrast, more developed jurisdictions have adopted streamlined systems that facilitate faster evidence collection and cross-border coordination, reflecting the realities of an interconnected digital environment. Collectively, these findings indicate that Bangladesh must pursue comprehensive legal and institutional harmonization to strengthen its response to transnational cybercrime. This requires reforming existing procedures, enhancing forensic and investigative capacities, establishing specialized cybercrime courts, improving cooperation with foreign authorities, and engaging more directly with global technology service providers. Without such reforms, Bangladesh will remain vulnerable to increasingly sophisticated cyber threats that undermine national security and public trust in the digital ecosystem.

Recommendations

Based on the findings of this study, several legal, procedural, and institutional reforms are necessary for Bangladesh to strengthen its capacity to investigate and prosecute cross-border cybercrime effectively. The following recommendations outline a comprehensive harmonization strategy grounded in global best practices:

Establish Clear Extraterritorial Jurisdiction for Cybercrime Offences

Bangladesh should have clear provisions in the statute that allow it to prosecute cybercriminals who may commit a cybercrime from a foreign location, as long as the adverse impact of the crime is felt in Bangladesh Reflected in jurisdictional doctrines applied in the US (under the CFAA) and that of EU-Member States, it will allow Bangladesh to claim jurisdiction in applicable transnational cases.

Join the Budapest Convention on Cybercrime

Embracing international cooperation, access to consistent definitions of cybercrimes, expedited investigation processes, emergency data preservation channels, and the 24/7 global law enforcement cooperation network would become available to Bangladesh with its accession to the Budapest Convention. It would drastically diminish bandwidth on the protracted MLAT structures and garner Bangladesh a seat at the global cyber governance table.

Negotiate Bilateral or Multilateral Data-Sharing Agreements

Going ahead, Bangladesh should seek to enter into agreements such as the U.S. CLOUD Act Executive Agreements or enter into regional cooperation frameworks. These agreements would provide expedited, direct access - avoiding the decades-long MLAT delay for quicker movement of electronic evidence kept by large service providers and speeding up loss of evidence.

Reform MLAT Procedures and Strengthen International Cooperation

Hence, Bangladesh must streamline its processes for MLAT, even as it seeks methods other than MLAT, by forming dedicated MLAT cells in the Home ministry, embracing digital channels for submitting

requests, and while ensuring adherence to international standards of timeliness and completeness. An increased focus on building on INTERPOL, Europol and SAARC/BIMSTEC cyber cooperation mechanisms would similarly enhance information sharing.

Develop Specialized Cybercrime Courts and Prosecutorial Units

These courts must have judges with appropriate digital evidence training and exposure to cross-border legal principles. Bangalrean Having a National Cyber Prosecution Authority, or specialized unit within the Attorney General's Office, would bolster handling of complicated transnational cases by adding consistency and expertise.

Expand Forensic Capacity and Invest in Advanced Technologies

Day-to-day law enforcement agencies and government establishments should invest to develop state-of-the-art digital forensic laboratories, and effective chain-of-custody protocols, and tools to analyze encrypted, cloud-based, and distributed data. In partnership with international organizations, institutionalize specialized training programs for investigators, prosecutors and judicial personnel.

Adopt Uniform Standards for Digital Evidence Collection and Preservation

The Evidence Act and the procedural codes of Bangladesh should be revised to spell out specific rules for electronic evidence, such as metadata retention and hash, chain-of-custody rules, and rules for compliance with international standards of admissibility.

Strengthen Interagency Coordination and Create a Central Cyber Command Structure

Lack of cyber coordination makes investigations harder There should be a mechanism in Bangladesh for a central cyber command that can adopt an all-hands-on-deck strategy by binding all key players under it like BTRC, Digital Security Agency, law enforcement cyber units and intelligence bodies so that they can quickly decide effectively in a coordinated manner and sharing of information can take place easily.

Engage with Private Sector and Technology Companies

Nearly all the digital evidence resides with foreign service providers, so Bangladesh must have policies that allow for cooperation with them, specifically with companies like Meta, Google, and Apple. This could include: establishing liaison offices, providing standardized request templates, being involved in top level conversations and debates around transparency and access to data.

Promote Public Awareness and Preventive Cybersecurity Measures

Reforming the law has to be accompanied by prevention, including awareness campaigns, cyber-security education, and the collaboration of the private sector, especially cybersecurity firms. Higher digital skills will reduce susceptibility to cybercrime and increase reporting.

