Journal of Law and Human Rights

Vol. 3, No. 2, 2023

ISSN 1998-4278

Cybercrime and Its Effects in Bangladesh: A Need for Necessary Legislation

Nilay Das*

Abstract: The rate of cyber and technology-related crime in Bangladesh is progressively rising. In Bangladesh, it's a big problem. Information technology has already demonstrated the emergence of a glomming menace. A couple of them are the breach of the RAB website in 2008, the prime minister's phone call, and email threats. On the other hand, cybercrime is starting to pose a threat to the government. Because there isn't enough regulation in place to deal with this kind of crime, cybercriminals are essentially free to do it. Cybercrime is addressed in numerous sections of the Information and Communication Technology Act of 2006, the ICT (Amendment) Act of 2013, and the Cyber security Act (Bill). However, the actual act is not this one on information and communication technologies. There is a possibility to turn the criminal side into the safe side by passing this act. In light of these facts, a thorough Cybercrime Protection Act ought to be implemented. This article discusses the effects of cybercrime in Bangladesh with a particular emphasis on the workplace, personal life, and policy-making bodies and thinkers. This paper, in my opinion, would be beneficial to everyone who has pertinent concerns, but especially to policymakers.

Keywords: Effect, criminal profile, legislation, cybercrime, and cybercriminals.

Introduction

The history of cybercrime is brief yet filled with significant events. In addition to being a fascinating subject in and of it, learning about the past of cybercrime would allow individuals and society to learn from past mistakes. The earliest known cybercrime occurred in 1820. That should come as no surprise given that the abacus-which is believed to be the earliest computer-has been used in China, Japan, and India since 3500 B.C. Charles Babbage's analytical engine, however, marked the beginning of the contemporary computer era. First Virtual, the first online bank, opened its doors in 1994. For hackers, this meant a lot of new chances. Cybercrime was gradually gaining popularity. The Drug Enforcement Agency (DEA) and the Secret Service obtained the first Internet wiretap, which works similarly to a phone wiretap, in 1995. The DEA was able to take down a company that was selling illegal cell phone cloning tools. Cybercrimes have increased dramatically in Bangladesh, and the country's law enforcement apparatus is

* Senior Lecturer (Law), Rabindra Maitree University, Kushtia & M Phil. Fellow, Department of Law, Islamic University, Kushtia.

having a very hard time keeping up with these technological crimes. In Bangladesh, cybercrime is already a major issue for both the public and private sectors. The utilization of technological advancement has revolutionized both the public and private sectors within the past ten years. The company lost a great deal of secret information as a result of unauthorized system intervention, which resulted in significant financial losses. As previously noted, financial institutions stand out among other organizations as the most common targets of cybercrime that also affects people's personal lives. A few development partners have begun developing strategies to combat cybercrime and enhance efficient communication.

Conceptual Statement

Cybercrime is a broad term for illegal action in which a computer or network is used as the origin, a tool, a target, or a site for criminal activity. Numerous actions can be classified as belonging to one or more of these categories, which are not mutually exclusive. While the term "cybercrime" is more appropriately limited to criminal conduct when a computer or network is an essential component of the crime, it is also occasionally used to refer to more conventional crimes involving computers or networks, such as fraud, theft, blackmail, etc. The importance of cybercrime has increased along with the use of computers. As an international crime, cybercrime affects the entire world. For organizations, law enforcement, and other stakeholders, the sophistication of cybercrime assaults and the susceptibility of information available online pose severe concerns. These attacks target not only individuals or small businesses with little means of self-defense, but also extremely big corporations.

Objectives

The article's main goal was to determine how Bangladesh's cybercrime has affected technological advancement.

The research has set out to evaluate the following specific goals:

a) Explore various cybercrime categories, delving into the characteristics of both cyber criminals and victims;
b) Examine the repercussions of cybercrime on individual targets, shedding light on the specific challenges and consequences faced by personal victims;
c) Investigate the consequences of cybercrime on organizational entities, focusing on the unique threats and vulnerabilities posed to businesses and institutions;
d) Assess the impact of cybercrime on governmental entities, outlining the specific challenges faced by government agencies and highlighting the potential risks to national security;
e) Evaluate the essential legislative measures required in Bangladesh to effectively combat and address the growing menace of cybercrime.

