International Journal of Criminology & Justice (IJCJ)

VOLUME 1 ISSUE 1 (2025)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

International Journal of Criminology & Justice (IJCJ)

Volume 1 Issue 1, Year 2025
https://journals.e-palli.com/home/index.php/ijcj

Judicial Challenges in Prosecuting Cross-Border Cyber Crimes

Rejvi Ahmed Bhuiya[1*], Md. Hasan Chowdhury[2], Emmanuel Nweke Okafor[3], Md. Asaduzzaman[4], Shahrima Akter[5]

Article Information

Received: August 01, 2025
Accepted: September 06, 2025
Published: October 11, 2025

Keywords

Bangladesh, Cross-Border Cybercrime, Digital Forensics, International Cooperation, Judicial Challenges

ABSTRACT

Cybercrime has emerged as a serious global threat, and international cases are among the most challenging in terms of law and institutions. Bangladesh, as one of the fastest-growing digital frontiers, faces an increasing number of cyber threats undermining, especially its ICT Act (2006) and Digital Security Act (2018). Old laws, global cooperation failures, and poor forensic abilities present obstacles to successful conviction. The study aims to explore the judicial impediments, the jurisdictional problem, inadequacy of national law, international assistance, and the technical evidence in the context of prosecuting the cybercrimes perpetrated across the border in Bangladesh. The study is quantitative in nature, with a sample size of 400, consisting of ICT practitioners, lawyers, security personnel, and policy makers. Descriptive statistics were computed to examine professional perspectives and to establish any patterns. Findings revealed that outdated laws, unclear jurisdictions, and a lack of extradition agreements provide loopholes for cybercriminals. They also stressed that other contributing factors include lack of international cooperation, unsuccessful implementation of Mutual Legal Assistance Treaties (MLATs), and an inadequate forensic toolkit. Shortage of skills among research staff also undermines the handling and prosecution of evidence. The research indicates a pressing requirement for the reform of law, creation of specialized cyber courts, improved forensic infrastructure, and enhanced international cooperation to enable Bangladesh to combat transnational cybercrimes effectively.

INTRODUCTION

Cybercrime is generally defined as the use of a computer to commit illegal activities, such as hacking. It is the most common type of computer crime that an individual can potentially engage in. However, a standard definition has proven to be elusive, resulting in a wide range of understanding and responses related to cybercrime within and among various legal systems and sectors. The lack of consensus is a significant obstacle to developing holistic legislation and policies to fight cybercrime (Phillips *et al.,* 2022). Cybercrimes are prevalent worldwide and have become every country's nightmare. Moreover, even though cybercrime may seem like a worldwide problem, it is to a large extent. The World Cybercrime Index (WCI), used by expert surveys, identifies Russia, Ukraine, China, and the US as those that have the most cybercriminal activity (Bruce *et al.,* 2024). Each country has its own laws, which cause confusion and jurisdictional issues when prosecuting cross-border cybercrimes. The internet's distributed structure has made it hard to investigate the source of crimes, and criminals have been able to exploit legal terms to avoid prosecution. Budapest and MLATs The Budapest Convention and mutual legal assistance treaties (MLATs) take time and are not always signed by all countries, making country-to-country cooperation difficult, both morally and in practice (Ashurov, 2024). Even with international effort, without cooperation between nations being dependable, effective prosecution can be blocked and be a negative space of justice. It observes that Joint Investigation Teams (JITs) have not comprehensively tackled these problems, as sharing evidence, as well as operative powers, is impossible. Disjointed efforts and overlaps among those who are handling the investigations are complicating the investigations, which drives inefficiencies and causes harm to the victims, the paper remarks (Furger, 2024). Technological Barriers to Evidence Collection opens with a discussion of the difficulty law enforcement and intelligence agencies encounter when seeking access to evidence that is encrypted. Encryption plays an increasingly important role in safeguarding privacy and securing digital communications, yet it is posing new challenges for investigations (Van Daalen, 2023). With the rapid adoption of digital technology in Bangladesh, there has been a significant increase in cybercrimes, particularly cross-border ones. This rising menace also demonstrates the necessity of updated legislative tools to meet these emerging threats and to safeguard the public in cyberspace. The rise of cybercrime means more stringent laws and regulations to provide security and to combat criminal activities on the internet (Mahmud *et al.,* 2023). Bangladesh's ICT Act and Cyber Security Act have repeatedly exposed the shortcomings when it comes to cybercrimes spreading across the border. These laws,

