International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838, Print ISSN: 2664-682X
Received: 06-09-2024, Accepted: 07-10-2024, Published: 22-10-2024
Volume 6, Issue 4, 2024, Page No. 22-30

A study based on the effectiveness of cyber security Act-2023 in pursuit of preventing cyber crime: Bangladesh perspective

Sohrab Hossain[1], Tasnuva Rashid[2*], Kamrun Nahar[3], Thahmina Akhter[4]
[1] Lecturer, Department of Law, Faculty of Law, Comilla University, Cumilla, Bangladesh
[2] Lecturer, Department of Law, Faculty of Arts and Social Science, Gono Bishwabidyalay, Savar, Dhaka, Bangladesh
[3] Lecturer, Department of Law, Faculty of Liberal Arts, CCN University of Science and Technology, Cumilla, Bangladesh
[4] Apprentice Lawyer, Human Rights Activist, District and Session Judge Court, Cumilla, Bangladesh

Abstract
People are using digital equipment to communicate with others. These have a positive side such as easy communication and short time consumption. Besides it also has the negative side that various crimes are committed through this. Such as cyber defamation, cyber fraud, and hacking by unauthorized access to the computer. So first, we have to ensure cyber security to facilitate the use of digital equipment in communication. The Government of Bangladesh enacted the Cyber Security Act like other countries in order to prevent cybercrimes. Still, the effectiveness in case of controlling Cyber Crimes doesn't satisfy the philosophy behind enacting this Act due to some vague provisions and shortcomings. This study attempts to assess the effectiveness of the Cyber Security Act 2023 in preventing Cyber Crime in Bangladesh. We strongly believe that this study will be helpful for policymakers in making the act more effective by completing its objectives.

Keywords: Cyber security, effectiveness, legal framework, prevention, hacking and malware

Introduction
Cyber Security means the security of computers and network systems so that no one is allowed to unauthorized access the computer or network systems which creates an unhealthy environment for netizens such as hacking, etc. Cyber Crimes are committed in cyberspace which is the virtual platform where humans are physically absent and it is very tough to find any evidence. Bangladesh is at serious risk of Cyber Crime and the Government has enacted many laws and policies to prevent Cyber Crimes such as the Information and Communication Technology Act 2006, the Right to Information Act 2009, and the Cyber Security Act 2023. The objective of the Cyber Security Act is to ensure cyber security and make new provisions for the detection, prevention, suppression, and prosecution of crimes committed through digital electronic means and related matters but this seems to be impossible due to the lack of process of effectiveness. Besides the main objective of the study is to find out the gap between law and reality through the assessment of the effectiveness of the Cyber Security Act 2023 in the prevention of Cyber Crimes.

Objectives
There are three objectives of this Study which are given below;
a. To show the practical scenarios of Cyber Crimes in Bangladesh.
b. To assess the effectiveness of the Cyber Security Act 2023 regarding the prevention of Cyber Crimes.
c. To establish a module through recommendations by implementing which Cyber Crimes may be removed permanently.

Literature review
For the sake of completing this research work a lot of books, journals, articles, newspapers, booklets, and periodicals have been shown below.

a. **"Cyber Crime trend in Bangladesh, an analysis and ways out to combat the threat"** [1]
This study examines Cyberattacks that have occurred in the recent past. Based on the analysis, the trend of cyberattacks in Bangladesh's banking industry has been looked at. The study is further extended to identify the causes of cyber heist in the financial sectors.

b. **Cyber crime in Bangladesh: Implications and response strategy** [2]
This article analyzes the level of cyberspace penetration in the nation and the types of dangers that come with it in an effort to assess both our susceptibility and level of preparedness. And finally, the paper suggests an outline strategy to deal with Cyber Crime in Bangladesh.

c. **A critical analysis of the escalating cyber crime and its impact in Bangladesh** [3]
The objective of the paper is to critically analyze the nature and extent of Cyber Crime in Bangladesh and its impact on individuals, businesses, and the economy as a whole. It will then examine the reasons behind the increase in Cyber Crime in Bangladesh, including factors such as inadequate cyber-security measures, low awareness among the public, and the widespread use of digital technology. Finally, this paper also discusses the challenges faced by law enforcement agencies in tackling Cyber Crime and the measures that can be taken to address this issue.

d. **"Bangladesh is at serious risk of cyber crimes" (19th September 2022 at Dhaka Tribune)** [4]
The writer expressed great concern about Cybercrimes. She said that People in Bangladesh, from every sector, have poor or no concern about how their information is spread online, and about the protection of personal information which is why Cyber Crime in Bangladesh is increasing rapidly. There

is seemingly little interest amongst the general population to find out about this virus, and they have no idea how to protect themselves against it. Unfortunately, Cyber Criminals have used this to their advantage and are seeking to exploit those fears and uncertainty for financial gain.