Cybercrime

Cybercrime, broadly speaking, refers to offenses whose genus is a conventional crime and in which a computer is either the object or the subject of the criminal activity. Cybercrime is defined as a "crime against an individual or organization committed through the use of a computer." Cybercrimes are offenses done online or in a networked environment. Cybercrime refers to criminal activities that are carried out through the use of digital technologies, computer networks, and the Internet. These illicit activities encompass a wide range of offenses, including but not limited to hacking, identity theft, online fraud, malware distribution, and various forms of

cyber-attacks. Such criminal acts exploit vulnerabilities in computer systems, networks, and digital platforms, often resulting in financial losses, unauthorized access to sensitive information, and disruption of critical services.

Cybercrime Types with the Profile of Victims and Cyber criminals and their Reasons

The newest and possibly most complex issue in the cyber realm is cybercrime. "Those species, of which the genus is the conventional crime, and where either a computer is an object or subject of the conduct constituting a crime, may be said to be cybercrime." Cybercrime is defined as any illegal behavior that makes use of a computer, either as a target, an instrument, or a way to commit more crimes.

There are two main categories of computer-related crimes:

1. Computer usage without authorization. It can be carried out either by taking control of the victim's username and password or by breaking into their machine over the Internet using a Trojan Horse program's backdoor.
2. Developing or disseminating a harmful computer program (such as a Trojan Horse, worm, or computer virus) is one way to commit cybercrime.
3. Harassment and stalking online are examples of cybercrime.

Any offenses committed with the intent to interfere with the operation of a computer or computer system, whether through the misuse of electronic media or not. The top categories of cybercrime are as follows:

Hacking

Cyber intrusions, commonly known as hacking, involve unauthorized access into computer systems without the owner/user's permission. In the context of Bangladesh, hackers often engage in such activities to acquire sensitive information. Notably, an active hacking group, purportedly led by Dr. Nuker, who claims affiliation with the Pakistan Hacker Club, has reportedly targeted websites in India, including the Indian Parliament, Ahmedabad Telephone Exchange, Engineering Export Promotion Council, and the United Nations, India.

Virus Propagation

A computer virus is a form of software designed to attack other software, leading to potential consequences such as data loss, reduced bandwidth speed, and hardware damage. Examples of malicious software include Trojan Horse, Time Bomb, Logic Bomb, and Rabbit.

Unauthorized Software Distribution

Software piracy involves the illicit copying of genuine programs or the dissemination of products intended to be passed off as authentic. This act constitutes the theft of software and undermines the rightful ownership of intellectual property.

Online Explicit Content

Pornography has been identified as one of the earliest consistently successful e-commerce products, according to the official website of the Cybercrime Investigation Cell, Crime Branch, CID, Mumbai. The use of deceptive marketing tactics and mouse-trapping technologies by pornography websites entices users, including children, to access explicit content with a simple click of a mouse on the internet.

Credit Card Fraud
When customers enter their credit card details on a vendor's website, there is a chance that credit card fraud will occur during online purchases. Hackers may utilize a breach in electronic transaction security to obtain credit card information, which they could then use by pretending to be the cardholder. The fraudulent use of computerized bank accounts can lead to significant losses in value. If someone steals and misuses another person's credit card information, they could be charged with a crime and subject to various legal repercussions.

Sale of Illegal Articles
Illegal items, such as narcotics, weapons, and wildlife, are illicitly marketed through various means, including websites, auction platforms, bulletin boards, and email communication. Some auction sites are suspected of facilitating the sale of substances like cocaine under the guise of financial transactions. This poses a significant challenge in curbing the online trade of illegal articles.

Online Gambling
Numerous websites offer online gambling, raising concerns about their potential involvement in money laundering activities. While unconfirmed, there are suspicions of a possible connection to drug trafficking.

Intellectual Property Crimes
These crimes encompass a range of activities, including software piracy, copyright infringement, trademark violations, and theft of computer source code.

Email Spoofing
Email spoofing involves emails that falsely appear to originate from one source but are sent from another. The repercussions can extend to personal relationships. In a recent incident, a branch of the Global Trust Bank faced a significant withdrawal as customers received spoofed emails falsely claiming the bank's precarious financial situation, leading to concerns about potential closure. The spoofed emails were cleverly crafted to appear as if originating from the bank itself.

