



**DISSERTATION SUBMITTED TO DAFFODIL INTERNATIONAL
UNIVERSITY IN PARTIAL FULFILLMENT OF THE REQUIREMENT
FOR THE AWARD OF THE DEGREE**

MASTER OF LAW

Date of Submission: 10 July 2025

Department of Law

Faculty of Humanities and Social Science

Daffodil International University

LETTER OF TRANSMITTAL

Dr.S.M.Saiful Haque

Associate Professor and Head

Department of Law

Daffodil International University

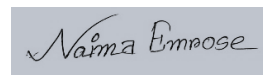
Dear Sir,

It's a great pleasure for me that I have been able to make research on "An Analysis of Cybercrimes in Bangladesh: Legal Framework, Emerging Trends, and Challenges". During conducting this research I have given all of my best effort to form the useful research and by collecting all the relevant information from different sources that it can fulfill your expectation.

Therefore, I shall remain grateful to you if you pass through this research paper for your evaluation and I would be like that if any valuable recommendation is formed from your part in this matter.

I am always available for any further clarification of any part of this paper at your convenience.

Sincerely yours,



Name: Naima Emrose

ID: 241-38-009

Program: LL.M (Final)

Department of law

Daffodil International University

LETTER OF APPROVAL

This is to certify that the work is done” An Analysis of Cybercrimes in Bangladesh: Legal Framework, Emerging Trends, and Challenges” is a real work done by Naima Emrose, ID: 241-38-009, Batch:42, Department of Law, Daffodil International University, done under my supervision in partial fulfillment for the research, work is done for the fulfillment of course requirements of LAW_812, from the Department of Law, Daffodil International University.



Dr.S.M.Saiful Haque

Associate Professor and Head

Department of Law

Daffodil International University

DECLARATION

I, thereby, declare that the work, present in this research is performed by me under the supervision of Dr.S.M.Saiful Haque, Associate Professor and Head Daffodil International University. I also assure that this research or no part thereof is being submitted anywhere for the award of any degree.



Naima Emrose

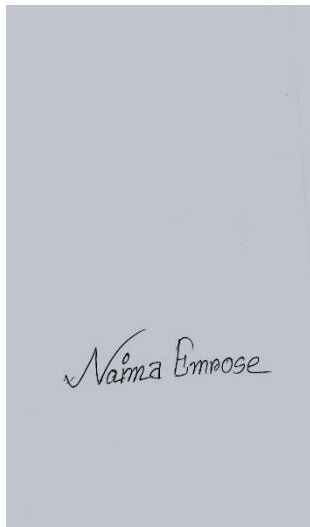
Candidate

ACKNOWLEDGEMENT

It is a great pleasure for me to thank that person who supports me to complete this research like family, friends and teachers. To begin with, I would like to express my gratitude to my supervisor supervision of Dr.S.M.Saiful Haque, Associate Professor and Head Daffodil International University, who was foundation of concepts and offer of suggestions. A great thanks due to this well observed teacher for supporting me.

DEDICATION

First of all, I am presenting very much respect and gratefulness to my ALLAH. I would like to express my appreciation and love to my mother for her detriment and to provide me the opportunities for higher education.



.....

Naima Emrose

ABSTRACT

This article discourses and evaluates the cybercrimes of Bangladesh. It also discourses about the legal framework for cybercrimes, emerging trends and challenges to prevent cybercrimes. Today's Bangladesh cybercrime is a major challenge. Now it has become one of the main problem. Cybercrime is now in everywhere which is causing harm to our society, culture, socio-economy development. Basically, it is causing harm to individual's reputation, property, asset, intellectual property, privacy etc. there are many kinds of cybercrimes in our country. Many research were approved on cybercrime but not a singal research work could put effective result to prevent cybercrime. To prevent cybercrime and creating a secure society, policymakers need to make a strong framework for cybercrime and need to adopt new methods. Through this we can make a secure society and secure Bangladesh.

LIST OF ABBREVIATIONS

PC	Penal Code 1860
ICT	Information and Communication Technology
CSA	Cyber Security Act
DSA	Digital Security Act
UN	United Nations
SAARC	South Asian Association for Regional Cooperation
BTRC	Bangladesh Telecommunications Regulatory Commissions
CTTC	Counter Terrorism and Transnational Crime

TABLE OF CONTENT

Contents	Page No
Letter of Transmittal	iii
Letter of Approval	iv
Declaration	v
Acknowledgement	vi
Dedication	vii
Abstract	viii
List of Abbreviations	ix

CHAPTER ONE

Introduction

1.1	Background of the study.....	1
1.2	Objective of the Research.....	1-2
1.3	Significance of the Research.....	2
1.4	Research question.....	2
1.5	Research Methodology.....	3
1.6	Limitations of Research.....	3

CHAPTER TWO

An Overview and Conceptual Framework of Cybercrime

2.1	Overview.....	4
2.2	Definition and Categories of Cybercrimes.....	4-5
2.3	Reasons of Cybercrime.....	5-6
2.4	Evaluation of Cybercrime: Global and Local Context.....	6
2.5	Key Components of Cybercrime.....	6-7

CHAPTER THREE

Cybercrime Trends and Statistics in Bangladesh

3.1	Cybercrime rate statistics in Bangladesh.....	8
3.2	Common types of Cybercrime in Bangladesh.....	9
3.3	Impact of Cybercrime on Individual and organizations.....	9-10
3.4	Role of Social media and Emerging Technologies in cybercrime.....	10

CHAPTER FOUR

Legal Framework for Addressing Cybercrime in Bangladesh

4.1.1	Information and Communication Technology Act 2006.....	11-12
4.1.2	Cyber Security Act, 2023.....	12-13
4.1.3	Penal Code 1860.....	13

4.1.4	Digital Security Act, 2018.....	13-14
4.2	International Conventions and Treaties Related to Cybercrime.....	15
4.3	Role of Cybercrime Units in Bangladesh.....	15-16

CHAPTER FIVE

Challenges in Combatting Cybercrime in Bangladesh

5.1	Gaps in Legislation and Policy Implementations.....	17
5.2	Lack of Technical Expertise among Law Enforcement.....	17-18
5.3	Issue of Privacy and Data Protection.....	18
5.4	Social Cultural Barriers in Reporting Cybercrimes.....	18-19
5.5	Inadequate awareness and Digital Literacy.....	19

