Cybercrime and Criminal Justice in Bangladesh: An Examination of Emerging Threats and Legal Responses

Nafiul Haque Kingshuk[1*], Sultana Samiya Rahman[2]

[1]Department of Criminology, University of Dhaka, Dhaka, Bangladesh
[2]Department of Law, North South University, Dhaka, Bangladesh

[*]Corresponding Contact:
Email: nafiulkingshuk@gmail.com

Manuscript Received: 16 April 2026
Revised Submission: 14 June 2026
Article Accepted: 20 June 2026
Article Published: 30 June 2026

ABSTRACT

Cybercrime has emerged as a significant challenge for contemporary criminal justice systems, particularly in developing countries undergoing rapid digital transformation. This study critically examines the relationship between emerging cybercrime threats and criminal justice responses in Bangladesh through a socio-legal review approach. Drawing upon legislative documents, official reports, and relevant scholarly literature, the study explores the evolving cyber threat landscape, assesses Bangladesh's legal and regulatory responses, and evaluates the institutional capacities of criminal justice actors responsible for preventing, investigating, prosecuting, and adjudicating cyber offences. The findings indicate that Bangladesh has made substantial progress through successive legislative reforms, evolving from the Information and Communication Technology Act 2006 and the Digital Security Act 2018 to the Cyber Security Act 2023 and, most recently, the Cyber Security Act 2026. Nevertheless, significant challenges remain in areas such as digital forensic capabilities, electronic evidence management, institutional coordination, specialized human resource development, cross-border cooperation, and operational preparedness. The study further highlights the growing implications of emerging cyber threats, including ransomware, AI-assisted fraud, deepfakes, synthetic identity crimes, and other technology-enabled offences. It argues that effective cyber justice requires more than legislative reform, emphasizing the need for stronger institutional capacity, rights-sensitive cyber governance, continuous professional training, effective implementation of the Cyber Security Act 2026, and enhanced international collaboration. The study contributes to the growing body of socio-legal scholarship on cybercrime and offers evidence-informed policy recommendations for strengthening Bangladesh's cyber resilience and criminal justice system.

Keywords: Cybercrime, Criminal Justice, Bangladesh, Cyber Security Act 2026, Digital Evidence, Cyber Governance

INTRODUCTION

Bangladesh's cyber regulatory framework has undergone several legislative transitions over the last decade. The Digital Security Act 2018, which attracted significant criticism regarding freedom of expression and civil liberties, was repealed and replaced by the Cyber Security Act 2023. Following subsequent political and regulatory developments, the Cyber Security Act 2023 was later repealed, leading to the promulgation of the Cyber Security Ordinance 2025. In 2026, the Ordinance received parliamentary approval and was enacted as the Cyber Security Act 2026 (also referred to as the Cyber Safety Act). These successive reforms illustrate the dynamic nature of Bangladesh's cyber governance landscape and the continuing effort to balance cybersecurity objectives with rights-based legal protections.

The rapid expansion of digital technologies has transformed modern societies in unprecedented ways. Over the past two decades, information and communication technologies (ICTs) have reshaped how governments operate, businesses conduct transactions, and individuals communicate and access services. Across the developing world, digital transformation is increasingly viewed as a key driver of economic growth, social inclusion, and administrative efficiency. Bangladesh is no exception. Through initiatives such as "Digital Bangladesh" and the more recent vision of building a "Smart Bangladesh" by 2041, the country has invested heavily in expanding internet access, digital public services, mobile connectivity, electronic commerce, and technology-driven governance systems.

These developments have generated significant benefits for citizens and institutions alike. Mobile financial services have increased financial inclusion, online platforms have simplified access to public services, and digital technologies have created new opportunities for business innovation and economic participation. However, the same technological advancements that create opportunities also introduce new vulnerabilities. As dependence on digital systems increases, so does exposure to cyber-related risks.

Recent global assessments indicate that cyber threats are becoming more sophisticated, adaptive, and financially motivated. Activities such as phishing, online fraud, ransomware attacks, identity theft, cyber extortion, and unauthorized system intrusions have become common features of the contemporary cyber threat landscape. Organized criminal groups, individual offenders, and even transnational networks now possess the ability to exploit technological weaknesses and human vulnerabilities for financial gain or other objectives. The growing prevalence of these threats has compelled governments around the world to reconsider existing legal frameworks and strengthen institutional mechanisms designed to combat cybercrime.

The widespread adoption of artificial intelligence (AI), machine learning, the Internet of Things (IoT), cryptocurrency, automation, and other emerging digital technologies has fundamentally transformed contemporary digital ecosystems while simultaneously increasing the scale, sophistication, and transnational nature of cyber threats. These technological developments have created new challenges relating to cybersecurity, digital fraud, electronic evidence, platform governance, and regulatory oversight, thereby necessitating adaptive legal frameworks, stronger institutional capacities, and evidence-based criminal justice responses. Consequently, governments worldwide are increasingly reforming cybercrime legislation and strengthening institutional mechanisms to effectively prevent, investigate, and prosecute emerging forms of cybercrime (Donepudi et al., 2020; Ganapathy et al., 2020; Hoque et al., 2020; Khan & Fadziso, 2020; Ahmed et al., 2021a; Ahmed et al., 2021b; Hussain et al., 2021; Ahmed et al., 2022; Page et al., 2021; Gazi et al., 2026a; Gazi et al., 2026b; Islam et al., 2025).

Bangladesh has experienced many of the same challenges. The rapid growth of internet usage, mobile banking, e-commerce platforms, social media engagement, and digital public services has expanded the country's digital footprint while simultaneously increasing its exposure to cyber risks. Reports of financial fraud, online impersonation, social engineering schemes, cyber harassment, and unauthorized access to digital accounts have become increasingly common. These developments raise important questions regarding the effectiveness of existing legal responses and the preparedness of criminal justice institutions tasked with preventing, investigating, prosecuting, and adjudicating cyber offences.

Addressing cybercrime requires more than the enactment of legislation. Effective responses depend upon the combined capacity of law enforcement agencies, prosecutors, judicial institutions, policymakers, and regulatory bodies. The ability to collect digital evidence, conduct forensic investigations, coordinate across jurisdictions, and respond to emerging technologies has become central to modern criminal justice administration. Consequently, evaluating cybercrime solely from a legal perspective provides an incomplete understanding of the broader challenges involved.

This study adopts a socio-legal perspective to examine the relationship between emerging cybercrime threats and criminal justice responses in Bangladesh. Rather than focusing exclusively on legal provisions, the study considers how laws operate within institutional, technological, and governance environments. Particular attention is given to the evolving cyber threat landscape, the effectiveness of recent legislative reforms, and the operational capacities of criminal justice actors responsible for enforcing cyber-related laws.

As Bangladesh continues its journey toward a digitally empowered future, ensuring the security and integrity of cyberspace remains a critical policy priority. Understanding whether existing institutions and legal frameworks are capable of responding to rapidly evolving cyber threats is therefore both timely and necessary. By critically examining emerging cybercrime trends alongside criminal justice responses, this study seeks to contribute to ongoing discussions concerning cyber governance, institutional preparedness, and the future development of a resilient cyber justice framework in Bangladesh.

PROBLEM STATEMENT

The expansion of digital technologies in Bangladesh has created new opportunities for economic development, financial inclusion, and public service delivery. At the same time, however, it has exposed individuals, businesses, and government institutions to a growing range of cyber threats. Over the past decade, incidents involving online fraud, unauthorized access to digital systems, identity theft, cyber harassment, and technology-facilitated financial crimes have become increasingly visible. These developments have raised concerns regarding the ability of existing legal and institutional mechanisms to respond effectively to evolving forms of cyber offending.