Research methodology

The research methodology of the study "A Study based on the Effectiveness of Cyber Security Act-2023 in pursuit of Preventing Cyber Crime: Bangladesh Perspective" has been used to analyze the legal framework to find out the gaps between the execution of Cyber Security Act and executed Cyber Crimes in Bangladesh. The present study is based on the qualitative method. This study has been conducted based on observation, fieldwork, interviews, etc. We have collected data on legal issues from primary sources, e.g., national legislation as well as secondary sources, e.g., Articles and research monographs. The following methodology has been adopted in this research. Such as Literature Review, Analysis of Legal Framework, Interviews of the various stakeholders, Case study, Analysis of contents, Analysis of collected data, etc.

Sources of data

Both primary and secondary data have been used for conducting this research. Primary sources of data for this study are relevant laws, rules, ordinances, case laws, etc. Some primary data have been collected through face-to-face interviews from the authorities of various departments or institutions that are responsible for preventing Cyber Crimes. The secondary sources of data for this study are books, published and unpublished theses, articles, legal reports, newspapers, judicial decisions, internet sources, etc. To complete this study, we have collected information from various agencies, academicians, students, and various stakeholders in Bangladesh.

The rationale of the Study

The Cyber Security Act has been enacted to rebut Cyber Crime in Bangladesh but due to vague provisions and inadequacy of punishment the act is less effective. Consequently, offenders are doing this crime without any type of fear. This study has examined this Act and found the various loopholes for its ineffectiveness. I believe that this study will be helpful to find out the different weaknesses of the existing legislation and policy which is the main hindrance of the availability of Cyber Crimes and the offender remains far from punishment.

Importance of the study

Most people are unaware of Cyber Crimes and cyber-related legislation. They do not know how this crime is committed. Besides this inadequacy of punishment is also responsible for the widespread of this crime. At the end of this study, we have given several significant recommendations to be more effective of this Act and it's a matter of hope that if the highest authority considers these recommendations, we strongly believe that Cyber Crimes will be removed.

Scope and limitations of the study

In Bangladesh, there are so many laws regarding preventing Cyber Crimes such as the Information and Communication Technology Act 2006, the Right to Information Act 2009, the Pornography Control Act 2012, etc but this Study is based on only the Cyber Security Act -2023 where Cyber Crime is related only and Bangladesh is included in this study without comparison other countries is another limitation.

Conceptual discussion

Cyber Crime is a crime carried out using digital devices and networks. To sum up, it is a type of activity that can be occurred through improperly using technology. The improper use includes using technology to commit fraud, identity theft, data breaches, computer viruses, scams, and expanded upon many other malicious acts [5].

Definition of cyber crime

1. Generally Cyber Crimes mean which crimes are committed in cyberspace using Computers and Electronic Media. Such as hacking, cyber defamation, etc.
2. According to Oxford Learners Dictionary-Cyber Crime is committed using the Internet, for example by stealing someone's personal or bank details or infecting their computer with a virus [6].
3. Porf. S.T Viswanathan has given 3 possible definitions of Cybercrimes which are as follows;
    a. Any illegal action in which a computer is the tool or object of the crime i.e. any crime, the means or purpose of which is to influence the function of a computer,
    b. Any incident associated with computer technology in which the victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain,
    c. Computer abuse is considered as any illegal, unethical, or unauthorized behavior relating to the automatic processing and transmission of data [7].
4. Cyber Crimes are classified into five categories by the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders in 2000: computer espionage, unauthorized access, damage to computer data or programs, sabotage to prevent a computer system or network from operating, and unauthorized interception of data within a system or network [8].

Types of Cyber Crime

Here, we have tried to find out the different types of improper use of technology that cause crime on individuals, property, and society that have been discussed below.

1. Phishing scam

These scams use phony emails or texts to fool victims into divulging private or business information. Cybercriminals employ social engineering techniques to deceive individuals into divulging personal data, including credit card numbers and login credentials [9].

2. Ransomware attack

This particular kind of virus prevents users from accessing data or devices indefinitely unless the data owner pays a ransom. Generally speaking, ransomware operates by infiltrating a computer system and encrypting its contents, rendering them unreadable without a decryption key [10].

3. Hacking/misusing computer networks

The act of obtaining unauthorized access to data on a computer or network is known as criminal hacking. Hackers steal data ranging from government intelligence to corporate secrets and personal information by taking advantage of flaws in these systems. Hackers also breach networks to interfere with government and corporate processes. According to the FBI, computer and network intrusions cost billions of dollars every year [11].

4. Internet fraud

Perhaps the most prevalent Cyber Crime offense is fraud which is enabled by the internet. Via websites and email addresses, criminals can conceal their identities on the internet, giving them a way to commit crimes without ever having to meet their victims face-to-face. Some criminals may also be a part of a larger criminal gang whose members are dispersed over the globe and who also never get together [12].