[1] Faculty of Graduate School, Program of Peace Studies and Diplomacy, Siam University, Bangkok, Thailand
[2] Independent Researcher, Dhaka, Bangladesh
[3] Faculty of Graduate School, Program of Peace Studies and Diplomacy, Siam University, Bangkok, Thailand
[4] Foreign Exchange Division, Mercantile Bank PLC, Dhaka, Bangladesh
[5] Department of Law, Times University Bangladesh, Faridpur, Bangladesh
[*] Corresponding author's e-mail: azrejvi@ru.ac.bd

even in the sphere of national cyber-threats, are ill-suited for global jurisdictional concerns, enforcement, and cooperation across national borders. Since cybercrime activities are mostly cross-border in nature, the existing laws in Bangladesh are insufficient to combat sophisticated transnational cybercrimes (Onwuadiamu, 2025) fully. The cybercrime threat in Bangladesh is growing in tandem with the increasing number of internet users and digital services. This increase is notwithstanding; the country's cybercrime units are underfunded, staffed by poorly skilled personnel, and do not have the infrastructure that is required to solve such crimes. Despite the existence of laws like the ICT Act (2006) and the Digital Security Act (2018), these are inadequate, and it is not clear how far they include the whole spectrum of crimes of the cyberworld, such as social media and cross-border attacks, etc (Chowdhury & Fahim, 2020). As new cyber threats emerge, Bangladesh's law enforcement response has lagged. The field of policing faces internal and external challenges in Internet-based criminal investigations. They are hamstrung from within by dismal logistics, inadequate training, and an avalanche of routine tasks, which often prevent them from dedicating time to complex digital cases (Siddiqua, 2024). The lack of strong consent standards, the absence of timely data breach notifications, vague provisions that limit freedom of expression, and restricted investigative capacity erode enforcement. Critical infrastructures are inadequately protected, and cross-border crime control is undermined by the lack of international cooperation (Ahmed & Arifuzzaman, 2025). Therefore, the main aim of the study is to explore the complex legal, jurisdictional, and cooperative issues that arise when trying to prosecute cybercrimes that span multiple countries, and to understand how these challenges hinder effective justice and international collaboration.

LITERATURE REVIEW

A study by Rana (2023) found that the reported cybercrime has surged in Bangladesh with increased internet access, social media expansion, and inadequacy of security systems. Big hits like the 2016 Bangladesh Bank heist show how the system is wide open for massive theft, while sites like Facebook are abused in the commission of crimes. Even though the country has laws such as the ICT Act 2006 and Digital Security Act 2018, there are still gaps; they are often used against dissenters, and they are also not the best way to deal with cross-border crimes. Prosecution is also weak due to jurisdictional issues, no extradition treaties, narrow tribunals, a lack of technical knowledge, and a small forensic capacity, all of which mean that most violators can escape the reach of justice. Another study, Rahman (2023), presented that advocates have to encounter many problems to deal with cyber crimes, especially in Rajshahi. In particular, there are some prominent challenges to gathering, preserving, and proving digital evidence, because many investigators and attorneys do not have enough technical competence to deal with forensic data efficiently. Crimes that cross borders can make cases still more complicated, with questions of admissibility and jurisdiction. Limitations on resources, such as a lack of technology and forensic labs, as well as funding, undermine the prosecution process. Hossain *et al.* (2024) present that Bangladesh presents a notable judicial hurdle in prosecuting cross-border cybercrimes. "While the Cyber Security Act 2023, as well as other laws, are available, they are ineffective due to not being well defined, with few sanctions, which are not deterrents. Weak international cooperation and a lack of established guidelines for mutual legal assistance also impede the prosecution of crimes with foreign flavours, such as the Bangladesh Bank cyber heist. The establishment of powerful deterrence by increasing the punishment, the creation of specialized cyber courts at the district level, state-of-the-art forensic institutes, and more cooperation at the international level are required to break the deadlock. A significant study conducted by Ehsan and Saquib (2024) found that prosecution of cross-border cybercrimes in Bangladesh confronted significant obstacles on account of the jurisdictional overlaps, lack of legal infrastructure, and the absence of proper international cooperation. Even when cybercrimes do cross national borders, the judicial system in Bangladesh is hampered by antiquated processes, a lack of technical capabilities, and inadequate practices for the collection of digital evidence. Legal ambiguities and interplay between the Digital Security Act 2018 and the Cyber Security Act 2023 make prosecution difficult and often give rise to concerns for freedom of expression and privacy rights. MLATs and regional cooperation are also underutilized. In the same perspective, Momtaz (2024) viewed that one of the biggest hindrances in the field is that cybercrimes are taking place from outside of this country, and the Bangladesh courts have no jurisdiction over them, with servers/facilitators/suspects/victims being scattered in multiple locations, including Bangladesh. This challenge of international cooperation is further exacerbated by the limited cybercrime-related bilateral and multilateral treaties that have been entered into by Bangladesh. The consequence is that the collection of evidence across national boundaries, extradition, and enforcement of judgments continue to be highly problematic. Previous investigations have highlighted that Bangladesh has weak laws and a lack of forensic capabilities and cooperation from other nations to fight cross-border cybercrimes. However, much of this research only highlights problems without comparing the experience of Bangladesh to other countries or explaining why global tools such as the Budapest Convention are rarely applied in the country. The voices of victims and the need for practical reforms, such as specialized cyber courts or better-trained investigators, are also missing. This study aims to bridge that gap by looking at these issues together and suggesting realistic ways forward for Bangladesh.