In response to these challenges, Bangladesh has undertaken a series of legislative reforms aimed at strengthening cyber governance and improving legal responses to cybercrime. Bangladesh's legal response to cybercrime has evolved through multiple legislative reforms, including the Digital Security Act 2018, the Cyber Security Act 2023, the Cyber Security Ordinance 2025, and the current Cyber Security Act 2026. While these reforms demonstrate continuing governmental efforts to address emerging cyber threats, questions remain regarding enforcement effectiveness, institutional preparedness, and the practical administration of cyber justice.

Another important concern relates to the transnational nature of cybercrime. Offenders may reside in one country, victims in another, and critical evidence may be stored on servers located elsewhere. Traditional investigative and prosecutorial approaches are often insufficient in such circumstances. Consequently, effective cybercrime control requires not only appropriate domestic legislation but also efficient mechanisms for international cooperation, information sharing, and mutual legal assistance (UNODC, 2024a).

Against this backdrop, an important question emerges: To what extent are Bangladesh's legal and criminal justice institutions prepared to address the rapidly changing cyber threat environment? Although legislative reforms have attracted considerable attention, less emphasis has been placed on evaluating whether the institutions responsible for implementing those laws possess the capacity, resources, and adaptability necessary to respond effectively to contemporary cyber threats. Addressing this issue is essential for understanding the strengths and limitations of Bangladesh's current cyber justice framework (UNODC, 2024b).

Research Gap

Although scholarly and policy discussions relating to cybercrime in Bangladesh have increased in recent years, several important gaps remain evident. Existing studies have predominantly concentrated on descriptive analyses of cyber legislation, general cybersecurity awareness, or isolated categories of digital offences. Relatively limited attention has been devoted to examining cybercrime from an integrated criminal justice perspective encompassing law enforcement agencies, prosecutorial mechanisms, judicial processes, and international cooperation frameworks.

Furthermore, the rapidly evolving nature of cyber threats necessitates continuous reassessment of institutional preparedness and legal adaptability. Much of the available literature does not adequately address how emerging cyber risks interact with existing criminal justice structures or whether recent legislative reforms have translated into meaningful improvements in enforcement effectiveness. The practical implications of institutional capacity constraints, digital evidence management, and cross-border cooperation remain underexplored within the Bangladeshi context.

This study seeks to address these gaps by adopting a socio-legal approach that integrates analyses of emerging cyber threats, legal responses, and criminal justice institutions. By situating cybercrime within the broader framework of criminal justice governance, the study aims to contribute to a more nuanced understanding of Bangladesh's preparedness to address contemporary and future cyber challenges.

The primary objective of this study is to critically examine the relationship between emerging cybercrime threats and criminal justice responses in Bangladesh. The study focuses on identifying major cybercrime threats affecting the country, assessing the evolution and effectiveness of relevant legal frameworks, evaluating the preparedness and institutional capacity of criminal justice agencies, and examining the challenges associated with cybercrime prevention, investigation, prosecution, and adjudication. Based on these findings, the study also seeks to propose evidence-based recommendations for strengthening Bangladesh's cyber justice and cybersecurity governance framework.

Research Questions

To achieve these objectives, the study addresses the following research questions:

RQ1: What emerging cybercrime threats are shaping the contemporary cyber landscape in Bangladesh?

RQ2: How effective are Bangladesh's existing legal and regulatory frameworks in responding to evolving cyber threats?

RQ3: What institutional challenges do criminal justice actors encounter in the investigation, prosecution, and adjudication of cybercrime cases?

RQ4: What reforms and strategic interventions are necessary to enhance Bangladesh's capacity to combat cybercrime while safeguarding due process and the rule of law?

SIGNIFICANCE OF THE STUDY

This study contributes to the growing body of knowledge on cybercrime and criminal justice in several important ways. Academically, it advances socio-legal scholarship by integrating analyses of cyber threats, legal responses, and institutional capacities within a unified analytical framework. Rather than conceptualizing cybercrime solely as a technological issue or legislative concern, the study situates cyber offending within the broader criminal justice ecosystem.

From a policy perspective, the findings may assist policymakers in identifying weaknesses within existing legal and institutional arrangements and in formulating adaptive, technologically informed, and accountable cyber governance strategies. The study may also support law enforcement agencies, prosecutors, and judicial actors in recognizing operational constraints and prioritizing capacity-building initiatives.

Practically, as Bangladesh advances toward becoming a digitally empowered society, ensuring the security, integrity, and accountability of cyberspace has become essential for sustainable development. By critically examining emerging cyber threats alongside criminal justice responses, this study seeks to inform the development of a resilient and inclusive cyber justice framework capable of addressing both present and future challenges while maintaining public confidence in the administration of justice.

METHODOLOGY

A clear methodological framework is essential for ensuring the credibility and reliability of research findings. This study adopted a qualitative socio-legal review approach to examine the relationship between emerging cybercrime threats and criminal justice responses in Bangladesh. The methodology was designed to facilitate a systematic analysis of legal developments, institutional responses, and contemporary scholarly literature relevant to cybercrime governance.

Research Design

This study employed a qualitative socio-legal review design using an integrative review approach. Socio-legal research recognizes that laws operate within broader social, institutional, and technological contexts rather than in isolation. Accordingly, the study examined cybercrime as both a legal and governance issue involving law enforcement agencies, prosecutors, courts, policymakers, and other stakeholders.

The integrative review approach was selected because it allows the synthesis of evidence from diverse sources, including legislation, academic literature, policy documents, and institutional reports. This approach was considered appropriate for evaluating emerging cyber threats, legal responses, and institutional preparedness within the Bangladeshi context.

Data Sources

The study relied on both primary and secondary sources.

Primary Sources

Primary sources included:

- Cyber Security Act 2026 and relevant preceding legislation;
- Government policies and official reports;
- Institutional publications;
- Reports issued by international organizations relating to cybercrime and criminal justice.

Secondary Sources

Secondary sources included:

- Peer-reviewed journal articles;
- Review papers;
- Comparative legal studies;
- Criminology and cybersecurity literature;
- Reports published by international organizations and research institutions.

Literature Search Strategy

Relevant literature was identified through structured searches of major academic databases and institutional repositories, including Google Scholar, Scopus, Web of Science, and official organizational websites. Searches were conducted using combinations of keywords such as:

- "Cybercrime" AND "Bangladesh";
- "Cybercrime" AND "criminal justice";
- "Cyber Security Act" AND Bangladesh;
- "Digital evidence" AND prosecution;
- "Cyber governance" AND criminal justice.

Additional sources were identified through reference tracking and review of relevant publications.

Data Analysis

The collected materials were reviewed and analyzed using a thematic approach. Relevant information was categorized into key themes, including emerging cyber threats, legal and regulatory responses, criminal justice institutions, operational challenges, and governance issues. The analysis focused on identifying patterns, institutional strengths and weaknesses, and areas requiring policy and legal reform.

Emerging Cybercrime Threat Landscape in Bangladesh

The rapid expansion of digital technologies has transformed Bangladesh into one of South Asia's emerging digital economies. While this transformation has generated substantial socioeconomic benefits, it has simultaneously expanded opportunities for cyber-enabled criminal activities. The increasing dependence on online financial systems, social networking platforms, e-commerce services, and digital public infrastructures has exposed individuals, businesses, and government institutions to a diverse range of cyber threats. Understanding the nature and evolution of these threats is essential for developing effective legal responses and strengthening criminal justice capacities.