CHAPTER SIX

Comparative Analysis: Best Global Practice

6.1	Cybercrime Legislation in Developed Countries.....	20
6.2	Analysis of Regional Initiatives in South Asia.....	20-21
6.3	The Role of International Cooperation in Tackling Cybercrime ...	21-22

CHAPTER SEVEN

Conclusion

7.1	Discoveries.....	23
7.2	Recommendations.....	23-25
	REFERENCE.....	26

CHAPTER ONE

Introduction

1.1 Background of the Study

It is undoubtable true that we live in a digital age. Our life become computer centralized. As we become more and more centralized, the concern to protect unauthorized access increased. This development not only give positive vibe but also has given rise to new problems. Cybercrime is rapidly emerging in our country for the last decade. Now it is the reason of most of the social aggressions and crimes in our country every year .Basically, cybercrime is spreading in Bangladesh through mobile phone, internet, social media and electronic device. Unfortunately, in rural areas cybercrime is increasing day by day. The poor economic condition of peoples in our country is the main cause of cybercrime. Besides, lack of awareness of the people and unsecure use of digital technologies are core causes of cybercrime. It is not only causing harm to individual, intellectual property, socio-economic development but also causing harm to political stability, national security and sovereignty. Cybercriminal dose cybercrime through mobile phone, internet, social media, digital devices, computer, laptop etc. For instance, hacking, software piracy, internet fraud, ransomwares etc. are some of cybercrimes. Last few years cybercrime has increased 281.76% in Bangladesh and most of the victims are female.

Most of the cyber criminals does this crime because of money. In our country most of the cybercriminals are young people who are aware of digital security and digital device. There are many research has been carried out on the cybercrime in Bangladesh but no research could prevent and reduce cybercrime in Bangladesh. To decrease cybercrime policy makers need to update the policies of our country and need to eradicate of loopholes of the policies and need to aware people about cybercrimes. For want of these steps cybercrime is a major issue in our country.

1.2 Objective of Research

My research objectives are as follows:

- A. The key objective of this research is to find out the causes of cybercrime in Bangladesh.

- B. Which age people are becomes victim of cybercrime most
- C. To find out what are the cyber emerging trends of Bangladesh.
- D. TO find out the challenges of cyber security act and find out ways and means of taking effective measures to reduce the cyber offences.
- E. To analyze cybercrimes and emerging trends of different countries perspective.

This paper is to analyze the cybercrimes of Bangladesh: legal framework and emerging trends. Also to analyze various types cybercrimes in Bangladesh

1.3 Significance of the Research

Before conducting my research I tried to learn basic loopholes of the cyber security act and the emerging trends and legal framework. The significance of my studies is, it will help to learn about the cybercrimes of Bangladesh. It also help to know about the types of cybercrimes, causes of cybercrimes and about the victims of cybercrime. It will also help it know the challenges to prevent cyber security. There are many research in this field but everyone has failed to give a proper solution about this. My work will remove this gaps. I strongly believe that my work will clarify all gaps and loopholes. In addition, this research maybe very much helpful for the students of law to enrich their own wisdom.

1.4 Research Question

My research Questions are as follows:

1. Is there any law to protect the Cybercrime in Bangladesh?
2. What is the main reason behind the cybercrime?
3. What are the types of cybercrimes?
4. What are the changes is essential to protect cyber life?

1.5 Research Methodology

I have employed a dogmatic, analytical, and characteristic technique in this study, as well as findings for many kinds of data and statistics. Typically, it is analytical and draws from both primary and secondary sources. First, I studied a number of journal papers about cybercrime and its causes, reviewed a few books written by different students, and visited a few websites. I have gathered data from articles in newspapers. I understand both international and national legislation. I will critically evaluate the provided data items using an analytical approach.

1.6 Limitations of Research

There are many limitations for conducting this research is immense reliance on online journals, books and reports. Moreover, unavailability of data related to practical situation related to this research is not available and most of them are not updated. It is the limitation of this research. Essentially, there are lot of information, but we cannot say that this study is 100% authentic. There is another limitation is shortage of time and budgets. In fact, it is very hard to conduct a study in a short and limited period.

CHAPTER TWO

An Overview and Conceptual Framework of Cybercrime

2.1 Overview

The way we are living is going through a significant change as a result of new communication systems and digital technology. Last ten years, The Internet has grown significantly. Now, International borders are no longer a barrier to this type of crime. The number of internet users in Bangladesh is raising rapidly. Cybercrime is also rising quickly in Bangladesh, there is currently no system in place to address it. The phenomenon of growing cybercrime is very life-threatening right now in our country. Over the recent years people are in large number is facing this crimes. Not only people of our country facing this challenges but also government is facing this challenge to prevent this crime. This delinquency is generally committed by mobile phone, internet and computer. This crime is spreading in an alarming rate in our villages and rural areas. There is no way for patrolling this information superhighway like traditional police patrolling. For this most of the crime is happening. Most of the cybercrimes victims of our country is females and online users. Utmost al of the cybercriminals does these delinquencies for want of money. But sometimes they does these for spreading rumors. Basically, all sections of people of our country is facing this problem. Over a few years this crime has increase 276% in our country. So, in today's Bangladesh cybercrime is a big problem. Most of the experts has given this opinion that the main reasons for the ineffectiveness of our law is lack of legal support and social and public awareness about computer and computer related crimes and technologies.

2.2 Definition and Categories of Cybercrimes

Technology enabled crime area is always evolving. Cybercrime is a crime which is comprise of unlawful practice using computer, internet, mobile phone, focusing on harming networks, snitching data or committing fraud. This besets activities like prohibited enter, identity theft and online scams. Basically, any unauthorized work that takes place in the digital world and targets computer systems, networks, or data can be classified as cyber-crime. Cybercrime can generally be defined as a unlawful activity involving an information technology structure. Such as: illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions

of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (theft), and electronic fraud¹. In Bangladesh Cybercrimes can be normally divided into 3 main categories-

- The First Category Cybercrimes is committed against individual comprise of various crimes like dispatch of Child pornography, harassment of any one with the use of a computer such as e-mail, social media and websites
- Cybercrimes which is done against all forms of property is the second category. These crimes is committed through computer defacement or ruin of other's assets, transmission of destructive program.
- Crimes against Government can be defined as the third category of cybercrime. Cyber terrorism is another separate category of cybercrime.