Research Questions

From the background of this study, the key research questions emerge as follows:

1. In what ways do differences in countries' laws and jurisdictions make it harder to bring cybercriminals to justice across borders?

2. What real obstacles do nations face when trying to work together, share evidence, and coordinate in tackling cross-border cybercrimes?

Objectives

The following specific objectives guide the study:

1. Explore the challenges different countries face in creating laws that effectively address cross-border cybercrimes.

2. Examine the complexities involved in determining which country's laws should apply when cybercrimes cross national boundaries.

3. Investigate how countries collaborate or struggle to coordinate efforts in prosecuting cybercrimes that span multiple jurisdictions.

4. Analyze the difficulties in collecting and handling digital evidence from multiple countries, especially with differing legal standards and privacy laws.

Theoretical Framework

In pursuing the prosecution of cross-border cybercrimes, this study has employed the thought of International Legal Pluralism, as initially developed by Teubner (1997), to articulate the problem. Legal pluralism at heart is the idea that the world is not governed by a single "legal system" of individual, coercive domination, but by multiple legal systems, many of which overlap and some of which even cooperate, but many of which also come into conflict with one another. These systems range from national to international laws, from bilateral treaties to informal country-to-country agreements. This concept is particularly relevant in the context of cybercrime. Crimes committed online seldom remain in one country. The hacker might be sitting in one country, the victim in another, and the servers anywhere in the world. This has left a significant quantity of confusion: Which laws should apply, who has a right to investigate, and how can countries share evidence when their legal rules are so very far apart?

When it comes to the five objectives of this study, international legal pluralism also provides insight into the first two goals, on the difficulty of creating good laws and the problems with the jurisdiction decision-making process when there is not a "master law" that lays down the law. Moreover, for the third objective, which is to cooperate, this framework explains why countries so often fail to collaborate: They are operating under different rules, protocols, and priorities. Moreover, in fourth place, even if and when some evidence is collected, every country has its own rules about privacy, admissibility, and enforcement. The guiding theory for this research, international legal pluralism, helps explain why law enforcement's job in prosecuting cybercrime across borders is so messy and challenging. It also emphasizes the importance of greater international cooperation and more adaptable legal instruments capable of reconciling different systems.

MATERIALS AND METHODS

This study uses a quantitative research approach to understand the judicial challenges of prosecuting cross-border cybercrimes in Bangladesh. The aim is to capture the real experiences and perceptions of people directly connected to this issue, including legal practitioners, cybercrime investigators, ICT experts, and policymakers. By focusing on their views, the study seeks to measure how jurisdictional differences, weak international cooperation, and technological barriers affect the prosecution process. To gather primary data, a structured survey questionnaire is used. The questions were supposed to be simple, easy to answer, including topics such as legislative framework, collecting evidence, international cooperation, and the effectiveness of prosecution in general. A 5-point Likert scale is used in which individuals can rate their agreement, ranging from " strongly disagree " to " strongly agree. This makes it possible to capture a range of opinions in a measurable way. The sample size for the survey is calculated using Cronbach's formula. The formula considers the margin of error, the confidence level, and the estimated variation that exists in the population to ensure that the sample size is statistically valid for the extrapolation of the results.

