CYBERCRIMES IN BANGLADESH:

CAUSES, EFFECTS, AND PREVENTION MECHANISMS

INSCRIBERSHIP PROGRAMME 2023-2024

MEDIA, LAW, AND DIGITAL SPACE COHORT

Map of Justice

A PATH TOWARDS A JUST SOCIETY

CYBERCRIMES IN BANGLADESH: CAUSES, EFFECTS, AND PREVENTION MECHANISMS

Published on
October 2024

Published by
Map of Justice
Mobile: +88 0174 329 9007
Email: mapofjustice@gmail.com
Web: www.mapofjustice.org

About Media, Law, and Digital Space Cohort of *Inscribership Programme 2023-24*

The Media, Law, and Digital Space Cohort is part of a six months Inscribership Programme aimed at conducting research and advocacy in order to address the moral and legal challenges that underpin the creation and use of media in the digital age. It carries out activities to raise awareness in the relevant areas. The Programme ran from 10 September 2023 to 10 March 2024. The cohort consists of one Inscriber and four Programme Assistants.

As part of the activities of the Programme, the Inscriber organised three online workshops with School, College and University students across Bangladesh and collected primary data. In addition, the inscriber conducted interviews with relevant stakeholders and experts in the field of cybercrime.

Principal Researcher

Gazi Mahfuz Ul Kabir, Inscriber, Media, Law, and Digital Space Cohort – Inscribership Programme, Map of Justice.

Mr. Kabir has been actively engaged in the fields of digital forensics and cyber security for more than a decade. Currently, he is working as a Deputy Manager, Safeguarding and Grievance Management Committee, BRAC.

Programme Assistants

- Mohsina Mahin, LLB, East West University
- Md Ilyash Islam Sakil, LLB, East West University
- Nowshin Jannat Nusaiba, LLB, East West University
- Fariha Tasnim, LLB, Jagannath University

Editors

Shahriar Yeasin Khan, Barrister-at-Law (Lincoln's Inn), Executive Editor, Map of Justice

Tohinur Islam, Executive Director and Co-Founder, Map of Justice

Maimuna Syed Ahmed, Lecturer, Independent University, Bangladesh, Co-founder, Map of Justice

Programme Director

Tohinur Islam, Executive Director and Co-Founder, Map of Justice

TABLE OF CONTENTS

EXECUTIVE SUMMARY V

KEY RECOMMENDATIONS VI

1. INTRODUCTION 1

1.1 Cybercrime: An Overview 1

1.2 Objective 6

1.3 Methodology and Scope: 6

2. ONGOING PROLIFERATION OF CYBERCRIME IN BANGLADESH 8

2.1 Women are the Primary Victim of Cyber Harassment 9

2.2 Revenge Pornography – A Burning Issue 11

2.3 Cybercrime and AI – A Rising Concern for Bangladesh 12

3. CYBERCRIME IN BANGLADESH: 14

3.1 Causes of Cybercrime in Bangladesh 14

3.1.1 Interview Findings 14

3.1.2 Focused Group Discussion (FGD) Findings: 15

3.2 Statistical Analysis and Expert Opinions on Cybercrime in Bangladesh 16

3.2.1 Demographics of Victims of Cybercrimes 17

3.2.2 Demographics of Perpetrators of Cybercrimes: 18

3.2.3 Nature & Frequency of Complaints 18

3.2.4 Complaints Disposal and Rate of Conviction: 19

3.3 Effects of Cybercrimes in Bangladesh: 20

3.4 Gaps in the Existing Legal Framework: 21

4. FINDINGS 24

4.1 Contextual Analysis on Cyber Offences 24

4.2 Empirical Analysis on Students in Bangladesh: 25

5. PREVENTING CYBERCRIME: RECCOMENDATIONS AND WAY FORWARD 29

6. CONCLUSION 32

EXECUTIVE SUMMARY

Cybercrime is an act of criminal offence that either targets or uses a computer, a computer network, or a networked device against its victims. The key difference between cybercrimes and conventional crimes is the presence, or absence of the perpetrator in the physical space where such a crime has been committed. In Bangladesh, there are several different types of cybercrimes that takes place across the country. The most common ones are cyber-sexual harassment; revenge pornography; financial crime and online blackmail; online child sexual exploitation; social media hacking and data breach; and last, and perhaps the most dangerous in the current global context, cybercrime with AI, whereby cybercriminals are nowadays able to perpetrate scams, distribute malware, make deepfake videos and voice cloning all with very limited effort and in extremely short time periods.

Given the variety, vastness, and various advancements in technology of the issue at concern, this study has been adopted with the primary purpose of thoroughly examining the state of cybercrime in Bangladesh, reflecting on its prevalence and underlying causes, with a particular emphasis on the vulnerabilities and experiences of students in the country.

The key findings of this study are as follows:

a) Lack of awareness and understanding about the preventive measures in the event of suffering from an attack;
b) Lack of reported instances of cyber offences resulting in the 'hidden/unreported' offenders to not be left unaccountable;
c) Lack of institutional capacity to investigate and prosecute cybercrimes
d) Development in the psychology of cybercriminals resulting in them to repeat and reproduce the offences to 'find joy';
e) Lack of accurate and up-to-date data in the public domain with regards to the cases of cybercrime cases, and/or these data are not accessible.

Cybercrime enabling factors and challenges:

a) Use of pirated software;
b) Negligent, improper, and/or illegal use of websites and social media platforms;
c) Lack of skilled/trained professionals in cybercrime analysis and investigation;
d) Weak, inadequate, and inefficient laws on preventive measures;
e) Lack of proper technical infrastructure to support implementation of existing laws;
f) Weak family and social bonding.

KEY RECOMMENDATIONS

The key recommendations from this study are as follows:

- Develop a clear strategy for cybersecurity; outline government agencies', private sectors' and citizens' objectives, roles, and responsibilities. Additionally, establish an agency or task force that will coordinate and implement this strategy effectively.
- Raise awareness through campaigns on cyber safety practices, educate people on recognising different cyber-attacks, the importance of securing data and the significance of reporting cyber incidents. Incorporating cybersecurity education in school curriculums from an early age is imperative.
- Ensure adequate allocation of budget and resources towards cybersecurity infrastructure, law enforcement capabilities, and judicial processes to combat cybercrime.
- Enhance training programs for law enforcement personnel in cybercrime detection, investigation techniques, and digital forensics.
- Simplify procedures and streamline the legal and procedural frameworks involved in reporting, investigating, and prosecuting cybercrimes to ensure prompt and efficient actions.
- Policy and legislative reform: re-evaluate and modernise existing policies and legislation adhering to best practice principles related to cybercrime and digital security.
- Collaboration with the private sector: encourage and promote collaborations between government entities, technology companies, telecommunications providers, etc., to share intelligence reports on cyber threats; strengthen national resilience against cyber-attacks.
- Foster international cooperation: engage in collaborations, treaties, or agreements aimed at combating cybercrime by facilitating border investigations and promoting information sharing.

By following these recommendations, Bangladesh would be able to significantly improve its ability to combat and prevent cybercrimes and protect its people, businesses, and address pertinent and longstanding civil-society and national security concerns.

1. INTRODUCTION

1.1 Cybercrime: An Overview

Cybercrime essentially is a crime which is committed using digital networks, and it is committed within the confines of the digital sphere, but its effects permeate beyond into the physical world.

Cybercrime lacks a legal definition in Bangladesh. Different countries, organisations and agencies have come with various definitions including:

- UK Crown Prosecution Service: "Cybercrime is an umbrella term used to describe two closely linked, but distinct ranges of criminal activity. The Government's National Cyber Security Strategy defines these as:

  > (a) Cyber-dependent crimes - crimes that can be committed only using Information and Communications Technology ('ICT') devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g., developing, and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity).
  >
  > (b) Cyber-enabled crimes - traditional crimes which can be increased in scale or reach using computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft)."[1]

- The Council of Europe Convention on Cybercrime defines it as a broad category of hostile acts, such as unauthorised data interception, system interferences that jeopardise network integrity, availability violations, and copyright infringements.[2]
- European Commission (EC): "Cybercrime consists of criminal acts committed online by using electronic communications networks and information systems."[3]
- United Nation Office on Drug Crimes (UNODC): "Cybercrime is an act that violates the law, which is perpetrated using information and communication technology (ICT) to either target networks, systems, data, websites and/or technology or facilitate a crime."[4]
- Royal Canadian Mounted Police: Cybercrime is "any crime where a cyber element (that is, the internet and information technologies such as computers, tablets or smart phones) has a substantial role in the commission of a criminal offence."[5]

[1] UK Crown Prosecution Service, 'Cybercrime - prosecution guidance' (London, 01 May 2018) <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance> accessed 1 June 2024.

[2] Committee of Ministers of the Council of Europe, 'Explanatory report to the Convention on Cybercrime' <http://www.oas.org/juridico/english/cyb_pry_explanatory.pdf> accessed 1 June 2024.

[3] European Commission, 'Cybercrime' <https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en> accessed 1 June 2024.

[4] UN Office on Drugs and Crime, 'Cybercrime in brief' <https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-in-brief.html> accessed 1 June 2024.

[5] Royal Canadian Mounted Police, <https://www.rcmp-grc.gc.ca/en/cybercrime-defined> accessed 1 June 2024.

- Cisco: “Cybercrime is illegal activity involving computers, the internet, or network devices.”[6]
- Kaspersky: “Cybercrime is [a] criminal activity that either targets or uses a computer, a computer network or a networked device.”[7]

Cybercrime encompasses a wide range of criminal activities which are constantly evolving and taking new forms. [8] The majority of these crimes fall into one of two distinct categories:

(i) cyber-dependent crimes, which can only be committed with the use of a computer/phone, computer/phone networks, or other information and communication technologies;

(ii) cyber-enabled crimes, which are the digital versions of traditional crimes made possible using computers/phones, computer/phone networks, or even artificial intelligence.

Conventional crimes targets individuals or physical assets in a manner very different from cybercrimes which, in the current digital age, has expanded the scope for criminals to target specific individuals as well as physical assets with simply a few clicks in the digital space.

As is the case with most gendered crimes across the world, women and girls suffer the most due to the inherent vulnerabilities that they are subjected to, given the society they live in, and the existing gender relations in physical and digital spaces. The motivation for committing such cybercrimes in most cases revolve around financial gains.[9] However, occasionally cybercrime aims to damage computers or networks for reasons other than monetary profit. These could be political or personal.[10]

This report focuses on the following six forms of cybercrimes that are, at present, the most committed cybercrimes in Bangladesh.[11]

[6] Cisco, ‘Cybercrime: What is cybercrime?’ <https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybercrime.html> accessed 1 June 2024.

[7] Kaspersky, ‘What is cybercrime? How to protect yourself’ <https://www.kaspersky.com/resource-center/threats/what-is-cybercrime> accessed 1 June 2024.

[8] Blessing Guembe, Ambrose Azeta, Sanjay Misra, Victor Chukwudi Osamor, Luis Fernandez-Sanz and Vera Pospelova ‘The Emerging Threat of Ai-driven Cyber Attacks: A Review’ (2022) 36(1) Applied Artificial Intelligence <https://www.tandfonline.com/doi/full/10.1080/08839514.2022.2037254> accessed 1 June 2024.

[9] Regner Sabillon, Jeimy J Cano, Jordi Serra-Ruiz, and Víctor Cavaller, ‘Cybercrime and Cybercriminals: A Comprehensive Study’ (2016) 4 International Journal of Computer Networks and Communications Security 165 <https://www.researchgate.net/publication/304822458_Cybercrime_and_Cybercriminals_A_Comprehensive_Study> accessed 1 June 2024.

[10] ibid.

[11] Staff Reporter, 'নিজের অজান্তেই সাইবার হয়রানির শিকার হচ্ছে গ্রামীণ নারীরা' *Samakal* (Dhaka, 14 October 2023) <https://samakal.com/bangladesh/article/201713> accessed 1 June 2024.

I. Social Media Hacking and Data Breach

Hacking entails obtaining unauthorised access to a website's web server, database, files, or other interfaces. The main methods used to hack a website are SQL injection, XSS attacks, DNS spoofing, phishing attacks, social engineering tools, brute-force attacks, and vulnerability discovery. It is now a worldwide phenomenon for all kinds of people.