2.3 Reasons of Cybercrime

Evil and virtue cohabit in life. The Internet has also some negative aspects. It is very difficult to find one major reasons for cybercrime: The study of cyber criminology cases mostly states that there is a direct connection between crime and age. In Bangladesh cybercrime is happening for various reasons. First of all A large amount of Bangladeshi people has a lack of awareness regarding cyber threats and safe online practices. This lack of awareness makes people more liable to phishing scams, identity theft, and further types of cyber fraud. Secondly, people in our country commit these crimes for want of money. Because in today's Bangladesh people are facing economic vulnerabilities. Thirdly, most of the people of our country is illiterate about the security of the technologies. Digital technologies and connectivity is increasing among the peoples, organizations and in business but they have not proper awareness and security to protect their cyber life from cyber-attacks. Fourthly, in Bangladesh e-commerce is raising very quickly. So this fast growing e-commerce and digital payments is creating golden opportunities to commit cybercrimes by cybercriminals. Fifthly, our technologies is not much developed like other countries. Sixthly, a research shows that there is a direct relationship between the gender of users and the rate of

¹ Information and Communication Technology Act 2006 (Bangladesh)

visiting porn sites among them 82% men and 5% women. Seventhly, The virtuality of Internet and the possibility of multiple and false characteristics and their non-disclosure help cybercriminals to commit crimes without disturbing about revealing their actual identity. Eighthly, lack of infrastructure and expertise about cybersecurity is another main reason. So it is difficult to protect the cyber challenges which is occurring outside our national jurisdiction.

2.4 Evolution of Cybercrime: Global and Local Context

In 1834, before inventing internet, the first cybercrime had happened in France. The attackers entered French telegraph system and stole all the financial information regarding financial market. In 1962, Allen Scherr had originated a cyber-attack against the MIT computer networks, thieving passwords from their database via punch card which was the first modern cybercrime. In 1971, BB Thomas first created the computer virus at BBN Technologies. After successfully hacking into AT&T's inner systems and altering their computers' clocks, Ian Murphy became the first person who was convicted for cybercrime. In Bangladesh in early 2000s cybercrime became most visible problem with the availability of internet. The first notable cybercrime of Bangladesh occur in 2004 where the hackers, hacked government websites and changed them with unauthorized content. In Bangladesh, financial scam through email began from 2005-2006. In 2006, the most mentionable cybercrime occurred in Bangladesh where the hackers tried to steal 1\$ billion through SWIFT network from Bangladesh Bank. All this incident mentions about the vulnerabilities of our cyber security. Nowadays young peoples of Bangladesh are using cyber cafes like their dating spaces. There are separate cabins for pairs in cyber cafes where they share intimate moment and record video secretly and after that they upload it in many websites. In Bangladesh, now we can see a lot of existence of illegally hosted pornographic websites in local context. Bangladesh has made pornography illegal but because of ineffectiveness of cyber law these criminals are get rid of punishment.

2.5 Key Components of Cybercrime

We are living in a age which is exclusively depend on science and technology. It is for committing a need there need two elements and they are Actus Reus and Mens Rea. In cybercrime, Actus reus are much more forwarding and wide-ranging which is very hard to prove in case of cybercrime.

Mens' re is comprised of two parts for cybercrime. The first is it needs to be proved that there was an aim to get the data from a specific device and the second is there was knowledge about Actus reus when the crime was commencing. Now it is established that there are three factors required for committing crime. They are a supply of motivated offenders, the availability of suitable opportunities and the absence of capable protectors. Our digital age offers fertile ground for offending. Internet permits users to interconnect with many people, without difficulty and inexpensively. The estimated 1.6 billion people, approximately 24 % of the world's population, provide an extraordinary pool of potential offenders and victims on internet. Now a days the technology is ubiquitous and comparatively easy to use which is ensuring its accessibility to both offenders and victims.

CHAPTER THREE

Cybercrime Trends and Statistics in Bangladesh

3.1 Cybercrime rate statistics in Bangladesh

Cybercrime rate is rapidly increasing in Bangladesh but the tendency to take legal action is very low in our country. There are various cybercrime in Bangladesh happening in every year. Among them social media and online account hacking is major problem which is 21.65% of total cybercrime in Bangladesh. Cyber Crime Awareness Foundation (CICAF) recently published a report. There they have interviewed 132 people. Among these people 78.78% victims are 18-30 years old, 13.65% victims are below under 18 years and 7% victims are above 31 years old. The most concern issue is 59% victims are women. They also published that 11.35% cybercrime has increased in Bangladesh which is related with child pornography. Among these victims 47.72% has lost their social status and 40.15% has faced financial loss and destruction. All these victims are mentally distressed, frustrated and some attempted to commit suicide. Surprisingly, the rate of taking legal action against these crimes are only 12%. Between these 81.25% has filed general diary and only a few which is 18.75% has filed written complain. Those who ever filed complain 87.50% has claimed that they have not got any positive outcome and 12.50% did not make any comment as their case is running. The proportion of cybercrime victims under 18 decreased to 13.65% in 2023, indicating a shift in targeted demographics. The emergence of new types of cybercrimes, termed "neo-cybercrimes," doubled in 2023, comprising 11.85% of total cybercrime cases. Additionally, 11.35% of victims were affected by pornography-related cybercrimes. In 2023, over 700,000 web threats were detected and blocked for businesses in Bangladesh, marking a 28% increase from the previous year. On average, businesses experienced over 2,000 online attacks each day. According to a recent report from Threat Intelligence Platform, Bangladesh has been identified as one of the nations facing the most significant increase in cyber incidents globally, reporting a 105% rise from the second to the third quarter of 2024. This movement in events highlights the country's upward cybersecurity contests, placing it second only to Japan (108%) and closely followed by France (130%) in percentage growth.

3.2 Common Types of Cybercrime in Bangladesh

There are many kinds of cybercrimes in Bangladesh. Among them some common crimes are:

Identity theft: It is a type of cybercrime which mentions stealing some person's information using digital means and uses them for fraud and illegal intention.

Online Fraud: It is a types of cybercrime which is done in online or in internet, using digital devices and its purpose is to cheat people providing incorrect information, tactics etc.

Cyber stalking and Harassment: Cyber stalking is a common type of cybercrime which means to stalk or harass people, group, or body using internet or other electronic or digital device. It can be include identity theft, defamation, false accusation etc.

Phishing and Malware Attacks: Phishing means such type of cyber-attack where criminals targets individuals through massage, phone call, email etc. Malware attacks means cyber-attacks which is done through illegal software to cause harm to targeted computer and done unauthorized acts.

Hacking and Data Breaches: Hacking is the act which is done through digital devices and networks by occurring unlawful entree to an account or in computer system. Data breaches means exposing information which was very private, confidential and sensitive and was unauthorized for access.