Cronbach's formula for sample size determination is used to calculate the sample size for this study. The formula is as follows:

$n = (Z^2 \ .p \ .(1-p))/E^2$

Where,

n = Required sample size

Z-score corresponding to the desired confidence level (for example, a 95% confidence level would correspond to Z=1.96

p = Estimated proportion of the population that exhibits the characteristic of interest (since we do not know the exact proportion, p is usually set at 0.5 for maximum variability)

E = Margin of error (expressed as a decimal, for example, 0.05 for a 5% margin of error)

Step-by-Step Process

Determine Confidence Level: A standard confidence level for social research is 95%, which corresponds to a Z-score of 1.96.

Estimate Proportion (p)

If the proportion of employees exhibiting the characteristic is unknown, it is conservative to use p = 0.5, as it maximizes the sample size.

Set Margin of Error (E)

The margin of error represents the precision of the estimate. A common choice is E = 0.05 (i.e., 5% margin of error).

Apply Formula

Plugging these values into the formula, the sample size will be calculated.

For example, assuming a 95% confidence level (Z = 1.96), an estimated proportion of 0.5 (p = 0.5), and a margin of error of 5% (E = 0.05):

$n = ((1.96)^2 .0.5.(1-0.5))/(0.05)^2 = 384.16$

The sample size has been appropriately determined to ensure the result is reliable. Based on the formula for calculating sample size for proportions, we obtained that approximately 384 subjects are required. To ensure the data are robust and in case there are non-responses in some cases, the study targeted 400 participants in total. A stratified random sampling technique is used to select the participants to represent all voices from various institutions and professions equitably.

After data has been gathered through the survey, this software (version 25 of SPSS) is applied to conduct the analysis. Descriptive statistics, means, proportions, and frequency tables summarize responses. We will also compare patterns between groups (e.g., lawyers vs. police officers vs. ICT experts). The study is conducted in accordance with ethical principles. All participants received the study's objective and decided to participate voluntarily. "You will be consented prior to beginning, and your name and answers will be kept confidential". By taking this approach, the study aims to present a roadmap of the challenges for Bangladesh in tackling cross-border cybercrimes and make some practical recommendations to enhance laws and institutions in order to ensure stronger safeguards for people in the cyber era.

RESULTS AND DISCUSSIONS

Demographic Information

Table 1: Demographic Information

Age	**Frequency**	**Percentage**
20-30	119	29.75%
31-40	90	22.5%
41-50	83	20.75%
51-60	108	27%
Gender		
Female	120	30%
Male	280	70%
Occupation		
ICT Expert	112	28%
Lawyer	93	23.25%
Police Officer	99	24.75%
Policy Maker	96	24%
Education		
Bachelor	190	47.5%
Master	134	33.5%
PhD	76	19%
Years of Experience		
1-10	136	34%
11-20	164	41%
21-30	100	25%
Region		
Dhaka	60	15%
Chittagong	64	16%
Sylhet	61	15.25%
Barishal	53	13.25%
Khulna	58	14.5%
Rajshahi	54	13.5%
Rangpur	50	12.5%

Table 1 summarizes the demographic data that we obtained from our survey.

There is a wide variety of respondents by demographic characteristics. Age-wise, most of the respondents were 20-30 years (29.75%), and 51-60 years (27%) dominated the respondents, followed by 31-40 (22.5%)

and 41-50 (20.75%) categories. Regarding the gender distribution, there is a significant disparity; men (70%) vastly outnumber women (30%). In terms of occupation, participants come from a wide range of sectors and professions, from ICT professionals (28%) to lawyers (23.25%), police officers (24.75%), and policy makers (24%), indicating diverse points of view. The percentage with different education levels was as follows: Bachelor's degree holders (47.5%), those with a Master's degree (33.5%), and those with a PhD (19%). With regard to experience, the standard size was 11–20 years (41%), followed by 1–10 years (34%) and 21–30 years (25%), in which we find both inexperienced and experienced professionals. Last, regional representation demonstrates that respondents hail from all parts of Bangladesh, with a slightly higher prevalence from Chittagong (16%), Sylhet (15.25%), and Dhaka (15%), but is relatively uniformly dispersed among the seven divisions.

The Challenges Several Countries Face

Figure 1 shows that outdated or weak laws are the biggest obstacle in fighting cybercrime, while issues like inconsistent definitions and poor cross-border provisions make things even harder. This means the law itself often fails before a case even reaches prosecution.