In recent times, social media is one of the most popular platforms for communication and connection, as well as, at high risk of being targeted by cyber criminals. Cybercriminals use various social media platforms for hacking and data breaches. In Bangladesh, personal data breach rating is higher than website or server leaks.[12]

II. Cyber Sexual Harassment

Online or cyber sexual harassment encompasses a wide range of behaviours that use digital content (images, videos, posts, messages, pages) on a variety of different platforms be it private or public. It can make a person feel threatened, exploited, coerced, humiliated, upset, sexualised, or discriminated.[13] This report specifically focuses on peer-to-peer online sexual harassment taking place between or committed against youths. Individuals who perpetrate such conduct regularly use methods such as publicly humiliating their targets, intimidating them, and issuing threats to exercise control over them. Some examples of cyber harassment that are frequently encountered include:

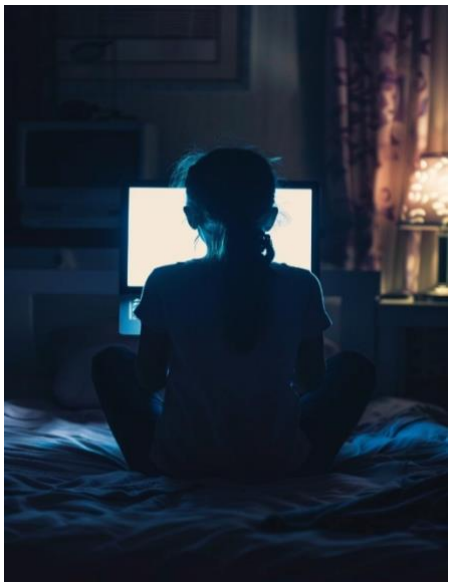
- Uploading private or embarrassing photos of someone;
- Threatening someone through abusive messages or comments of a sexual nature on social media platforms such as Facebook, Instagram, Snapchat, IMO and so on;
- Forcing or threatening someone to share sexual images of themselves on social media;
- Sending or posting rumours about someone to damage his/her reputation or image;
- Threats of publishing sexual images or videos to sextort someone;[14] and

[12] TBS Report, 'Over 5 crore Bangladeshi citizens' personal data 'exposed' online' *The Business Standard* (Dhaka, 8 July 2023) <https://www.tbsnews.net/bangladesh/millions-bangladeshi-citizens-data-exposed-online-661958> accessed 1 June 2024.

[13] Dustin Albert and Laurence Steinberg 'Judgment and decision making in adolescence' (2011) 21(1) Journal of Research on Adolescence 211 <https://doi.org/10.1111/j.1532-7795.2010.00724.x> accessed 1 June 2024.

[14] Emon Rahman, 'ফেসবুকে সুন্দরী তরুণীদের বন্ধুত্বের ফাঁদে সর্বস্বান্ত' *Jugantor* (21 January 2024) <https://www.jugantor.com/national/765656/ফেসবুকে-সুন্দরী-তরুণীদের-বন্ধুত্বের-ফাঁদে-সর্বস্বান্ত> accessed 1 June

- Sextortion, which is the act of forcing someone to do something, particularly to engage in sexual activity, by threatening to disclose the nude photos or other explicit material about them.[15]



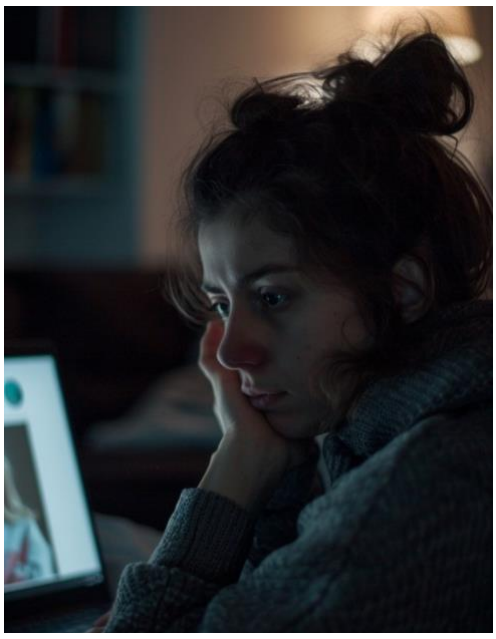
III. Online Child Sexual Exploitation

Online child sexual exploitation includes a wide range of behaviours and situations. Most commonly this includes grooming, live streaming, consuming child sexual abuse material, coercing, and blackmailing children for sexual purposes. This could include an adult engaging a child in a chat about sexual acts, asking a child to abuse material, coercing, and blackmailing children for sexual purposes.

Cyber criminals use various social media platforms to manipulate children. This could include an adult engaging a child in a chat about sexual acts, asking a child to perform sexual acts, to expose themselves or share a sexual image, taking or making and sharing or showing indecent images of children, etc.[16]

IV. Revenge Pornography

Revenge pornography or commonly known as revenge porn, which is non-consensual dissemination of sexually explicit material targeting the sexual integrity of the victims by sharing the sexually explicit media of the victim online, and therefore seriously damaging both the sexual integrity and identity of the victim.[17] It has become a relatively new cyber offence. Releasing intimate images without consent that expose someone's privacy is a breach of the law and should be prosecuted. They demand large financial expenses, create significant mental and social damage, and increase the possibility of physical violence.



2024; Zoom Bangla Desk, 'ফেসবুকে সুন্দরী তরুণীদের বন্ধুত্বের ফাঁদে সর্বস্বান্ত' *Zoom Bangla* (21 January 2024) <https://inews.zoombangla.com/beautiful-young-women-are-all-in-the-trap-of-friendship-on-facebook/> accessed 28 September 2024.

[15] Cambridge Dictionary, 'Sextortion' <https://dictionary.cambridge.org/dictionary/english/sextortion> accessed 1 June 2024.

[16] Australian Centre To Counter Child Exploitation (ACCCE) 'What is online child sexual exploitation?' <https://www.accce.gov.au/sites/default/files/2021-06/Factsheet%20-%20What%20is%20online%20child%20sexual%20exploitation%3F.pdf> accessed 1 June 2024.

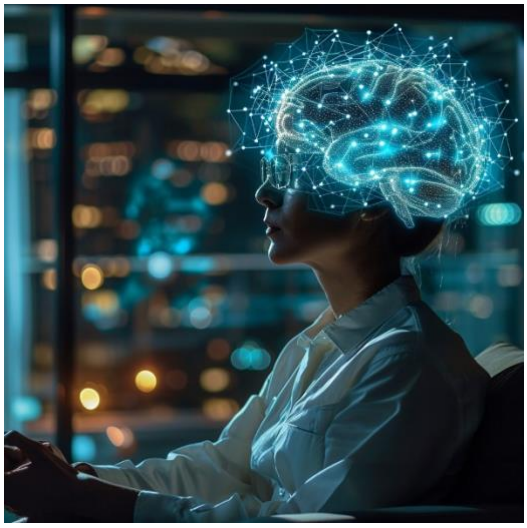
[17] EIGE, 'Cyber violence against women and girls' (*European Institute for Gender Equality*, 23 June 2017) <https://eige.europa.eu/publications-resources/publications/cyber-violence-against-women-and-girls> accessed 1 June 2024.

V. Financial Crime and Online Blackmail

The term "financial crime" is broad concept, but this study concentrates on one aspect of it where cybercriminals financially gain by blackmailing and threatening the victim by saying they will reveal any private pictures, videos, or sexual content of the victim in the public platform and pressurises the victim to give money.[18] In a survey of 'Stop Online Violence Against Women: Challenges and Way Forward' by Action Aid, 2.62% said their pictures of intimate moments were posted secretly, and they were later blackmailed for money with a threat to release their personal information.[19] 228 out of 359 women, or 63.51% of them, experienced online violence. This indicates that 64 Bangladeshi women out of every 100 who regularly engage in social media platforms must deal with online harassment and violence in one way or another. Compared to the prevalence rate of 50.19% from the previous year, this represents an increase according to a poll carried out in November 2021.[20]

VI. Cybercrime with AI

The emergence of new technology is shaping the world rapidly. With the rise of artificial intelligence (AI), cybercrime with AI is also rising as it provides tools to help cybercriminals gain access to breach computer networks by sending emails that entice recipients to divulge personal information or by creating fake photos or videos that are used to threaten victims.[21] Various AI-generated tools in Telegram are being used to create deep fake videos and obscene images and then such images or videos are being spread on social media. Recently, a female content creator – Noureen Afrose who lives in Chittagong, Bangladesh became a victim of cyber harassment by an AI dress remover bot. By using her photo, a fake nude video was created for malicious purposes.[22] Cybercrime with AI is a threat to an individual's right to privacy and consent. Using



[18] Nurul Amin, 'সাইবার জগতে নতুন নতুন ফাঁদ' *Prothom Alo* (Dhaka, 8 May 2023) <https://www.prothomalo.com/bangladesh/crime/ru0cynodo1> accessed 1 June 2024.

[19] Action Aid, 'Stop Online Violence Against Women: Challenges and Way Forward' (*Action Aid*, 29 November 2022) <https://actionaidbd.org/post/publications/research-findings-online-violence-against-women> accessed 1 June 2024.

[20] ibid.

[21] Vincenzo Ciancaglini, Craig Gibson and David Sancho, *Malicious Uses and Abuses of Artificial Intelligence* (Trend Micro Research 2020) <https://unicri.it/sites/default/files/2020-11/AI%20MLC.pdf> accessed 1 June 2024.

[22] RTV News, 'নওরীনের 'ডিপ ফেক' ভিডিও বানিয়ে অর্থ দাবি!' RTV News (9 August 2023) https://www.rtvonline.com/social-media/234961/> accessed 1 June 2024.

photo-shopped photographs/videos to harass someone grew from 5.85% to 6.93% from 2021 to 2022.[23] Recently, scammers stole over $25 million from a multinational commercial enterprise. In this scam, the scammers used deepfake technology to convince an employee in the firm's accounts-payable department that the worker had properly validated a payment request previously sent to him via email. The request in question was to issue a $25 million USD payment. To ensure the legitimacy of the request, the employee requested for a video conference, which was arranged accordingly. Later it was revealed that everyone in the video call was fake.[24]

1.2 Objective

This study has collected and organised valuable and relevant data on cybersecurity in the context of Bangladesh. Additionally, the research has also analysed the cybersecurity measures that has been implemented so far in Bangladesh. The collected data in this report includes perspectives and real-life experiences, which will be valuable for academics and legal professionals engaged in research and advocating for legal measures related to cyber harassment and data security.

This study encompasses several objectives as follows –

1. To gather a substantial amount of data using various qualitative research methods, like workshops and interviews;
2. To bridge the knowledge gap between key stakeholders in a country where awareness about the impact of cyber harassment and data security concerning technological advancements is currently lacking;
3. To explore the outcomes, underlying factors, and criminal behaviours exhibited by individuals engaged in cyber activities;
4. To find resolutions for the challenges posed by cyberspace. It will concurrently analyse the existing laws and policies concerning cybercrime and data protection to identify any weaknesses or gaps that need to be addressed; and
5. To go beyond evidence and provide a foundation for future research and policy development in this arena of studies.

1.3 Methodology and Scope:

This study thoroughly examined the state of cybercrime in Bangladesh as well as its prevalence and underlying causes, with a particular emphasis on the vulnerabilities and experiences of school and college students. To provide a solid contextual foundation for the study, the paper follows the qualitative analysis approach.

---

[23] CCAF, 'গবেষণা প্রতিবেদন: বাংলাদেশে সাইবার অপরাধ প্রবণতা-২০২২' (*CCABD*, 13 August 2022) <https://ccabd.org/বাংলাদেশে-সাইবার-অপরাধ-2/> accessed 3 September 2024; TBS Report, '55% cybercrime victims failed by police: Survey' *The Business Standard* (Dhaka, 13 August 2022) <https://www.tbsnews.net/bangladesh/55-cybercrime-victims-failed-police-survey-476406> accessed 1 June 2024.