Overview of Bangladesh's Digital Ecosystem

Bangladesh has experienced remarkable growth in digital connectivity over the past decade. Government-led initiatives promoting digital transformation have accelerated internet penetration, mobile technology adoption, and the expansion of digital public services. Mobile financial services (MFS), online banking, e-commerce platforms, and social media have become integral components of daily life.

However, rapid digitalization has also increased the country's exposure to cyber risks. The International Telecommunication Union (ITU, 2024) notes that expanding digital infrastructures often create vulnerabilities when cybersecurity awareness, institutional preparedness, and technical safeguards do not evolve at the same pace as technological adoption. Similarly, INTERPOL (2024) identified the Asia-Pacific region as experiencing increasingly sophisticated cyber-enabled criminal activities due to accelerated digital transformation and evolving criminal tactics. Within Bangladesh, growing digital engagement has expanded the pool of potential victims and increased opportunities for financially motivated offenders, organized cybercriminal networks, and malicious actors exploiting human vulnerabilities.

Financial Cybercrime

Financially motivated cybercrime represents one of the most significant cyber threats affecting Bangladesh. The widespread adoption of mobile financial services, internet banking, and digital payment systems has created new opportunities for fraud and unauthorized financial gain.

Phishing Attacks: Phishing remains among the most frequently reported forms of cyber-enabled financial crime. Offenders typically impersonate trusted institutions, including banks, mobile financial service providers, or government agencies, to deceive victims into disclosing confidential information such as passwords, one-time passwords (OTPs), or account credentials. The effectiveness of phishing attacks often depends on exploiting human trust rather than technical vulnerabilities. Social engineering techniques increasingly utilize persuasive language, urgency cues, and fraudulent digital identities to manipulate victims into compromising sensitive information.

Mobile Financial Services Fraud: The rapid expansion of mobile financial services has enhanced financial inclusion throughout Bangladesh. However, cybercriminals have exploited users' limited cybersecurity awareness through fraudulent calls, deceptive text messages, and impersonation schemes designed to obtain verification codes and unauthorized access to accounts. Victims frequently suffer direct financial losses, while such incidents may undermine public confidence in digital financial systems.

Online Banking Fraud: Online banking services have also emerged as targets for cybercriminal activities. Fraudulent websites, credential theft, malware infections, and unauthorized transactions constitute common mechanisms through which offenders exploit weaknesses in digital financial practices. INTERPOL (2024) observed that financial cybercrime continues to evolve in sophistication, often involving organized criminal groups operating across national boundaries.

Social Media and Identity-Related Crimes

The growing popularity of social media platforms has transformed communication and social interaction within Bangladesh. However, these platforms have simultaneously become environments where various forms of cyber-enabled victimization occur.

Identity Theft and Impersonation: Identity-related offences involve the unauthorized use of another person's personal information, photographs, or online identities for deceptive purposes. Offenders may create fraudulent profiles to solicit money, deceive acquaintances, damage reputations, or facilitate other criminal activities. The consequences of identity theft extend beyond financial losses and may include reputational harm, emotional distress, and erosion of trust in digital environments.

Cyber Harassment and Online Abuse: Cyber harassment constitutes an increasingly prominent concern, particularly among women and vulnerable populations. Online abuse may include threatening messages, persistent intimidation, dissemination of private information, and coordinated harassment campaigns. Unlike conventional harassment, cyber harassment often transcends geographical limitations and may occur continuously through multiple digital channels. The anonymity afforded by online environments can further embolden offenders while complicating enforcement efforts.

Online Blackmail and Sextortion: Cybercriminals increasingly exploit private information and digital communications to extort victims. Offenders may threaten to disclose sensitive content unless victims comply with financial demands or other coercive requests. Such incidents can have profound psychological consequences and frequently remain underreported due to fear of stigma and social repercussions.

Table 1: Emerging Cybercrime Categories in Bangladesh (2022–2025)

Threat Category	Common Methods	Primary Targets	Potential Impact
Financial Cybercrime	Phishing, OTP fraud, account takeover	MFS users, bank customers	Financial losses, reduced trust
Identity Theft	Fake profiles, impersonation	Social media users	Reputational damage, deception
Cyber Harassment	Threats, abusive communications	Women, youth, public figures	Psychological harm
Online Blackmail	Sextortion, disclosure threats	Individual users	Emotional distress, extortion
Online Banking Fraud	Credential theft, fraudulent transactions	Banking customers	Unauthorized financial transfers
Social Engineering	Fraudulent calls and messages	General public	Information compromise

Ransomware and Malware Threats

Ransomware and malware attacks have emerged as some of the most disruptive forms of cybercrime globally. Although Bangladesh has not experienced ransomware incidents on the same scale as certain developed economies, the increasing digitization of organizations has heightened the country's vulnerability to such threats.

Malware refers to malicious software intentionally designed to compromise, disrupt, monitor, or gain unauthorized access to digital systems. Common forms of malware include viruses, worms, spyware, trojans, and ransomware. Ransomware, in particular, encrypts victims' files or systems and demands payment in exchange for restoring access.

According to INTERPOL (2024), ransomware groups operating across the Asia-Pacific region have become increasingly sophisticated, often employing "double extortion" tactics whereby attackers not only encrypt data but also threaten to disclose sensitive information publicly unless ransom demands are met. These attacks frequently target organizations with inadequate cybersecurity safeguards, outdated software systems, and insufficient incident response capacities.

Emerging Threats in the AI Era

The rapid advancement of artificial intelligence (AI) technologies has generated transformative opportunities across multiple sectors. However, AI has also introduced new risks by enabling cybercriminals to automate, personalize, and scale malicious activities.

AI-Assisted Phishing: Traditional phishing attacks relied heavily upon generic messages distributed to large numbers of potential victims. Contemporary AI tools enable attackers to generate highly personalized and linguistically sophisticated communications tailored to individual targets. Such messages often appear more credible and therefore increase the likelihood of victim compliance.

Deepfakes and Synthetic Media: Deepfake technologies utilize AI techniques to generate realistic but fabricated audio, image, and video content. These synthetic materials may be used to impersonate trusted individuals, manipulate public perceptions, facilitate fraud, or undermine institutional credibility. The potential misuse of deepfakes presents significant legal and evidentiary challenges for criminal justice systems. Distinguishing authentic digital evidence from manipulated content may become increasingly difficult without specialized expertise and technological tools.

Synthetic Identity Fraud: Synthetic identity fraud involves the creation of fictitious identities through the combination of real and fabricated personal information. These identities may be exploited to establish fraudulent financial accounts, evade detection, and facilitate broader criminal schemes. As digital identity verification systems become more prevalent, the misuse of AI-assisted identity generation techniques may emerge as an increasingly important concern.

Automated Cyberattacks: Artificial intelligence may also enhance the efficiency of cyberattacks through automation. Attackers can employ AI tools to identify vulnerabilities, adapt malicious code, and optimize attack strategies with limited human intervention. Although AI itself is not inherently malicious, its misuse illustrates the evolving nature of cybercrime and underscores the importance of adaptive legal frameworks and institutional preparedness.

The preceding discussion demonstrates that cybercrime in Bangladesh encompasses both established and emerging forms of digital offending. While financial cybercrime and identity-related offences currently represent the most visible threats affecting ordinary users, technologically sophisticated risks, including ransomware attacks and AI-enabled offences, are becoming increasingly significant. To facilitate a clearer understanding of the relative prominence of these threats, Figure 1 provides a visual summary of the major cybercrime categories discussed in this chapter.

