'Navigating Cyber Security Challenges and Legal Frameworks in Bangladesh: An In-Depth Exploration'

Ms. Suraya Momtaz

Assistant Professor, Department of Law,

Southern University Bangladesh, Country: Bangladesh

DOI: https://dx.doi.org/10.47772/IJRISS.2024.801056

Received: 29 December 2023; Accepted: 04 January 2024; Published: 02 February 2024

ABSTRACT

This paper implies a comprehensive exploration of the landscape concerning cyber security issues and the associated legal structures in the context of Bangladesh. It suggests a study or analysis that delves into the complexities of managing and addressing cyber security challenges within the country while concurrently examining the existing legal frameworks that govern cyber-related activities. This title indicates an intention to explore how individuals, organizations, and the legal system navigate the intricacies of cyber security concerns and the laws and regulations aimed at addressing them within the specific context of Bangladesh.

INTRODUCTION

In essence, cyber security serves as the proactive defense against cyber crime. It involves the tools, practices, and strategies aimed at preventing, detecting, and responding to malicious activities in the digital space. Cyber crime, on the other hand, encompasses various illegal activities conducted using computers and networks, exploiting vulnerabilities and causing harm to individuals, organizations, or systems. Strong cyber security measures are crucial in mitigating and combatting cyber crime threats. The term *cyber crime* is synonymous with the term *computer-related crime,* which, in turn, may involve only with a computer or it may involve cyber crime implying the use or abuse of computer networks, such as the Internet, for criminal activity. Cyber crime has had a short but highly eventful history.[1] Apart from being an interesting study by itself, observing the history of cyber crime would also give the individual and society the opportunity to avoid the mistake made in past. The past recorded cyber crime took place in the year 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.[2] In 1994 the first online bank opened, called First Virtual. This opened up a lot of opportunities for hackers. Cyber crime was slowly becoming more popular. In 1995 the Secret Service and Drug Enforcement Agency (DEA) obtained the first Internet wiretap, which is exactly like a phone wiretap. The DEA was able to shut down a company who was selling illegal cell phone cloning equipment.[3] It is a *network of networks* ***[4]*** that consists of millions of private and public, academic, business and government networks of local to global scope that are linked by copper wires, fiber-optic cables, wireless connections, and other technologies. The World Wide Web is a huge set of interlinked documents, images and other resources, linked by hyperlinks and URLs. In October 2023, there were 5.3 billion internet users worldwide, which amounted to 65.7 percent of the global population.[5] Of this total, 4.95 billion, or 61.4 percent of the world's population, were social media users. In developing world Internet users are about 57% and in developed world it is amount to 90%. [6] The country now has over 12.61 crore internet users, according to the latest data of the Bangladesh Telecommunication Regulatory

Commission (BTRC).[7]Of them, more than 11.40 crore are mobile internet subscribers and 1.20 crore broadband users.[8]

SIGNIFICANCE OF THE RESEARCH

This research investigates the approaches for countering computer crime in Bangladesh comparing the other countries, in the context of the guidelines of international organizations, such as the CoE and the Financial Action Task Force (FATF). It does so in order to identify how improvements are needed in combating cyber crime globally specifically in Bangladesh. This paper examines the approaches used for a critical analyzing and combating cyber crime in, Bangladesh which represent a spectrum of economic development and culture. In the case of Bangladesh, we also examine the causes and effect of recent incident of hacking of Bangladesh Bank‘s reserve.

Research Objectives

The objective of this thesis is to analyze the extent to which there is a common and effective approach to combating cyber crime nationally and the extent to which such efforts are succeeding and improvements are needed in Bangladesh. This paper examines the nature of cyber crime and the different and sometimes contrasting definitions and taxonomies that are used to classify computer crime and cyber crime, and proposes some elaborations to those. It also reviews and compares the current legislation for combating computer crime and cyber crime used in Bangladesh. We address the following more specific objectives:

- To review and analyze different definitions and taxonomies of
- To review and compare the current legislation for combating computer crime and cyber crime used in Bangladesh to ensure cyber security as well.

Research Question

Arising from the above, the following specific research questions have been formulated:

Q-1: How well-suited are the existing definitions and classifications of Cyber crime, along with the current legislation, for ensuring cyber security in Bangladesh?

Q-2: What measures can enhance the international consistency and precision in reporting computer-related crimes and their prosecution, and what enhancements are necessary?

Q-3: What viable approaches exist to diminish cyber crime, and how feasible are their applications to ensure cyber security in Bangladesh?

RESEARCH METHODOLOGY

This Paper is based on analytical and descriptive in nature. It was almost difficult to do wide fieldwork because of lack of time and opportunity. This paper is based on secondary data collected from text-books, journals, Newspaper, websites etc. The collected data have been processed and prepared in the past form in order to make the study more informative, analytical and useful for the users.

Conceptual Issue: Cyber crime

A primary problem for the analysis of cyber crime is the current absence of a consistent definition.[9] Cyber crime is a container-concept that holds many different crimes, performed in almost complete concealment by anonymous and creative offenders, in different contexts and in a continuous digitalizing era. The

definition of cyber crime is extremely wide and can be interpreted in many different forms. The definitions of cyber crime have evolved experientially.[10]Cyber crime is a term that most people will still define as hacking or a virus. As of today, cyber crime has grown than just the later: cyber crime is a pervasive threat for today‘s Internet dependent society.

Under the Cyber crime Act 2001 of Australia, the term cyber crime refers to crimes that target computer data and systems. The USA Department of Justice, Computer Crime and Intellectual Property Section, defines computer crimes as ‘crimes that use or target computer networks, which we interchangeably refer to as computer crime, cyber crime, and network crime and refers to viruses, worms and Denial of Service attacks.

A working definition is offered by Thomas and Loader (2000), who conceptualized cyber crime as ‘computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks’[11].

A prominent Advocate Daggal Pawan Specialist on cyber crime define as ‘any criminal activity that uses a computer either an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime.[12]

Characteristics of Cyber Crime [13] Before examining the legal strategies to check cyber crime, it is necessary to examine the peculiar characteristics of cyber crime:- Cyber crime thrives on technology as its primary tool. Those behind cyber crimes are tech-savvy individuals—essentially technocrats—proficient in navigating the intricate realms of computers and the internet.

1. The efficiency of cyber crime is unparalleled; it operates in real-time, achieving website breaches or fraudulent activities within mere seconds or minutes.
2. Geographical boundaries mean nothing to cyber crime. A perpetrator sitting in one corner of the globe can instantly infiltrate systems located continents away. For instance, a hacker based in the US can swiftly breach a system stationed in Japan.
3. Cyber crime unfolds in cyberspace, where the criminal exists physically outside this realm. Every phase, from planning to execution, occurs within this digital domain.
4. The potential damage inflicted by cyber crime is staggering. It can obliterate heavily invested websites or infiltrate high-security platforms like banks and defense departments, resulting in colossal losses.
5. Proving cyber crime in a court of law poses immense challenges due to the elusive nature of the cyber criminal, their anonymity, and the ability to simultaneously impact multiple countries beyond their physical location. Gathering concrete evidence becomes a complex task in such scenarios.