[24] Joseph Steinberg, 'Scammers Steal Over $25 Million By Using AI Deepfake Video Call To Convince Suspicious Employee That A Phishing Email Is Legitimate' (*Joseph Steinberg*, 4 February 2024) <https://josephsteinberg.com/scammers-steal-over-25-million-by-using-ai-deepfake-video-call-to-convince-suspicious-employee-that-a-phishing-email-is-legitimate/> accessed 1 June 2024.

The methodology includes a thorough review of existing research works on both regional and global perspectives on cybercrime. This includes case studies, legal frameworks, and cyber security strategies.

Primary data is gathered through student surveys. They provide first-hand information about the experiences and opinions of students regarding cybercrime.

Expert opinions were also collected through interviews with law enforcement officers and cybercrime specialists and other relevant stakeholders.

Specific recommendations for cyber security awareness programs were developed through data analysis from online discussions and workshops with students across the country.

To enhance the research, a thorough analysis of recent cybercrime cases in Bangladesh has been conducted with the goal of identifying patterns, motives, and vulnerabilities.

Additionally, the study includes a thorough analysis of policy and legal mechanisms to assess the efficacy of Bangladesh's current cyber security policies, pointing out any weaknesses and making suggestions for improving the legal framework against cybercrime.

The study's scope includes a comprehensive evaluation of cybercrime looking at the numbers and growing rates of cybercrime in Bangladesh, including the specific kinds of cybercrime committed as mentioned above. The study analyses the underlying causes of the six cybercrimes by considering technological infrastructure, legal enforcement mechanisms and socioeconomic factors. Additionally, the research attempts to develop practical ideas for stopping cybercrime, with a focus on awareness-raising campaigns, educational programs, and technological solutions, particularly for vulnerable young students. The scope includes offering concrete policy suggestions to strengthen Bangladesh's cyber security laws and regulations, with an emphasis on enhancing law enforcement capacities and fostering international collaboration.

2. ONGOING PROLIFERATION OF CYBERCRIME IN BANGLADESH

Cybercrime is a relatively old problem that has gained newer grounds in modern times and has slowly but gradually seeped into the Bangladeshi society. The first cyber-attack happened in France well before the internet was even invented - in 1834, when two thieves stole financial market information by hacking the French Telegraph System.[25] In Bangladesh there is no specific date of the first recorded cybercrime but the most popular cybercrime which went viral was on 23 August 2004, when an e-mail was sent to the Bangla daily *Prothom Alo*, containing a threat to prime minister.[26] Another famous example is from 2008, when the website of the Rapid Action Battalion (RAB) was hacked. The hacker, Shahee Mirza wrote on the RAB website, 'You do not know what cyber security is or how to protect yourself.'[27]

A large proportion of the total population of Bangladesh from all strands of society are unaware of cybercrimes and cybersecurity laws. Because of their lack of knowledge of the subject, they get easily targeted by cyber criminals and as a result cybercrimes are constantly on the rise.[28] Thus, whilst cybercrimes have become a concerning global issue, Bangladesh is also not an exception in this regard. While the country is trying to move forward along with the evolving world, the development of this digital era has resulted in an increase in cybercrimes.

According to the 2024 research report by the Cybercrime Awareness Foundation (CCAF), cybercrime in Bangladesh doubled to 11.85% in one year, with most victims being women.[29] It is to be noted that CCAF works towards increasing awareness about crime, cyber security, and strengthening the nation's resilience in the event of a cyber-incident, and to engage and educate partners in the public and private sectors through events and initiatives. In Bangladesh, there were 131 million internet users as of December 2023, as per the recent released data by Bangladesh's telecom regulator.[30] With such a large userbase, new forms of cybercrime are constantly being created, changed and the rate of cybercrime is constantly on the rise. The most frequently committed cybercrime in Bangladesh is Identity Theft, Phishing,

[25] Lauren M Cherry and Peter P Pascucci, 'International Law in Cyberspace' (*American Bar Association*, 27 January 2023) <https://www.americanbar.org/groups/law_national_security/publications/aba-standing-committee-on-law-and-national-security-60-th-anniversary-an-anthology/international-law-in-cyberspace/> accessed 3 September 2024.

[26] Md. Khurshid Alam, 'Cybercrime in Bangladesh: Implications and Response Strategy' (2011) 10(2) NDC Journal 20 <https://ndcjournal.ndc.gov.bd/ndcj/index.php/ndcj/article/view/82> accessed 3 September 2024.

[27] ibid.

[28] Tariqur Rahman Khan, 'সাইবার অপরাধের ধরনে বদল, বেশি ঝুঁকিতে নারী ও শিশুরা', *Prothom Alo* (Dhaka, 20 May 2023) <https://www.prothomalo.com/technology/cyberworld/uzt8hfr86x> accessed 3 September 2024; Staff Reporter, 'সাইবার জগতে নারীর সুরক্ষা' *Shomoyer Alo* (Dhaka, 3 December 2023) <https://www.shomoyeralo.com/details.php?id=247236> accessed 3 September 2024.

[29] TBS Report, 'Cybercrime in Bangladesh doubles to 11.85% in one year, most victims women: Study' *The Business Standard* (29 June 2024) <https://www.tbsnews.net/bangladesh/crime/one-ten-cybercrime-victims-bangladesh-affected-pornography-study-887306> accessed 3 September 2024.

[30] Staff Reporter, 'Internet users in Bangladesh reach 131m as of 2023' *Dhaka Tribune* (Dhaka, 12 February 2024 <https://www.dhakatribune.com/bangladesh/339218/internet-users-in-bangladesh-reach-131m-as-of-2023> accessed 3 September 2024.

Malware, Revenge Pornography, Child Pornography, Cyber sexual harassment, Online Scams, DDOS attack, hacking etc.[31]

In Bangladesh, the cyberspace is one of the most common places where women are harassed through various cyber-attacks.[32] Not only in Bangladesh, but also most Asian women are vulnerable in cyberspace.[33]

Most of the victims are young, mostly between teens to 20s, and the larger proportion are women.

2.1 Women are the Primary Victim of Cyber Harassment

> Nila (Pseudonym), on social media, met a person residing in the Middle East. They married in private, but things did not turn out as Nila had hoped. She divorced her spouse after discovering he was having an affair. Her ex-husband then created many fake social media accounts in her name and began sharing her personal images.
>
> @Action Aid Report 2022

Notably in Bangladesh, women are the biggest victims of cyber harassment,[34] and this trend is on the rise. Until 30 June 2023, approximately 22,732 women sought assistance from the Police Cyber Support for Women (PCSW) wing, a unit which was established in 16 November 2020 dedicated towards increasing awareness of cybersecurity issues and to exclusively offer female victims of cyberspace the necessary technological and legal support. Amongst them, 90% of women did not want to take any legal action which highlighting the urgency of addressing this issue.[35]

This highlights the vulnerability of women in Bangladesh no matter where they go, what they do, and how they dress and speak.[36] Whilst there are many reasons, most of the time Bangladeshi women become victims because of sending personal photos, videos, and sensitive information through the internet.

Some examples of cyber harassment that are frequently encountered include:

- Spreading hate speech online,
- Uploading private or embarrassing photos of someone,
- Threatening someone through abusive text or comments of sexual nature on social platforms such as Facebook, Instagram, Snapchat, Imo and so on,
- Forcing or threatening someone to share sexual images of themselves on social media,

[31] Khondokar Hafijur Rahaman and Md Abul Hasam, 'A Social Review on Nature & Reason of Cyber-Crime and the Laws Regarding Prevention in Bangladesh' (2021) 5(7) International Journal of Research and Innovation in Social Science 171.

[32] BLAST, 'Cyber violence against women' (*Bangladesh Legal Aid and Services Trust*, December 2017) <https://www.blast.org.bd/content/publications/Cyber-violence.pdf> accessed 3 September 2024.

[33] Adhora Ahmed, 'A Cyberspace Unsafe for Women' *The Daily Star* (Dhaka, 8 April 2021) <https://www.thedailystar.net/shout/news/cyberspace-unsafe-women-2073937> accessed 3 September 2024.

[34] Fatima Tuz Zohra, 'হয়রানির বিষয়ে নিশ্চুপ ৮৫% নারী' *Kalerkantho* (Dhaka, 4 February 2023) <https://www.kalerkantho.com/print-edition/first-page/2023/02/04/1242733> accessed 3 September 2024.

[35] ibid.

[36] Editorial, 'Cyber violence against women' (*Bangladesh Post*, 10 May 2023) <https://bangladeshpost.net/posts/cyber-violence-against-women-111528> accessed 3 September 2024.

- Sending or posting rumours about someone to damage his/her reputation or image,
- Threat of publishing sexual images or videos (Revenge pornography).

Cyberbullying is one branch of harassment that falls under cyber-sexual harassments committed in Bangladesh. In addition to this, cyber-sexual harassments are also committed through creating fake IDs to harass others, revenge pornography, etc.

To identify the underlying causes of cyber-sexual harassments and the reasons behind its rise, we examined hacking tutorials, scripts, blogs, and other content from 2010-2024 related to Ethical Hacking on Google, YouTube, Github and TOR Network. As per our findings, until 2012-2013, the number of cyber-harassments in Bangladesh were very low because there were fewer tutorials available online at that time. Because of the lack of awareness and specialist knowledge about the topic at that time, random people could not attack anyone's personal account or data. Before 2012 ethical hacking tutorials were very few in Google or regular online surface, but in 2013 people started uploading ethical hacking tutorials, hacking script and blog articles about hacking. Thus nowadays, adults and children alike are getting interested in and learning about being a hacker from watching hacking related movies and online tutorials. Currently, various tutorials are being given on YouTube. Besides, various hacking courses are being taught in the name of certified ethical hacking courses. Furthermore, there are many movies about hacking which really makes their viewers attracted towards hacking, and many children who watch these movies become interested in hacking.[37] With regards to the incidents of cyber-harassment in Bangladesh today, it is interesting to note that many perpetrators are below 18 years of age.[38] These young people knowingly, or unknowingly are learning various tutorials from YouTube, GitHub, GitLab, Hacking forums etc, and they are unaware about the law and how to apply them.

To understand the gravity of the current situation, a representative example may be helpful. For instance, let us say a person is angry with another person and wants to hack someone's social media account or wants to spread AI-made nudity. Now, if he searches for any such content on YouTube, he can easily gather knowledge from YouTube or can take control of other's IDs by doing different types of phishing attacks like by using Kali Linux through his computer or Termux through his mobile. Nowadays phishing pages can bypass any kind of Two-step Verification (2FA) like with the script of AdvPhishing, shark phishing, BannerPhishing, etc., which cannot be detected. Besides, attackers use different link masking scripts like MaxPhisher, URL-masking, URL-mask from GitHub so that the victim cannot identify which link is real and which is not. There are already many such tutorials on online sites and on YouTube about hacking. Telegram bot is now a game changer for scammers and hackers because different types of bots are now available for phishing and scamming attacks. So, if a newcomer in the hacking world can perform his attack without Termux or Kali Linux. Different types of tutorials already exist on YouTube. The worst part is, different types of scammer groups using ethical hacking tags, and they teach people different kinds of hacking through which they can easily harm others.

[37] Nichola Daunton, '"I was a teenage hacker": Two child hackers share their stories' *Euronews* (31 May 2023) <https://www.euronews.com/next/2023/05/31/i-was-a-teenage-hacker-two-child-hackers-share-their-stories> accessed 3 September 2024.

[38] Sheikh Jahangir Alam, 'যেভাবে সাইবার অপরাধে জড়াচ্ছে শিশুরা' *Bangla Tribune* (Dhaka, 12 July 2019) <https://www.banglatribune.com/law-and-crime/505561/> accessed 3 September 2024.

Due to the availability of various tutorials on YouTube and online, it is very easy to carry out cyberattacks while properly maintaining their security. Also, in the name of teaching hacking through different apps, many people are teaching different types of banner phishing as well as different types of scamming for money. That is the reason the level of cybercrime is increasing.

2.2 Revenge Pornography – A Burning Issue

Now if a person wants to upload some kind of revenge pornography online while keeping his personal identity hidden, then he can attack his/her by hiding his online identity by watching various tutorials like IP hiding method, using TOR network, and making fake identity to publish a thing. Most of the hacking tutorials are online so people can use this in a good way or a bad way.