The coloured bar chart visually summarizes the relative prominence of major cybercrime categories discussed in this chapter. The figure is intended to provide a conceptual representation of the evolving threat landscape rather than precise statistical prevalence estimates.

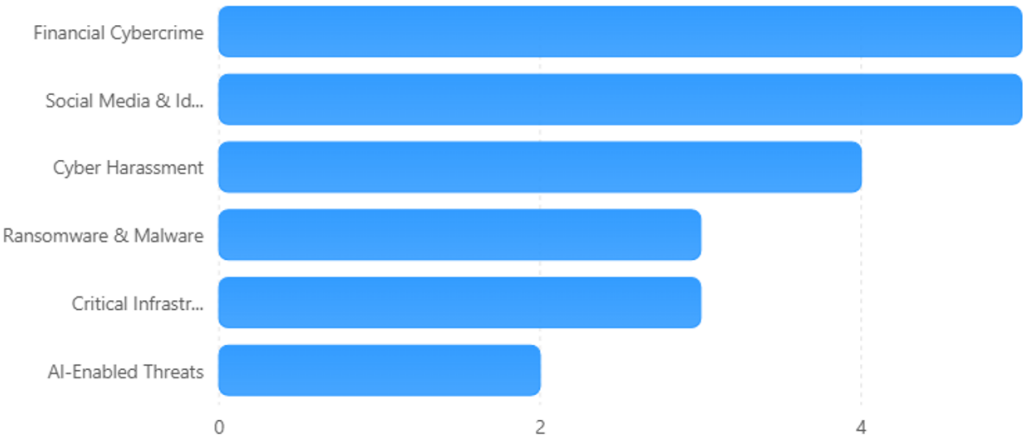

Figure 1. Illustrative Distribution of Major Cybercrime Categories Affecting Bangladesh.

Suggested Categories for Figure 1

Cybercrime Category	Relative Prominence
Financial Cybercrime	High
Social Media & Identity Crimes	High
Cyber Harassment & Online Abuse	Moderate–High
Ransomware & Malware	Moderate
Critical Infrastructure Threats	Moderate
AI-Enabled Threats	Emerging

As illustrated in Figure 1, financial cybercrime and social media-related identity offences constitute the most prominent categories within Bangladesh's contemporary cyber threat landscape. Cyber harassment and online abuse also represent substantial concerns, particularly for vulnerable populations. Although ransomware attacks and threats targeting critical infrastructures remain comparatively less visible, their potential consequences are severe. Moreover, AI-enabled threats, including deepfakes and synthetic identity fraud, represent emerging risks that may significantly reshape future patterns of cyber offending.

Interpretive Note: Financial cybercrime and identity-related offences currently represent the most visible categories affecting ordinary users, whereas AI-enabled threats constitute emerging risks with the potential to expand significantly in future years.

BANGLADESH'S LEGAL AND REGULATORY RESPONSES TO CYBERCRIME

The evolution of cybercrime legislation in Bangladesh reflects the country's broader transition toward a digitally connected society. As digital technologies increasingly permeated economic, governmental, and social activities, traditional legal mechanisms proved inadequate for addressing emerging forms of cyber-enabled offending. Consequently, Bangladesh gradually developed a specialized legal framework aimed at regulating cyberspace, criminalizing cyber-related offences, and empowering institutions responsible for investigation and enforcement. This chapter critically examines the evolution of Bangladesh's cybercrime legislation and evaluates the principal provisions of the Cyber Security Act 2023, which currently constitutes the cornerstone of the country's cyber regulatory regime.

Evolution of Cybercrime Legislation in Bangladesh

Bangladesh's legal response to cybercrime has evolved through three major legislative phases: the Information and Communication Technology Act 2006 (ICT Act), the Digital Security Act 2018 (DSA), and the Cyber Security Act 2023 (CSA). Each legislative transition reflected changing technological realities, institutional experiences, and societal concerns.

The Information and Communication Technology Act 2006

The Information and Communication Technology Act 2006 represented Bangladesh's first comprehensive attempt to regulate offences committed through digital technologies. Introduced during the early stages of the country's digital development, the ICT Act primarily focused on facilitating electronic transactions, recognizing digital signatures, and criminalizing certain forms of unauthorized access and computer-related offences. Although the Act marked an important milestone, it was enacted at a time when cybercrime remained relatively limited in scale and sophistication. Consequently, its provisions were not designed to address contemporary threats such as ransomware, social engineering attacks, AI-enabled fraud, or large-scale data breaches. The Act subsequently underwent amendments, particularly in 2013, which expanded penalties and enforcement powers. However, concerns emerged regarding certain provisions relating to broad criminalization and potential implications for civil liberties.

The Digital Security Act 2018

In response to expanding digitalization and growing cyber threats, Bangladesh enacted the Digital Security Act (DSA) 2018. The DSA sought to consolidate cyber-related offences and provide a more comprehensive legal framework governing digital environments. The Act introduced provisions addressing:

- Unauthorized access to computer systems;
- Digital fraud;
- Identity-related offences;
- Damage to computer systems;
- Cyber-related threats affecting national security;
- Offences involving digital communication platforms.

While the DSA expanded the state's legal capacity to address cyber-related misconduct, it also generated substantial debate among academics, journalists, civil society organizations, and international observers. Critics argued that certain provisions employed broad terminology that could potentially affect freedom of expression and increase discretionary enforcement powers. Consequently, the DSA became one of the most contested pieces of cyber-related legislation in Bangladesh's legal history.

The Cyber Security Act 2023

Responding to sustained criticism of the Digital Security Act 2018 and the need for legal reform, Bangladesh enacted the Cyber Security Act 2023, which repealed and replaced the earlier legislation (Government of the People's Republic of Bangladesh, 2023). The Act sought to modernize the country's legal response to cybercrime while addressing concerns regarding several provisions of the previous framework. It reflected the government's recognition that increasingly

sophisticated cyber threats required a more adaptive and balanced legal regime capable of protecting digital security while supporting the continued growth of the digital economy.

Although many offences, investigative powers, and institutional responsibilities remained substantially similar to those under the Digital Security Act 2018, the Cyber Security Act 2023 introduced several modifications relating to penalties, procedural safeguards, and the classification of certain offences. The Act therefore represented an important transitional stage in the evolution of Bangladesh's cybercrime legislation. Subsequently, additional legal reforms culminated in the enactment of the Cyber Security Act 2026, which further updated the country's cybersecurity framework to address emerging technological challenges and evolving cyber threats.

The Cyber Security Ordinance 2025

The Cyber Security Ordinance 2025 was introduced as an interim legislative measure to strengthen Bangladesh's cybersecurity framework pending comprehensive statutory reform. The Ordinance amended several provisions of the Cyber Security Act 2023 by addressing emerging technological challenges, refining enforcement mechanisms, and introducing measures to combat AI-generated harmful content and other evolving cyber threats. It also laid the legislative foundation for the subsequent enactment of the Cyber Security Act 2026, which incorporated and further expanded many of these reforms.

Cyber Security Act 2026

Following subsequent legal reforms, the Cyber Security Ordinance 2025 was replaced by the Cyber Security Act 2026, which further modernized Bangladesh's cybercrime framework. The 2026 Act introduced additional provisions addressing emerging technological challenges, including AI-generated harmful content, while refining enforcement mechanisms and updating several procedural and substantive aspects of the country's cybersecurity regime.