5. Cyber bullying

It is also referred to as cyberbullying. It involves sending or disseminating damaging and dehumanizing content about other people, which is embarrassing and may contribute to the development of psychological issues. Lately, it has been increasingly prevalent, particularly among youth. It can happen on a laptop, smartphone, or tablet and take place on websites like chat rooms, online forums, social media, email, and text messaging [13].

6. Software piracy

Software piracy can be exemplified by downloading a new, non-activated copy of Windows and using so-called "Cracks" to get a working license for Windows activation. That's seen as software piracy. Music, movies, and images can all be downloaded illegally in addition to software. According to BSA, up to 37% of software installed on personal computers worldwide is not authorized [14].

7. Online drug trafficking

The emergence of cryptocurrency technology made it simple to carry out drug trades without attracting the notice of law authorities and send money in a private, secure manner. Drug marketing on the internet increased as a result of this. Online sales and trafficking of illegal narcotics, like cocaine, heroin, and marijuana, are very popular, particularly on the "Dark Web" [15].

8. Cyber extortion

Cyber Criminals may demand money to return sensitive information they have stolen or to cease their malicious actions, such as denial-of-service assaults. This practice is known as cyber extortion. Users of your e-commerce website might not be able to buy your goods or services until you pay the hacker's requested amount if the hacker performs a distributed denial of service attack [16].

9. Intellectual-property Infringements

It is the infringement or breach of any intellectual property rights that are protected, including industrial designs, patents, trademarks, and copyrights. A wide range of actions can be considered crimes pertaining to intellectual property, including manufacturing, using, importing, or selling something without the owner's consent [17].

10. Online recruitment fraud

It is a common Cyber Crime in the present world. The fraudulent firms post job openings in order to profit financially from candidates or even utilize their personal information [18].

11. Cyber defamation

The act of making false or disparaging words about someone online or through other digital communication channels, such as social media platforms, emails, or instant messaging, is referred to as cyber defamation, sometimes known as online defamation. Cyber defamation occurs when defamation takes place with the help of computers and or the internet. E.g. someone publishes defamatory matters about someone on a website or sends an e-mail containing defamatory information to all of those friends [20].

These are the common Cyber Crimes in the world as well as in Bangladesh.

Cyber crimes in Bangladesh

Cyber Crimes are those crimes that are committed by using cyber equipment such as Computers or the internet. The world is now suffering from Cyber Crimes which is a great risk for developed countries. Yet now it has not been defined by any statutory law.

The Cyber Crime Awareness Foundation (CICAF) conducted a study between April 15, 2023, and April 15, 2024, involving interviews with 132 victims which reveals that 78.78% of the victims are young adults aged 18 to 30, and 59% are women. Notably, the rate of cyberattacks on children under 18 has decreased to 13.65% of the total cybercrimes. Victims often face severe repercussions, with 47.72% experiencing social loss, 40.15% suffering financial loss, and nearly all enduring emotional distress. Despite these significant impacts, only 12% of victims sought legal recourse, and 87.5% reported receiving no benefit from their actions. They emphasized the need for developing Indigenous cyber solutions through public-private partnerships, training, and skill development to safeguard the country's cyber sovereignty [21].

The Cyber Crime Awareness Foundation (CICAF) released another report that showed that over 73% of cybercrime victims do not seek legal counsel, and of those who do, over half felt the support was insufficient. A survey issued yesterday stated that only 7% of the victims received the support they had hoped for. According to Kazi Mustafiz, head of the organization, the information is based on comments from 199 people who got in touch with them after being the target of online abuse between February 15, 2021, and March 2, 2022. The news conference was held at the Crime Reporters Association of Bangladesh in the capital. The participants reported that they had experienced intimidation, threats of defamation, and sexual material via phone calls and social media [22].

Case study: 1

1. Birth and death registration database leak case [23]

A large-scale data leak from the nation's birth and death registration office's database was revealed by a tech-based online news outlet. Later, it was allegedly revealed that an education board had released the student's private information. A man posing as a college instructor called the parents of a student at Bakalia Government College in

Chattogram and told them their son was receiving a government stipend of 15,000 takas. With tact, this so-called teacher took down the guardian's debit card number and then the OTP code that he got on his cell phone. Everything was going according to plan until the guardian discovered that $30,000 had been withdrawn out of his account without authorization and sent to a mobile banking service number.

Case study: 2

2. The Bangladesh bank cyber heist case [24]

The Bangladesh Bank Heist of 2016 was a highly sophisticated cyberattack that resulted in the theft of over $81 million from the Central Bank of Bangladesh. The attack was a combination of social engineering, insider help, and malware, and it serves as a stark reminder of the importance of robust cybersecurity measures. The attack began on February 4th, 2016, when hackers managed to infiltrate the Bangladesh Bank's computer systems. Using a malware called "SWIFT Client," the attackers were able to gain access to the bank's SWIFT credentials, which enabled them to communicate with other banks and financial institutions around the world to transfer funds internationally. It is a matter of sorrow that CID failed to file a probe report and has now taken 80 dates to complete its probe into the case filed over the heist [25].