Revenge pornography is becoming a burning issue in Bangladesh.[39] Most of the time this crime starts with a relationship breakup, but nowadays, revenge pornography also spreads after divorce by any of the related parties. Sexual privacy violations, particularly the non-consensual release of explicit photos that betray someone's confidence, deserve to be punished criminally. They undercut the trust necessary for intimate relationships by denying people the right to choose whether and when they are sexually exposed to the public. Additionally, they cause severe emotional and societal trauma, demand high financial expenses, and raise the possibility of physical violence.[40]

> Alamgir Hossen, the accused, and the victim had a relationship, but as the accused was married, the victim broke their relationship. After their separation, the accused used to disturb the victim and to stop him, the victim threatened him by calling the local people. To take revenge, the accused edited porn pictures of the victim and used to send it to her through IMO and threatened her to upload it on social media. Later, when a case was filed against him, he was found guilty and, 30000 taka was imposed on him as fine.
>
> @Daily Bangladesh (6 April 2021) <https://www.daily-bangladesh.com/colorful-life/240920>

According to the data of PCSW, from the middle of November 2022 to 30 June 2023, about 6,000 further complaints were received. With 2,075 complaints, publishing and disseminating private photographs and information about women online topped the list.[41] About 30% of cases pending in tribunals are romance scandals, where a woman's private moments are captured with or without her consent. 1.75% said their photos were edited and published on pornography sites.[42] 3.06% of individuals surveyed admitted to being photographed or videotaped while being sexually assaulted, and those images or videos were later shared on social media.[43]

---

[39] Tribune Editorial, 'Zero tolerance for revenge porn' *Dhaka Tribune* (Dhaka, 3 March 2016) <https://www.dhakatribune.com/opinion/editorial/122229/zero-tolerance-for-revenge-porn> accessed 3 September 2024.

[40] Nazmul Huda, 'The trap of pornography' *Manabzamin* (28 April 2023) <https://mzamin.com/news.php?news=52899> accessed 3 September 2024.

[41] Iqbal Mahmud, 'Cybercrimes rampant' *The New Age* (Dhaka, 09 July 2023) <https://www.newagebd.net/article/206233/cybercrimes-rampan> accessed 28 July 2024.

[42] Tribune Desk, 'Study: 63.51% of women in Bangladesh face online violence' *Dhaka Tribune* (Dhaka, 27 November 2022) <https://www.dhakatribune.com/bangladesh/299185/study-63.51%25-of-women-in-bangladesh-face-online> accessed 3 September 2024.

[43] ibid.

Recently, the Criminal Investigation Department of Bangladesh apprehended a total of nine individuals who were implicated in the dismantling of a child and adolescent pornography network operating primarily through the social media platform: Telegram, commonly referred to as "The Pompom Group", in Bangladesh.[44] Throughout a duration exceeding one year, the investigative division of the Bangladesh police asserted that the criminal syndicate had been employing "sensitive/indecent videos" featuring minors and adolescents as a means of coercing victims and profiting from their exploitation.

The reason behind the increase of cybercrime and the gap in investigation and prosecution is most of us who are victims of cyber harassment or revenge pornography do not want to go to the police. Furthermore, many of those who want to report to the law enforcement agencies do not know where to go to get a remedy. If someone's Facebook ID is hacked or if they are blackmailed online with their pictures or videos or threatened with the spread of revenge pornography, then they do not know where to go. Although there are DMP, Cyber Cell, CTTC, CID Cyber Cell, PCSW, help/hotline numbers like 13219, 1098, 109, and several other helpline numbers for cyber harassment in Bangladesh, many of us do not know where to go in an emergency. Also, many people have trouble understanding where to get any benefits due to the lack of a specific number for cyber sexual harassment. For this reason, people ask hackers to get back the ID in exchange for money or request them not to harass. Due to these reasons, the level of harassment increases and the hacker remains out of reach. Even if someone wants to get legal support properly from district level, many police stations do not want to accept the cyber case after hearing the cyber issue. In many cases, due to our ignorance, we destroy various types of cyber documents and digital evidence without understanding. For these issues, such information does not come up during forensics and the criminals get away from the law enforcement agency. Even if a proper forensic report is given, many times lawyers are not able to present it properly in court due to a lack of knowledge about cyber forensics. Analysing different types of data from last year, in cyber cases the culpability of the criminals is proven in less than 4% of cases. A report published on *Prothom Alo* in 2021 mention that 7% of cyber cases are not proven in court. When asked about this, Special Public Prosecutor (PP) Nazrul Islam, who was handling such cases on behalf of the state, told Prothom Alo that the post on which the case was filed on the social media was not found during the investigation. The defendants deleted it. In many cases witnesses do not appear. Therefore, in the end the allegations cannot be proved.[45]

2.3 Cybercrime and AI – A Rising Concern for Bangladesh

Another concern is the rise of AI and deepfake technology presenting a complex set of challenges for Bangladesh. Without proper knowledge about its ethical use or how to prevent its illegal use, Bangladesh is already struggling to cope up with the rapid growth of technology.[46] Deepfake technology, which involves the creation of fake videos or audio

[44] Staff Correspondent, 'Blackmailing gang busted' Daily Sun (Dhaka, 23 May 2023) <https://www.daily-sun.com/printversion/details/690867> accessed 3 September 2024.

[45] Asaduzzaman, '৯৭ ভাগ মামলাই টেকেনি', *Prothom Alo* (Dhaka, 20 September 2021) <https://www.prothomalo.com/bangladesh/crime/৯৭-ভাগ-মামলাই-টেকেনি> accessed 3 September 2024.

[46] RS Team, 'ভিডিওর এই নারী তানজিন তিশা নন, ডিপফেকের শিকার অভিনেত্রী' (*Rumour Scanner*, 3 January 2024) <https://rumorscanner.com/fact-check/this-woman-in-the-video-is-not-tanjin-tisha-but-the-actress-victimized-by-deepfake/99118> accessed 3 September 2024; Makful Hossaion, 'Now Bangladeshi actresses fall victim to deepfake, how to detect these videos' *Prothom Alo* (Nourin Ahmed Monisha tr, Dhaka, 14 January 2024) <https://en.prothomalo.com/entertainment/qb3srbu14q> accessed 3 September 2024.

recordings poses significant risks in a society where we are not strong in digital forensics of original data. Deepfake forensics is far away from us. In Bangladesh, this can lead to the spread of information further exacerbating existing tensions and potentially swaying public opinion, pornography, fake videos, and fake statements through deceptive content that is hard to distinguish from reality. Furthermore, the use of deepfakes to fabricate narratives or impersonate individuals can result in privacy breaches and reputational damage causing harm to people's reputations and mental well-being. The widespread use of technology also threatens the credibility of journalism and media as it becomes increasingly difficult to differentiate between manipulated content potentially eroding public trust in news sources. Moreover, considering the potential for tensions, in the country deepfakes may be used in future to incite violence or propagate false narratives about ethnic or religious communities, further destabilising societal harmony.

When it comes to handling cybercrime there are distinctions, between Bangladesh and the other first world countries. Developed countries has advantages with its laws, advanced preventive measures, and a higher level of awareness. On the hand Bangladesh is still in the process of developing its capabilities in the legal, academic and awareness areas. Bangladesh needs significantly more time and skilled persons in these sectors to prevent cybercrime with AI.

3. CYBERCRIME IN BANGLADESH:

This part of the report talks about causes, incidences, effects of cybercrime in Bangladesh, and the gap in the existing legal framework on cybercrime.

3.1 Causes of Cybercrime in Bangladesh

In this modern era, use of technology has been more prevalent in every sector. One of the main reasons behind this increasing rate of cybercrime is the use of pirated software.[47] About 90% of software in Bangladesh is pirated, which is leading us towards a vulnerable situation.[48] By implanting backdoors in servers, injecting shells in database, injecting keyloggers to steal access, advanced spoofing etc perpetrators fool online platform and misuse the data of victims. Additionally, though the number of computer users has increased in Bangladesh in the past few years, police reports regarding computer-related offences are reported very rarely.[49] As a result, criminals are frequently committing crimes and not being punished for such crimes.

3.1.1 Interview Findings

To understand the alarming situation of cybercrime and various aspects, Map of Justice interviewed several notable individuals who are experts in the field.

Tanvir Hassan Zoha, Managing Director, Backdoor Private Ltd, and an expert in Digital Forensics, was one of them. When asked about the reasons behind cybercrime, he provided insightful information regarding the about the motives of the criminals as the motives is the cause that moves people to induce certain action. According to him, the human brain has a hormone called dopamine, which gives us pleasure or pain based on our actions. Happiness or peace varies from person to person. Criminals involved in cybercrime seem to find some sort of joy or peace when committing cybercrime or violating another's privacy. Depending on the person, it can be an 18-year-old person or a person from a well-to-do family. Gradually they get addicted to it and their brain urges them to do these kinds of work. That is, it is cl ear that the advancement of information technology as well as the psychology of criminals plays an important role in committing cybercrime.

Rezwanur Rahman, MVP, Microsoft and an expert in Digital Forensic said that compared to other countries, among all other countries in Asia, Bangladesh has the highest crime rate in this context. There are many reasons for this, and some of the main reasons are illegal use of the internet and social media, easy access to pornography websites, lack of academic and family supervision, and lack of proper law enforcement by the administration. The number of children below the age of 18 as victims of cybercrime is alarmingly increasing. He described that his own sister was targeted by deepfake AI images. He was familiar with some of the personnel from Cyber Security agencies and police, and with their assistance, he was able to prevent the images from going viral. But the fact is most of the general people have no

[47] Moriom Akter Mou, 'The Causes And Impacts Of Cybercrime In Bangladesh' (*DIU Blog*, 4 February 2023) <https://blog.daffodilvarsity.edu.bd/the-causes-and-impacts-of-cybercrime-in-bangladesh/> accessed 3 September 2024.

[48] ibid.

[49] Alam (n 26).

connection with the agencies against cybercrime. He was concerned that in case of an emergency what general people can get service is a big question.

Except for two units from CID cyber cell and CTTC there are no other police establishments who are properly capable to deal with cybercrime issues.[50] Lack of trained investigators, equipment and manpower is another major reason for this increasing rate. On the other hand, criminals are more expert in using technology and using new and different methods to commit cybercrime. In this regard, Rezwanur Rahman said that cybercriminals often use very advanced technology and techniques, which make them difficult to detect and catch. Also, cybercriminals often commit crimes from different locations in different countries, which creates legal complications. He feels that ensuring personal and corporate data protection and privacy is a major challenge. Criminals often use cryptocurrency, which keeps their transactions secret and complicates investigations. Tanvir Hassan Zoha said that there are many challenges to combat cybercrime in front of Bangladesh and slowly these are emerging from these challenges. Earlier there was no judgement delivered on cybercrime related cases, which shows a big shortcoming of the legal system of the country that makes the criminals to be fear free in committing cybercrime. He thinks that the technology of law enforcement in Bangladesh is not updated according to the way criminals are updating with technology.

Negligence is another reason because of which perpetrators get easy access and gain control over the computer. Cybercrime perpetrators can be of any age. When asked about the tendency of children below 18 years to commit cybercrimes, especially online hacking, Rezwanur Rahman said that children's interests are responsible for their criminal tendencies. Considering hacking as a very exciting topic and with hacking techniques and videos readily available on the internet, especially on YouTube, children easily become adept at committing such crimes and become criminals.

Kazi Mustafiz, Founder and President of Cybercrime Awareness Foundation said that the guardians and parents of children are not aware about the regular activities of their children in relation to cybercrimes. They do not monitor their children appropriately and fail to ensure their children are aware of cybercrimes and the ways of avoiding it. They need to represent and teach both the positive and negative aspects of using the internet; that is how they can make their children more aware of the different aspects of the internet. Children should not get addicted to it; they must use 'Niyontrito Projukti'. Therefore, lack of safe internet usage practices, vigilance, knowledge practices, proper policies etc. can also be attributed as one of the major causes of cybercrime. Moreover, all the data is routinely destroyed, thus lack of evidence is an obvious problem.[51] Again, further collection of data from beyond territorial extent may paralyse the system of crime investigation.