Cyber Defamation
Cyber defamation is the term for defamation committed using computers and/or the internet. This type of defamation can harm a person's reputation or the standing of a business, bank, or other organization.

Cyber Stalking
Engaging in cyber stalking entails tracking a person's online activities, which may involve posting messages on platforms frequented by the victim, regularly entering chat rooms the victim uses, and incessantly bombarding the victim with emails. This behavior can cause significant distress and invasion of privacy.

E-mail Bombing
Email bombing is the act of sending an excessive amount of emails to the victim, causing the mail servers of a company or email service provider to crash, or the victim's email account to

crash in the event of an individual. Thousands of emails arrive without stopping until the targeted account or server is rendered unavailable.

Data Diddling
Data diddling involves the manipulation of raw data, typically occurring just before computer processing, with subsequent reverting to the original state after processing is complete. Government offices can fall prey to data diddling programs that are illicitly inserted during the computerization efforts of private entities.

Salami Attacks
Salama assaults, which involve minute adjustments done in such a way as to go unnoticed in certain situations, are frequently used in financial crimes. An employee of the bank may, for example, install a program on the servers that takes a small sum out of each customer's account. Even though individual account holders might not notice this illegal deduction, the cumulative effect enables the bank employee to make a sizeable monthly profit.

Causes of Cybercrime
Hart argues that "human beings are vulnerable, so the rule of law is required to protect them" in his essay "The Concept of Law." Applying this idea to the domain of cyberspace, we might state that because computers are inherently vulnerable, laws are necessary to protect them against cybercrime.

The reasons contributing to the vulnerability of computers include:

Capacity to store data in a relatively small space
Computers possess the unique ability to store data in compact spaces, making it easier for information to be accessed or compromised, whether through physical or virtual means.

Ease of access
Safeguarding a computer system against unauthorized access is challenging due to the potential for breaches not only resulting from human error but also from complex technology. Cybercriminals employ tactics such as secretly implanted logic bombs, keyloggers for stealing access codes, advanced voice recorders, retina imagers, etc., to deceive biometric systems and bypass firewalls.

Complexity
Computers operate on intricate operating systems, consisting of millions of codes. Given the fallibility of the human mind, lapses can occur at any stage. Cybercriminals exploit these vulnerabilities, penetrating computer systems to execute their illicit activities.

Negligence
The concept of negligence is intricately linked to human behavior. Consequently, there is a significant likelihood of negligence occurring while safeguarding computer systems, potentially allowing cybercriminals to exploit vulnerabilities and take control of the system.

Loss of Evidence
The loss of evidence poses a frequent and apparent challenge, particularly as data is routinely destroyed. Additionally, the collection of data beyond the territorial jurisdiction can impede the effectiveness of crime investigations in this system.

Profile of Cyber Criminals
Cybercriminals encompass diverse groups or categories, each justified by the specific objectives they pursue. The following are the categories of cyber criminals:

a) Children and adolescents aged between 6 and 18 years often exhibit delinquent behavior driven by curiosity and a desire to explore. Additionally, they may seek recognition or superiority within their peer group, and psychological factors can contribute to their actions. For instance, the Bal Bharati (Delhi) case resulted from harassment faced by the delinquent from friends.

b) Organized hackers, typically working collaboratively to achieve specific objectives, are often driven by political biases or fundamentalism. Notably, Pakistani hackers are renowned globally and frequently target Indian government sites to fulfill political aims. Additionally, entities such as NASA and Microsoft are constant targets for hackers.

c) Professional hackers/crackers are motivated by financial gains. Employed to hack rival sites and obtain credible information, they may also be tasked with identifying and rectifying system vulnerabilities to enhance security.

d) Workers who are unhappy, including those who have been fired by their company or who have grievances. Seeking revenge, they commonly resort to hacking their employer's system as a form of retaliation.

Impact of cybercrime against individuals
Cybercrimes directed on individuals comprise a range of offenses, including the dissemination of child pornography and the harassment of emails. Notable examples of cybercrimes include the trafficking, distribution, and dissemination of pornographic and other offensive material. Cyber harassment also adds to a related area: significant crimes including infringement of citizens' rights. This includes harassment that is sexual, racial, religious, or of other types.

Harassment via E-mails
Email harassment is akin to traditional harassment through letters. Bangladesh recently witnessed the urgency to address cybercrimes after threatening emails were sent to the Bengali Daily Prothom Alo, targeting prominent political figures. This prompted the establishment of the country's first cybercrime control unit, given the absence of a nationwide computer infrastructure and a dedicated security system.