Cyber Crime v/s Conventional Crime :

Cybercrime is the most complicated problem in the cyber world. Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime.[14] Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime‖.[15] Some people suggest that the advent of virtual crimes‘ marks the establishment of a new and distinctive social environment with its own ontological and epistemological structures, interactional forms, roles and rules, limits and possibilities. Other people see cyber crime‘ as a case of familiar criminal activities pursued with some new tools and techniques. Grabosky [16] suggested that cyber crime was simply ‘a case of old wine in new bottles’. If this was the case, cyber crime could be fruitfully explained, analysed and understood in terms of established criminological classifications.[17]. Apparently, there is no distinction between cyber and conventional crime. However, on a deep introspection we may say that there exists a fine line of

demarcation between the conventional and cyber crime, which is appreciable. The demarcation lies in the involvement of the medium in cases of cyber crime.

In contrast to the off-line world where criminals need to be physically present at the crime scene and can commit one offence at a time, criminals in cyberspace do not need to be close to the crime scene, they do not have to travel to the target country, and can attack a large number of victims globally with a minimum of effort and risk through hiding their identity.[41] The information capabilities of the Internet change the nature of crime, as they provide cyber criminals with simple, cost effective and repeatable means of conducting rapid global-scale attacks, while remaining anonymous and/or unreachable for law enforcement.[42] Cyber crime opens new doors to criminals where they have the power to defraud entire institutions in ways that would not have been possible traditionally. Housing billions of gigabytes of sensitive information and valuable date, the Internet is very appealing to criminal organizations, who can act anonymously (and so remain more unpunished). Finally, one of the differences between cyber crime and traditional crime is the evidence of the offenses: traditional criminals usually leave traces of a crime, through fingerprints, physical evidences. On the other hand, cyber criminals rely on the Internet via which they commit their crimes, and leaves little evidence.

What motivates individuals to engage in cyber criminal activities?

Cyber criminals find motivation in various facets—be it a sense of curiosity, the pursuit of notoriety, monetary gain, gratification of personal desires (like stalking or harassment), political agendas (such as activism), espionage, or even engaging in cyber warfare. However, upon investigation, financial gain emerged as the primary driving force behind cyber crime. Testimony revealed that cyber crime has evolved into a highly profitable venture, leveraging cyber attacks involving personal data theft, fraudulent activities, unauthorized access to financial systems, and online extortion. Moreover, an underground economy has emerged, enabling cyber criminals to trade goods and services associated with cyber crime for monetary benefits.[44]

What are the common demographics of individuals involved in cyber crime?

A variety of different people commit cyber crime including individual hackers, organised crime groups, corrupt company employees and foreign intelligence operatives.[18] Witnesses suggested that, currently, perpetrators of cyber crime tend to be financially-motivated organised criminal networks with decentralised and flexible structures, and consisting of members from a variety of different countries. The majority of these attacks are said to originate from outside of Australia.[19] organised cyber criminal networks differ from traditional real world‘ organised crime groups in that there is not necessarily a hierarchical structure where all cyber attacks committed through the network are coordinated from the top. These criminal networks have a decentralised structure where members are anonymous and relatively independent. When a cyber criminal, or group of cyber criminals, wishes to commit a cyber attack, they may use the network to source the resources and skills for that particular operation.[20]

These cyber crime networks may consist of members from many different countries. The Committee heard that most cyber attacks appear to originate from America, China, Europe and Russia. It was also stated that organised criminal networks are appearing in South-East Asia. It was suggested that cyber criminals may find it easier to operate in countries were governmental institutions or the rule of law is not as strong, or where cyber crime makes a significant contribution to the growth of a developing economy.[48]

Cyber crime networks also target users from other countries in order to take advantage of traditional law enforcement boundaries that make it much harder for their crime to be investigated. [49]

Who are the victims of cyber crime?

The spectrum of cyber crime victims is diverse and expansive. It encompasses individuals, businesses, governmental organizations, and even entire sectors. Individuals fall prey to cyber crime through various means like identity theft, online scams, or personal data breaches. Businesses face significant risks, from financial fraud to intellectual property theft, impacting their operations and credibility. Governmental bodies encounter cyber threats jeopardizing sensitive information and national security. Additionally, sectors such as healthcare, finance, and education grapple with cyber attacks that disrupt services and compromise critical data. Ultimately, anyone connected to the digital realm is susceptible to becoming a victim of cyber crime. Home users are also vulnerable to cyber attacks due to low levels of online security. Cyber criminals seek information and money from home users through the use of scams, phishing schemes and malware. Due to their low level of security, home computers are highly vulnerable to being recruited to botnets.[21] Additionally, home users that fall victim to an online scam are more likely t be targeted by further scams. Cyber criminals note users who have responded to scams and place them on asucker list 'which may then be used to distribute further scams to these vulnerable home users.[22][55]As the Internet is a resource shared among several different sectors of society, attacks on one section of Australian society may have flow on effects for other areas of society. [23]For example, due to the vulnerability of home users, botnets are often comprised predominantly of home computers. These botnets can then be used to launch attacks against businesses and governments.[24]

Nature of Cyber Crime [25]

A cyber criminal can destroy websites and portals by hacking and planting viruses, carry out online frauds by transferring funds from one corner of the globe to another, gain access to highly confidential and sensitive information, cause harassment by e-mail threats or obscene material, play tax frauds, indulge in cyber pornography involving children and commit innumerable other crimes on the Internet. It is said that none is secure in the cyber world. The security is only for the present moment when we are actually secure. With the growing use of the Internet, cyber crime would affect us all, either directly or indirectly.

Kinds of Cyber Crime

In our modern era, computers have transitioned from mere conveniences to indispensable tools woven into the fabric of our daily existence. While many of us possess only a cursory understanding of computer security threats, we're familiar with terms like "virus" and "worm." However, it's crucial to delve deeper into the realm of cyber activities where computers serve as instruments for unlawful deeds. These illicit actions often entail adapting traditional crimes through computer utilization. Below lies a compendium of prevalent cyber crimes, some of which wield extensive reach and substantial harm.

Hacking

_Hacking' is a term with multiple meanings. It can refer to testing and exploring computer systems, highly skilled computer programming or the practice of accessing and altering other people's computers. Hacking may be carried out with honest aims or with criminal intent. [26]

In relation to cyber crime, and for the purpose of this report, hacking refers to the practice of illegally accessing, controlling or damaging other people's computer systems. A hacker may use their own technical knowledge or may employ any of the cyber crime tools and techniques that are listed below.

Malicious software (Malware)

Malware is a general term for software designed to damage or subvert a computer or information system.[27]

A range of different types of malware exists:

viruses, worms and trojans are pieces of computer code or computer programs that automatically infiltrate computer systems, to degrade computer performance or to deliver other types of malware.[28] a backdoor permits a computer to be remotely controlled over a network,[29] rootkits are sets of programs that hide malware infections on a computer by concealing infected files and turning off anti-virus protection programs;[30] and keystroke loggers and spyware are programs that illegally capture data from a computer (spyware is related to a legitimate type of software called adware, described below).[31]

Virus, Trojans and Worms [32]

Trojans and Worms a computer virus is a programmed designed to replicate and spread, generally with the victim being oblivious to its existence. Computer viruses spread by attaching themselves to programmers like word processor or spreadsheets or they attach themselves to the boot sector of a disk. When an infected file is activated or when the computer is started from an infected file is activated or when the computer is started from an infected disk, the virus itself is also executed. Just as a virus can infect the human immunity system there exist programs, which, can destroy or hamper computer system. Trojan horse is defined as a ―malicious, security-breaking program that is disguised as something benign‖ such as a directory lister, arc hiver, game, or a program to find and destroy viruses. A computer worm is a self-contained program that is able to spread functional copies of itself or its segments to other computer systems. Unlike viruses, worms do not need to attach themselves to a host program.