3.1.2 Focused Group Discussion (FGD) Findings:

A focus group discussion organised by "Map of Justice" was conducted on school-going students. It has been seen that they are not aware of the issues related to cybercrime. They are using these platforms without understanding and as a result, they are being harassed online

[50] ibid.

[51] CCAF, 'গবেষণা প্রতিবেদন: বাংলাদেশে সাইবার অপরাধ প্রবণতা-২০২৩' (*Cyber Crime Awareness Foundation*, 20 May 2023) <https://ccabd.org/বাংলাদেশে-সাইবার-অপরাধ-3/> accessed 3 September 2024.

in various ways. Tanvir Hassan Zoha also stated that when children below 18 years go through the adolescent phase, mental depression is seen mostly in them. Children of this phase mainly join online forums to share their thoughts and feelings, and they have very little awareness and awareness about cybercrime. As a result, they connect with strangers on these platforms and subsequently suffer harassment. They do not understand that a person they meet online may not be the same in real life. This lack of understanding among children is one of the reasons why they become victims of cybercrime. Additionally, when children have distance from their parents or guardians and lack healthy communication, they tend to become mentally and emotionally dependent on people they meet online, sharing personal information and thoughts with them. This situation also raises the danger of cybercrime for them.

Rezwanur Rahman, when interviewed, expressed a similar opinion. He also said that children become victims of cybercrime due to communication gaps between children and parents. He blames this communication gap as the reason why today's children are more victims of cybercrime than in the past. Earlier children could share their thoughts, feelings, and other matters with their parents or guardians, but nowadays, they cannot do so due to various reasons. That is why they are using online platforms to express their mental frustrations and other feelings and are at the risk of cybercrime. In addition, he also said that in Bangladesh, sometimes the boys and girls of schools, colleges or universities are not given the idea, training or knowledge of cybercrime, sexual crime, or how to protect themselves. 70% of the people of Bangladesh do not have proper knowledge of what is cybercrime and what is covered by cybercrime.

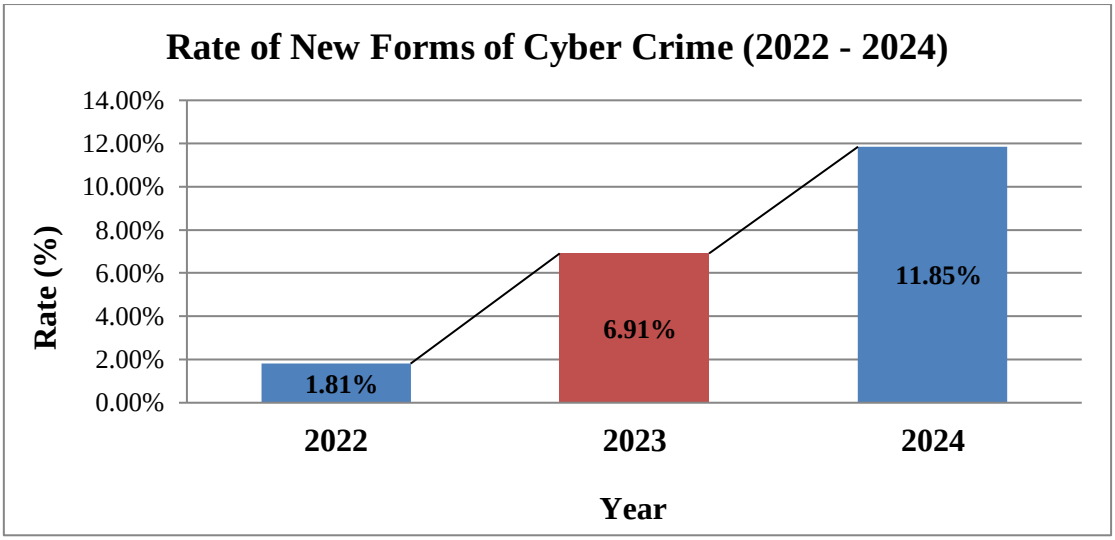
3.2 Statistical Analysis and Expert Opinions on Cybercrime in Bangladesh

As per the report of the Cybercrime Awareness Foundation (CCAF), in 2022, the rate of new forms of cybercrime was 1.81%.[52] This rate increased to 6.91% in 2023,[53] and nearly doubled to 11.85% in 2024.[54]

[52] CCAF 2022 (n 23).

[53] CCAF 2023 (n 51).

[54] CCAF, 'গবেষণা প্রতিবেদন: বাংলাদেশে সাইবার অপরাধ প্রবণতা-২০২৪' (*CCABD*, 29 June 2024) <https://ccabd.org/wp-content/uploads/2024/07/CCAF_Research_2024_V14.pdf> accessed 3 September 2024.



3.2.1 Demographics of Victims of Cybercrimes

A recent study by CCAF revealed that social media and online account hacking is the most widespread type of cybercrime in Bangladesh, making up 21.65% of reported incidents. According to the study, 78.78% of the victims are aged 18 to 30, while 75% of the affected individuals are women.[55]

Nazrul Islam Shamim said that the rate of cases in cyber tribunals with women victims is high; especially girls, who are most common victims of sexual harassment, through the spread and publication of various fake/edited videos and pictures. Moreover, based on his observation of all the cases filed, he found that most of the victims are either divorced women or teenage girls, especially the class of people who are in a better position in the society. Thus, regardless of age, anyone is susceptible to cybercrime. In this regard, Kazi Mustafiz acceded stating that people of all ages file complaints of cyber harassment. Noticeably, in the past few years, more underage victims are filing complaints of cybercrimes. By way of comparison, he said that the rate of underage victims has increased by 140.87% since 2018.

Rezwanur Rahman opined that, 95% of people aged 16 to 40 are unaware of cyberspace safety, which is why they are at most risk of falling prey to cybercrime. As per his observation, most of the cybercrime complaints received are filed from Dhaka and Chattogram districts, but the people of other districts also fall victim to cybercrime. The people of Dhaka who are aware of the cybercrime, knows how to take legal action against it, and willing to do so, successfully files a complaint. The rural people are mostly not aware of such issues, therefore the number of the complaints filed from such areas are comparatively less.

Alternatively, one may be completely unable to realise that s/he may be at the mercy of cybercrimes. Md. Saimum Reza Talukder, Senior Lecturer, School of Law, BRAC University stated that most victims do not even realise that they have been the victim of a cybercrime. Furthermore, even when they do realise, they do not know where to file the complaints. It is

[55] FE Online Desk, 'Social media and online account hacking most prevalent cybercrime in Bangladesh: Study' *The Financial Express* (Dhaka 29 June 2024) <https://thefinancialexpress.com.bd/sci-tech/online-account-hacking-most-prevalent-cybercrime-in-bangladesh-study> accessed 3 September 2024.

the state's responsibility to acknowledge its limitations, and make the information regarding the available help services and mechanisms accessible for all.

3.2.2 Demographics of Perpetrators of Cybercrimes:

While investigating the complaints received by the PCSW wing of the police,[56] officials have found the involvement of women in at least 10% of the incidents. They also say that in cases of harassment on social media, 36% of men demand money from women because of personal conflicts, threatening to spread personal information on social media.

After reviewing the complaints, it was found that the number of students among the accused is more. In at least 10% of cyber harassment cases against women, women have been accused. Investigation has revealed that personal conflict is the main reason for this.[57]

3.2.3 Nature & Frequency of Complaints

The dedicated PCSW wing received 28,201 complaints till 30 June 2023 of instances of cyber offences. From the inception of the PCSW wing till 15 November 2022, 22,304 complaints were received on six criteria, including fake ID, ID hack, blackmailing, mobile harassment, spreading offensive content and others. Since 16 November 2022, informational changes have been made within the categories, and divided into eight types of complaints. As of 30 June 2023, 8,874 complaints have been received in these eight categories - doxing, impersonation, ID hack, blackmailing, cyber bullying, spreading offensive content, mobile harassment, and others.[58]

According to the information received from the police headquarters, from 16 November 2020 to 30 September 2023, various complaints were received on Facebook messenger, hotline number and e-mail. Many victims have communicated with the headquarters through multiple different channels. As a result, the number of registered service seekers is 44,408 people.[59] Unfortunate, 83% of these cybercrimes go unprosecuted.[60]

After conducting research on 6 districts of Bangladesh, Action Aid reported that 14.91% women file complaints against cyber harassment.[61] According to the report of PCSW, since November 2020, more than 22 thousand women have contacted them regarding cyber harassment.[62] In 2022, a total of 171 cases of cybercrime were filed, of which 20.46% cases were of pornography and online harassment, and 29.23% cases were of online fraud, as per the report of DB Cyber and Special Crime Branch.[63]

---

[56] ibid.

[57] Mahmud (n 41).

[58] ibid.

[59] Riad Talukdar, 'সামাজিক যোগাযোগমাধ্যমে নারীদের হয়রানি করছে নারীরাও' *Bangla Tribune* (Dhaka, 15 October 2023) <https://www.banglatribune.com/others/820264/> accessed 28 July 2024.

[60] Khandaker Farzana Rahman, 'Cyber Crime: Current Status and Actions' *Samakal* (Dhaka, 23 February 2023) <https://www.samakal.com/sports/article/2307186582/> accessed 28 July 2024.

[61] Action Aid (n 19).

[62] Rahman (n 60).

[63] ibid.

Kazi Mustafiz informed that complaints against 80% cyber harassment issues are not filed in Bangladesh. In the remaining 20% cases that are filed, most are instances of cyber bullying. According to him, children also file cybercrime complaints and children are more victims of social media related crimes as the complaints of social media related crimes are mostly files in the cyber cell such as cyber bullying, harassment in the comment section etc. The 80% of victims who are not filing complaint against it have several reasons of not filing it- they are either in fear of their social status, or they do not want to disclose the matter, or they are not aware of the ways of filing complaint, or they think they will not get relief after filing a complaint.

Rezwanur Rahman said that among all other types of cybercrimes, blackmailing, child pornography, hacking, and phishing have been noticed more recently, and he believes that both children and adults are at risk of becoming victims of data leak, pornography, child pornography, blackmailing, etc.

3.2.4 Complaints Disposal and Rate of Conviction:

It may be noteworthy that the number of prosecutions for cybercrime has decreased significantly after the Digital Security Act 2018 was replaced by the Cyber Security Act 2023. The Public Prosecutor (PP) of Dhaka Cyber Tribunal **Nazrul Islam Shamim** was interviewed by Map of Justice, and he said that the number of cases filed during the Digital Security Act was very high. At present, the cases filed under the Cybersecurity Act of 2023 are very less.