Case study: 3

3. Agrani Bank's client data stolen from staff's emails [26]

The 12,000 clients' data was stolen by a hacker group that gained access to the state-owned Agrani Bank Limited's email server. On May 17, the group "KillSec" then requested via the messaging app "Messenger" a ransom of ERU 5,000, or roughly 628,000 tk, in order to delete the data. On June 6, they made the client's data available on the dark web after failing to receive any ransom.

Case study: 4

4. Caught in 'Easy Money' scam case [27]

Faysal Ahmed, a pseudonym, was caught up in a web of lies that started with an innocent-seeming WhatsApp chat. Faysal was tricked into a fraudulent scheme that ultimately cost him a lot, with the promise of internet employment that paid for basic product or service reviews. He got added to the "Advanced Tasks 444" Telegram group. At first drawn by the promise of quick money, Faysal worked hard to complete the duties given to him. He did receive money for a period, up to Tk 7,895. The narrative then began to take a sinister turn. The scammer convinced Faysal to register on a website named "C-Finance" by posing as a job provider. He was required to pay Tk 9,000 as a registration fee. The stakes increased and he was instructed to submit Tk 36,000 a few days later. Faysal eventually paid Tk 9.09 lakh in various installments, only to discover afterward that he had been duped. However, it was already too late.

Reasons for cyber crimes

There are so many reasons for the rapid growth of Cyber Crimes in Bangladesh which are given below;

1. Less effective of the existing legal frameworks

There are so many laws in Bangladesh in the prevention of Cyber Crimes but due to low punishment and vague provisions these are less effective and consequently, People do not feel any hesitation to commit Cyber Crimes.

2. Availability of modern communication equipment

Many think that the availability of modern communication equipment is the main cause of Cyber Crime.

3. Easy access

Any person may get easy access to another computer through a hacking password and the offender may commit any type of Cyber Crime.

4. Difficult to identify of offense and the offender

It is very difficult to identify of offense and offender in the case of Cyber Crimes because the evidence is lost for which offenders are inspired to commit it.

5. Growth of digital marketing

Digital marketing is also responsible for widespread Cyber Crimes because here various digital payment gateway is used for payment where a great chance to commit fraud.

6. Lack of awareness

Most people are unaware of using modern communication equipment where anyone has easy access to any network or computer system and commit a crime without his knowledge.

These are the most common types of committing Cyber Crimes.

Legal Framework for the Prevention of Cyber Crimes in Bangladesh

The Government has passed some laws, rules, and policies in the prevention of Cyber Crimes where some are completely related to the prevention of Cyber Crimes, and others laws are partly related. These are given below:

a. The Information and Communication Technology Act 2006
b. The Cyber Security Act 2023
c. The Cable Television Network Management Act, 2006 (19)
d. The Cable TV Network Guidelines and Licensing Rules 2010 (09)
e. The Pornography Control Act 2012
f. The Information and Communication Technology (Amendment) Act 2013
g. The Right to Information Act 2009
h. The Mutual Legal Assistance in Criminal Matters Act 2012
i. The Mutual Legal Assistance in Criminal Matters Rules 2013
j. National Broadcast Policy 2014 (5.1.3)
k. Government E-mail Policy 2018 (14.2)
l. National Information and Communication Technology (ICT) Policy 2018 (3.2)
m. The National Mass Media Policy 2017 (amendment 2020) (3.3.1)
n. Information and Communication Technology (Investigation) Rule 2022
o. The Bangladesh Telecommunication Regulation Act 2001 (Section 66)
p. The Nari o Shisu Nirjatan Daman Ain 2000 (Section 14)
q. The Children Act 2013 (Section 81)
r. National Cyber Security Strategy 2014

These are the Legal Frameworks for the prevention of Cyber Crimes in Bangladesh. However, our present study is based on only the Cyber Security Act 2023.

Critical review on the cyber security Act 2023

First, we have to know the History of the Cyber Security Act 2023. The first Cyber law in Bangladesh was enacted in 2006. This time is called the Pre-Facebook era. There only the use of the Internet is increasing slowly. The Information and Communication Technology Act was passed in 2006 to control the crimes of that time as part of the United Nations Commission on International Trade Law (UNCITRAL). The UNCITRAL adopted the UNCITRAL model law on electronic commerce in 1996 by UN resolution 51/162 [28] with the object of providing a common legal platform for the countries to model their domestic laws relating to electronic commerce. The law provides a media atmosphere to include the operation of other laws. Although this law does not define e-commerce [29]. But the UNCITRAL model law defines 'Electronic Data Interchange' as "the electronic transfer from computer to computer of information using an agreed standard to structure the information" [30]. But when Facebook came and people became addicted to this media to a large extent, they started getting involved in various crimes. And then the government passed the Digital Security Act in 2018. But there was a lot of talk about this law in national and international circles that it is a black law where Freedom of speech is not protected. Finally, the government repealed the Digital Security Act and passed the Cyber Security Act 2023 where it has been said that the government will also enact the Cyber Security Rules. Although the Rule is not enacted yet now.