Cyber-stalking
Defined as "pursuing stealthily," cyber-stalking involves tracking a person's online movements through messages on bulletin boards, chat-room entries, and constant email bombardment. This

form of harassment poses serious threats and underscores the need for effective cyber security measures.

Pornography
Online pornography takes various forms, from hosting prohibited materials on websites to the production and downloading of obscene content. Such materials can harm the minds of adolescents and lead to corruption. Notable cases include the Delhi Bal Bharati and Bombay cases, where individuals engaged in forcing slum children into obscene photographs faced legal consequences.

Defamation
Imputing false intent to lower a person's esteem, cyber defamation mirrors conventional defamation but occurs through virtual mediums. Instances include the hacking of an individual's email account to send defamatory emails, exemplified by the case where Rohit's account was compromised to spread false information about his personal life.

E-mail Spoofing
Spoofed emails misrepresent their origin, deceiving recipients about their true source. Cybercriminals exploit e-mail spoofing for various purposes, such as spreading viruses. A notable case involves Rajesh Manyar, a student falsely accused of threatening a nuclear detonation, with the spoofed email traced to his account.

Fraud & Cheating
Online fraud and cheating, a growing menace in cyberspace, manifest in credit card crimes, contractual fraud, and deceptive job offerings. Legal actions have been taken against individuals like Azim, a call center engineer found guilty of fraudulently obtaining credit card details and making unauthorized purchases online, leading to his conviction and probation.

Impacts against individuals' property
Computer Vandalism
Computer vandalism involves the intentional destruction or damage to another person's property, extending to physical harm inflicted on computers or their peripherals. Acts of computer vandalism may include theft, whether of the entire computer, specific components, or peripherals attached to the computer, as well as physical damage to computer systems.

Transmitting Virus/Worms
Viruses are programs that attach themselves to files or computers, circulating and affecting data by altering or deleting it. Worms, on the other hand, replicate without needing a host and can consume a computer's memory space. Notable instances include the Love Bug virus, affecting a significant percentage of global computers with estimated losses of $10 million, and the Internet worm released by Robert Morris in 1988.

Logic Bombs
Logic bombs are event-dependent programs designed to execute specific actions when a trigger event occurs. Some viruses may also be considered logic bombs, lying dormant until activated, such as the Chernobyl virus, which becomes active on a specific date.

Trojan Attacks
Derived from the concept of the Trojan Horse, Trojan attacks involve unauthorized programs gaining control over another system by posing as an authorized program. The installation often occurs through methods like email, as seen in a case where a cybercriminal installed a Trojan on a U.S. film director's computer during a chat, obtaining and exploiting sensitive information.

Web Jacking
Similar to hijacking, web jacking involves unauthorized access and control over another's website. Perpetrators may alter or mutilate information on the site for political or financial gain. Examples include Pakistani hackers compromising the MIT website and placing obscene content and the "goldfish" case where a site was hacked, information changed, and a ransom of US $1 million was demanded.

Internet Time Thefts
In Internet time thefts, the perpetrator gains access to a victim's login ID and password, utilizing the victim's internet surfing hours. An early case in India involved Colonel Bajwa, highlighting the challenges faced by law enforcement in understanding the nature of cybercrime.

Intellectual Property Crimes/ Distribution of Pirated Software
Offenses against intellectual property, including software piracy, copyright infringement, and theft of computer source code, constitute crimes where the owner is unlawfully deprived of their rights. A landmark judgment in Hyderabad convicted individuals for unauthorized copying and selling of pirated software, setting a precedent in addressing intellectual property crimes.

Impact of cybercrime against organizations
Unauthorized Control/Access over Computer System
Commonly known as hacking, this activity involves gaining unauthorized control or access over a computer system. However, it is important to note that the term "unauthorized access" is distinct from the legal connotation of hacking in Indian law. The 2000 Act uses a broader definition for hacking, preventing the interchangeability of these terms to avoid confusion.

Possession of Unauthorized Information
The first major cybercrime incident in the Barisal region occurred in June 2003 when cyber pirates gained access to the Internet account of the Barisal DC office. The password allowed the hackers to access the account from other places in the municipality, including an IT company, a joint secretary's and an ADC's homes, and a pharmaceutical company.