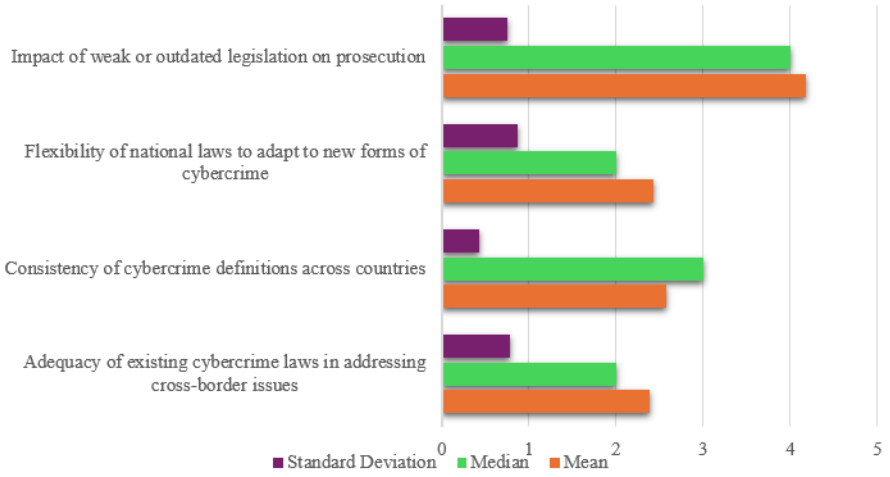

Figure 1: The challenges several countries face

Again, as Figure 1 shows, poor or outdated laws have a profound impact on cybercrime prosecutions, which received the highest agreement (mean = 4.3, median = 4, SD = 0.5). This demonstrates that outdated legislation is doing a great deal to hinder prosecutions and let those who commit crimes get away with it. Almost as low is the flexibility of laws to meet new cyber-crimes (mean = 2.4, median = 2, SD = 0.6). In contrast, consistency of definitions among countries (mean = 2.6, median = 3, SD = 0.3) and adaptability of existing laws to deal with cross-border matters (mean = 2.3, median = 2, SD = 0.7) are still weak, which means there are open spaces between national and international systems. This corroborates with Rana (2023), who stated that Bangladesh's ICT Act (2006) and the Digital Security Act (2018) are outmoded and ill-designed, and thereby impotent in dealing with up-to-date and cross-border cybercrimes.

The Complexities Involved in the Country's Laws

Figure 2 highlights that countries often clash over who has the right to prosecute, with few working extradition treaties or strong agreements to solve these disputes.

Figure 2 illuminates the complications that confront jurisdictions in the investigation of transnational cybercrimes. The transparency of jurisdiction authority receives moderate scores (mean = 2.6, median = 3, SD = 0.4), indicating that courts are often uncertain as to which agency has the right to prosecute. The prevalence of jurisdictional conflicts has a higher mean = 3.8, median = 43, and SD = 0.5, showing that issues between nations are still a significant deterrent. On the other hand, there are few extradition treaties for offenders (mean = 2.1, median = 2, SD = 0.3), denoting a lack of international mechanisms. So too, the average level of success of 100 per cent when adjudication IS used (mean = 2.4, median = 2, SD = 0.5), indicates that treaties are not doing an excellent job in resolving disputes. In this respect, this finding validates Ehsan & Saquib's (2024) argument about jurisdictional overlaps, the absence of extradition treaties, and poor cross-national cooperation as the main barriers for fragmented and ineffectual cross-border cybercrime prosecutions.

Countries' Collaboration or Struggle to Coordinate Efforts in Prosecuting Cybercrimes

Figure 3 points out that the most challenging part is forming effective joint investigation teams, since countries rarely share evidence smoothly or use legal treaties effectively.

Figure 4 highlights the difficulty of international cooperation in the investigation and prosecution of cybercrimes. International cooperation on investigations