Critical Review

1. **Incomplete Law:** This Act is not a complete law because it has to take assistance from various laws such as the Code of Criminal Procedure-1898 [31], the Right to Information Act 2009 [32], the Penal Code-1860 [33], the Information and Communication Technology Act-2006 [34], etc.

2. **Priority like General Law:** There is a provision of the Cyber Security Act where it has been said that notwithstanding anything contained in the Cyber Security Act, the Right to Information Act, 2009 (Act No. XX of 2009) shall apply to a matter related to the right to information over the Cyber Security Act [35]. That means less effectiveness occurs due to less priority over the other Laws.

3. **Qualifications and disqualifications for being appointed as a director general and a director of the national cyber security agency are not mentioned**: The Government shall, by notification in the official Gazette, establish an Agency to be called the Cyber Security Agency consisting of 1 (one) Director General and such number of Directors among the persons having expertise in computer or Cyber Security [36]. But it's a matter of concern about the sentence 'among the person having expertise in computer and Cyber Security' who does not need to be a citizen of Bangladesh and finally, any person who may be also a foreign citizen has a great chance to be appointed in this post and to breach this security.

4. **Qualification of the employee in Digital Forensic Lab is not specified:** For carrying out the purposes of this Act, there shall be one or more digital forensic labs under the control and supervision of the Agency [37] and the Agency shall conduct it with suitably qualified and trained manpower [38]. But here the specific qualification of the manpower is not mentioned by this Act. The Specific Qualifications mean having expertise in the related sector. This is a vague provision.

5. **The number of members in the Cyber Security Council is excessive:** For carrying out the purposes of this Act, the National Cyber Security Council shall be composed of 16 (sixteen) members, and The Prime Minister of the Government of the People's Republic of Bangladesh shall be the Chairman of the Council [39]. Making decisions quickly will be barred due to more members and the other negative side is, the presence of the Prime Minister where other members will not feel free to give opinions.

6. **Low Punishment:** The average punishment of an offense under this Act is three to five years. Some offenses under this act can lead to death but due to low punishment offenders don't get any fear to do this offense. Such as intentionally inserting or trying to insert any virus malware or harmful software into any computer or computer system or computer network [40]; or creating pollution or inserting malware in any digital device that may cause or is likely to cause death or serious injury to a person [41], or intentionally publishes or transmits anything in the website or digital layout that creates enmity, hatred, or hostility among different classes or communities of the society, or destroys communal harmony, creates unrest or disorder, or deteriorates or advances to deteriorate the law and order situation, then such act of the person shall be an offense [42].

7. **Only Fine as Punishment:** If any person publishes or transmits any defamatory information as described in section 499 of the Penal Code (Act XLV of 1860) on the website or any other electronic form [43], then such act of such person shall be an offense and shall be fined only where the offender may be inspired to do it again.

8. **Punishment is not mentioned in the offense committed by a Company:** Where an offense under this Act is committed by a company, every owner, chief executive, director, manager, secretary, partner, or any other officer or employee or representative of the company who has direct involvement with the offense shall be deemed to have committed the offense [44] unless he can prove that the said offense was committed without his knowledge or that he made every effort to prevent the said offense. But it's a matter of concern that no specific punishment is mentioned here.

9. **Time limit for Investigation is so more:** The time limit for investigation is so more [45] which may create a bar in the establishment of justice. So, this time limit should be reduced by a mandatory order.

10. **Extra pressure on the CJM and CMM:** When a police officer has reason to believe that any offense has been committed or is likely to be committed under this Act, then he may, for reasons of such belief to be recorded in writing, obtain a search warrant upon an application to the Tribunal or the Chief Judicial Magistrate or the Chief Metropolitan Magistrate [46] which is the extra pressure on CJM and CMM. So, it should be repealed.

11. **Duration of data protection is not satisfactory:** The Director-General may order the person or organization in charge of that computer or computer system to preserve data for 90 (ninety) days if they believe that any data stored in the system should be kept for the benefit of an investigation under this Act and also the Tribunal may, on application, extend the period of preservation of such data, but it may not be for more than 180 (one hundred and eighty) days in total [47]. This data storage duration must be extended till the final disposal of the case.

12. **Bar to take Cognizance of offense directly:** The Tribunal shall not take cognizance of any offense except upon a report made in writing by any police officer [48]. The general people are discouraged from lodging complaints due to barriers under this Act.