3.3 Impact of cybercrime on Individuals and organizations:

Cybercrime causes a serious impact on individuals and organizations. Cybercrime causes financial loss, social status loss, reputation loss to an individual. Most of the time these individuals face a lot of mental pressure, emotional trauma, frustration and commits suicide. Sometimes it causes harm to relationships. Organizations, business whoever victims of these crimes causes a great monetary loss? Sometimes faces intellectual property loss such as patents, copyrights etc. cybercrimes may create unstable situations in organizations. Sometimes it creates operational

disruptions and makes revenue loss. These cyber-attacks may mislay hope in digital facilities and expertise.²

3.4 Role of Social media and Emerging Technologies in Cybercrime

Social media plays a very important role for spreading cybercrime. Most of the time social media ask for users email, password, ip address, mobile number or bank account number. Whenever individuals provide these information, cybercriminals collects these information through phishing, malware, data breaches and online fraud. Cybercriminals often use illegal links, applications, messages, email, and spy software to commit cybercrimes. Social media also provide a vast form of personal information of individuals. Cybercriminals can easily use these information to exploit people

² Cyber Crimes in Bangladesh (SlideShare,2024) <https://www.slideshare.net/slideshow/cyber-crimes-in-bangladesh-252707211> accesses 2 February

CHAPTER FOUR

LEGAL FRAMEWORK FOR ADDRESSING CYBERCRIME in BANGLADESH

4.1.1 Information and Communication Technology Act 2006 (Amended in 2013) or ICT Act

The Information and Communication Technology Act, 2006 was introduced in Bangladesh in 2006 for preventing cybercrimes, crimes related to computer and internet, e-commerce, banking, hacking, identity theft, cyber fraud, cyber terrorism etc. later this act was amended in 2013. This act states about the establishment of Cyber Tribunal in Bangladesh to deal cyber related crimes and ensure speedy trial. Section 54-56 of this act stipulates about the penalty of cybercrimes, unsanctioned entry, evils to computer network and system and data theft. It has provisions for monetary compensation. This act also provides penalties for the cyber terrorism and activities which causes threats to national security. This act provides permission to the Government for monitoring online activities and provide security to sensitive and personal data. Section 57 of ICT act mentions that a person who is convicted for uploading discourteous and explicit contents on website is punishable for 10 years³⁴ imprisonment and a fine of one core taka. This kind of fine is very unfair because the amount is too high beside per capita income. At first it was unbailable offence. After the amendment in 2013 it became cognizable offence. So the arrest without warrant went to police's hand and there were huge scope for misusing this power. They also misused this power by arresting bloggers and peoples. This section also snatched freedom of expression.

Section 66 states that any individual who intentionally terminates, alters, or knowingly causes another person to conceal, destroy, or modify any computer source code utilized in a computer, computer network, or computer program shall face a penalty of up to three years in prison, a fine of two lakh taka, or both. Section 67 states that anyone who intentionally or knowingly causes a wrongful loss or damage to the public or any individual, or engages in actions that destroy, delete, or alter any information within a computer resource, or reduces its value or utility, or impacts it negatively by any means, commits the offense of 'hacking.' Section 68 of this act outlines the

³ Sonal Srivastava, 'How Has Social Media Contributed to the Spread of Cybercrimes? - An Analysis' (iPleaders, 6 May 2021) <https://blog.iplayers.in/how-has-social-media-contributed-to-the-spread-of-cybercrimes-an-analysis/> Accessed 3 February 2025

⁴ Sharebiz, 'Information and Communication Technology Law and some Things' (Sharebiz, undated) <https://sharebiz.net> accessed 4 February 2025

penalties for hackers, indicating that anyone found guilty of hacking may face a prison sentence of up to three years, a fine of up to two lakh, or both.

4.1.2 Cyber Security Act, 2023 (CSA)

For providing more security of cyber life Cyber Security Act, 2023 was enacted in Bangladesh. Through this act the most controversial act of Bangladesh which is Digital Security Act, 2018 was replaced.

The main objective of this act was to prevent the offences which was committing through electronic means or digital means. This Act mentions about the formation of a Cyber Security Agency who would be responsible for monitoring cyber security measures.

According to this act, government may call for special protection for any computer network, infrastructure and computer network. This act also provide permission to build National Cyber Security Council for create policies, and ensure cyber security. Four non-boilable offences introduced in this act which is mentioned in section 4.

Section 8 gives power to the government to remove and block data from digital media. This limitations can greatly hamper in data insertion. This section also provides power to the Director General to stop the internet which can affect our banking, social and corporate life. Government very easily can misuse this power for their own interest. For example, government of Bangladesh misused their power and shutdown internet in Bangladesh in July-August 2024 during the anti-quota protest.

Section 14 stipulates non boilable offences. This act has an excellent section which is section 34. It mentions about false case. False case has been considered as a crime and there have provisions for punishment for filing false case. Section 27 deals with cyber terrorist acts its punishment. Hacking related crimes has been introduced in section 33.⁵

Section 42 provides power to police for arrest any person without warrant. It was also in Digital Security Act which is an obstruct for freedom of speech. This ⁶section violets freedom of opinions,

⁵ The Daily Star, 'Fare speech vs Section 57' (The Daily Star 2015)
<https://www.thedailystar.net/frontpage/news/free-speech-vs-section-57-130591> accessed 29 June 29, 2025

⁶ Zaif Faiaz , ' Cyber Security Ordinance 2024: Progress or Pitfall? The Daily Star (Dhaka, 26 December2024)
<https://www.thedailystar.net/tech-startup/news/cyber-security-progress-or-pitfall-3785116> accessed 29 June 2025

media and speech and generates threat for⁷ exploiting authorities. Again this section does not define any time limitation for producing those arrested people before any court or any magistrate. So Police force can easily arrest any person without warrant and can detain them as long as they want.

This act does not effectively gives any specific protection to the girls, woman, children and vulnerable people who are the victims of cybercrime.

According to Section 8, 21,25,28,29, 31,32,43,53 there are some restrictions for exercising freedom of speech in electronic media. It is totally opposite with the intention of this act according to its proposal which creates an illogical restrictions.

Section 21 and 28 of this is act are vague and broad and does not specifically define the words like Propaganda, Campaign.

There is a serious conflict between Children Act 2013 and Cyber Security act 2023. Children Act has been introduced specially for kids and child and for this reason this act shall prevail above all acts. Again Cyber Security Act 2023, section 3 mentions this act shall prevail over all act. So there creates a conflict when a child joins a cybercrime.