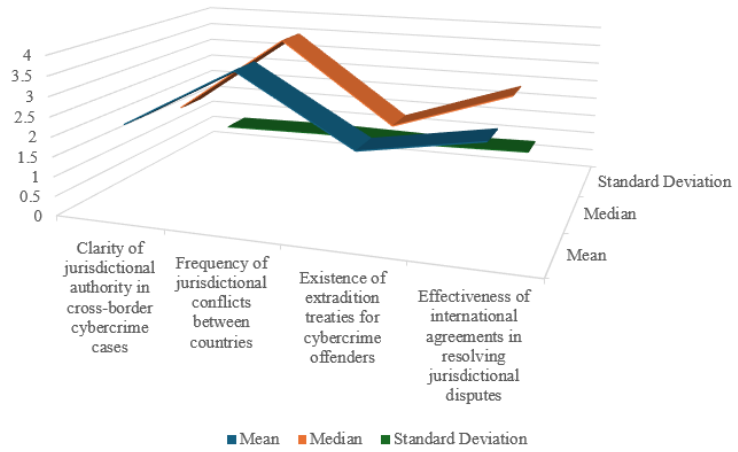

Figure 2: The complexities involved in a country's laws

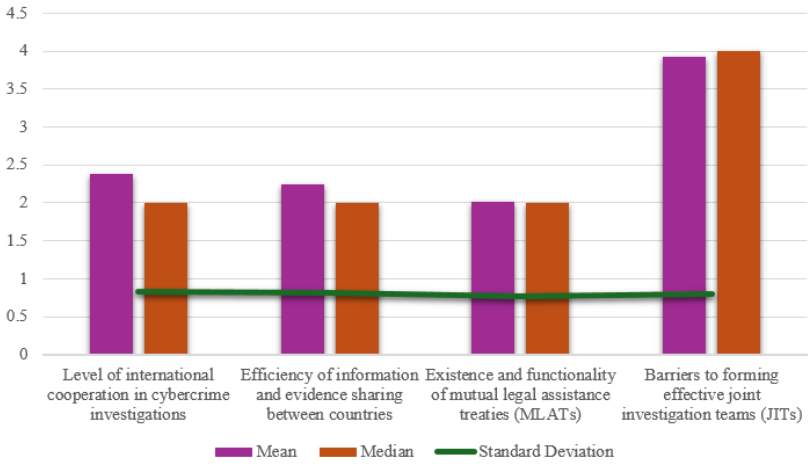

Figure 3: Countries' collaboration or struggle to coordinate efforts in prosecuting cybercrimes

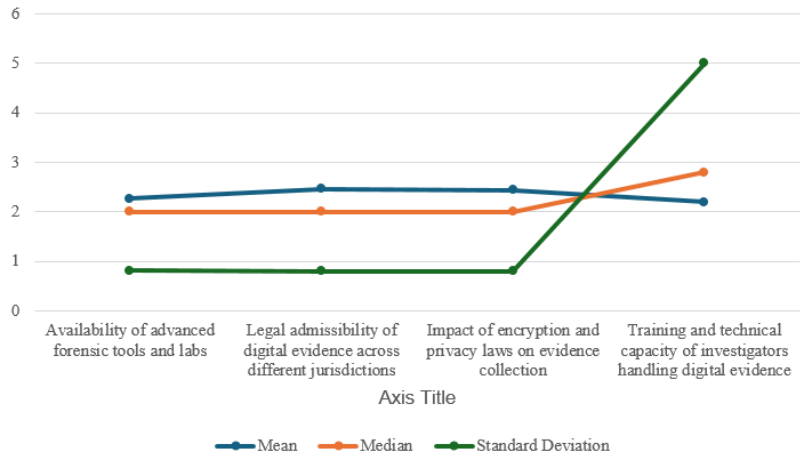

Figure 4: Difficulties in collecting and handling digital evidence

is reported as being moderate (mean = 2.3, median = 2, SD = 0.8) while sharing of information and evidence is reported to be equally low (mean = 2.2, median = 2, SD = 0.7). E, the presence of MLATs, (F) the relevance of MLATs for cooperation (mean = 2.0, median = 2, = SD 0.7), and thus demonstrate that they hardly work in practice. In contrast, obstacles to establishing strong JITs that are good to purpose are perceived as the most formidable challenge (mean = 3.9, median = 4, SD = 0.8), a finding indicative of institutional barriers and distrust among countries. This finding is in line with that of Momtaz (2024), who pointed out that in the absence of strong bilateral and multilateral agreements, it was a difficult task for Bangladesh to secure evidence from

abroad and to collaborate with other countries, rendering JITs unhelpful and cooperation disconnected.

Difficulties in Collecting and Handling Digital Evidence

Figure 4 reveals that investigators struggle most with limited training and a lack of advanced forensic tools, while encryption and privacy laws add further hurdles.