Cyber Pornography [33]

Cyber pornography refers to the distribution, production, or consumption of sexually explicit content facilitated through digital means, particularly over the internet. This includes images, videos, or any form of explicit material that is accessed, shared, or created using digital devices and online platforms. Cyber pornography can involve various legal and ethical issues, particularly concerning consent, age, and the exploitation of individuals. Almost 50% of the web sites exhibit pornographic material on the Internet today. Pornographic materials can be reproduced more quickly and cheaply on new media like hard disks, floppy discs and CD-ROMs . Another great disadvantage with a media like this is its easy availability and accessibility to children who can now log on to pornographic websites from their own houses in relative anonymity and the social and legal deterrents associated with physically purchasing an adult magazine from the stand are no longer present. Furthermore, there are more serious offences which have universal disapproval like child pornography and far easier for offenders to hide and propagate through the medium of the Internet.

Spam

Spam refers to unsolicited emails, or the electronic equivalent of junk mail. Spam is often disseminated in large amounts by sending out generic emails to large lists of email addresses.[34] Spam may be sent through normal email accounts provided by an ISP, free online email services such as Hotmail, hijacked email servers, offshore companies that specialise in sending bulk mail, or the large number of computers connected to a botnet. [35][69] Additionally, in order to avoid anti-spam programs that identify generic emails or offending spammer email addresses, spammers employ programs which subtly change each email or hide the actual spammer‘s email address.[36] Spammers can acquire lists of email addresses by: using different pieces of address- harvesting software to locate, steal, decipher and compile email addresses; hacking into the information systems of organisations; creating fake websites which fool users into entering their email address on the website; or through buying lists of email addresses on the black market.[37] Spam has a variety of uses including: the mass delivery of legitimate advertising;the mass delivery of scams and

phishing schemes;33 and the delivery of malware and in turn the expansion of botnets.[38]

Cyber Stalking [39]

Cyber Stalking can be defined as the repeated acts harassment or threatening behavior of the cyber criminal towards the victim by using internet services. Stalking in General terms can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, vandalizing victim‘s property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim and the same has to be treated and viewed seriously. It all depends on the course of conduct of the stalker. Stalking is a problem that many people especially women is familiar with real life. These problems occur on the Internet as well, in what has become known as cyber stalking or on line harassment.

Phishing

Phishing describes an online attempt to assume the identity of, or mimic, a legitimate organization for the purpose of convincing users to divulge personal information such as financial details, passwords, usernames and email addresses.[40] The AIC provided the following example of a phishing website.

Figure 2.1 shows the top section of a web page which appears to be from the legitimate Bank of the West ‘website.

Figure 2.1 Example of phishing website

Source-Australian Institute of Criminology, Exhibit No. 5, p. 8.

However, as demonstrated below in Figure 2.2, upon closer inspection of the address in the top bar of the browser, it can be seen that the W in Bank of the West‘ has been replaced with two V‘s to give the appearance of a W.

Figure 2.2 Close up of web address in phishing website

Source-Australian Institute of Criminology, Exhibit No. 5, p. 8.

Cyber Terrorism [41]

Cyber terrorism may be defined to be —the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to

intimidate any person in furtherance of such objectives. ‖ The role of computer with respect to terrorism is that of modern thief who can steal more with a computer than with a gun. The terrorist may be able to do more damage with a keyboard than with a bomb. Computer and information technology has exploded in recent times. No doubt, the great fears are combined in terrorism; the fear of random, violent, victimization segues well with the distrust and out-rights fear of computer technology.

Identity theft and identity fraud

Through the use of keystroke loggers, spyware, and phishing websites cyber criminals may obtain a wide range of personal details. This is known as identity theft. These stolen details may then be used to commit identity fraud‘ (such as illegally accessing a victim‘s bank or credit card account, or taking out loans under a victim‘s name), sold online to other cyber criminals or used to fabricate fake official documents such as passports.[42] Stolen information may also be used to commit further cyber crime activities. For example, a cyber criminal may use a stolen identity to open a new Internet account with an ISP from which to commit criminal acts.[43]

Cyber Crime Related to Finance [44]

There are various types of Cyber Crimes which are directly related to financial or monetary gains by illegal means, to achieve this end, the persons in the cyber world who could be suitably called as fraudsters uses different techniques and schemes to be fooled other peoples on the internet. Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. It may assume different forms. Some of the cases of online fraud and cheating that have come to light are those pertaining to credit card crimes, contractual crimes, online auction frauds, online investment schemes, offering jobs, etc.

Cyber Crime with Mobile & Wireless Technology [45]

At present the mobile is so developed that its becomes somewhat equivalent to personal computer, as we can do a lot of work on our mobile phones which were earlier possible on the computers only, such as surfing, sending e-mails etc. There is also increase in the services which were available on the mobile phones such as Mobile Banking which is also prone to cyber crimes on the mobile as it is on the Internet. Due to the development in the mobile and wireless technology day by day, the day is not far away when the commission of cyber crimes on the mobile will become a major threat along with other cyber crimes on the net.

Denial of Service Attack (DoS Attack)

A Denial of Service (DoS) attack refers to a malicious attempt to disrupt the normal functioning of a network, system, or online service by overwhelming it with a flood of excessive traffic or requests. The primary goal of a DoS attack is to make a website, server, or network resource unavailable to its intended users by exhausting its resources or causing it to crash. This is typically achieved by flooding the target with an overwhelming volume of data, thus rendering the system unable to respond to legitimate requests. DoS attacks can cause significant downtime, loss of revenue, and disruption of services for the targeted entity. It is very difficult to control such attacks. The attack is initiated by sending excessive demands to the victim‘s computer‘s, exceeding the limit that the victim‘s servers can support and making the server‘s crash. Denial-of-service attacks have had an impressive history having, in the past, brought down websites like Amazon, CNN, Yahoo and eBay.[46]

E-mail Bombing

Email bombing refers to a cyber attack in which an individual or group inundates an email account with an

overwhelming volume of emails, rendering the account unusable. This attack aims to overwhelm the recipient's inbox, causing it to exceed its storage capacity or making it incredibly difficult for the user to find and access legitimate emails among the flood of incoming messages. Email bombing can disrupt communication, hinder productivity, and potentially cause the email service to malfunction or become temporarily inaccessible. In the Russian internet community, there is another sense for mail bomb. There, mail bomb is a form of denial of service attack against a computer system (mail server). After most of the servers began checking mail with antivirus software, the Trojan viruses tried to send themselves compressed into archives, such as ZIP or RAR. Then mail servers began to unpack archives and check their contents too. That gave black hats the idea to make a huge text file, containing, for example, only the letter z repeated millions of times. Such a file compresses into a relatively small archive, but being unpacked by early versions of mail servers might waste the free space on its disks and cause denial of service Also known as a Zip bomb.[47]