13. **Directory Order of Taking Expert Opinion:** The Tribunal or the Appellate Tribunal, while conducting the proceedings, may take the expert opinion of any person experienced in computer science, digital forensics, electronic communications, data protection, etc [49]. Here 'may' means the directory order that has no binding force.

14. **Time-limit for disposal of Cases is indefinite:** The time limit for disposal of cases under this Act is directory order. The time fixed by this Act may be extended from time to time by written application [50]. That means no time limit is fixed for the disposal of the case within the above-mentioned time. So, in ensuring justice, this time limit should be fixed by mandatory order.

15. **Nature of Offense under this Act:** The offenses under this act are various in nature. Such as some are cognizable and others are non-cognizable [51]. All offenses under this Act should be cognizable.

16. **Confiscation order of the lawful equipment:** If any lawful computer, computer system, or any other computer equipment is found with the equipment that is liable under this Act, these are also subject to seizure [52]. It's so illegal. So, it should not be directed to seizure of that equipment is lawful.

17. **An offense committed by a Government Employee belonging to an official Computer shall not be liable to forfeitable:** If any computer belonging to any Governmental organization or any statutory body or any material or instrument related thereto is used for committing an offense, it shall not be liable to forfeiture [53]. It is the opportunity for Government employees to commit offenses by using Government equipment. So, the punishment should be increased for offenses committed by Government employee for using their official computer, material, or instrument.

We have critically examined this Act in the following ways to assess how effective it is looking forward to prevent Cyber Crimes.

Interview

To make the research more meaningful we have conducted various interviews with various people where three interviews have been given below:

1. Interview-1 (With an Advocate)

Researcher- Which Bar are you practicing as an Advocate?
Advocate- District Bar Association, Kushtia which is situated in the western part of Bangladesh.
Researcher- How many years have you been practicing at this Bar?
Advocate- More than three years.
Researcher- Are you a Civil or Criminal Practitioner?
Advocate- Both.
Researcher- Which laws are enforced for controlling Cybercrime in Bangladesh?
Advocate- Especially, the Information and Communication Technology Act 2006 and the Cyber Security Act 2023
Researcher- Has the Government taken any initiative to control Cyber Crime?
Advocate- Yes, enactment of various legislation, the establishment of Cyber Tribunal, Agreement of Cooperation with the foreign country, etc.
Researcher- Do you think that only laws are enough to control Cyber Crime?
Advocate- No, public awareness is also a need to control.
Researcher- Have you ever been the victim of Cyber Crime?
Advocate- Yes and that was 2022.
Researcher- Did you take any action for this?
Advocate- I took the initiative of mutual negotiation.
Researcher- Why you didn't take any legal steps?
Advocate- Because this is a complex procedure.
Researcher- What type of Cyber Crime is committed more often in Bangladesh?
Advocate- Cyber defamation, Cyber fraud, Cyber threat, and hacking, etc.
Researcher- Please suggest to the government how to control Cyber Crime.
Advocate- To be more effective in-laws, the creation of awareness of the people.
Researcher-Thank you so much for giving your valuable time.
Advocate- You are welcome.

2. Interview-2 (With a Judicial Officer)

Researcher- Sir, I have some questions on the effectiveness of the Cyber Security Act in order to prevent Cybercrimes if you feel free may respond to these questions.
Judicial Officer- How can I help you?
Researcher- Thanks. Sir, do you think that the Cyber Security Act is enough to prevent Cyber Crimes?
Judicial Officer- I think Cyber law is insufficient to curb Cyber Crimes.
Researcher- Sir, why our law enforcement agencies have been failed to deal with Cybercrimes?

Judicial Officer- Lack of logistical equipment, Lack of proper training, and the immaturity of the investigation officer.
Researcher- Sir, do you think that the Cyber Tribunal in Divisional City is a hindrance to prevent Cyber Crimes?
Judicial Officer- Yes, it is very difficult for a common victim to file a case and get redressal from Mofswal village to the divisional town.
Researcher- Sir, do you think that the existing forensic lab is enough?
Judicial Officer- No, only one Forensic Lab situated in Malibag is not sufficient at all for an overpopulated country like Bangladesh.
Researcher- Sir, is the enforcement of the law enough to rebut Cyber Crimes?
Judicial Officer- No, awareness programs should be conducted in every family and school regarding children.
Researcher- Sir, do you think that there are so many shortcomings in the Cyber Security Act 2023?
Judicial Officer- Yes, such as the duration of the investigation and the trial procedure is much higher which should be reduced.
Researcher- Sir, do you think that in checking Cyber Crimes, the government's initiative is satisfactory?
Judicial Officer- The government has taken many initiatives but it should be more in number.
Researcher- Sir, what kind of recommendation do you want to give to the government in checking Cyber Crimes?
Judicial Officer- The establishment of an IT cell in every district, a Tribunal in every district, more forensic labs, and well-trained personnel must be ensured.
Researcher- Thank you so much for your unlimited help.
Judicial Officer- Welcome.