4.1.3 PENAL CODE 1860

Though this act is very old, provides provision for cybercrime. Before enacting Information and Communication Technology Act, 2006 cybercrimes were delta with this act. Still this act provides penalties for online fraud, defamation and identity fraud. Section 499-500 can be applied for online defamation. Section 503-506 can be used for online threats or criminal intimidation. Section 420 can be applied for online fraud or cheating. Section 292 can be used for online publication of explicit materials. Sections 468-471 can be used for forgery or digital forgery.

4.1.4 Digital Security Act, 2018

Digital security act was introduced in Bangladesh in 2018 for preventing cybercrime, online fraud, discrimination; sectarianism; fanaticism; terrorist propaganda; and hatred against religious or ethnic minorities through social media, print media or any other electronic media. **This act provided** safeguard from cyber threats. The grievous punishment which was

⁷ Shamsad Binte Ehsanand Md Najmus Saquib, 'Balancing Cybersecurity and Individual Rights:A Critical Analysis of Bangladesh's Cyber Security Act 2023' (2024) Journal of Creative Writing vol 8,no 1 (28nJune 2024) <https://doi.org/10.70771/jocw.v8i1.109> accessed 29 June 2025

prescribed by the act attend as a warning against engaging in cybercrimes. The Digital Security Act 2018 creates a barrier for freedom of speech and liberty which is protected by our constitution.

This legislation suffers from a lack of precise definitions, explanations, and exceptions. There are at least 14 non-boilable offenses that infringe upon human rights. Section 8 of this legislation establishes two types of authority: that of the director general and that of law enforcement agencies. The authority to block content has negatively impacted the freedom of expression. The criteria for content blocking in this act are ambiguous, allowing the government to potentially misuse their authority, which has occurred in the past. We remain fully dedicated to upholding the dignity and accurate portrayal of our Liberation War, and based on previous attempts to distort its history, we recognize the necessity of taking action in this matter. The term “Spirit of Liberation War” is quite ambiguous. If we don’t provide a clearer definition of the “crimes” included in this section and explicitly outline what qualifies as a “crime,” there is a potential for significant misuse of this law and the harassment of journalists, with penalties reaching life imprisonment or a fine of up to Tk 30 million, or both.

The most concerning issue of this act that it grants the police authority to enter any location, examine any computer system, confiscate any computer network and its servers, conduct personal searches on individuals, and also DETAIN anyone based on suspicion. First of all the potential for arrest without an warrant had inevitably hamper reporters from performing their duty. When law enforcement gains the capability to arrest without a warrant solely on mere SUSPICION, then the freedom of the press will be stifled by this law. Among the 20 or so stipulations concerning crimes and punishment in this law, 14 are classified as cognizable and non-bailable. Considering that law enforcement can make arrests without a warrant and based solely on suspicion, this legislation poses a genuine risk to media freedom since many crimes have been categorized as cognizable and non-bailable.⁸.

⁸^ The Editors’ Council, ‘Why We Oppose Digital Security Act’ (Prothom Alo, 29 September 2018) <https://en.prothomalo.com/opinion/Why-we-oppose-Digital-Security-Act> accessed 6 July 2025.

4.2 International Conventions and Treaties Related to Cybercrime

Budapest Convention is the first International Convention upon Cybercrime. Bangladesh is not a signatory party of this convention but has shown interest to align with some of this convention's principles. Bangladesh collaborates with the UNITED NATIONS OFFICE on DRUGS and CRIME (UNODC) to develop initiatives aimed at preventing cyber threats and establishing a legal framework. Bangladesh also an active participant of International Telecommunication Union (ITU). It provides technical guidance and policy guidance for contesting cybercrimes.⁹

4.3 Role of Cybercrime units in Bangladesh

Bangladesh has now turned into Digital Bangladesh. So, for ensuring security of Digital Bangladesh. It has established various agencies focused on preventing cybercrime, including the Bangladesh Telecommunication Regulatory Commission (BTRC), Bangladesh Computer Security Incident Response Team (bdCERT), and the Counter Terrorism and Transnational Crime (CTTC) Units. It also have established different specialized cybercrime police stations, 'IT Crime Forensic Lab' to fight against cybercrime or crime related with computer and other technologies. These cybercrime units investigate offences like hacking, online scam, identity theft, monetary scams, online defamations etc. It also works on analyzing digital evidences, monitors online platforms, detects cybercrimes and activities that may create threat to national security, retrieves data, analyze cyber-attack patterns, and trace online activity. These units also cooperate with internet providers and social media platforms to remove abusive contents and provide

⁹ Law Adviser Dr Asif Nazrul, 'Govt to repeal nine controversial sections of Cyber Security Act ' Dhaka Tribune (Dhaka 6 May) accessed 3 March 2025

strategies about data protection and social media usages. It also arranges awareness program and campaign for making people aware about cyber life.¹⁰

¹⁰ United Nations, *Basic Facts About the Global Cybercrime Treaty* (UN, 2025) <https://www.un.org/en/peace-and-security/basic-facts-about-global-cybercrime-treaty> accessed 29 June 2025.

Mohammad Jamil Khan and Shariful Islam, 'New police unit to check cyber crime' *The Daily Star* (Dhaka, 7 January 2018) <https://www.thedailystar.net/frontpage/new-police-unit-check-cyber-crime-1515997> accessed 5 July 2025.

Mohammad Shahadat Hossain and Mahfuza Mallika, 'Cyber Security Governance Under the Cyber Laws of Bangladesh: An Overview' *International Journal of Research and Innovation in Social Science (IJRISS)*, vol 9(4), 2025, 3796–3811 <https://rsisinternational.org/journals/ijriss/articles/cyber-security-governance-under-the-cyber-laws-of-bangladesh-an-overview/> accessed 5 July 2025.