Software Piracy and Copyright
An anonymous study of more than 4,800 San Diego students found that 38% of teenagers participated in software piracy. This global issue is also prevalent in Bangladesh, where a substantial number of computer users habitually employ pirated software, contributing to intellectual property violations.

Financial Institutions at Risk
Financial institutions in Bangladesh are vulnerable to cyber security threats, particularly as more and more internet services like stock exchange trading and online banking are being

implemented. Despite these advancements, providing the highest level of security remains a challenge. Cybercriminal networks exploit vulnerabilities in the country's technology infrastructure, with recent incidents, such as the interruption of DSE transactions, causing substantial losses for small entrepreneurs.

Impact of Cybercrime against the Government

Cyber terrorism emerges as a distinct form of crime within this category, signifying the exploitation of the internet medium by individuals and groups to threaten governments internationally and instill fear among citizens. This criminal activity escalates to terrorism when an individual "cracks" into a government or military-maintained website. Reports highlight the internet's growing utilization by terrorist organizations, posing a significant global threat.

Cyber Terrorism against Government Organizations

Making the distinction between cyber terrorism and cybercrime becomes essential. Even though they are both crimes, the distinction is important. Cyber terrorism is a global issue with implications on both the home and international fronts, while cybercrime usually relates to domestic problems with potential international repercussions. Attacks on sensitive computer networks, hate websites, hate emails, and distributed denial of service attacks are examples of common online terrorist tactics. Terrorists with a strong technological background use sophisticated encryption, including 512-bit encryption, which is almost impossible to decrypt. Osama Bin Laden, the LTTE, and attacks on the US Army's deployment system during the Iraq War are a few examples. The deliberate use of disruptive activities, or threats of them, in cyberspace to advance social, intellectual, religious, political, or related goals, or to intimidate others who are pursuing these goals, is known as cyber terrorism.

Another definition broadens the scope to encompass every act of cyber terrorism, defining a terrorist as someone engaging in wanton killing, violence, disruption of essential services or means of communication, or damaging property with the intent of causing fear among the public, adversely affecting harmony between diverse groups, coercing the government, or endangering the nation's sovereignty and integrity. A cyber terrorist is an individual who uses computer systems to achieve these objectives, making every act done in pursuit thereof an act of cyber terrorism.

Legal Response to Cybercrime in Bangladesh

On September 13, the Cyber Security Bill 2023 was approved by Parliament, eliminating the need for bail for offenses falling within four of its sections. The much-discussed Digital Security Act, which prohibited bail for offenses under 14 provisions, is to be replaced by this proposal. The Bill gives police inspector-rank officers the authority to search and detain anyone without a warrant. On the other hand, filing a fictitious case is regarded as illegal and carries consequences. The Bill was moved by State Minister for ICT Division Zunaid Ahmed Palak, and it passed by voice vote. The four non-bailable offenses include hacking-related crimes, damaging computers and computer systems, breaking into critical information infrastructures, and engaging in cyber terrorism.

According to the law, there is no bail for violations against four sections. Section 17 deals with breaching critical information infrastructures, whereas Section 19 deals with computer system

damage, Section 27 deals with cyber terrorism and related offenses, and Section 33 deals with hacking-related crimes. Due to a provision that was added to the proposed bill, the cases that have already been filed will be governed by the Digital Security Act. Sections 17 through 33 of the draft Cyber Security Act 2023 list the violations and associated penalties. Opposition party members criticized different provisions of the Bill, claiming that the constitution already grants freedom of speech and recognition to independent media. Nonetheless, the system of restricting these constitutionally guaranteed rights has been guaranteed by a number of this Bill's sections.

Several participants called for changes to the rules regarding warrantless searches and arrests. State Minister Palak responded to these criticisms by stating that although the constitution recognizes freedom of thought and expression, it is not unrestricted." Being free does not entail infringing upon the rights of others. Saying whatever comes to mind does not equate to freedom. It's not about treating people badly," he declared. He claimed that everyone in the opposition agreed that the bill is necessary. "The Cyber Security Act is the only option for creating a transparent, responsible, and safe Smart Bangladesh."