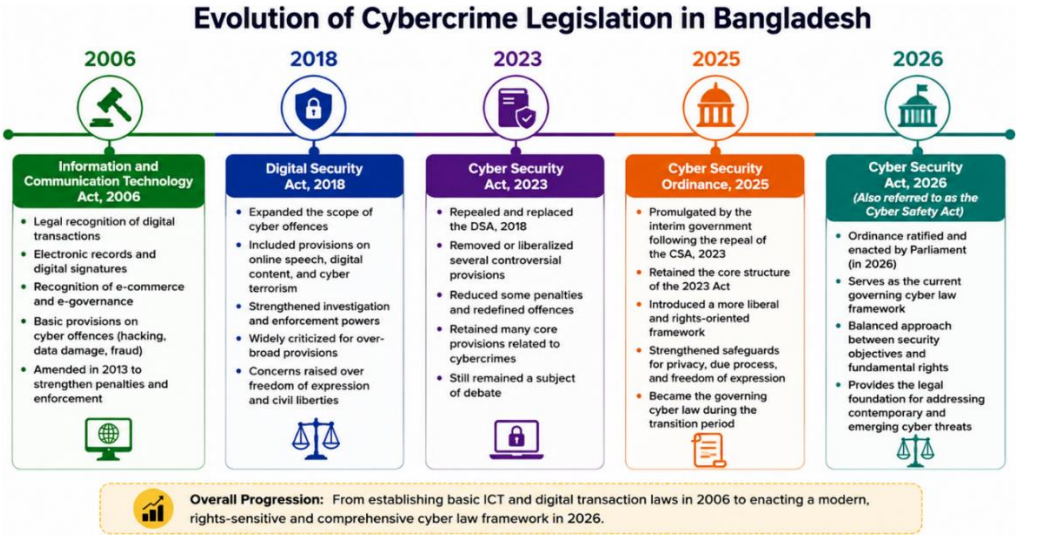

Figure 2: Timeline Illustrating the Evolution of Bangladesh's Cybercrime Legislation.

The timeline provides a visual summary of Bangladesh's legislative progression and demonstrates how legal responses have evolved alongside changing technological realities and policy priorities.

The Cyber Security Act 2026: Major Provisions

The Cyber Security Act 2026 represents the latest stage in the evolution of Bangladesh's cybercrime legislation and serves as the country's principal legal framework for addressing offences committed in cyberspace. Building upon the Cyber Security Act 2023, the 2026 Act broadens the scope of cybersecurity governance by incorporating updated definitions of cyberspace, cyber incidents, and digital harms, while responding to technological developments such as artificial intelligence (AI)-generated content and sophisticated online misinformation. The Act seeks to enhance the protection of individuals, institutions, and critical information infrastructure by strengthening investigative mechanisms and promoting greater institutional coordination among law enforcement agencies, regulatory authorities, and relevant public and private stakeholders. It also reinforces the legal basis for preserving and examining electronic evidence, which remains central to the successful investigation and prosecution of cyber-related offences.

Table 2: Comparative Evolution of Bangladesh's Cybercrime Laws

Feature	ICT Act 2006 (2006)	Digital Security Act 2018 (2018)	Cyber Security Act 2023 (2023)	Cyber Security Ordinance 2025 (2025)	Cyber Security Act 2026 (2026)
Primary Objective	Legal recognition of ICT and electronic transactions; promotion of ICT sector and e-governance	Comprehensive digital security regulation and expansion of cybercrime provisions	Modernized cybersecurity governance; rationalization of penalties and offences from DSA 2018	Rights-oriented and balanced cyber regulatory framework introduced by interim government	Parliament-approved framework for effective cybersecurity governance and protection of digital rights
Cyber Offence Coverage	Limited; focused on basic computer-related offences	Substantially expanded; included new categories of digital offences	Expanded with modifications and clarifications	Retained major offences with refinements and rights-based safeguards	Comprehensive and contemporary coverage of emerging cyber threats
Digital Fraud Provisions	Partial and limited coverage	Comprehensive provisions for digital fraud and online offences	Retained and improved with some reductions in penalties	Strengthened consumer protection and due process safeguards	Enhanced framework for digital fraud investigation and prosecution
Electronic Evidence Focus	Limited recognition of electronic evidence	Moderate emphasis on electronic evidence	Enhanced provisions for admissibility and handling of digital evidence	Improved standards for electronic evidence and privacy protection	Stronger safeguards and procedural clarity for digital evidence
Investigation Powers	Present but limited	Significantly expanded investigative powers	Retained with refinements to prevent abuse	Balanced investigative powers with rights protections	Clear, accountable, and proportionate investigative powers
Search and Seizure Powers	Limited scope	Broad and extensive powers	Continued with procedural refinements	Introduced stricter procedural safeguards and oversight	More structured and judicially supervised process
Rights-Related Debate	Relatively limited	High level of criticism over freedom of expression and privacy	Criticized but improved in several areas	More liberal and rights-oriented framework	Balanced approach between security and fundamental rights
Legislative Status	Partially active for technical and procedural matters; largely superseded	Repealed	Repealed	Enacted as Ordinance and served as governing law	Current governing law (Enacted by Parliament); referred to as Cyber Safety Act by some

A notable feature of the Cyber Security Act 2026 is its recognition of emerging cyber threats associated with AI-enabled deception, including manipulated images, audio, and video intended to mislead the public or facilitate criminal activities. The Act also introduces provisions intended to improve cooperation with international technology platforms by enabling the timely removal of unlawful or harmful online content where legally justified. Furthermore, the legislation expands regulatory powers relating to the prevention of misinformation, cyber-enabled fraud, identity-related offences, unauthorized access to computer systems, and attacks targeting critical digital infrastructure. These measures reflect Bangladesh's effort to modernize its cybersecurity framework in response to rapidly

evolving technological risks while strengthening the capacity of competent authorities to investigate, prevent, and respond to increasingly complex forms of cybercrime. Although the Cyber Security Act 2026 significantly updates Bangladesh's legal framework, its long-term effectiveness will depend upon consistent implementation, institutional capacity, technical expertise, judicial oversight, and continued legislative adaptation to emerging technologies and the transnational nature of cybercrime.

The legislative evolution described above demonstrates Bangladesh's growing recognition of cybercrime as a multidimensional challenge requiring specialized legal responses. While successive reforms have strengthened the country's regulatory capacity, the effectiveness of these measures cannot be assessed solely through statutory analysis. Questions concerning implementation, institutional preparedness, proportionality, and alignment with international standards remain critically important. Accordingly, the subsequent sections of this chapter critically evaluate the strengths and limitations of Bangladesh's current legal framework and examine its implications for rights-sensitive cyber governance.

STRENGTHS OF THE CURRENT LEGAL FRAMEWORK

The enactment of the Cyber Security Act 2026 represents the latest stage in the evolution of Bangladesh's cybercrime legislation. The current framework emerged following a series of legislative reforms that included the Information and Communication Technology Act 2006, the Digital Security Act 2018, the Cyber Security Act 2023, and the Cyber Security Ordinance 2025. While debates concerning cybersecurity regulation and civil liberties continue, the Cyber Security Act 2026 provides a more contemporary legal foundation for addressing cyber-related offences and emerging technological risks.

Contemporary Recognition of Cyber Threats

One of the principal strengths of the current framework is its recognition of the evolving nature of cybercrime. The Cyber Security Act 2026 addresses a broad spectrum of cyber-related offences, including unauthorized access to computer systems, digital fraud, identity-related crimes, cyber-enabled financial offences, and activities affecting cybersecurity and public order. This broader approach reflects an increased awareness of the diverse and rapidly changing cyber threat landscape confronting Bangladesh.