E-mail Spoofing

Email spoofing is a deceptive technique used by malicious actors to falsify the sender's identity in an email message. In this practice, the sender manipulates the email header information to make it appear as though the message is originating from a different source than the actual sender. This technique is often employed to trick recipients into believing that the email is from a legitimate or trusted source, increasing the likelihood of the recipient opening the message or taking action, such as providing sensitive information or clicking on malicious links. Email spoofing can be used for phishing attacks, spreading malware, or carrying out other forms of cyber crime by exploiting the trust associated with recognizable email addresses or domains. E-mail spoofing is possible because Simple Mail Transfer Protocol (SMTP), the main protocol used in sending e-mail, does not include in authentication mechanism. Although an SMTP service extension allows an SMTP client to negotiate a security level with a mail server, this precaution is not often taken. If the precaution is not taken, anyone with the requisite knowledge call connects to the server and use it to send messages. To send spoofed e-mail, senders insert commands in headers that will alter message information. It is possible to send a message that appears to be from anyone, anywhere, saying whatever the sender wants it to say. Thus, someone could send spoofed e-mail that appears to be from you with a message that you didn't write.[48]

Although most spoofed e-mail falls into the "nuisance" category and requires little action other than deletion, the more malicious varieties can cause serious problems and security risks. For example, spoofed email may purport to be from someone in a position of authority, asking for sensitive data, such as passwords, credit card numbers, or other personal information — any of which can be used for a variety of criminal Purpose. The Bank of America, eBay, and Wells Fargo are among the companies recently spoofed in mass spam mailings. One type of e-mail spoofing, self-sending spam, involves messages that appear to be both to and from the recipient.

Data Diddling [83]

Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the databases or application, or anyone else involved in the process of having information stored in a computer file. The culprit can be anyone involved in the process of creating, recording, encoding, examining, checking, converting, or transmitting data. This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the after the processing is completed. Electricity Boards in India have been victims to data diddling programs inserted when private parties were computerizing their systems. For example, a person entering accounting may change data to show their account, or a person entering accounting may change data to sho9w their account, or that or a friend or family member, is paid in full. By changing or failing to enter the information, they are able to

steal from the company. To deal with this type of crime, a company must implement policies and internal controls. This may include performing regular audits, using software with built-in features to combat such problems, and supervising employees.[49]

Salami Attack [50]

A Salami Attack, also known as salami slicing, is a type of cyber crime where small and often imperceptible amounts of money or data are stolen systematically over time. In the context of cyber crime, a Salami Attack involves stealing tiny increments or fractions of assets, whether they are financial funds, data, or resources, with the intention that each individual theft appears insignificant and might go unnoticed. However, when accumulated over numerous transactions or instances, these small slices or amounts accumulate to a substantial sum or impact. his technique is often utilized in financial crimes where the attacker takes small amounts from many accounts or transactions to avoid detection. It can also refer to stealing tiny pieces of data or resources from various sources, which, when combined, can be valuable or damaging. Salami Attacks rely on the principle that taking small, seemingly insignificant amounts might not trigger immediate attention or raise suspicions, enabling the attacker to continue their activities over an extended period without detection.

Logic Bombs

Logic bombs are segments of code intentionally inserted into software or systems to execute a malicious action when specific conditions are met. Unlike viruses or worms, logic bombs don't replicate themselves or spread independently; instead, they remain dormant until triggered by predetermined criteria, such as a particular date, event, or specific user actions. Once activated, a logic bomb can perform various malicious actions, such as deleting or corrupting data, disrupting system operations, or launching other forms of cyber attacks. These can be particularly damaging if they affect critical systems or sensitive data.

Individuals with authorized access to systems or networks might clandestinely implant logic bombs to cause harm, seek revenge, or manipulate systems for personal gain. Organizations and individuals often employ security measures to detect and prevent logic bombs from being implanted, as their activation can result in significant disruptions and damages.[51] Some logic bombs can be detected and detected and eliminated before they execute through a periodic scan of all computer files, including compressed files, with an up-to-date anti-virus program. For best results, the auto-protect and e-mail screening functions of the anti-virus program should be activated by the computer user whenever the machine is online. In a network, each computer should be individually protected, in addition to whatever protection is provided by the network administrator. Unfortunately, even this precaution does not guarantee 100 percent system immunity. The most common activator for a logic bomb is a date. The logic bomb checks the system date and does nothing until a pre-programmed date and time is reached. At that point, the logic bomb activates and executes its code. A logic bomb could also be programmed to wait for a certain message form the programmer. The logic bomb could for example, check a web site once a week for a certain message. When the logic bomb sees that message, or when the logic bomb stops seeing that message, it activates and executes its code.[52] This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs, e.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus.

GLOBAL EXTENT OF COMPUTER CRIME

Computer crime or cyber crime is the FBI's number three priority. Also, according to the FBI 's estimation, computer crime in the USA costs industry about $400 billion in 2004[53].According to Reuters, 2006, the Department of Trade and Industry in the UK says that computer crime has increased by 50% over the last two years (2004 and 2005)[92][54]. At the International level, high-technology crime is one of Interpol 's top

five priorities[55].

Statistics on the scale of computer cyber crime are mostly estimations based on surveys. According to the Australian Computer Crime and Security Survey[56], the total average loss per organisation in 2006 for computer crime, electronic attack, and computer misuse or abuse has increased 63% per organisation compared to 2005. Also in USA, according to the IC3 2005 Internet Crime Report [57], the IC3 (Internet Crime Complaint Center) received 231,491 complaints in 2005 which is 11.6% more than 2004 complaints. In Japan, there are 1,802 cyber crime reported cases to the National Police Agency in the first half of 2006 which has increased by 11.8% compared to the first half of 2005.[58]. The UK National Hi-Tech Crime Unit (NHTCU) estimates the cost of cyber crime on companies based in UK is at least US$4.61 billion in 2004[59]. Also, according to the USA Treasury Department, the proceeds from cyber crime have overtaken the proceeds from illegal drug sales netting an estimated US$105 billion in 2004[60]. In addition, according to IDC report, a market research firm based in the USA, the 2003 showed more than 60% of computer hackers have targeted financial institutions. Besides that, the total loses in 2006 from Phishing attacks increased to $2.8 billion which is double the total lost in 2004[61] . Kshetri (2009) indicates that cyber crimes is costing consumers and businesses such as banks and credit card companies billions of American dollars each year[62]. He indicated that the crime rate is linked to the economic opportunities which contribute to motivation for committing a computer crime. The cost of cyber crime is high and without forgetting the cost of controlling cyber crime that is being spent from the organizations which are relying on their computer technology to do business.

day and age when everything from microwave ovens and refrigerators to nuclear power plants are being run on computers, cyber crime has assumed rather sinister implications.