CHAPTER FIVE

CHALLENGES in COMBATTING CYBERCRIMES in BANGLADESH

5.1 Gaps in Legislation and Policy Implementations

Our country has entered into digital age but our laws has not entered into digital frame because most of the laws are outdated. They have no capacity to try these new crimes. Most of our laws based on traditional framework which is failing to meet new cyber threats, AI driven attacks and deep fakes. Our present legislations are not able to address emerging cyber threats such as dark web threats, crypto currency connected crimes and cloud based attacks. Lengthy legislative process also there are a lot of legal gaps for preventing cybercrime. First of all, many legal framework regarding cybercrime has been outdated. Cybercrime committing style is changing in every minutes. These laws are failing to keep pace with this firstly growing crimes. Secondly, there are lot of lacking in specifying provisions or clarifying provisions. Cyber security Act 2023 has lacking for clear definitions of terms like "threat to digital security" and "national integrity", "false information", "offensive content", "deterioration of law and order". These could lead misleading interpretation. Most unfortunately "cybercrime" definition is also vague. Thirdly, this act contains many provisions which creates treats to freedom of expression especially in online platforms and social media. Fourthly, these act provides harsh penalties, severe fines and many non-boilable offences. All these crimes leads lengthy detention without any kind of trial. Fifthly, ICT act 2006, section 57, is often uses to for oppressing journalists, bloggers, political opponents.

5.2 Lack of Technical Expertise among Law Enforcement

ICT Act 2006, did not created a legal strong legal framework for effective investigations and prosecuting cybercrime. This act does not provide strong expertise and resources for protecting cyber threat and emerging trends. These lacking making ineffective this law. This law did not provide any advanced technology and security team for combating modern cyber security challenges. Cyber security Act 2023 does not protect white hat hackers which causes discourage

¹¹in cyber security research. This act also does not provide a well formatted response protocols for cyber incidents which shows a weak security.

5.3 Issues of privacy and data protections

Bangladesh is a developing country which recently entered in digital world. So it needs a strong security for data and privacy. Unfortunately it has not a steadfast data protection law for protecting personal and sensitive data. Its existing laws such as Cyber security act 2023, ICT Act 2006 only focuses on cybercrime, frameworks etc. and does not focuses on privacy protections. The government has access to huge number of personal data of every people of the country. They collects it from various media such as, telecom operators, financial institutions, social media and monitoring media system. So, Government can easily misused these data because our law is silent about this matter. Many offices, companies, corporations collect and store a huge amount of data of our country. But our law does not provide clear and strict provision about collection, store or share these personal and sensitive data.

5.4 Social-cultural Barriers in Reporting Cybercrimes

Cybercrimes are rapidly spreading in Bangladesh. But individuals are not reporting about cyber offences. The main cause is social and cultural barrier. In Bangladesh most of the cyber victims are woman and child. Most of the time woman victims face difficulties, reputation damage when they reports about online harassment, blackmail or revenge porn. Its male dominated society

¹¹ **Mohammad Shahadat Hossain and Mahfuza Mallika**, ‘Cyber Security Governance Under the Cyber Laws of Bangladesh: An Overview’ *SecurityWorldBD* (Bangladesh, published online) <https://securityworldbd.com/details-page/156> accessed 5 July 2025.

Moriom Akter Mou, ‘The Causes and Impacts of Cybercrime in Bangladesh’ *DIU Blog* (Daffodil International University, n.d.) <https://blog.daffodilvarsity.edu.bd/the-causes-and-impacts-of-cybercrime-in-bangladesh/> accessed 5 July 2025.

Mohammad Mamunur Rashid and Sharmin Akter, ‘**Combating Cybercrime in Bangladesh: National and International Legal Frameworks**’ *Society & Change*, vol VIII, no 1, January–March 2014 (uploaded 12 Jan 2024) https://www.researchgate.net/publication/377336709_Combating_Cybercrime_in_Bangladesh_National_and_International_Legal_Frameworks accessed 5 July 2025

blames and judge the victims rather perpetrators. These judgments affects that victims personal life, affects relationships and sometimes spread defamations. For the fear of all these causes most of the victims remains silent. Sometimes family discourage victims to raise voice against this crime for protecting so called “family honor”. Some people thinks if they report these crimes it will causes life threat for this they also fear for reporting cybercrime.

5.5 Inadequate awareness and Digital Literacy

Most of people of Bangladesh are not educated. They does not know how to use digital devices and not aware of security about these devices. Most of the people do not know about safe online practice. Most of the people uses online banking and e-commers platforms. In rural areas most of the people share their banking account password and for this they faces financial loss. Again online betting sights providing phishing links, lucrative advertise and people without knowing enter those sites and faces financial frauds, data breaches and privacy protections. All these happens because of digital literacy and awareness.¹²

¹² ‘Causes of Crimes in Bangladesh’ *Lawyers & Jurists* (online)
<https://www.lawyersnjurists.com/article/causes-of-crimes-in-bangladesh/> accessed 5 July 2025.

Ahmet Nuredini, *Challenges in Combating the Cyber Crime* (*Mediterranean Journal of Social Sciences*, Vol 5 No 19, 8 September 2014) DOI:10.5901/mjss.2014.v5n19p592
https://www.researchgate.net/publication/274129560_Challenges_in_combating_the_cyber_crime accessed 5 July 2025.

CHAPTER SIX

Comparative Analysis: Global Best Practices

6.1 Cybercrime Legislation in Developed Countries

Cybercrimes is a serious problem which has been begun to spread after 2000. Now it has converted anxiety for all stages of individuals. Almost 156 countries of the world has enacted cyber law. These laws and patterns of crimes and punishment varies by regions by regions and country to country. The highest cybercrime legislation adaptation rate is in Europe which is 91% and the lowest is in Africa which is almost 72%. Almost all the developed countries has adopted cybercrime legislation. These legislation emphases in pornography, child pornography, data breaches, cyber stalking, online fraud, unauthorized access, illegal activity in computer system or criminalizing acts. Almost all developed countries has enacted a cybercrime legislation which is align with Budapest Convention.

6.2 Analysis of Regional Initiatives in South Asia

Bangladesh is a south Asian country. Most of the south Asian country has faced challenges to protect rising cyber threats, digital transformation and increasing dependence on digital technology. Many initiatives and collaboration has been established to increase cyber security. Among them SAARC Cyber Security Initiatives are remarkable. The South Asian Association for Regional Cooperation has established the necessity of cyber security and has taken steps to prevent cybercrimes and enhance regional ¹³cooperation. SAARC Cyber security Action Plan mainly

¹³ International Telecommunication Union, *Asia-Pacific Good Practices in National Cybersecurity* (ITU-D ICT Applications & Cybersecurity, 2014) https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Asia_Pacific_Good_Practices.pdf accessed 5 July 2025.

focuses on information sharing,¹⁴ capacity building and cooperation against cyber threats among the south Asia region. It encourages its members to share best practice and cyber studies on cyber security and cyber security policies. It encourages its member states to adopt solid data protection laws and helps to align the laws to maintain international standards. Under this plan SAARC is also establishing a regional format for cooperation on cybercrime investigations. For improving South Asia's technical expertise it is setting up Cyber security Training centers. BIMESTEC cyber security cooperation also developing a common structure between its member countries for a common cyber security. It is enhancing a strong legal structure against cybercrime. SAARC has made CERT-to-CERT collaboration between its member states. It plays an important role for preventing and protecting national and regional infrastructure in south Asia. It also helps for drafting and formatting cyber security policies and framework. Two South Asian country Bhutan and Nepal have been benefited from this program.