3. Interview-3 (With a Victim)

Researcher- How old you are?
Victim- I am 25 years old
Researcher- Which class you are studying?
Victim- I studied till class eight.
Researcher- Do you have any idea about Cyber Crime?
Victim- I have a rough idea.
Researcher- Can you say different types of Cyber Crimes?
Victim- Yes, such as Cyberbullying and Cyber Fraud.
Researcher- Have you ever been a victim of Cyber Crimes?
Victim-Yes, that was Cyber Fraud.
Researcher- Which initiative you have taken first for this?
Victim- I did not take any initiative for my remedy because no evidence was recorded.
Researcher- Do you know that there are some laws to control this crime?
Victim- I don't know about this.
Researcher- Which things are more responsible for Cyber Crimes you think?
Victim- The low mentality of the people and the availability of smartphones and the internet.
Researcher- Do you know about visible initiatives taken by the Government to control Cyber Crime?
Victim-No.
Researcher- Do you know that, the victim may file a complaint to the Tribunal for remedy?
Victim- I have no idea.
Researcher- Do you think it should be inserted in the curriculum for more awareness?
Victim- Yes, it will be good.
Researcher- Which things are more necessary to control Cyber Crime you think?
Victim- Highest amount of punishment and execution of punishment.
Researcher- Thank you so much for your cooperation.
Victim- Most welcome.

Result discussion

For completing the research, we have taken into consideration of literature review, various interviews, and assessment of the effectiveness of Cyber Security Act 2023 and finally, it is clear to us that the application of the Cyber Security Act 2023 is enough to reduce cybercrime but not sufficient to remove permanently. So, first, the Cyber Security Act must be amended through the enhancement of punishment and clearance of various vague provisions and besides this, the people must be conscious of using Electronic Media and the personnel must be well-trained and skilled.

Findings

These are the core findings of the study which are given below;

1. It is an incomplete law.
2. This Act does not define Cyber Crime.
3. Lack of adequate coordination among the different authorities formed by law in ensuring Cyber Security.
4. Inadequate punishment is the main hindrance to Cyber Security.
5. Personnel are not well-trained in this sector.
6. Lack of awareness of the People.
7. The provision 'Mens rea' is not inserted in this Act to prove the Cyber Crime.
8. No provision has been inserted relating to cybercrime when a minor is a victim.

Recommendations

We have given a bundle of recommendations and strongly believe that Cyber Crimes will be controlled if the Government considers it. The recommendations are;

1. The average punishment under this Act is three to five years imprisonment. So, this punishment must be increased.
2. Clarification regarding Cyber Crimes, Cyber Terrorism, and False Information must be ensured under this Act.
3. The provision of Minors' offense under this Act must be inserted.
4. Autonomous must be given to the authority formed under this Act.
5. A Complete Cyber Court Must be established in every district whose Judges Panel will be experts in cyber laws and Cyber Crimes.
6. An IT Cell must be established in every district.
7. Governments' patronizing must be ensured also to the Private Sector and NGOs regarding the creation of awareness of the people in using cyber platforms.
8. Coordination and Cooperation must be increased among the authorities formed by different laws in checking Cyber Crimes.
9. International Cooperation with other states or organizations must be increased to resist Cyber Crimes.
10. A National Technical Team must be formed whose work will be to identify offenders and equipment.
11. Cyber Security must be recognized as Human Rights.

12. Strengthening the Artificial Intelligence regulations for the detection of Cyber Crimes.
13. All offenses under this act should be Cognizable.
14. A provision of 'Work in good faith of the Government, the agency and all other employees' should be inserted in this Act.
15. Well-trained law enforcement agencies must be ensured.
16. Ensuring necessary logistic equipment. Such as digital forensic lab.

Conclusion

Technology has brought speed to our national life but it has also created many difficulties. Personal Privacy protection is a human right but due to the use of this technology, this privacy is being destroyed. People are getting stuck in various obstacles by using mobile, and the internet which is not easily identified. Cyber Defamation, Cyber Threats, and Cyber Fraud are some of the serious social crimes. One of the reasons for this phenomenon is the availability of modern technology. Bangladesh is one of the countries in South Asia which is also being shadowed by various forms of Cyber Crimes. The Government has enacted various laws to ensure Cyber Security where the Cyber Security Act 2023 is one of them. The study aims to assess and determine how effective the Act is in controlling Cyber Crimes in Bangladesh. As part of the study, we have critically reviewed and evaluated this Act and finally found some shortcomings that are the main hindrance in completing the objectives of this Act. We believe that this Act is not enough to remove Cyber Crimes besides the different authorities such as law enforcement agencies, advocates, and Judges must be well trained in this sector. Finally, we have recommended some issues to consider for the Government. We are hopeful that if the Government as well as policy makers consider it based on realistic scenarios of the effectiveness of this Act then it will be module to amend the Act for which Cyber Crimes will be controlled in the future.