LEGAL FRAMEWORK

“This segment examines both national and international strategies employed to tackle computer crime and cyber crime.” The first sub-section examines the initiatives of international bodies such as the United Nations (UN), European Union (EU), Council of Europe (CoE), Group of Eight (G8) and Interpol in countering computer and cyber crime at the international level. Sub-section two provides a very brief summary of relevant legislation in .The third sub-section investigates the various government initiatives in Bangladesh combat computer crime. The last sub-section discusses the methods employed by law enforcement agencies in these four countries to tackle computer crime and cyber threats.

INTERNATIONAL INITIATIVES TO COMBAT COMPUTER CRIME

In this segment, we delve into the initiatives undertaken by international organizations to combat computer crime and cyber threats. The study explores the roles and actions of the UN, EU, CoE, G8, and Interpol in preventing and addressing computer crime and cyber threats.

United Nations (UN)

The UN is an international and worldwide organization. Its goals are to facilitate and support the collaboration in international law and security, economic development, social progress and in solving human rights issues[63]. The UN has many agencies that are working to implement the organizations main principles. In fact, one of the UN agencies is the United Nations Office on Drugs and Crime (UNODC) which is responsible for assisting members in combating crime[64]. In 2000, the *UN Convention against Transnational Organized Crime* was adopted in order to fight transnational organized crime. It intends to facilitate a legal framework for international cooperation in countering criminal activities and the increasing connections between terrorist crimes and transnational organized crime[65]. In 2001, the UN produced a

report called 'Conclusions of the Study on Effective Measures to Prevent and Control High- Technology and Computer- Related Crime'[66]. The report recommends setting strategies and enhancing international cooperation to counter and prevent computer crime. Furthermore, during the Eleventh United Nations Congress on the Prevention of Crime in 2005, there was a workshop on measures to combat computer-related crime. There was a discussion as to what should be done about collaboration between countries and private sectors in combating computer crime. The workshop concluded by giving the following recommendations in order to combat computer or cyber crime[67]:

- The UN should assist member countries in combating computer
- UNODC should provide the technical support and training to the member
- Enhancing and encouraging international law enforcement
- Encouraging the member states to update their legislation and strength their computer crime laws.
- work between governments, non-governmental organizations and the private sector should take place to counter computer crime.

The ITU also addresses current global challenges such as strengthening cyber security. Following the UN General Resolutions on 'Combating criminal misuse of information technology‖, the ITU took the lead for Building confidence and security in the use of information and communication technologies[68]. In 2009, ITU developed the ITU Toolkit for Cyber crime Legislation which is designed to provide countries with sample legislative language and reference materials that can assist in the establishment of harmonized cyber crime laws and procedural rules[69]. In April 2010, the UN members rejected a proposal for a global cyber crime treaty[70]· There were many reasons behind this rejection which includes not reaching agreement on some issues such as transferring of digital evidence, and that such a treaty would take a long time to resolve, and the EU and USA view that there is no need for a new treaty since the CoE Convention exists.

European Union (EU)

The EU enhances cross-border cooperation between member countries. Indeed, the EU's Commission and the Council of the EU are focusing a lot of effort on combating cyber crime. In January 2001, the EU's Commission adopted a statement on 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer- related Crime[71] . The statement emphasized that an inclusive policy program to combat cyber crime should include at least the following four key conditions [72]·The adoption of adequate, substantive, and procedural legislative provisions to deal with both domestic and transnational criminal activities;

- The availability of a sufficient number of well-trained and well-equipped law enforcement personnel;
- The improvement of the cooperation between all stakeholders, users and consumers, industry, and law enforcement; and
- The need for ongoing industry and community led

Council of Europe (CoE)

The CoE was established in 1949 and has now 47 member countries. In addition, there are five countries that are attending the CoE's meetings as observers which include the USA and Canada. The CoE addressed the rising threats created by computer-related crime from the late 1980s. After that, in 1989, the CoE published a study and suggestions which indicated the need for laws criminalizing unlawful acts using computer networks. From that time on, the CoE was involved in many projects in combating computer crime or cyber crime. Indeed, in 2001, 29 CoE's member countries and the USA signed the Council of Europe Convention on Cyber crime. The Cyber crime Convention requires from the members the following [73]:

- Develop laws against
- Make sure that the law enfor cements have the essential procedural authorities to investigate and prosecute cyber crime offences.
- Supply global collaboration to other countries to combat

Articles 2 to 10 of the CoE Convention describe the types of cyber crime offences and Articles 11 to 22 indicate that the member countries should adopt legislation that establishes ancillary liability and sanctions, procedural law, and jurisdiction. Articles 23 to 35 refer to international cooperation and mutual assistance. Articles 36 to 48 describe signature, entry into force, accessing, effects and others for the purpose of this Convention. Currently, on the 19th of May 2010, the CoE Convention on Cyber crime has 47 member countries of the CoE and nine non-member countries. The CoE Convention on Cyber crime opens first for signature before it enters into force 2 for the CoE member countries and also for non-member countries. The CoE Treaty Office (2010) indicated that 46 member countries of the CoE and non-member countries had signed the CoE Convention on Cyber crime, although only 17 of them had entered it into force[74].

Group of Eight (G8)

The G8 is a group of eight of the world‘s main industrial countries. The G8 countries are Canada, France, Germany, Russia, Italy, Japan, the UK and the USA. The G8 focused on combating crime such as its work on transnational organized crime. The G8 established five Subgroups of the Lyon Group to employ and adopt the forty recommendations developed by G8. One of the G8‘s subgroups was the G8‘s Subgroup on High-Tech Crime. The G8‘s Subgroup on High-Tech Crime assists, advises and helps the member countries in combating cyber crime. It offers some recommendations to help its members to review their legislation.

According to the third paragraph of Article 36 of the CoE Convention on Cyber crime:

*….In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2 ….*ensure that high-tech illegal acts are criminalized by all member countries[75]. In conclusion, G8 encourages its members to enhance their own laws in particular areas of concern to the G8 such as organized crime, high-tech crime, and terrorist communications and organisations.

Interpol

The International Criminal Police Organization, widely known as Interpol, is an organization that facilitates the collaboration between all of the police forces around the world.. Interpol developed and implemented an international police communications system called 1-24/7. The purpose of this system is to enable and facilitate the exchange of information among the member police forces. The police forces from the member countries can look for and verify data with direct access to Interpol‘s databases. In fact, Interpol supports and facilitates the international collaboration among the police forces in combating worldwide crime such as cyber crime. Cyber crime is considered by Interpol as one with the greatest increase in scale and quantity among other crimes. Because Interpol has facilitated a secure communications system for collecting, storing, analyzing, sharing and requesting information, the member countries can retrieve data from the system‘s database with regard to criminal activities such as cyber crime. The system supports the members 24 hours a day, 7 days a week. Moreover, other features of Interpol‘s work on combating cyber crime are designed to[76]:

- Assist cooperation between the member countries via a list of contact officers reachable for cyber crime investigation.