6.3 The Role of International Cooperation in Tackling Cybercrimes

International telecommunication Union: It is one of the old days nationwide Global Association in the world which was structured in 1865. It has 153. Member whose primary goal is to enable International connectivity by communication networks. It plays a important role in Cyber relates issues and also in cyber security issues. It launched the ITU Global Cyber security Agenda in 2007. Developing solutions for adequate cybercrime legislation and establishing institutional and human ability to prevent cybercrimes are among its seven main objectives. It has established a high-level specialists group made up of professionals from its member groups to enhance global security.

Interpol: A professional association for international police collaboration and crime prevention is the International Criminal Police Organization. Founded in 1923, it currently consists of 194 member nations. Cybercrime is one of the branch of crime where Interpol focuses. To facilitate police action it cooperate between its member states and share data, crime pattern, threats and

¹⁴ International Criminal Police Organization (INTERPOL), *Cybercrime* (INTERPOL, online) <https://www.interpol.int/en/Crimes/Cybercrime> accessed 5 July 2025.

trends. To develop prevention and disruption strategies, data generated is used to assist the member's states. It has also created two secure platform to facilities cyber related crimes.

United Nations (UN): The most powerful organizations in today's world which was established in 1945 and it has 193 members. The aims of this organization is to maintain peace of the world but it also actively involved in preventing cybercrime. Its worldwide initiative UNODC offers technical support for international collaboration among developing nations, capacity building, and preventive and awareness-raising. For controlling cybercrimes worldwide this program acts like repository.¹⁵

¹⁵ International Telecommunication Union, *United Nations Convention against Cybercrime* (UNODC, online) <https://www.unodc.org/unodc/en/cybercrime/convention/home.html> accessed 5 July 2025.

CHAPTER SEVEN

CONCLUSION

7.1 Discoveries

After these investigations, the following problems have been recognized:

- Cybercrime is the most alarming issues in Bangladesh and behind this problem unawareness of people, technical knowledge, and availability of internet is a cause of concern.
- There is no age barrier for using internet.
- Bangladesh has different provisions and acts regarding cybercrime and cybersecurity but not enough for cybercriminals and protect digital Bangladesh.
- Availability of internet and unsafe use of computers and mobile phones misguiding our society.
- There are not enough digital lab in our country.
- Lack of knowledge about the use of digital devises and networks.
- Unemployment and poverty.
- Availability of computer, smart phones and networks.
- Most of the women are victim of cybercrime
- People share their personal life and sensitive information through social media without security.
- People does not want to complain in police because of their dignity.
- Lack of social, moral, technical education cybercrime is increasing.
- It is changing crime types
- Affecting social-moral conditions.

7.2 Recommendations

In this paper some issues has been identified. These issues can be solved by taking and approving some actions.

- People need to aware about cyber life.
- Every people need to know about the security and using procedure of internet.

- Digital awareness program need to raise among people.
- Cyber security act need to improve
- Vague provisions need to clarify properly.
- Forensic investigation capacity need to develop.
- Need to establish special cyber security courts.
- Need to prepare expert police, judges and prosecutor for handling cyber cases.
- Develop the security of financial sector.
- Enforce strict policies about fake account, fraud, digital scam, defamation etc.
- Increase digital lab facilities.
- White hat hackers need to raise.
- Increase the international collaborations and adopt digital technologies.
- Need strong and authentication system for online transaction.
- Age limits need to specify for using different websites and internet.
- Special corner need to establish for cybercrime victims.
- Cybercrime cases need to finish quickly.
- Cyber security education should be introduced in every school, college and university.
- Encourage people to report for any kind of cybercrime.
- National cyber incident response plan need to develop.
- All users must maintain the most recent security fixes installed on their operating systems, browsers, and software.
- To restrict the visibility of personal information, people should review and modify their privacy settings on social media.
- We should regularly back up our important data and store it securely.
- Adopt international cooperation to share intelligence and collaborate on combating cybercrime.
- Ability to handle cybercrime cases need to improve.
- Government need to establish clear channels for reporting cybercrimes and ensure prompt and effective responses.

Almost all the adult people of our country uses digital devises, banking system and internet. When using these, we need to aware about the security of this devices. We need to keep our personal life private. We should not share such kind of information, pictures, videos in online platforms which can be used against us or anyone can blackmail us using these information.

REFERENCE

PRIMARY SOURCES

LEGAL INSTRUMENT

1. Penal code 1860
2. Information and Communication Act 2006
3. Digital security act ,2018
4. Cyber security act 2023
5. Bangladesh Telecommunication Regulation Act 2001
6. The Information Security Guidelines 2014
7. The pornography control act 2012
8. UN

SECONDARY SOURCES

JOURNAL ARTICLES

1. MBossler Adam and Tamar Berenblum, 'Introduction: new directions in cybercrime research' [2019] 42(5) Journal of crime and justice 495-499
2. Rajia Sultana, 'Cyber crime in Bangladesh: need for unique cyber law' [2024] 10(5) International Journal of Law 31-33
3. Mohammad Manunur roshid and Sharmin Akhter, 'Combating Cybercrime in Bangladesh: National and International Legal Frameworks' [2014] VIII (1) Society & Change
4. Md Aktarul alam chowdhury and Md Hasnath kabir fahim, 'An Insight Into The Cybercrimes And Cyber Security Measures In Bangladesh Quest For Operative Legal Remedies' [2020] 63(6) Solid State Technology
5. Brigadier General md khurshid alam and Md Hasnath kabir fahim, 'CYBERCRIME IN BANGLADESH: IMPLICATIONS AND RESPONSE STRATEGIES' [2011] 10(2) NDC Journal 20-35
6. Kudrat-E-Khuda Babu and MdAbu Bakar siddik, 'Cybercrime in the social media of Bangladesh: an analysis of existing legal framework' [2022] 14(1) Int J Electronic and Digital Forensics
7. Regner Sabillon and JeimyJ Cano m, 'Cybercrime and Cybercriminals : A Comprehensive Study' [2016] 4(6) International Journal of Computer Networks and Communications Security 165-176
8. Nuredini A, *Challenges in Combating the Cyber Crime (Mediterranean Journal of Social Sciences* Vol 5 No 19, 8 September 2014) DOI:10.5901/mjss.2014.v5n19p592 https://www.researchgate.net/publication/274129560_Challenges_in_combating_the_cyber_crime accessed 5 July 2025.
9. Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies*, 17(2), 220- 239. doi:10.14254/2071-8330.2024/17-2/12
10. Ehsan, Shamsad Binte and Md Najmus Saquib, 'Balancing Cybersecurity And Individual Rights: A Critical Analysis of Bangladesh's Cyber Security Act 2023' (2024) *Journal of Creative Writing* 8(1) (28 June 2024) <https://doi.org/10.70771/jocw.v8i1.109> accessed 29 June, 2025.