Acknowledgment

My co-authors deserve special recognition for their outstanding contribution to this study. I would like to acknowledge that this study would not have been completed without their continuous effort. I would also like to express my sincere gratitude to my teachers, fellow researchers, students, and the persons associated with me for their invaluable advice to help me make this study significant.

Conflict of interest

We have solely carried out this work. It has not been previously submitted to any other persons or institutions. So, there is no conflict of interest about the authorship and genuineness of this article in the present or future.

References

1. https://www.researchgate.net/publication/324468467_Cyber_crime_trend_in_Bangladesh_an_analysis_and_ways_out_to_combat_the_threat, DOI:10.23919/ICACT.2018.8323799, February 2018
2. Brigadier General Md. Khurshid Alam, ndc, psc. Cybercrime In Bangladesh: Implications And Response Strategy. Ndc E-Journal,2011:10(2):20-35. Retrieved from https://ndcjournal.ndc.gov.bd/ndcj/index.php/ndcj/article/view/82
3. Md. Sohel Rana/ CIFILE Journal of International Law (CJIL),2024:l5(9):39-48.
4. https://www.dhakatribune.com/opinion/op-ed/294341/bangladesh-is-at-serious-risk-of-cyber-crimes
5. https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybercrime.html
6. https://www.oxfordlearnersdictionaries.com/definition/american_english/cybercrime
7. Professor S.T. Viswanathan has given three definitions in his book The Indian Cyber Laws with Cyber Glossary.
8. The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders was held in Vienna on April, 2000, 10-17.
9. https://www.recordedfuture.com/threat-intelligence-101/cyber-threats/types-of-cybercrime
10. https://www.britannica.com/technology/malware
11. https://online.norwich.edu/online/about/resource-library/5-types-cyber-crime-how-cybersecurity-professionals-prevent-attacks
12. https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance
13. https://www.kaspersky.com/resource-center/preemptive-safety/cyberbullying-and-cybercrime
14. https://online.norwich.edu/online/about/resource-library/5-types-cyber-crime-how-cybersecurity-professionals-prevent-attacks
15. https://www.notguiltyadams.com/faqs/what-is-online-drug-trafficking-.cfm
16. https://www.fortinet.com/resources/cyberglossary/cyber-extortion
17. https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance
18. https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and prevention
19. TY - JOUR, AU - Khan, Niha, Vidyapeeth, Bharati, Shaikh, Anisa, PY - 2023/06/01, T1 - Understanding of cyber defamation and its impact: A critical analysis, VL-13
20. Cyber Crimes and Law by Justice Md. Azizul Haque, p-47 and Cri LJ journal, 2009, 228
21. Dhaka Tribune (29 Jun 2024)
22. The Daily Star (14 August 2022)
23. 'Students' personal info compromised, guardians deceived', Published on 22 February 2024, https://en.prothomalo.com/bangladesh/ofp8cabw1p
24. https://www.linkedin.com/pulse/case-study-bangladesh-banking-heist-digialert
25. The Daily Star (04 September, 2024)
26. https://en.prothomalo.com/bangladesh/4z5a34483c
27. https://www.thedailystar.net/news/bangladesh/news/caught-easy-money-scam-3525761
28. https://documents.un.org/doc/resolution/gen/n97/763/57/img/n9776357.pdf
29. Cyber Law and Crimes by Justice Md. Azizul Haque (2nd Edition 2023), p-41
30. Article 2(b) of the UNCITRAL model law on Electronic Commerce-1996
31. Section 42(a) & 49 of the Cyber Security Act-2023
32. Section 3(2) of the Cyber Security Act-2023
33. Section 2(b) of the Cyber Security Act-2023

34. Section 2(a & l) of the Cyber Security Act-2023
35. Section 3(2) of the Cyber Security Act-2023
36. Section 5(1) & 6(1) of the Cyber Security Act-2023
37. Section 10(1) of the Cyber Security Act-2023
38. Section 11.2(a) of the Cyber Security Act-2023
39. Sections 12(1) of the Cyber Security Act-2023
40. Sections 19(1)b of the Cyber Security Act-2023
41. Sections 27(1)b of the Cyber Security Act-2023
42. Sections 31(1) of the Cyber Security Act-2023
43. Sections 29 of the Cyber Security Act-2023
44. Sections 35 of the Cyber Security Act-2023
45. Sections 39 of the Cyber Security Act-2023
46. Sections 41 of the Cyber Security Act-2023
47. Sections 43 of the Cyber Security Act-2023
48. Sections 47 of the Cyber Security Act-2023
49. Sections 50(1) of the Cyber Security Act-2023
50. Sections 51 of the Cyber Security Act-2023
51. Sections 52 of the Cyber Security Act-2023
52. Sections 53(3) of the Cyber Security Act-2023
53. Sections 53(4) of the Cyber Security Act-2023