- Enhance the exchange of information on cyber crime between the member
- Support member countries in the incidence of cyber crime investigations or
- Build up partnerships with other international and private

Also, Interpol has established collaborative work with the private sector in countering the spread of computer crime or cyber crime. For example, Interpol and Microsoft organized the meeting of the BotNet Task Force (initiated by Microsoft in 2004) to tackle and address the growing threats of Botnets. Additionally, Interpol and the G8 High Tech Crime Group support the recommendations provided by the USA and the UK law enforcement agencies for changes to the Internet Corporation for Assigned Names and Numbers (ICANN)[77]. The USA's FBI and the UK's Serious Organized Crime Agency (SOCA) proposed that the ICANN should conduct customer due diligence and impose stronger rules on registers for generic top-level domains (g TLDs) such as .com [78]. They aim to make it very difficult for criminals to register domain names under fake or false identifications.

CYBER CRIME AND CYBER LEGISLATIONS

Cyber crime is increasingly becoming major threats to national and international governments in the digital era. In recent years, jurisdictions worldwide have been forced to evaluate their legal systems to deal with the growing threats of computer-related crimes. For that, the aim of this subsection is to investigate and identify current computer crime and cyber crime legislation in Bangladesh.

Present Scenario of Cyber Crime in Bangladesh

Bangladesh has been carrying out anti- cyber crime activities from last year providing training for a group of professionals and developing software. According to Deputy Inspector General (DIG) of the CID of the Police, as part of the strategy, the Crime Investigation Department (CID) o f the Police would run a cyber crime laboratory later if its plan went accordingly. The DIG said by initiating the anti-cyber crime activities, Bangladesh had come to the age of combating high-tech crimes though no single cyber crime was recorded in the country. Some of the incidents that bring the notice of the public are: E-mail threatening to the Prime Minister Sheikh Hasina from a cyber café, Hacking the mail of BRAC Bangladesh, stealing the transaction report of Dhaka Stock Exchange through hacking , inserting porno movies to the web site of Bangladesh National Parliament,inserting the porno movies to the website of Jamate Islami Bangladesh,inserting the porno movies to the website of the Daily Jugantor newspaper, E-mail threatening to World Bank Dhaka Office and the Bangladesh Bank cyber heist, was a theft that took place in February 2016.

The Information and Communication Technology Act 2006

The Government of Bangladesh responded by coming up with the first cyber law of Bangladesh. The Information and Communication Technology Act (ICT), 2006. The ICT Act defines various terms, which are innovative in the legal lexicon in Bangladesh. The law consists of a preamble, 97 sections and four schedules.

Jurisdiction under ICT Act 2006

The cyber tribunal under the section may be given jurisdiction of whole Bangladesh or one or more session jurisdiction; and the tribunal will only judge the cases of crimes under the Act. The special tribunal may sit and continue its procedure on a place at a certain time and government will dictate all this by its order. The parliament of Bangladesh has enacted Information and Communication Technology Act, 2006 which defines certain activities as crime. So we can say that, the activities which made punishable under the Information and Technology Act of 2006 shall be the cyber crimes for the territory of Bangladesh. The activities are:Mischief of computer and computer system ,Alteration of source code of commuter ,Hacking

in computer system ,publication of f alse, indecent and defamatory statement or information inelectronic form ,access in reserve system ,false representation and concealment of information, false electronic signatur certificate , transmission of secrecy , disclosing electronic signature for cheating , committing crime through computer.

Establishment of Cyber Tribunal

The Government shall, by notification in the Official Gazette, establish one or more Cyber Tribunals to be known as Tribunal at times for the purposes of speedy and effective trials of offences committed under this Act.151 The cyber tribunal that is stated in sub-section (1) of the section will comprise of a Session judge or an Assistant Session Judge appointed by the government with consulting with the Supreme Court; and such a judge appointed will be introduced judge, cyber tribunal.

Establishment of Cyber Appellate Tribunal

The ICT Act envisages the establishment of the Cyber Appellate Tribunal at one or more places as the government may deem fit. Section 82(1) of the ICT Act provides that the government shall, by notification in the Official Gazette, establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal. The cyber appellate tribunal will be comprised of a chairman and two members appointed by the government. The chairman will be such a person, who was a justice of the Supreme Court or is continuing his post or capable to be appointed as such and one of the member will be as an appointed judicial executive as a district judge or he may be retired and the other will be a person having the knowledge and experience in information and technology that is prescribed. The chairman and the members will be in their post minimum 3 years and maximum 5 years and the conditions of their service will be decided by the government. The Cyber Appellate Tribunal shall have the power to hear and settle the appeal made against the judgment of cyber tribunal and session court. The appeal tribunal will have authority of supporting, canceling, changing, or editing the judgment of the cyber tribunal. The decision of the appellate tribunal will be final. The Cyber Appellate Tribunal does not seem to be vested with any original jurisdiction; it has been vested with the powers of a Civil Court in respect of, interalia, summoning and examining of witnesses, requiring production of document receiving evidence ,issuing commissions and reviewing its decisions.

EFFECTS OF CYBER CRIME

Direct Effect:

Online fraud [79]

There are many types of fraud targeted at the public, ranging from credit and debit card fraud, lottery scams,419‖ fraud, non-delivery fraud and fraud perpetrated through online auction websites. Additionally, the public is at risk from fraud involving fake goods, such as watches or clothing, or more seriously from fake and unsafe pharmaceuticals bought online. None of these are unknown offline, but cyber criminals are able to use the internet to perpetrate these offences on a mass scale, and are able to use the internet to hide their real identities and locations. This is not just a UK problem – according to the US Internet Crime Complaint Centre (IC3)[80]' the total loss from fraud on the internet reported to them was $560m in 2009, with the most significant loss coming from non-delivery of goods.

Identity theft[81] [160]

The driver behind the majority of data thefts is the profitability of compromised private information, particularly detailed financial information. Criminals obtain large quantities of data, such as credit card data

and sell it either directly to those able to realise its monetary value through fraud, or to those who act as data brokers, aggregating data from different sources and selling it to other criminals. Criminals of all types and levels, including individuals looking to carry out small-scale, high volume frauds are able to buy compromised private data directly from the primary sources. ID crime can also be used to facilitate virtually all forms of serious crime including money laundering and human trafficking. Individuals are targeted primarily for user names and passwords to enable criminals to access, and in some cases to control online accounts. These are usually bank accounts but other types, such as online brokerage accounts, may also be compromised. Criminals also attempt to gain private details of their payment card accounts. This can be achieved by tricking the account holder into revealing private data through fake emails and websites (phishing‖) or by infecting the account holder‘s computer with malicious software (malware‖) that automatically intercepts and forwards data to the criminal. Individuals are also victimized by attacks on businesses, where data is stolen in bulk. Although public awareness of these threats is improving, the attacks are becoming increasingly sophisticated.

Child protection[82]

The use of the internet by children is significant. They use it, for example, for social networking, gaming and as a research tool for school projects. However, it is a mechanism through which those who seek to harm children are able to operate. Children can use the internet, and meet people through it, without some of the traditional barriers that have in the past prevented them meeting what adults would term ―strangers‖. Moreover, it is increasingly a place where child sexual abuse within families or extended families is recorded and shared through images or video with likeminded individuals across the world. The transfer of illegal images of child sexual abuse as well as communications between offenders, is made easier by new technology, and there are times when the public accidentally see such image. Harassment and bullying are significant issues, especially for children, who often cite these as their own areas of greatest concern. The nature of the technology, which children often carry with them all the time, allows bullying to take place not only in school but continue outside. This can make the victim feel threatened and unable to escape the bullying, leading to a feeling of powerlessness.