The Bill now includes a new section on the offense of submitting false complaints and cases, as well as the associated penalties. According to this section, it is illegal for anybody to submit or make a complaint under any section of this act knowing that there is no legitimate reason to do so, to hurt someone else. Both the person who submitted the complaint and the person who filed the action in this instance will be penalized by the guidelines for the initial offense. The amount of the penalty for the major offense, which is greater than the other offenses listed in the relevant section, may be decided if a case or complaint is filed under more than one part of this act.

The bill states that a tribunal may accept a written complaint from an individual and hold a trial for the offense of making a false complaint. The bill's Section 42 gives police the authority to search and detain anyone without a warrant. Inspector-level officers in this section have taken the place of sub-inspector-level officials and are authorized to search and make warrantless arrests. The Digital Security Act also contained this provision. The ability to erase and prevent data from digital media is granted by Section 8 of the bill. According to this section, law enforcement agencies "subject to data analysis, have reason to believe" that any information released or distributed via digital or electronic media could have an impact on the nation's or any region's economic activity, security, defense, cohesion, or religious practices.

If such material violates morals or public order or incites hatred towards people of color, law enforcement organizations may request, via the Director General of the BTRC, that it be blocked or removed. According to Gonoforum MP Mukabbir Khan, this law is among the best at stifling free speech and criticism. It has only been used to stifle criticism directed at either the ruling party or the government over the past four and a half years. He claimed that when it comes to using the law, journalists have suffered the most. "This legislation has significantly restricted their ability to express themselves. The police are now able to search bodies and enter residences thanks to this act. It has granted unrestricted authority to take control of any computer network, including servers. The police now have more authority than under any other statute. According to MP Fakhrul Imam of the Jatiya Party, the law has changed in several ways. However, reporters expressed their dissatisfaction.

The Constitution guarantees the right to freedom of expression, ideas, and the press. The fundamental law is the Constitution. A law restricting the right to free expression would be unconstitutional.

The Digital Security Act, according to Jatiya Party MP Pir Fazlur Rahman, was divisive for all people. All that the Cyber Security Act does is alter it. Additionally, this will impede the practice of free journalism and expression. Arrests without a warrant are authorized by Article 42. The Act mandates that journalists have extra protection. He claimed that the Press Council could exercise some degree of oversight. Opinion expression is guaranteed by the constitution. There are obstacles to the freedom of thought and expression because of this law. According to him, instances under the Digital Security Act involving journalists make about 27% of all cases. The plaintiffs are typically members and staff of the ruling party.

According to Shamim Haider Patwari, a Jatiya Party MP, this law is required for some technical concerns. However, there hasn't been much application of digital security law in these situations. According to him, claims of damage to consciousness and sentiments are the basis for the primary lawsuit. He asserted that freedom of speech, press, and mind are guaranteed by the Constitution. These laws are unconstitutional as they currently stand. With certain sentencing reductions, the Act maintained the same meaning of the offense. The media will censor themselves more as a result of this rule. Hafiz Uddin Ahmad, a member of the Jatiya Party, stated that he opposed Section 42 and suggested that it be removed along with all other unconstitutional parts. According to MP Mujibul Haque of the Jatiya Party, writers write for the benefit of the nation. "The Press Council could have been involved in their problems. Article 42 authorizes the power of warrantless arrests. The misuse of this law is a risk.

Offences	Penalty in the DSA	Penalty in the CSA
Section 21: Propaganda against the spirit of the Liberation War, the father of the nation, the national anthem, or the national flag	Ten-year imprisonment	Seven-year imprisonment
Section 28: Offence of hurting religious sentiments	Five-year imprisonment (non-bailable offense)	Two-year imprisonment (bailable offense)
Section 29: Defamation in the context of news coverage	Three-year imprisonment	No imprisonment, a maximum fine of tk. 25 lakh will be imposed, three to six months in jail in default of payment.
Section 31: Destroying communal harmony	Seven-year imprisonment	Five-year imprisonment
Section 32: Disclosing Official Secrets	Fourteen-year imprisonment	Seven-year imprisonment

Chart 1: The Most significant changes under the CSA are shown in the chart

Cyber Tribunal

As per Section 68 of the Information and Communication Technology Act, 2006, the government is mandated to establish one or more cyber tribunals for the expeditious and efficient

adjudication of cases under the Act. These tribunals exclusively handle offenses specified in the Act, and the government determines their local jurisdiction. In consultation with the Supreme Court, the government appoints a Sessions Judge or Additional Sessions Judge as the judge of the Cyber Tribunal.