Legislative Evolution and Adaptability

The development of Bangladesh's cybercrime legislation demonstrates a continuing effort to adapt legal responses to technological change and societal concerns. The ICT Act 2006 primarily focused on electronic records, digital signatures, e-commerce recognition, and basic cyber offences. Subsequently, the Digital Security Act 2018 expanded the scope of cybercrime regulation but attracted criticism regarding freedom of expression and civil liberties. In response, the Cyber Security Act 2023 introduced several reforms and reduced certain penalties. Following further legal and political developments, the Cyber Security Ordinance 2025 introduced a more rights-oriented regulatory approach, which was later ratified by Parliament and enacted as the Cyber Security Act 2026. This legislative progression illustrates the state's willingness to revise and refine its cyber governance framework in response to changing circumstances.

Enhanced Institutional Awareness

Successive legislative reforms have contributed to greater institutional awareness regarding cybersecurity governance and cybercrime prevention. The existence of a dedicated cyber legal framework has encouraged capacity-building initiatives, inter-

agency coordination, professional training, and the development of specialized investigative capabilities within criminal justice institutions. These developments have strengthened the overall preparedness of relevant agencies responsible for responding to cyber-related offences.

Foundation for Cyber Governance

The Cyber Security Act 2026 also provides an important foundation for broader cybersecurity governance. Effective cyber governance requires cooperation among government institutions, law enforcement agencies, financial organizations, technology providers, regulatory bodies, and civil society stakeholders. The current framework facilitates such collaboration while supporting national efforts to enhance cyber resilience, improve digital trust, and strengthen the security of Bangladesh's expanding digital ecosystem.

CRIMINAL JUSTICE INSTITUTIONAL CAPACITY AND OPERATIONAL CHALLENGES

The effectiveness of cybercrime legislation ultimately depends upon the capacity of institutions responsible for its implementation. Even the most comprehensive legal framework cannot achieve its intended objectives without adequately equipped investigative agencies, competent prosecutors, informed judicial actors, and effective coordination mechanisms. As cyber threats become increasingly sophisticated, the ability of criminal justice institutions to adapt to evolving technological realities has emerged as a defining factor in national cyber resilience. This chapter examines the institutional architecture responsible for cybercrime responses in Bangladesh and critically evaluates the operational capacities and constraints affecting the administration of cyber justice.

Cyber Security Agency (CSA)

Bangladesh's institutional response to cybercrime involves multiple agencies with distinct yet complementary responsibilities in cybersecurity governance, law enforcement, and criminal investigation. At the national level, the Cyber Security Agency (CSA) is primarily responsible for developing cybersecurity policies, coordinating national cybersecurity initiatives, protecting critical information infrastructure, monitoring cyber threats, and supporting the implementation of the country's cybersecurity strategy. Although the CSA plays an important role in cybersecurity oversight and coordination, the investigation of individual cybercrime cases is principally undertaken by specialized law enforcement agencies. Within the Bangladesh Police, the Cyber Crime Investigation Division of the Dhaka Metropolitan Police (DMP) primarily addresses cyber offences occurring within the Dhaka metropolitan area, including online harassment, cyberbullying, identity impersonation, fake social media accounts, and various forms of digital fraud. For more serious and technically complex cyber offences, the Cyber Police Centre of the Criminal Investigation Department (CID) has nationwide jurisdiction to investigate offences such as financial cyber fraud, hacking, digital forensic evidence, and organized cybercrime. The effectiveness of Bangladesh's cybercrime response therefore depends upon effective coordination, information sharing, and technical capacity across these institutions.

Institutional Architecture for Cybercrime Response in Bangladesh

Bangladesh's response to cybercrime is based on a multi-institutional framework involving law enforcement agencies, investigative bodies, prosecutors, and the judiciary. Bangladesh Police serves as the primary agency for receiving complaints and initiating investigations, while the Criminal Investigation Department (CID) handles complex cases requiring digital forensic analysis, technical expertise, and inter-agency coordination.

Specialized cyber support mechanisms also address emerging forms of cyber victimization and online abuse. Following investigations, prosecutorial authorities evaluate evidence and conduct cybercrime prosecutions, which often involve complex digital evidence and cross-jurisdictional issues. The judiciary plays a crucial role in adjudicating cybercrime cases, ensuring due process, fairness, and the proper interpretation of cyber-related laws within an evolving technological environment.

Investigative Capacity and Digital Forensics

The investigation of cybercrime relies heavily upon the ability of institutions to identify, preserve, analyze, and present electronic evidence. Digital forensics has consequently become one of the most important components of modern criminal investigations.

Collection of Electronic Evidence

Unlike conventional evidence, digital evidence may exist in multiple locations simultaneously and can be altered rapidly if not preserved appropriately. Investigators may encounter evidence originating from:

- Computers and laptops;
- Mobile devices;
- Cloud storage services;
- Social media platforms;
- Financial transaction systems;
- Network logs.

The timely identification and preservation of such evidence are essential to maintaining evidentiary integrity.

Chain of Custody

Maintaining a reliable chain of custody remains fundamental to evidentiary credibility. A documented chain of custody helps establish:

- Who collected the evidence;
- When it was collected;
- How it was stored;
- Whether it remained unaltered;
- Who accessed it during the investigation.

Breakdowns in chain-of-custody procedures may undermine the admissibility or reliability of digital evidence during prosecution.

Digital Forensic Analysis

Digital forensic analysis involves the scientific examination of electronic devices and data to identify information relevant to criminal investigations. Common forensic activities include:

- Data recovery;
- Metadata examination;
- Device imaging;
- Timeline reconstruction;
- Log analysis;
- Extraction of deleted information.

These processes require specialized tools, technical expertise, and adherence to recognized procedural standards.

Technical Expertise

Technological sophistication among cyber offenders continues to increase. Encryption technologies, anonymization techniques, virtual private networks (VPNs), and cloud-based infrastructures frequently complicate investigations. Consequently, effective investigative responses depend upon continuous investment in technical training and professional development.

Cyber Intelligence

Modern cybercrime investigations increasingly incorporate intelligence-led approaches aimed at identifying patterns, trends, and emerging threats. Cyber intelligence supports investigations through:

- Threat monitoring;
- Trend analysis;
- Information sharing;
- Identification of criminal networks;
- Early warning mechanisms.

The integration of intelligence capabilities enhances both reactive and preventive dimensions of cybercrime control.