Hate Crimes and Terrorism [83]

The internet facilitates the prolonged, consistent perpetration of hate crime‖ and some victims can experience hate incidents and hate crimes over a prolonged period of time at roughly the same level of intensity. Whether this is an email sent anonymously or a website dedicated to spreading abhorrent messages, this can have a high impact on victims and communities when it is part of a pattern of repeat victimisation. Even when not part of a pattern of victimisation, research has found that _minor‘ hate crimes can produce as much emotional harm for victims as so called serious offences.

Fraud[84]

As with the threat to the public, fraud is a major concern for businesses. This may be through legitimate businesses being defrauded online, or through unfair competition from fraudulent businesses. The mechanisms for such frauds may be through goods being paid for with stolen or forged credit cards, or through credit card companies having to reimburse consumers who have had their details compromised

Data security [85]

The data that online criminals need to commit theft or fraud can be acquired from individuals or from companies. Commercial data breaches are a sensitive issue for companies that are the victims, and this makes it difficult to assess the scale of the threat and also to determine whether the biggest risk comes from external attackers or corrupt insiders. Successful data thefts result mostly from attacks on three vulnerable

areas: data held by individual internet users; data stored centrally; or data in transit between an individual and an organisation, such as on laptops, memory sticks or other moveable media.

The threat to Government [86]

As well as the threat posed to the general public, cyber crime poses a number o challenges for Government. Government can be the target of attacks from online criminals, who target the services provided by Government for the public with the aim of financial gain, or for gathering data on individuals. The increasing availability of government services online provides opportunities for criminals. Fraudulent applications for services such as benefits / tax credits, and tax repayments may be perceived by criminals to be less well monitored or to offer more anonymity and less human interaction than more traditional fraud would require. There is a risk that the increasing provision of services online by Government will lead to more attempts to defraud Government.

Indirect Impacts [166]

The Government strongly supports the use of the internet, and recognises the benefits that it gives to our society, both the public and business. The Digital Britain Report made clear that crime on the internet is a concern, and has the potential to prevent the full take up of the benefits of the internet. There is also the possibility that some of the benefits already in place would be undermined if crime were to affect many more people than it does. Although the relationship between fear of crime on the internet and the use of the internet needs to be examined further, as shown by the OFT report it is reasonable to suppose that the fear of crime acts as a deterrent to use. This may be especially true for consumers and small businesses, who are the targets of attacks from criminals, but who have limited ability to defend themselves. There are also indirect costs to businesses that have invested in online capacity, but do not get a return on their investment due to the consumer‘s fear of using those services.

CRITICISM AND WEAKNESSES

A proverb goes Prevention is better than cure‘. For prevention of numerous cyber crimes it is better to initiate advanced technological actions. These are technological precautionary affairs for prior prevention. We will rather try to find out the legal and other remedies and their lacking available in Bangladesh for curing the alleged cyber crimes. As per the provisions of the ICT Act a good number of other procedural and structural hurdles also exist which are as follows:

Firstly, a session judge or an additional session judge will preside over the Cyber Tribunal[87] and a bench of three members including a chairman who will be an ex or acting judge or a competent person to be a judge of Supreme Court and an ex or acting Dist. Judge and an ICT expert, two other members of the bench, will preside over the Cyber Appellate Tribunal[88][169] and like the other criminal cases Public Prosecutors will prosecute on behalf of the state in this regard. The problem is that judges and the lawyers are the experts of laws, not of technology, more specifically of internet technology. So judges as well as the lawyers should be trained and made expert in technological knowledge for ensuring the justice of technological disputes. In case of Cyber Appellate Tribunal the judges have the opportunity to be assisted by the ICT expert. But is it possible to give the verdict on the basis of another‘s knowledge? The reality in our country is that so far no initiative is taken by the government to train up the judges for acquiring the minimum technological knowledge required for ensuring justice.

Secondly, a police officer not below the rank of a Sub-Inspector can be the IO (Investigation Officer) [89] regarding the cyber crimes. Like the judges, police officers also have no opportunity to gather the required technological knowledge due to the lack of proper initiatives. There is no provision for them to be assisted by any ICT expert like the judges of Cyber Appellate Tribunal. So, is it possible for such a police officer to

make a proper investigation into such matters? Moreover, it may result in a snag to justice.

Thirdly, the government bears the responsibility not only of forming the cyber tribunals but also of preparing terms and conditions of the service of the judges of those proposed tribunals [90]. Regrettably neither a single rule has been framed nor has a project or a proposal been taken or passed so far by the state. Proper execution of statutes ensures the rule of law. Circumstances say that inadequate execution of the ICT Act, 2006 is one of the root causes for the increasing cyber crimes in Bangladesh. The solution of those aforementioned problems demands that the state must take nippy steps along with logistic and financial assistance.

Fourthly, The ICT Act, 2006, that the order of the Government appointing any person as the Presiding officer of a Cyber Appellate Tribunal shall be final and shall not be called in question in any manner and no Act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.[91] The said provisions is a violation of the Fundamental rights of the citizens as are enshrined in Chapter III of the Constitution of Bangladesh and the said provision is not convenient and is likely to be struck down by the courts. The Government cannot claim immunity in appointment to Cyber Appellate Tribunal, as the same is contrary to the spirit of the Constitution of Bangladesh. So, under the Constitution of Bangladesh, all proceeding and Act of the Cyber Appellate Tribunal are null and void-ab-initio.

Fifthly, Domain Name‖ is the major issue, which related to Internet thoroughly. But the ICT Act, 2006 does not define ―domain Name‖ and the rights and liabilities. Domain Name‖ owners do not find any mention in the ICT Act. There is no provision about the Intellectual Property Rights of domain Name‖ owners. These need proper attention.[92]

Case Study: Hacking Of Reserve of Bangladesh Bank known as '2016 Bangladesh Bank heist':

In February 2016, instructions to steal US$951 Million from Bangladesh Bank, the central bank of Bangladesh, were issued via the SWIFT network. Five transactions issued by hackers worth $101 million from a Bangladesh Bank account at the Federal Reserve Bank of New York succeeded, with $20M traced to Sri Lanka (since recovered) and $81M to the Philippines. The Federal Reserve Bank of NY blocked the remaining 30 transaction accounting for $850 million in 30 transactions at the request of Bangladesh Bank. [93]

Investigation by Bangladesh

Initially, Bangladesh Bank was uncertain if its system had been compromised. Governor of the Central bank engaged World Informatix Cyber Security, a US based firm, to lead the security incident response, vulnerability assessment and remediation. World Informatix Cyber Security brought in the leading forensic investigation company Fire Eye Mandiant for the investigation. These cyber security experts found "footprints" and malware of hackers which suggested that the system had been breached. The investigators also said that the hackers were based outside Bangladesh. An internal investigation has been launched by Bangladesh Bank regarding the case. The Bangladesh Bank's forensic investigation found out that malware was installed within the bank's system sometime in January 2016, which gathered information on the banks operation on international payment and fund transfers.[94]

The case also highlights the threat of cyber attacks to both government and private institutions by cyber criminals using real bank codes to make orders look genuine. SWIFT has advised Banks using SWIFT Alliance Access system to strengthen their cyber security posture and ensure they are following SWIFT security guidelines. Bangladesh is reportedly the 20th most cyber- attacked country, according to a cyber

threat map developed by Kaspersky Lab which runs in real time.