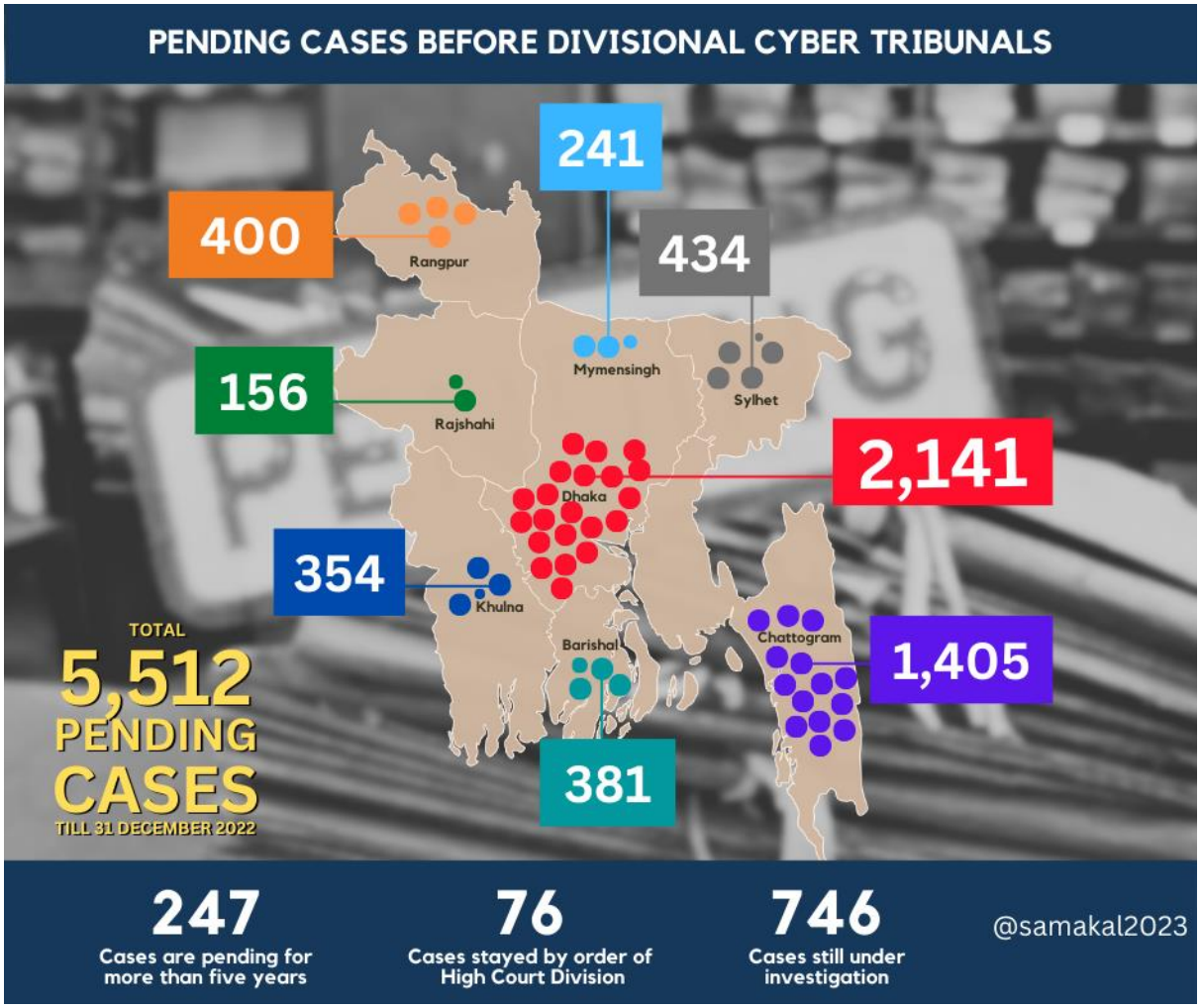
The number of victims who have sought legal assistance have decreased in recent years. According to CCAF's assessment in 2023, 26% of the 199 people they have assessed, filed complaints to the police against cyber criminals and 7% people got their desired relief.[64] However, in 2024, only 12% sought legal redress, of which 81.25% filed General Diary, while the remaining persons filed written complaints to the respective magistrates. Those who sought the assistance from the law enforcement agencies, 87.5% of them were not satisfied with their services, or lack thereof, while the rest made no comments about the issue.[65]

In this context, it is to be noted that despite the reduced number of cases being filed under the new law, the number of cases pending before the court is still quite high, with the conviction rate being quite low. As per the information provided in the Annual Confidential Report (ACR) submitted to the Supreme Court, till 31 December 2022, a total of 5,512 cases were pending before the respective eight divisional cyber tribunals. 2,141 of these cases were pending in Dhaka, 1,405 in Chittagong, 156 in Rajshahi, 354 in Khulna, 381 in Barisal, 434 in Sylhet, 400 in Rangpur, and 241 in Mymensingh. Amongst these, 247 cases are pending for more than five years, which evinces the low rate of conviction. While the proceedings of 76 cases have been stayed by the order of the High Court Division,[66] 746 of the total number of cases were still under investigation.

[64] CCAF 2023 (n 51).

[65] CCAF 2024 (n 54).

[66] Abu Saleh Roni, 'আইন পরিবর্তন হলেও সাড়ে ৫ হাজার মামলার খড়্গ' *Samakal* (Dhaka, 08 August 2023) <https://samakal.com/bangladesh/article/188540/> accessed 9 September 2024.



Nazrul Islam Shamim said that cybercrime cases are generally taken seriously only after investigation. At the time of investigation, in most cases, due to the failure to prove the allegations, redress is not possible. This is because it is almost impossible to accurately identify the evidence if the victim's social media ID is deleted or removed from the platform. If the investigation is unable to produce accurate information of the offence, it is considered unsuccessful, and thus, the victim gets no remedy.

3.3 Effects of Cybercrimes in Bangladesh:

The offences of cybercrime affect victims physiologically, financially, socially, and physically. Victims often experience distress including anxiety, depression, and post-traumatic stress disorder.[67] Sometimes they feel helpless and vulnerable. Cyber sexual harassment has the potential to significantly impact the mental well-being of its victims, resulting in challenges related to self-esteem, self-blame, and even suicidal ideation.[68] These individuals may also encounter social stigma and undue judgment, which further contributes to a culture that places blame on the victim rather than addressing the actions of the perpetrator. This can

[67] Rudra Russell, 'Private Lives Shattered in the Cyber World' *Dhakatimes* (Dhaka, 20 August 2022) <https://www.dhakatimes24.com/2022/08/20/274839> accessed 9 September 2024.

[68] Mohammad Jamil Khan, 'Evolution of Cybercrime: Women, the worst sufferers as usual' *The Daily Star* (Dhaka, 16 June 2022) <https://www.thedailystar.net/news/bangladesh/crime-justice/news/evolution-cybercrime-part-3-women-the-worst-sufferers-usual-3048576> accessed 9 September 2024.

result in isolation and further emotional distress. Education and career paths can be influenced by cyber harassment. Victims may avoid attending school or participating in forums due to fear or discomfort; workplace harassment can also impact job performance and hinder career advancement. In cases, cyber harassment can escalate to stalking or violence, thereby endangering the safety of victims. Unfortunately, victims of cyber harassment often face barriers when it comes to reporting these incidents. They may fear retaliation, worry about privacy concerns, or simply lack awareness about reporting mechanisms. As a result, many incidents go unreported. On the other hand, a child who falls victim to cyber harassment may experience long-term consequences that affect their growth, self-esteem, and trust in platforms.

Nazrul Islam Shamim said that children are victims of this cybercrime due to lack of family awareness, and many children commit suicide without informing their family about the crime. Because when the child's parents or guardians are not able to do parenting properly, the child is also unable to communicate with them about the problems that are happening to him/her, thus becoming a victim of crime, and often opting for suicide out of frustration.

3.4 Gaps in the Existing Legal Framework:

Bangladesh is currently facing a steady rise in cybercrimes as technology continues to advance. Unfortunately, the country's legal system has not kept up with these changes, making it difficult to combat cyber threats effectively.

The Information and Communication Technology Act 2006, which was introduced in 2006 and later amended in 2013, was initially created to define, and penalise some cybercrimes against the state. The new Cyber Security Act 2023 has been stretched beyond its purpose to purportedly also cover cybercrimes. Despite this expansion, the act fails to address cyber threats, child pornography, sextortion and has no framework to protect victims of AI-generated crimes. These extremely pertinent issues for which so many people suffer in Bangladesh, has not been addressed by the Cyber Security Action, 2023, as has been demonstrated in this report, including through the statistics in the previous section. Meanwhile, existing laws, like the Cyber Security Act, 2023 and the Pornography Control Act, 2012 also do not sufficiently address issues such as cyber harassment, revenge pornography, and other forms of undue aggression in the cyberspace.

These omissions have resulted in a very weak defence by the State apparatus against cybercrime in Bangladesh, putting victims in an extreme situation of vulnerability. On top of all these issues, the Digital Security Act, 2018, and its successor, the Cyber Security Act, 2023, despite its aims to strengthen security, has faced widespread criticism due to its questionable interpretation of freedom of speech, which could potentially clash with constitutional and human rights.

Most importantly, the Cyber Security Act, 2023, which is supposed to play the leading role in Bangladesh's fight against cybercrime, unfortunately, lacks the very definition of what exactly qualifies as cybercrime. While it does criminalise cybercrime related activities, it fails to classify or define the nature of cybercrimes comprehensively, including when it comes to addressing online content related issues. This lack of specificity hampers the effectiveness of the law in tackling crimes on platforms such as Telegram groups and Reddit posts. It must be noted that very recently, Asif Nazrul, Advisor, Ministry of Law, Justice, and Parliamentary Affairs of Bangladesh said that initiatives would be taken to reform the Cyber Security Act, 2023, soon.[69]

The introduction of the term 'pseudonymized data' in the draft Data Protection Act 2023 is another problematic aspect of the law. In the Bangla draft, pseudonymized data has been bracketed while defining 'anonymized data' and included both pseudonym as well as de-identify within the definition.[70] In the unofficial English draft, however, 'anonymized data' has only been defined as "data which has undergone the process of de-identification",[71] with no proper explanation for pseudonymized data. It is to be further noted that both the terms have been grouped together and use in multiple provisions. Both these terms have been incorrectly treated as similar terms in the act, which creates the possibility of causing confusion within the framework itself, as well as increases the scope of complexity in its enforcement. This confusion highlights the importance of involving experts who possess an understanding of

[69] Online Desk, 'অচিরেই সাইবার নিরাপত্তা আইন সংস্কারের উদ্যোগ নেওয়া হবে: আসিফ নজরুল' *Bangladesh Pratidin* (Dhaka, 29 September 2024); <https://www.bd-pratidin.com/national/2024/09/29/1033346> accessed 29 September 2024; TDS Report, 'CSA to be amended soon: Asif Nazrul' *The Daily Star* (Dhaka, 29 September 2024) <https://www.thedailystar.net/news/bangladesh/rights/news/csa-be-amended-soon-asif-nazrul-3715536> accessed 29 September 2024.

[70] *Draft* Data Protection Act 2023 <https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/page/6c9773a2_7556_4395_bbec_f132b9d819f0/উপাত্ত%20সুরক্ষা%20আইন%2C%20২০২৩%20১১.১০.২৩.pdf> accessed 3 September 2024.

[71] *Draft* Data Protection Act 2023 [Unofficial English Translation] <https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/page/6c9773a2_7556_4395_bbec_f132b9d819f0/Data%20Protection%20Bill%20%20v15%28English%29%2016.01.23.docx> accessed 3 September 2024.

identities and privacy concerns when drafting laws in this domain. One notable gap in Bangladesh's approach to cyber security is the absence of a law specifically addressing forensics. Despite having security rules under the Cyber Security Act, 2023, and some forensic guidelines in place these current legal provisions do not align with demands. As cybercrime cases continue to rise there is a need for digital forensic experts, like never before. In Bangladesh digital forensic experts often face challenges, in finding opportunities to collaborate with the police and security forces. Unfortunately, the police have not implemented this practice to take help from cyber experts effectively. The introduced cyber security bill, although it criminalises offenses, shares the shortcomings as its predecessors by failing to define cybercrime or address its content properly. Similarly, the proposed Personal Data Protection Act is plagued by conflicts in definitions and fails to establish punitive measures for cybercrime. Instead of integrating with Bangladesh's Penal Code 1860 to provide a solid legal framework it only imposes monetary fines disregarding the broader risks associated with cybercrime.

Legal experts have highlighted the insufficiency of laws in dealing with harassment, on digital platforms emphasising the urgent need for comprehensive legislation. The use of evidence rules further complicates the prosecution of offences related to media, indicating a pressing demand for legal reform that keeps up with technological advancements. On the other hand, the *Nari o Sishu Nirjaton Daman Ain* falls short in addressing the complexities of harassment. In a case (*BNWLA v. Government of Bangladesh*) the concept of harassment was clarified but was not extended to cover digital platforms creating a significant gap in legal protections against online harassment.

The judicial system also faces its set of challenges arising from complexities. Judges and lawyers who play a role in adjudicating cybercrime cases often find themselves at a disadvantage due to their familiarity, with the technical aspects of these crimes. This results in the tribunals being left overburdened. The cyber tribunal in Dhaka needs more time, expertise, and training to deal with these cases. Efforts are being made to incorporate cybercrime training into the curriculum of the Judicial Administration Training Institution to bridge this knowledge gap. The backlog of pending cybercrime cases further highlights the challenges within the process. Addressing these issues requires an endeavour to refine and expand Bangladesh's legal and judicial framework governing cybercrime.