The Cyber Tribunal initiates a trial under the following circumstances:

i. Based on a report from a police officer not below the rank of sub-inspector.
ii. Upon a complaint filed by a controller appointed under this Act or any other person authorized by the controller.

The trial procedure follows Chapter 23 of the Criminal Procedure Code, 1893 (Trial Procedure by the Court of Sessions) to the extent that it is consistent. If the accused is absconding, the tribunal can proceed with the trial in absentia. In such cases, the tribunal issues an order published in two Bengali newspapers, summoning the accused on a specified date. The Cyber Tribunal applies the provisions of the Criminal Procedure Code, possessing the same powers as a Sessions Court in its original jurisdiction. The trial must be concluded within six months from the date of framing charges, with an option for a three-month extension. The tribunal pronounces its judgment within ten days after concluding the trial, with the provision for a ten-day deferral.

Cyber Appellate Tribunal

The government is required to establish one or more cyber appellate tribunals. Each appellate tribunal comprises a chairman and two members appointed by the government. The chairman must be either a former judge of the Supreme Court, a sitting judge of the Supreme Court, or eligible for a Supreme Court judgeship. One member must be a retired District Judge or a current member of the judicial service, while the other must possess expertise in information and communication technology. Appointments are made for a term of 3-5 years.

The Cyber Appellate Tribunal does not have original jurisdiction; its role is to hear and dispose of appeals from the orders and judgments of the Cyber Tribunal and Sessions Court in appropriate cases. The decisions of the appellate tribunal are final, with the power to alter, amend, or annul the orders and judgments of the Cyber Tribunal. The appellate tribunal follows the appellate procedure of the High Court Division of the Supreme Court. In the absence of a cyber-appellate tribunal, appeals may be heard by the High Court Division.

Conclusion

In conclusion, as of now, Bangladesh has not experienced any significant cybercrime. However, the increasing reliance on computer and information technology by financial institutions, banks, insurance companies, and other non-government organizations raises concerns about the potential for cybercrime. While the use of computers for criminal activities, such as creating forged certificates and documents, has been observed in Bangladesh for some time, incidents directly targeting computers or computer systems remain relatively uncommon. The evolving landscape of technology adoption in the country underscores the importance of vigilance and proactive measures to address the potential risks associated with cyber threats.

References

1. Verton, Dan (2003), Invisible threat of cyber-terrorism, New York, NY: McGraw-Hill/ Osborne.
2. Ahmed, Dr. Zulfiquar, 2012 - Cyber Law in Bangladesh, National Law Book Company, Dhaka,pp-221-265
3. Tarun,2013“CyberCrime”,LSI.p.l.accessedon,http://www.legalserviceindia.com/articles/cyber.htm
4. Karzon Sheikh Hafizur Rahman, 2008-Theoretical and Applied Criminology, PalalProkashoni,Dhaka,pp-411-418
5. Nahar, Dr. Nurun, 2011- Fundamentals of Cyber Law, Bangladesh Law Book Company, Dhaka,pp-15-28
6. Kader, Monjur, 2008-Criminology (Cybercrime), University Press, Dhaka, pp-125-129.
7. BohamandHaley(2002)-InternetCrime,ThirdEdition,McGrasw-Hill,NewYork,p-137
8. DuggalPawan,http://www.slideshare.net/anthony4web/cribercrimes-and-due-diligence.
9. Nagpal R-What is Cyber Crime. http://issuu.com/rohas/does/ece
10. Ronald B. Standler, Collected from Internet, See http://www.rbs2.com/crime.htm.
11. http://www.asianlaws.orgiccyberlawlibrary/cc/what_cc.htm
12. Cyber Crime by partha sarathi patil http://www.naavi.org/pati/pati_cybercrime_dec03.htm.
13. Daily Prothomalo_23 August, 2004.
14. www://naavi.org)
15. E daily star_news_30.10.2008
16. Business_Standard_News_04.02.2024.
17. www-crime-research.org/library/cyber-terrorism.htm.
18. https://www.dhakatribune.com/bangladesh/325228/parliament-passes-cyber-security-bill 2023.
19. Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., & Savage, S. (2012). Measuring the Cost of Cybercrime. In Workshop on the Economics of Information Security (WEIS).