NEWSPAPER ARTICLES

1. Tribune Desk‘ Study: Hacking Social Media Accounts Most Prevalent Cybercrime in Bangladesh’ Dhaka Tribune (Dhaka, 29 June 2024) <https://www.dhakatribune.com/bangladesh/crime/350507/cyber-crime-study-social-media-hacking-most> accessed 10 January 2025

2. Star Business Report, 'Social media Hackings Tops Cybercrimes in Bangladesh Study' (The Daily Star,29 June 2024) <https://www.thedailystar.net/business/news/social-media-hacking-tops-cybercrimes-bangladesh-study-3644646> accessed 12 May 2025
3. Shrabani Paul,'Bangladesh is at serious Risk of Cyber Crimes' Dhaka Tribune (Dhaka,19 September 2022)<https://www.dhakatribune.com/openion/oped/294341/bangladesh-is-at-serious-risk-of-cyber-crimes> accessed 10 January 2025
4. Naznin Akhter,'Victimes of cyber violence: Women "easy targets" in cyberspace too' (Prothom Alo, 29 January 2025) accessed 1 February 2025
5. Zarif Faiyaz, 'Cyber Security Ordinance 2024: Progress or Oitfall? (The Daily Star,Dhaka, 26 December 2024) <https://www.thedailystar.net/tech-startup/news/cyber-security-ordinance-2024-progress-or-pitfall-3785116> accessed 27 February 2025
6. Nazrul, Asif, 'Govt to repeal nine controversial sections of Cyber Security Act ; (2025) Dhaka Tribune (Dhaka, 6 May 2025)
7. <https://www.dhakatribune.com/bangladesh/government-affairs/380517/adviser-amended-cybersecurity-ordinance> accessed 2March 2025
8. **The Editors' Council**, *Why We Oppose Digital Security Act* (Prothom Alo, 29 September 2018) <https://en.prothomalo.com/opinion/Why-we-oppose-Digital-Security-Act> accessed 6 July 2025.

Websites

1. Council of Europe, 'Bangladesh(Octopus Cybercrime Community) <https://www.int/en/web/octopus/bangladesh> accessed 16 may 2025
2. Roy & Associates, 'Cybercrimes and Cyberlaw in Bangladesh'(Roy and Associates, 1 May2021) <https://royandassociates.com.bd/cyber-crimes-and-cyber-laws-in-bangladesh> accessed 24 January 2025
3. Nafisa Naznin Lutfa, 'Cybercrime in Bangladesh' (Academia.edu.2018) https://www.academia.edu/36302577/Cyber_crime_in_bangladesh accessed 15 May 2025
4. Kazi Takbir Hossain and Sabbir Ahmed, 'Cyber Crime in Bangladesh' (SlideShare,26 August 2022) accessed 11 January 2025
5. Independent University, Bangladesh, 'Obydullah Al Marjuk Unreveils Key Cybercrime Study Report'(4 july,2024) accessed 15 January 2025
6. The Financial Express, ' Bangladesh Sees rise in cybercrime cases,but suspects are mostly acquitted' (6 September 2021) accessed 2 February 2025
7. The Lawyears & Jurists,'Cyber Crimes in Bangladesh' (The Lawyer & Jurists) accessed 3February 2025
8. International Criminal Police Organization (INTERPOL), *Cybercrime* (INTERPOL, online) <https://www.interpol.int/en/Crimes/Cybercrime> accessed 5 July 2025.

Books

- Dr Gazi & Associates ,Legal Frameworks Needed to Stop Cybercrimes in Bangladesh,(2025)
- Kazi Takbir Hossain and Sabbir Ahmed,Cyber Crime in Bangladesh (Green University of Bangladesh 2022)
- Jonathan Clough, Principles of Cybercrimes (2nd edn, Cambridge University Press 2015)

Bibliography

- 1.The Daily Star, 'Free Speech vs Section 57' (The Daily Star, 22August 2015) <https://www.thedailystar.net/frontpage/news/free-speech-vs-section-57-130591> accessed 29 June 29, 2025
- 2.United Nations, *Basic Facts About the Global Cybercrime Treaty* (UN, 2025) <https://www.un.org/en/peace-and-security/basic-facts-about-global-cybercrime-treaty> accessed 29 June 2025.

3. United Nations Office on Drugs and Crime, *United Nations Convention against Cybercrime* (UNODC) <https://www.unodc.org/unodc/en/cybercrime/convention/home.html> accessed 29 June 2025.
4. Council of Europe, *Convention on Cybercrime (Budapest Convention, CETS No 185)* (CETS No 185, opened for signature 23 November 2001) <https://www.coe.int/en/web/cybercrime/the-budapest-convention> accessed 29 June 2025.
5. United Nations Information Service Vienna (UNIS Vienna) <https://unis.unvienna.org/unis/index.html> accessed 29 June 2025
6. 'Causes of Crimes in Bangladesh' *Lawyers & Jurists* (online) <https://www.lawyersjurists.com/article/causes-of-crimes-in-bangladesh/> accessed 5 July 2025.
7. Rashid MM and Akter S, '**Combating Cybercrime in Bangladesh: National and International Legal Frameworks**' (2024) *Society & Change* vol VIII(1) https://www.researchgate.net/publication/377336709_Combating_Cybercrime_in_Bangladesh_National_and_International_Legal_Frameworks accessed 5 July 2025.
8. International Telecommunication Union, *Asia-Pacific Good Practices in National Cybersecurity* (ITU-D ICT Applications & Cybersecurity, 2014) https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Asia_Pacific_Good_Practices.pdf accessed 5 July 2025.