Encourage Regional Cyber Cooperation in South Asia

Bangladesh should propose a SAARC or BIMSTEC cyber coordination architecture that places priority on common protocols for digital evidence, reporting of cyber incidents and cyber threat intelligence at a regional level.

Adopt a Long-Term National Cybersecurity Harmonization Strategy

Bangladesh needs to formulate a national policy with a focus on the following: consistent laws with international cyber standards, institutional strengthening, direct cooperation mechanisms, periodic law reform reviews, and integration of global best practices.

6. Ethical Clearance

The research has been conducted in accordance with ethical standards, ensuring the values of integrity, honesty, and fairness was upheld throughout the study.

7. Acknowledgement

First and foremost, the author expresses sincerest gratitude to the Almighty for bestowing upon him the health, knowledge, ability, and opportunity to undertake and complete this research endeavor. Without His divine guidance and protection, this journey would not have been possible. The author also extends his heartfelt thanks to all individuals and

institutions whose support and cooperation contributed to the completion of this research.

8. Conflicts of Interest

The author declares that there is no conflict of interest.

9. References

Ahmed, M. F. (2025). The future of cybersecurity and data privacy in Bangladesh: Identifying the legislative gaps. *Asian Journal of Social Sciences and Legal Studies*, 347-357. https://doi.org/10.34104/ajssls.025.034700357

Alam, S. (2019). Cyber crime: A new challenge for law enforcers. *City University J.,* **2**(1), 75-84.

Ashurov, A. (2024). Jurisdictional challenges in cross-border cybercrime investigations. https://doi.org/10.5281/zenodo.11234768

Bruce, M. L. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. *PLOS ONE,* **19**(4). https://doi.org/10.1371/journal.pone.0297312

Chowdhury, M. A. (2020). An insight into the cyber-crimes and cybersecurity measures in Bangladesh: Quest for operative legal remedies. *Solid State Technology,* **63**(6).

Ehsan, S. B. (2024). Balancing cybersecurity and individual rights: A critical analysis of Bangladesh's Cyber Security Act 2023. *Journal of Creative Writing,,* **8**(1), 85-98. https://doi.org/10.70771/jocw.v8i1.109

Furger, A. (2024). Can they deliver? The practice of joint investigation teams (JITs) in core international crimes investigations. *Journal of International Criminal Justice,* **22**(1), 43-58. https://doi.org/10.1093/jicj/mqae005

Hossain, S. R. (2024). A study based on the effectiveness of Cyber Security Act 2023 in pursuit of preventing cybercrime: Bangladesh perspective. *Inter J. of Law, Policy and Social Review,* **6**(5).

Kandaker MMB., a. G. (2025). The right to privacy in the digital age: state concerns and initiatives in Bangladesh. *Asian J. Soc. Sci. Leg. Stud.,* **7**(1), 279-289. https://doi.org/10.34104/ajssls.025.027900289

Momtaz, S. (2024). Navigating Cyber Security Challenges and Legal Frameworks in Bangladesh: An in-depth Exploration. *Inter J. of Research and Innovation in Social Science*, 727-751. https://doi.org/10.47772/IJRISS.2024.801056

Onwuadiamu, G. (2025). Cybercrime in criminology: A systematic review of criminological theories, methods, and concepts. *J. of Economic Criminology,* **8**. https://doi.org/10.1016/j.jeconc.2025.100136

Phillips, K. D. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic Sciences,* **2**(2), 379–398. https://doi.org/10.3390/forensicsci2020028

Rahman, A. (2023). The examination of obstacles confronted by lawyers in the prosecution of cybercrime in Rajshahi, Bangladesh. Retrieved from 19. Rahman, A. (2023). The examination of obstacles confronted by https://doi.org/10.13140/RG.2.2.10793.36962

Rana, M. (2023). A Critical Analysis of the Escalating Cybercrime and its Impact in Bangladesh. *CIFILE Journal of International Law*.

Siddiqua, R. (2024). Challenges faced by police officers in investigating cybercrime: An exploratory study in Bangladesh. *International Journal of Humanities, Social Sciences and Education,* **11**(7), 150-161. Retrieved from https://doi.org/10.20431/2349-0381.1107014

Van Daalen, O. L. (2023). The right to encryption: Privacy as preventing unlawful access. *Computer Law & Security Review,* **49**. https://doi.org/10.1016/j.clsr.2023.105804

Citation: Kandaker MMB. (2026). Cybercrime prosecution in cross-border jurisdictions: legal challenges and paths to harmonization, *Asian J. Soc. Sci. Leg. Stud*., 8(1), 509-520. https://doi.org/10.34104/ajssls.026.05090520