Figure 4 highlights the difficulties in collecting and handling digital evidence in cross-border cybercrime cases. The availability of advanced forensic tools and labs scores moderately (mean = 2.3, median = 2, SD = 0.8), suggesting a shortage of proper infrastructure. Legal admissibility of digital evidence across jurisdictions shows similar challenges (mean = 2.5, median = 2, SD = 0.8), reflecting differences in legal standards. The impact of encryption and privacy laws on evidence collection also remains problematic (mean = 2.4, median = 2, SD = 0.8), as privacy protections often conflict with investigative needs. Most critically, the training and technical capacity of investigators records the widest gap (mean = 2.2, median = 2.8, SD = 5.0), pointing to inconsistent skills and inadequate preparation among those handling digital forensics. This finding is supported by the results of Rahman (2023), who found that the investigators in Rajshahi do not have the technical skills to effectively preserve and analyze digital evidence, which in turn led to weak prosecution despite being able to identify crimes unambiguously.

Findings

The survey data and statistics shed light on some of the significant legal, judicial, and technical challenges in attributing cross-border cybercrimes. The attitudes of the respondents about black letter laws, and the jurisdiction, cooperation, and evidence collection issues in a Bangladeshi context are depicted by these results.

1. The study is conducted through a survey on 400 respondents from Bangladesh, including ICT professionals, lawyers, police, and policymakers. Overall, all divisions were represented (see Table 1). However, most respondents were aged between 20 and 30 (29.75%) and 61 and 70 (27%), with a marked gender disparity (70% male, 30% female)—the variance of this sample allowed for the inclusion of perspectives from various professional and geographical contexts.

2. Respondents overwhelmingly believe that the most significant impediment to prosecuting cybercrimes is archaic and feeble legal systems. They argued that the laws, including the ICT Act (2006) and the Digital Security Act (2018), are inadequate to counter changing and cross-border cyber threats, which create loopholes for the cyber criminals to slip through and go scot-free.

3. Findings revealed persistent jurisdictional conflicts. Participants noted that cross-border jurisdiction can be murky, with few extradition treaties to resolve the tug of war. Such lacunae in international legal instruments result in conflicts and discrepancies that act as an obstacle to prosecuting perpetrators.

4. International cooperation was rated poorly. Countries do not exchange evidence very much. Read more at: Techniques Reader Comments Techniques said: Mutual Legal Assistance Treaties (MLATs) are not used enough. Though theoretically important, cooperation mechanisms have not proved very effective in practice, given institutional mistrust and coordination problems, and global prosecutions remain fragmented.

5. Gathering and processing evidence proved to be an extremely challenging task. The researchers found that digital forensic tools and forensic training were not widely accessible. Furthermore, issues arising from encryption and differing privacy laws worldwide have made it challenging to admit evidence, as well as weakening judicial processes and making prosecution in general less effective.

Recommendations

Legislation should also be reformed and updated to account for the new era of cybercrime if it is to help reduce the prevalence of cross-border cybercrime. They should be brought into line with international norms, remove legal loopholes, and introduce severe penalties that will serve as a genuine deterrent. Absence of such updates will allow hackers to exploit archaic setups.

1. There also needs to be greater international cooperation to respond to crimes that transcend national boundaries. Greater regional coordination through growing bilateral and multilateral agreements, proactively acceding to global conventions, and establishing regional platforms are helpful measures. They should make it easier to share evidence and prosecute cases.

2. Technical and legal considerations require the development of a dedicated cybercrime capability. We require advanced forensic labs throughout the country, centre-led cybercrime units with international connections, and cyber courts in place. These organizations will serve as the basis for effective enforcement of digital crimes.

3. One of the most important issues is training and developing the new generation of legal and investigative professionals. Ongoing programs need to be started for lawyers, judges, and investigators with certification courses in cyber law and digital forensics. Information sharing with jurisdictions that are cybercrime-sophisticated could improve professional standards.

4. Finally, we have to maintain a balance between privacy, security, and the protection of victims. There must be clear rules on the ability to lawfully access content, including strong safeguards to prevent unauthorized access and abuse of the system. Victims also need to be supported by legal assistance and protection to ensure that justice is delivered equally.

Limitations

This study has some limitations that should be considered. First, it is based on survey data collected from 400 respondents in Bangladesh and, thus, while being diverse, it may not represent the views of all stakeholders or

reflect international settings. The results are reports of what people think (or thought) through self-delusions, bias, ignorance of relevant law and technology, and so forth. Furthermore, the research takes a quantitative perspective, which implies that qualitative information from in-depth interviews or case studies was not pursued. Finally, the very dynamic character of cybercrime could result in some findings whose relevance has changed with new threats or legal provisions.