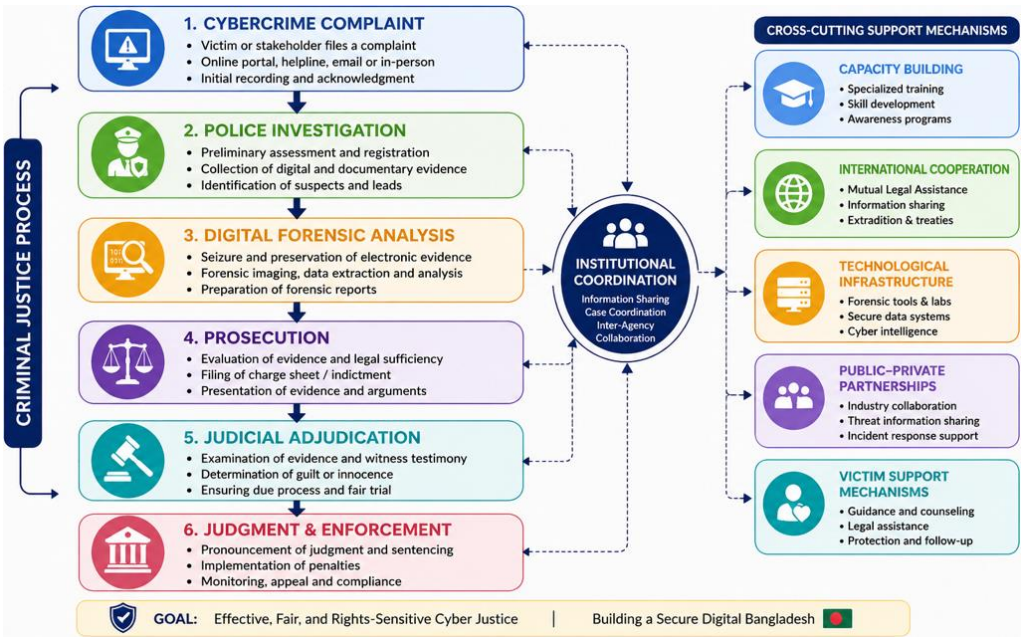

Figure 3: Criminal Justice Response Framework for Cybercrime in Bangladesh

The figure illustrates that cyber justice outcomes depend not solely upon individual institutions but upon the effectiveness of interactions across the broader criminal justice ecosystem.

Table 3: Institutional Roles and Operational Challenges in Bangladesh's Cybercrime Response

Institution	Primary Role	Major Operational Challenges
Bangladesh Police	Complaint intake and investigation	High caseloads, technological adaptation
Criminal Investigation Department (CID)	Specialized investigations and digital forensics	Resource and expertise limitations
Prosecutorial Authorities	Evidence assessment and courtroom advocacy	Complex technical evidence
Judiciary	Adjudication and procedural oversight	Need for continuous technological understanding
Specialized Support Mechanisms	Victim assistance and targeted interventions	Capacity and accessibility constraints
International Partners	Capacity building & cooperation	Jurisdictional complexities

Human Resource Constraints and Capacity Gaps

The effectiveness of cybercrime responses depends heavily upon the competence and preparedness of the individuals responsible for implementing legal mandates. While Bangladesh has gradually strengthened its institutional architecture, human resource limitations continue to represent one of the most significant barriers to effective cyber justice.

1. **Shortage of Specialized Personnel:** Cybercrime investigations require expertise in digital forensics, cyber intelligence, network analysis, malware investigation, cryptocurrency tracing, and electronic evidence management. However, the availability of adequately trained professionals remains limited.
2. **Need for Continuous Professional Development:** Rapid technological change demands ongoing training in emerging cyber threats, AI-enabled crimes, forensic technologies, digital evidence, and international investigative practices to maintain institutional effectiveness.
3. **Staff Retention Challenges:** Criminal justice institutions often face difficulties retaining highly skilled cyber specialists due to increasing demand for such expertise in the private sector, resulting in knowledge loss and reduced institutional continuity.
4. **Resource and Infrastructure Constraints:** Limited budgets, technological shortages, inadequate forensic tools, and insufficient investment in training, recruitment, and research can hinder the development of effective and sustainable cybercrime response capabilities.

Institutional Resilience and Future Readiness

The evolving cyber threat landscape requires institutions capable not merely of reacting to incidents but also anticipating future challenges. Institutional resilience involves the capacity to absorb disruptions, learn from experience, and adapt to emerging risks. Private organizations own and manage substantial portions of digital infrastructure. Consequently, sustainable cyber resilience depends upon constructive partnerships between government institutions and private stakeholders. Artificial intelligence, deepfakes, synthetic identities, and increasingly sophisticated cyber tools will continue to reshape future patterns of offending. Criminal justice institutions must therefore adopt forward-looking approaches emphasizing anticipation rather than reaction.

POLICY IMPLICATIONS AND RECOMMENDATIONS

Despite the progressive development of Bangladesh's cybercrime legislation, the effectiveness of its implementation continues to depend largely on institutional capacity. The existence of a comprehensive legal framework alone cannot ensure effective enforcement unless investigators, digital forensic specialists, prosecutors, and members of the judiciary possess the necessary technical knowledge and practical expertise to investigate, interpret, and adjudicate increasingly sophisticated cyber offences. Although specialized cybercrime units and digital forensic capabilities have been established and continue to expand, capacity development has not always kept pace with the rapidly evolving nature of cyber threats. Consequently, strengthening institutional competence, enhancing inter-agency coordination, and promoting continuous professional development remain critical priorities for improving the practical implementation of Bangladesh's cybercrime laws. Based on the preceding analysis, several policy implications and recommendations emerge:

1. **Strengthen Institutional Capacity:** Bangladesh should continue investing in specialized cybercrime investigation units, digital forensic laboratories, technological infrastructure, skilled human resources, and continuous professional training to enhance the effectiveness of cybercrime prevention, investigation, and enforcement.
2. **Enhance Prosecutorial and Judicial Preparedness:** Continuous capacity-building programs should be provided for prosecutors and members of the judiciary on digital evidence, cyber forensic principles, emerging technologies, and cyber legislation to ensure consistent, informed, and effective adjudication of cybercrime cases.
3. **Improve International Cooperation:** Given the transnational nature of cybercrime, stronger collaboration with international organizations and regional partners is necessary to facilitate intelligence sharing, mutual legal assistance, and cross-border investigations.
4. **Promote Public Awareness and Digital Literacy:** National cybersecurity strategies should emphasize public education on phishing, online fraud, social media safety, digital financial security, and emerging AI-enabled threats to reduce victimization risks.
5. **Advance Rights-Sensitive Cyber Governance:** Future reforms should balance cybersecurity objectives with fundamental rights by ensuring accountability, transparency, due process, proportionality, and public trust in cyber governance mechanisms.
6. **Develop a Future-Oriented Cyber Strategy:** Policymakers should adopt proactive approaches that support research, innovation, adaptive regulation, risk assessment, and multi-stakeholder collaboration to address emerging threats such as artificial intelligence, deepfakes, and synthetic identity fraud.

CONCLUSION

Cybercrime has emerged as one of the most significant challenges confronting contemporary criminal justice systems. As Bangladesh advances toward becoming a digitally empowered society, the opportunities created by technological innovation have been accompanied by increasingly sophisticated cyber threats affecting individuals, businesses, and public institutions. The evolving nature of cybercrime necessitates responses that extend beyond conventional law enforcement approaches and embrace adaptive, coordinated, and forward-looking strategies.

This study critically examined the relationship between emerging cybercrime threats and criminal justice responses in Bangladesh through a socio-legal perspective. The findings indicate that Bangladesh has made notable progress in strengthening its cyber governance landscape through successive legislative reforms, culminating in the enactment of the Cyber Security Act 2023. The country has also demonstrated growing institutional awareness of cybersecurity challenges and the importance of specialized responses to cyber-related offences.

However, the study further reveals that legal reform alone is insufficient to ensure effective cyber justice outcomes. Persistent challenges relating to institutional capacity, digital forensic expertise, electronic evidence management, prosecutorial preparedness, judicial understanding, and cross-border cooperation continue to influence the effectiveness of cybercrime responses. The emergence of technologically sophisticated threats, including ransomware, AI-assisted fraud, deepfakes, and synthetic identity crimes, further underscores the need for continuous adaptation and institutional resilience.