There is no plan of action to tackle cybercrime in relation to emerging issues like future cyber harassment, and AI-generated crimes show a significant oversight. Furthermore, the absence of programs aimed at rehabilitating those accused of cybercrimes or who are convicted suggests a preference for punitive over restorative justice when dealing with cyber-related issues.

4. FINDINGS

4.1 Contextual Analysis on Cyber Offences

New forms of cybercrimes are constantly being created and the number of cybercrimes is on rise. The increasing rate of cybercrimes is influenced by multiple factors including psychological behaviour of offenders, the gap among people regarding awareness, lacking of strict law and advancement of technology. Although people of all ages can be victims of cybercrime, most young people and women are in a vulnerable position due to various reasons.[72] From an interview, it was found that in cyber tribunals, the rate of cases regarding girls is high. Especially girls are becoming victims of sexual harassment through various videos and pictures. Most of the young of this generation are unaware and have an invisible gap with their parents. Because of this gap, they find it difficult and sometimes even impossible to share their feelings with their parents. As a result, if anyone becomes a victim, they fall into a dilution as their parents or any other guardian is not there to help. This made them easy targets for offenders. From our research, we found that a significant number of people do not file complaints. Behind this, fear and social reputation work as a vital factor. People have fear because of the gap of awareness. It is the responsibility of certain authorities to ensure awareness strategies at every level and normalise victims of cybercrime in society.

Behind the commission of cybercrime, psychological aspects, revenge mindsets and various other reasons exist. Greater availability and accessibility of learning resources regarding hacking has also made things easier for cybercriminals. Advancement of technology is needed, but as well as limited access to sensitive resources is necessary. Anyone from any place can learn how to commit crimes, and by hiding their own identity can harass or breach someone else's privacy. Among other several issues, such issues are equally liable for the rise of cybercrimes. The literature review and the research we have conducted both emphasised the gap of knowledge among people and recommended expanding of awareness strategies and strengthening policy level remedies.

As there are growing precedents of victims not getting remedies for the cybercrimes that may have been committed against them, and perpetrators are not caught and held accountable in most cases, there is also a concurrent growing reluctance amongst victims in filing complaints and cases to the police. The entire legal process is cumbersome and time consuming. Any complaint first goes through a long and inefficient investigation process, after which the court may take cases in its cognisance. As the investigation process takes a long time, in most cases it is seen that the various trails in the cyberspace is removed or changed. For instance, the victim's Facebook ID may be removed or deleted and the authorities fail to identify the various links and chains of causation and the investigation fails. As a result, the victim does not get the remedy.

Indeed, it was affirmed during the literature review for this report that sometimes the police do not want to accept cybercrime related cases, particularly because no well-planned and comprehensive training is provided for them. As a result, most of them are not even able to get any experience in investigating cybercrimes. As civil and criminal cases are time-

[72] Roni (n 66); Editorial, 'Why are cybercrimes going unpunished?' *The Daily Star* (Dhaka, 14 August 2022) <https://www.thedailystar.net/opinion/editorial/news/why-are-cybercrimes-going-unpunished-3094791> accessed 3 September 2024.

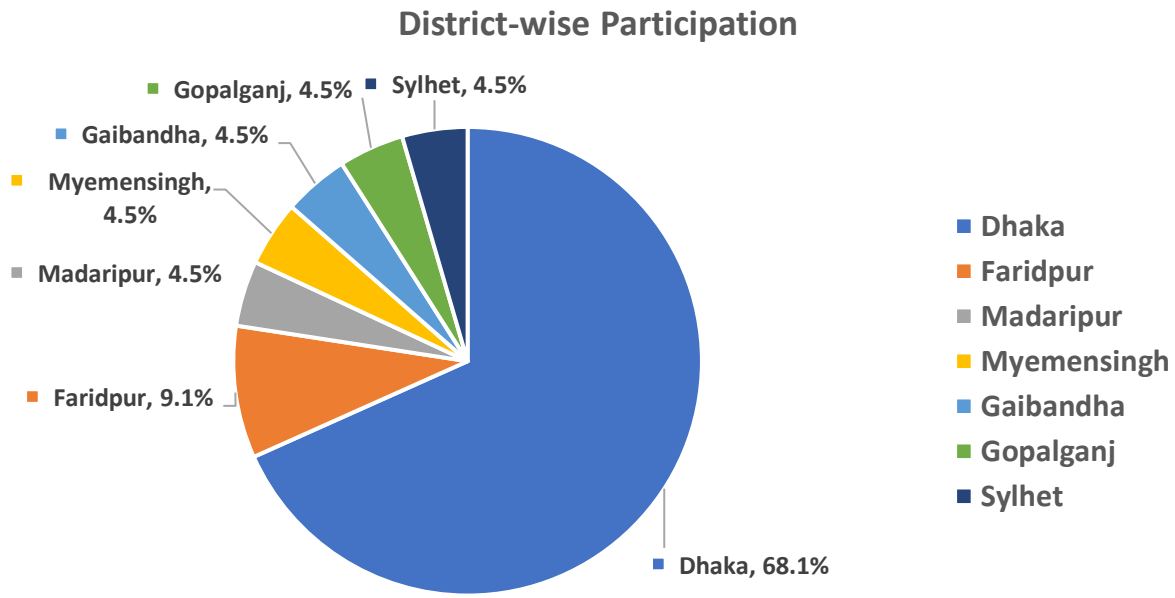
consuming, similarly to getting accustomed to cybercrime issues is a time-consuming process. Things have greatly improved in recent times. Many lawyers are also working on cybercrimes.

The analysis suggests that to decrease the rate of cybercrimes, there is a need for multiple strategies to be adopted; a combination of legal and institutional framework together must be the most effective one.

4.2 Empirical Analysis on Students in Bangladesh:

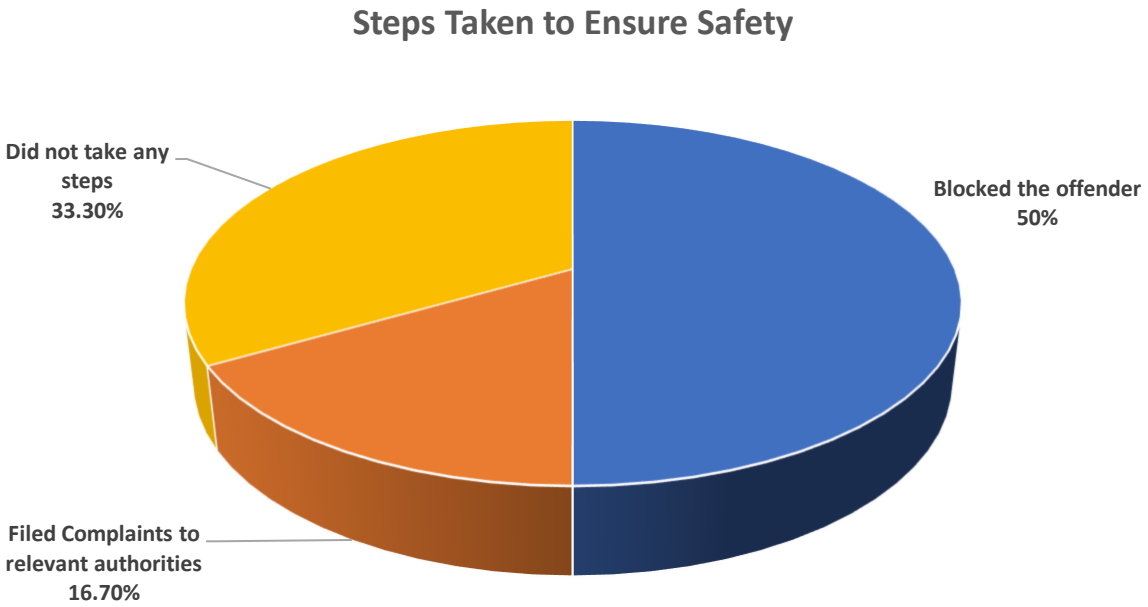
To understand and gauge students' conceptualisation of cyber related offences in Bangladesh, two focus group discussions (FGDs) were held with students from school, college, and university levels. Following the FGDs, the group was analysed under three categories. First, based on the location of the participants; second, based on their existing knowledge regarding cyber sexual harassment; and third, based on the measures they adopted to ensure safe online space for women or children, as well as steps they think that if taken would strengthen the existing laws and support systems.

Participants attended the virtual FGDs from several districts, the majority of which were from Dhaka with a 68.1% participation. Amongst the rest, 9.1% represented Faridpur, while the representation from Gopalganj, Madaripur, Sylhet, Gaibandha and Mymensingh were 4.5% each.

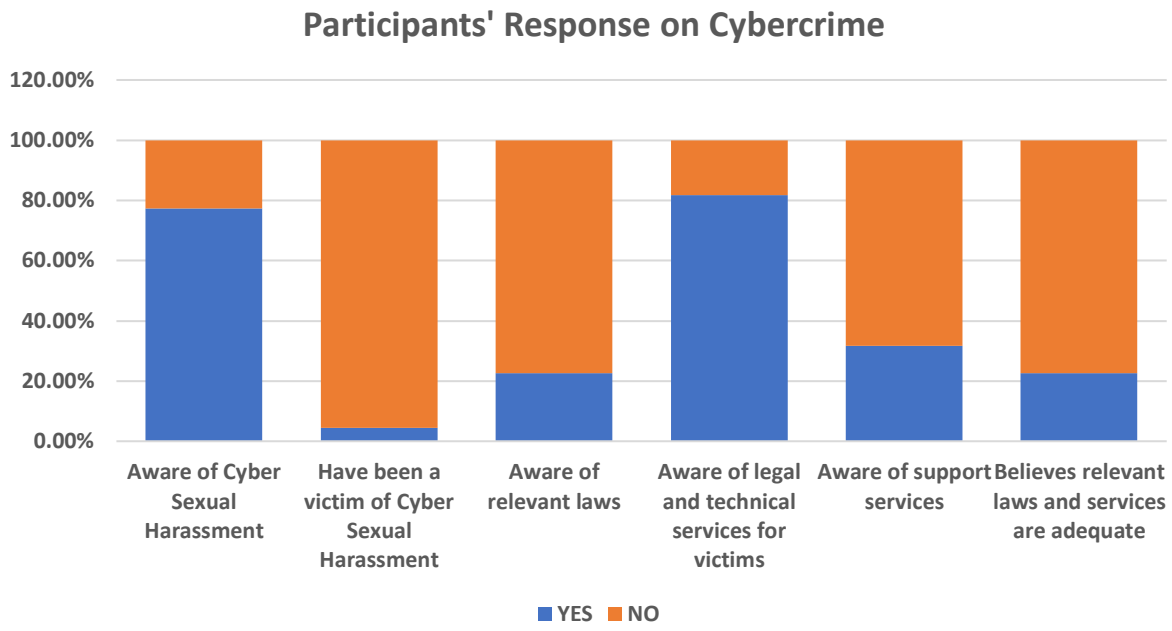


With regards to their knowledge on the concept of cyber offences, 77.3% of participants said they know about the sexual harassment, while 22.7% said they have no idea about what sexual harassment comprises of. Of the participants, 95.5% shared how they have never been a direct victim of sexual harassment on online platforms, while the remaining 4.5% did experience facing such harassment in the form of receiving indecent massages, images, and/or videos from other known/unknown accounts. 63.6% of all the participants shared that their family members, friends, and/or acquaintances were victims of online harassment.