CONCLUSION

The research in this paper has explored the legal and jurisprudential problems relating to the litigation of cross-border cybercrimes, focusing on the context of Bangladesh. The results indicate that the outdated legal normative framework, the gap between jurisdictions and international cooperation, and the insufficient technological capacity are the most relevant obstacles for an effective investigation and prosecution. Even though there are laws such as the ICT Act (2006) and the Digital Security Act (2018), these measures are inadequate to handle emerging and transnational cyber challenges. In addition, the absence of extradition agreements and the under-use of international agreements like the Budapest Convention and the under-utilization of Mutual Legal Assistance Treaties (MLAT) reflect the fragmented nature of international responses. From the perspective of technologies, insufficient forensic resources and a lack of training for investigators, as well as encryption problems, complicate the evidence gathering and admissibility across regions. These barriers can be addressed by ensuring that the reform process aims at harmonizing legal regimes with international best practices, forming specialized cyber courts, and investing in forensic capabilities. Just as important is nurturing regional and international collaboration, facilitated by multilateral treaties and mechanisms for sharing evidence. In the end, an entire, holistic approach that will allow the state's security, privacy, and the victim's protection is needed for building Bangladesh's (and the international system's) capacity to make cross-border cybercrime prosecutions a success.

REFERENCES

Ahmed, M. F., & Arifuzzaman, M. (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

Ashurov, A. (2024). *Jurisdictional Challenges in Cross-Border Cybercrime Investigations*. https://doi.org/10.5281/ZENODO.11234768

Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. *PLOS ONE, 19*(4), e0297312. https://doi.org/10.1371/journal.pone.0297312

Chowdhury, Md. A. A., & Fahim, Md. H. K. (2020). An Insight Into The Cybercrimes And Cyber Security Measures In Bangladesh: Quest For Operative Legal Remedies. *Solid State Technology, 63*(6). https://www.researchgate.net/publication/349588601_An_Insight_Into_The_Cybercrimes_And_Cyber_Security_Measures_In_Bangladesh_Quest_For_Operative_Legal_Remedies

Ehsan, S. B., & Saquib, Md. N. (2024). Balancing Cybersecurity and Individual Rights: A Critical Analysis of Bangladesh's Cyber Security Act 2023. *Journal of Creative Writing (ISSN-2410-6259), 8*(1), 85–98. https://doi.org/10.70771/jocw.v8i1.109

Furger, A. (2024). Can They Deliver? *Journal of International Criminal Justice, 22*(1), 43–58. https://doi.org/10.1093/jicj/mqae005

Hossain, S., Rashid, T., Nahar, K., & Akhter, T. (2024). A study based on the effectiveness of cyber security Act-2023 in pursuit of preventing cyber crime: Bangladesh perspective. *International Journal of Law, Policy and Social Review, 6*(5).

Mahmud, A., Sweety, J. B., Hossain, A., & Husin, M. H. (2023). Is the digital security act 2018 sufficient to avoid cyberbullying in Bangladesh? A quantitative study on young women from generation-z of Dhaka city. *Computers in Human Behavior Reports, 10*, 100289. https://doi.org/10.1016/j.chbr.2023.100289

Momtaz, Ms. S. (2024). 'Navigating Cyber Security Challenges and Legal Frameworks in Bangladesh: An In-Depth Exploration.' *International Journal of Research and Innovation in Social Science, VIII*(I), 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. *Journal of Economic Criminology, 8*, 100136. https://doi.org/10.1016/j.jeconc.2025.100136

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (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*. https://doi.org/10.13140/RG.2.2.10793.36962

Rana, Md. S. (2023). A Critical Analysis of the Escalating Cybercrime and Its Impact in Bangladesh. *CIFILE Journal of International Law, Online First*. https://doi.org/10.30489/cifj.2023.407899.1075

Siddiqua, Dr. R. (2024). Challenges Faced by Police Officers in Investigating Cyber Crime: An Exploratory Study in Bangladesh. *International Journal of Humanities, Social Sciences and Education, 11*(7), 150–161. https://doi.org/10.20431/2349-0381.1107014

Tenubar, G. (1997). *Global law without a state: A critique of legal theory*. Dartmouth Publishing.

Van Daalen, O. L. (2023). The right to encryption: Privacy as preventing unlawful access. *Computer Law & Security Review, 49*, 105804. https://doi.org/10.1016/j.clsr.2023.105804