The analysis suggests that Bangladesh's future preparedness will depend upon its ability to integrate legal innovation with practical implementation capacities. Strengthening criminal justice institutions through sustained investment in human resources, technological infrastructure, specialized training, and international cooperation should therefore remain national priorities. Equally important is the development of rights-sensitive cyber governance approaches that balance security objectives with due process, accountability, transparency, and the protection of fundamental freedoms.

Ultimately, cyber resilience is not solely a legal or technological objective; it is a governance imperative requiring collaboration among state institutions, private stakeholders, international partners, and citizens. By fostering adaptive institutions, promoting public awareness, and embracing evidence-informed policymaking, Bangladesh can enhance its capacity to address emerging cyber threats while maintaining public trust in the administration of justice.

In conclusion, the fight against cybercrime in Bangladesh will ultimately be defined not by the existence of legislation alone, but by the collective capacity of institutions and society to anticipate, adapt to, and respond effectively to an increasingly complex digital future. Strengthening this collective capacity represents both a contemporary necessity and a long-term investment in justice, security, and sustainable digital development.

Bangladesh's cybercrime legislation has evolved through several stages, beginning with the ICT Act 2006 and progressing through the Digital Security Act 2018, Cyber Security Act 2023, Cyber Security Ordinance 2025, and the current Cyber Security Act 2026. This legislative evolution reflects the country's ongoing attempt to develop a cyber-governance framework capable of addressing emerging threats while responding to concerns relating to civil liberties, due process, and institutional accountability.

AUTHOR CONTRIBUTIONS

The authors jointly conceived and designed the study, conducted the literature review and analysis, prepared the manuscript, and approved the final version of the manuscript.

Conflict of Interest

The authors declare that they have no conflict of interest.

Data Availability Statement

The data supporting the findings of this study are derived from publicly accessible sources cited throughout the manuscript. No proprietary or confidential datasets were used.

REFERENCES

Ahmed, A. A. A., Bynagari, N. B., Mustafa, M., Vishwakarma, S., & Azad, M. M. (2021). *IoT and machine learning based low cost home automation and security system and methodology using cell phone* (Canadian Patent No. 1188173). Canadian Patent Office.

Ahmed, A. A. A., Gupta, N., Iqbaldoewes, R., Krishna, M. M., Bandyopadhyay, R., & Mohajon, M. K. (2022). COVID-19 interior security tracking system based on the artificial intelligence. In *Proceedings of Second International Conference in Mechanical and Energy Technology: ICMET 2021, India* (pp. 465–473). Springer Nature Singapore.

Asha, P., Srivani, P., Doewes, R. I., Ahmed, A. A. A., Kolhe, A., Nomani, M. Z. M. (2021). Artificial intelligence in medical Imaging: An analysis of innovative technique and its future promise. Materials Today: Proceedings, 1-4. https://doi.org/10.1016/j.matpr.2021.11.558

Chen, T-C., Alazzawi, F. J. I., Salameh, A. A., Ahmed, A. A. A., Pustokhina, I., Surendar, A. & Oudah, A. Y. (2021). Application of machine learning in rapid analysis of solder joint geometry and type on thermomechanical useful lifetime of electronic components. Mechanics of Advanced Materials and Structures, https://doi.org/10.1080/15376494.2021.2014002

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608.

Donepudi, P. K., Banu, M. H., Khan, W., Neogy, T. K., Asadullah, A., & Ahmed, A. A. (2020). Artificial intelligence and machine learning in treasury management: A systematic literature review. *International Journal of Management, 11*(11), 13–26. https://iaeme.com/Home/article_id/IJM_11_11_002

Ganapathy, A., Redwanuzzaman, M., Rahaman, M. M., & Khan, W. (2020). Artificial intelligence driven crypto currencies. *Global Disclosure of Economics and Business, 9*(2), 107–118. https://doi.org/10.18034/gdeb.v9i2.557

Gazi, M. A. I., Shinwary, S. S., Khan, W., Alam, M. N., Hashim, F., Babiker, M. O. A., Hossain, A. I., & Senathirajah, A. R. B. S. (2026a). *Influence of green environmental management practices and supply chain integration on technological innovation performance: A conceptual review using PRISMA model. Sustainable Social Development, 4*(3), 1–21.

Gazi, M. A. I., Shinwary, S. S., Khan, W., Alam, M. N., Hashim, F., Senathirajah, A. R. B. S., & Hossain, A. I. (2026b). *Ethical implications of AI-driven educational management systems on equity and social justice in sustainability education: A comprehensive review. Multidisciplinary Reviews, 9*(11), 1–11.

Government of the People's Republic of Bangladesh. (2006). *Information and Communication Technology Act, 2006*. Bangladesh Government Press.

Government of the People's Republic of Bangladesh. (2018). *Digital Security Act, 2018*. Bangladesh Government Press.

Government of the People's Republic of Bangladesh. (2023). *Cyber Security Act, 2023*. Bangladesh Government Press.

Government of the People's Republic of Bangladesh. (2025). *Cyber Security Ordinance, 2025*. Bangladesh Government Press.

Government of the People's Republic of Bangladesh. (2026). *Cyber Security Act, 2026*. Bangladesh Government Press.

Hoque, M. R., Hossin, M. E., & Khan, W. (2016). Strategic information systems planning (SISP) practices in health care sectors of Bangladesh. *European Scientific Journal, 12*(6), 307–321. https://doi.org/10.19044/esj.2016.v12n6p307

Hoque, M. R., Sorwar, G., Alam, M. Z., Khan, W., & Hasan, R. (2020). Designing social networking mobile app for diabetes management. In *Proceedings of the International Conference on Information Resources Management (CONF-IRM 2020)* (pp. 1–14). https://aisel.aisnet.org/confirm2020/21/

Hussain, S., Ahmed, A. A. A., Kurniullah, A. Z., Ramirez-Asis, E., Al-Awawdeh, N., Al-Shamayleh, N. J. M., Julca-Guerrero, F. (2021). Protection against Letters of Credit Fraud. Journal of Legal, Ethical and Regulatory Issues, 24(Special Issue 1), 1-11. https://doi.org/10.5281/zenodo.5507840

International Telecommunication Union. (2024). *Global cybersecurity index 2024*. Author.

INTERPOL. (2024). *Asia and South Pacific cyberthreat assessment report 2024*. Author.

Islam, K. M. A., Khan, W., Bari, M. F., Mostafa, R., Anonthi, F., & Monira, N. A. (2025). Challenges of artificial intelligence for the metaverse: A scoping review. *International Research Journal of Multidisciplinary Scope, 6*(1), 1094–1101.

Khan, W., & Fadziso, T. (2020). Ethical issues on utilization of AI, robotics and automation technologies. *Asian Journal of Humanity, Art and Literature, 7*(2), 79–90. https://doi.org/10.18034/ajhal.v7i2.521

Khan, W., Ahmed, A. A., Vadlamudi, S., Paruchuri, H., & Ganapathy, A. (2021). Machine moderators in content management system details: Essentials for IoT entrepreneurs. *Academy of Entrepreneurship Journal, 27*(3), 1–11.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71. https://doi.org/10.1136/bmj.n71

United Nations Office on Drugs and Crime. (2024a). *Bangladesh Police and UNODC forge stronger cooperation with capacity-building initiatives*. United Nations Office on Drugs and Crime.

United Nations Office on Drugs and Crime. (2024b). *UNODC and Justice & Care raise awareness on mutual legal assistance in criminal matters*. United Nations Bangladesh.

--0--