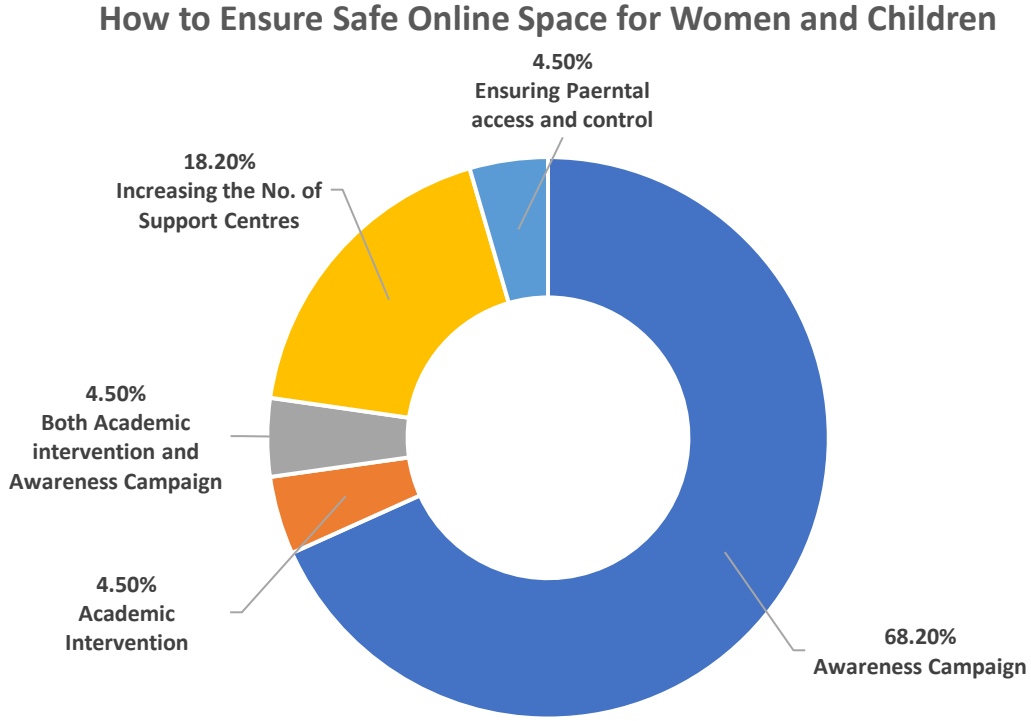
When discussing their response to such harassment and what steps they took to ensure their safety, 50% shared that they blocked the offender online. Among the remaining 50%, 16.7% of them filed complaints to certain authorities, which varied from guardians, and teachers, and among the remaining participants, some ignored the interaction. It was also noticed that many participants were hesitant in sharing such issues with their family members.



77.3% of the participants shared that they have no idea or knowledge about the laws on online harassment that are in effect in Bangladesh, while the remaining 22.7% knew about the relevant laws. Alternatively, an overwhelming 81.8% of the participants were aware of the technical and/or legal services available to the victims of online sexual harassment or any harassment. However, only 31.8% knew where to seek help immediately if they experience cyber-sexual harassment. It was interesting to note that 77.3% of them believed that Bangladesh's laws and service institutions are not adequate addressing cases of online harassment.



On asking which action they think is most necessary to ensure safe online space for women or children, 68.2% voted for raising awareness, 4.5% voted for incorporating prevention of sexual harassment related contents in educational textbooks. Another 4.5% of participants believed both academic intervention as well as awareness raising is required. 18.2% believed increasing the number of effective support centres across the country would be the best course of action. Another 4.5% were of the understanding that parental access to children's social media accounts and devices would help as they would be the first to know if their children are in trouble, and opined that compliance to religious discipline must be considered.



Lastly, the participants placed several recommendations towards the government when asked about probable steps that they think could be taken to strengthen the laws and support systems in Bangladesh, and ways to reduce the rate of online harassment; they are as follows:

1. Raise collective and individual awareness about the issue through campaigns, podcast shows, and workshops
2. Provide proper knowledge of safe internet use.
3. Establish a rapid response support team available and easily accessible to all.
4. Take sufficient measures to improve the overall cybersecurity of the country.
5. Improve cyber literacy across all sectors to minimise the damages.
6. Employ private ethical hackers for defensive security.
7. Raise awareness about the legal measures through news to inform the society as well as the offenders.
8. Draft stronger laws with punishments while creating separate institution to address this issue.
9. Practically implement the laws making them effective.
10. Take technical steps to ensure complete destruction of suspicious links, sites, profiles, etc., and its relevant data, once penal measures have been taken.
11. Increase the number of support centres in remote areas given the spread of digital devices therein.
12. Ensure victims receive sufficient socio-legal assistance, while implementing the High Court's directives to prevent sexual harassment.
13. Ensure victims' safety and security so that no one hesitates to take steps or inform relevant authorities when they witness any act of cybercrime.

5. PREVENTING CYBERCRIME: RECCOMENDATIONS AND WAY FORWARD

Combating cybercrime requires a comprehensive approach from the use of threat intelligence solutions to a robust legal framework. Although Bangladesh recognises the importance of cyber security, its existing legal framework is not keeping pace with the evolving cyber threat landscape. The way cybercrime is handled in Bangladesh reveals flaws in many aspects of the system, from public perception on cybercrime to the operation of laws and procedures, making it difficult to combat cybercrime in the nation. The country is now at a point where it needs an approach that not only strengthens measures against cybercrime, but also protects and regulate freedom of expression in the cyberspace. Therefore, to comprehensively address the issue of cybercrime in Bangladesh necessitates a strategy that encompasses policy reform, enhancing capabilities, and creating awareness.

This research suggests the following recommendations and way forward to combat cybercrime in Bangladesh:

Policy and Legislative Reform and Simplification: To combat cybercrimes, it is imperative to reduce the significant gaps in the relevant laws by repealing or amending existing laws.

- The definition for different cybercrimes needs to be incorporated in the laws as well as proportionate punishment for perpetrators should be provided in such laws. To that end, an initiative to codify cyber related laws can be taken for effective implementation of the laws. The United States model, where cybercrime laws are well defined and strictly enforced could serve as an example.
- Make a separate law for digital forensics. Laws or policies on this subject must be brought into line with modern times.
- Legislation on cybercrime should be made through consultation with experts to ensure accuracy and effectiveness.
  Conduct an assessment and streamline the legal and procedural frameworks involved in reporting, investigating, and prosecuting cybercrimes to ensure prompt and efficient actions are taken.

Need for Laws to Protect Individual Rights: The laws on cybercrime are made from a security perspective. For example, the Cyber Security Act, the ICT Act etc are made to ensure the security of the state. There is not much capacity for human rights or individual rights here. Therefore, legislative reform is needed incorporating human rights.

Ensuring Compliance of State Intervention with International Law: Revise legislation pertaining to surveillance in accordance with human rights norms to allay worries about state spying. Implement oversight mechanisms. Authorisation for surveillance activities is necessary to guarantee that government intervention is appropriate and effective.

Establishing a One-Stop Service (Dedicated Cybercrime Unit): The police should have a separate department or cell for all types of cybercrime and data security issues, where all types of digital crime issues will be dealt with across Bangladesh. This unit shall address cybercrime cases 24/7 to reduce the filing and administrative gaps and procedural hassle as

well as to ensure proper and timely justice. In addition, there should be special support wings for women and children within this separate unit.

Strengthening Cyber Security Units: The cyber security unit should include technically capable teams and management teams along with any other relevant experts. The unit needs to be well equipped with all the essentials including modern equipment. There should be a process for regular reviewing and updating of digital security rules and digital forensic guidelines in line with global technological advancements.

Increased Availability of Digital Forensics Experts: As cybercrime cases are increasing, forensic expert needs to be increased as well. If it cannot be increased, outsourcing must be availed, and cases must be conducted and investigated with the help of tech experts. Unfortunately, till date almost zero times the police have investigated with the help of such tech experts.

Create a Cyber Unit Dealing with High-level Cybercrime and Data Security Issues: A dedicated unit dealing with High-level Cybercrime and Data Security issues, such as financial cybercrimes need to be formed to guarantee swift and efficient tackling of the cases and ensure proportionate punishment for such criminals to create deterrence in the society.

Cybercrime Unit Monitoring Online Platforms: Explicit content transactions in Telegram, Discord and many other online platforms have increased and thus such platforms need to be monitored strictly. Many, under the guise of ethical hacking, a is committing illegal hacking; hence, all advertisements and posts related to hacking should be strictly monitored. Therefore, experienced law enforcement officers in a dedicated monitoring unit needs to be established to monitor and detect potential cybercrimes on online platforms.

Specialised Training for Legal Professionals and Members of Judiciary: The Bar Council and Law Commission should arrange training programs covering the technical aspects of cybercrime and security including collecting digital and forensic evidence in handling cybercrime cases for lawyers and judges. In addition, the JATI (Judicial Administration Training Institute) should provide different types including specialised training programmes concerning cybercrime to Judges to mitigate the cybercrime incidents. Lessons can be learnt from examples of the United States and the United Kingdom, two nations that have set up cybercrime divisions and police officer training programmes. In a similar vein, designing judicial-specific training courses that focus on the legal ramifications of cybercrime can significantly improve the efficiency of the adjudication procedure in Bangladesh.

Raising Awareness: Awareness raising about cyber safety practices is vital. This can be achieved through campaigns that educate people on recognising different cyber-attacks to secure data and the significance of reporting cyber incidents. Cybersecurity education in school curriculums from an age is imperative because, in the future, cybercrime will change its variants which may be difficult for students under 18 children to detect.

Distinguishing Ethical Hacking from Criminal Hacking: Increasing awareness regarding the distinction between hacking, which aims to enhance security systems and criminal hacking which intends to cause harm or exploit vulnerabilities is of utmost importance. Ethical hackers play an important role in cybersecurity. But their work should be clearly differentiated from malicious activities. Establishing a certification system for hackers

to the Certified Ethical Hacker (CEH) program can validate their work while addressing any misconceptions.

Regulating and Monitoring Ethical Hacking Courses: To ensure the quality and credibility of hacking courses it is necessary to establish a body responsible for monitoring these courses. This body would be responsible for approving, auditing. Periodically reviewing these courses to ensure that they meet standards without inadvertently promoting exploitative practices.

Developing Strategy and Allocating Budget: Developing a strategy for cybersecurity is essential. This strategy should clearly outline government agencies', private sector, and citizens' objectives, roles, and responsibilities. Additionally, it is essential to establish an agency or task force that will coordinate and implement this strategy effectively. Adequate allocation of budget and resources towards cybersecurity infrastructure, law enforcement capabilities, and judicial processes is essential to combat cybercrime.

Promoting Rule of Law: Strengthening the rule of law is essential for combating cybercrime. Establish oversight bodies for monitoring and assessing the enforcement of cybercrime laws, ensuring accountability and transparency.

Global Cooperation: Cybercrime frequently extends beyond borders, highlighting the importance of collaboration. Bangladesh should consider enhancing its involvement with frameworks and agreements like the Budapest Convention on Cybercrime. This would facilitate cooperation in investigations and the exchange of practices across borders.

Encouraging Public Private Data Sharing Agreements: collaboration between the government and international private sector by establishing agreements to share data if needed. That can be helpful to remove offensive content which violates community standards. But these agreements should prioritise data sharing under conditions that respect privacy concerns. It is important to establish guidelines for data requests that strike a balance between state security needs and individual privacy rights thereby fostering trust and cooperation.

By realising these measures, Bangladesh can bolster its cybersecurity infrastructure, enhance its regulatory frameworks, and cultivate a more secure digital space for its citizens. To reduce cybercrime rates, we must ensure that our laws are effective, police efficiently and promptly handle cases, and cybercriminals face appropriate punishment through a robust judicial process.

6. CONCLUSION

The current world is evolving rapidly so are the forms of the cybercrimes of which women and girls are the major victims in Bangladesh. This report centres on the six most committed forms of cybercrimes in Bangladesh which are Cyber Sexual Harassment, Revenge Pornography, Financial Crime and Online Blackmail, Online Child Sexual Exploitation, Social Media Hacking and Data Breach, and Cybercrime with AI. This study investigates the consequences, underlying factors, and criminal behaviours shown by individuals engaged in cyber activities; to find solutions for the challenges presented by cyberspace based on the sound and relevant primary sources. This study also goes beyond the existing evidence and lays the groundwork for future research and policy development. It also evaluated the present laws and regulations regarding cybercrime and data protection to identify the limitations or gaps that must be addressed. The result of the conducted research allowed us to formulate several proposals to identify areas for improving legal regulation and organisation of activities to strengthen cybercrime preventive mechanisms. The research also suggested many probable preventive measures that can be adopted to combat cybercrimes. Lastly, the research suggests several detailed recommendations to combat cybercrime effectively.