FINDINGS

- *Constitutional Safeguard:* Constitutional provisions against cyber crimes may escort the cyber warfare to a national temperament which may result in a better form than any other organizational and legal remedy. Constitutional amendment may be the introducing procedure of such provisions.
- *Special Wing of Police:* The Police Force through global partnership need to be able to meet the challenges of the technology to curb all crimes including Cyber Crime. U.K., U.S.A, India, Malaysia and some other developed countries have established special wings of police to combat the cyber war. Bangladesh can initiate such special police wings as a new armament against hi-tech threats along with other deterrent actions.
- *Cyber Crime Agency by Government:* On the last 23rd July of 2009 North Korea twisted Korea Internet and Security agency, a government agency uniting three of its preceding internet technology organizations. Now, this agency will endeavor to make North Korea a stronger and a safe advanced country in using internet. India and some other countries have also created such agencies. Considering the present situation of using internet and increasing cyber crime in Bangladesh, Government can also commence such types of agencies. The worth of such agencies is that these will be able to perform multidimensional actions like advancing the internet infrastructure, maintaining the ISPs, fixing the internet using charges, preventing the cyber threats etc.
- *Watch Dog Group:* These groups are enormously internet like the security oriented intelligence. They include capturing and receiving malicious software, disassembling, sandboxing, and analyzing viruses and trojans, monitoring and reporting on malicious attackers, disseminating cyber threat information etc. This doggy concept is not a new one. Shadow Server Foundation can be an example of Watch Dog Groups which was established in 2004. These may be individual as well as governmental. At present there is no such organization in Bangladesh, but in consideration with the escalating cyber threats, these doggy groups can be one of the vital constituents for developing Bangladesh as an advanced country especially in internet technology.
- *Public Awareness:*. Like other vital issues, the government should create awareness among the mass people all over the country through different media. Besides, NGOs and other organizations can commence campaign in this regard.

CONCLUSION

Cyber crime, within this global networked context, emerges as one of the most widespread present offenses and a futuristic threat. Human capacity is vast; eliminating cyber crime entirely from cyberspace seems impossible, but controlling it is feasible. Throughout history, legislation hasn't eradicated crime, only curtailed it. The approach lies in educating people about their rights and responsibilities, coupled with stricter law enforcement to combat crime. Undoubtedly, the ICT Act marks a pivotal moment in the cyber world. However, amendments to the Information Technology Act are necessary for greater effectiveness against cyber crime without impeding industry growth. The archaic Penal Code of 1860 fails to address modern cyber offenses. New laws are imperative to tackle crimes like conspiracy, fraud, and espionage occurring through the internet. The ICT Act of 2006 in Bangladesh filled a crucial void, necessitating corresponding amendments in older laws like the Penal Code 1860 and the Evidence Act 1872 to address cyber crimes adequately. The concept of cyber crime is a product of the information age, rapidly spreading through online communication channels by sophisticated criminals. Legislation should evolve to clamp down on technological crimes effectively, but existing laws globally face implementation challenges due to procedural complexities and inadequate execution systems. Exploiting these gaps, criminals engage in heinous activities like hacking, cyber terrorism, and misuse of intellectual property, jeopardizing individual

privacy and global security. The need of the hour is stringent legislation within national boundaries to combat cyber crime. Bangladesh, like any other country, must enact and enforce effective legal provisions to prevent cyber crimes and safeguard individual privacy and global peace.

FOOTENOTE

[1] Ali Obaid Sultan Alkaabi (2010)Combating Computer Crime: An International Perspective' *University of Southern Queensland*, p-01,; available at: http://eprints.qut.edu.au/43400/1/Ali_Alkaabi_Thesis.pdf,last accessed on 20th October, 2023

[2] Badsha Mia, (2021) Cybercrime and its impact in Bangladesh: A quest for necessary legislation' *Law Mantra*,Vol.2 Issue.5, Available at: http://journal.lawmantra.co.in/wp-content/uploads/2015/05/251.pdf ,last accessed on 15th October,2023

[3] Ibid

[4] Peter Norton, Introduction to Computers, Fifth Edition, (Career Education) 2002, p. 23

[5] Available at : https://www.statista.com/statistics/617136/digital-population-worldwide/ accessed on: 13/12/2023

[6] "Measuring digital development: Facts and figures 2021". Telecommunication Development Bureau, International Telecommunication Union (ITU). Accessed on: 16 November 2022.

[7]TBS Report 2023, https://www.tbsnews.net/bangladesh/telecom/internet-users-20-lakh-3-months-btrc-623810,accessed on : 21st October,2023.

[8] IBID.

[9] YAR, M. (2005), _The Novelty of Cyber crime ': An Assessment in Light of Routine Activity Theory.' European Journal of Criminology 2005; 2 ; P-407.

[10] Gordon, S., Richard, F. (2006), _On the definition and classification of Cyber crime, Journal in Computer Virology 2006, Volume 2, Issue 1, pp. 13-20.

[11] Proteus Manual (2015) Prevention, Information and support to victims of online identity theft', 2015, Lisboa, APAV.

[12] Supra note 2.

[13] Md.Nahidul Islam and Md. Ahsan Habib, _Cyber Crime and the Impact of the Information and Communication Technology Law in the Legal System: Bangladesh Perspective', p-04. Available at: http://www.juristlawjournal.com/article2.pdf,last accessed on 12th September,2023.

[14] Zibber Mohiuddin, (2006)*Cyber Laws in Pakustan: A situational analysis and way forward'* Available at: http://www.supremecourt.gov.pkijcarticles105.pdf.last accessed on 12th September,2023.

[15] Ibid.

[16] Grabosky, P.N., (2001), _Virtual criminality: Old wine in new bottles?'. Social and Legal Studies (10:2), 243-249:243

[17] YAR, M. (2005), The Novelty of Cyber crime': An Assessment in Light of Routine Activity Theory,' European Journal of Criminology 2005; 2 ;P- 407.

[18] Mr Michael Sinko witsch, Fujitsu Australia Ltd, Transcript of Evidence, 11 September 2009, p.47; Commander Neil Gaughan, AFP, Transcript of Evidence, 9 September 2009, p.11.

[19] Dr Russell Smith, AIC, Transcript of Evidence, p.9; AFP, Submission 25, p.3.

[20] Ibid.

[21] [54] AFP, Submission 25, p.5; Dr Russell Smith, AIC, Transcript of Evidence, 19 August 2009, p.13; ACCC, Submission 46, p.4; Mrs Nancy Bosler, ASSCA, Transcript of Evidence, p.1; Dr Russell Smith, AIC, Transcript of Evidence, 19 August 2009, p.14.

[22] Dr Russell Smith, AIC, Transcript of Evidence, 19 August 2009, p.14.

[23] Mr Anthony Burke (2009) Australian Bankers Association NSW Inc, Transcript of Evidence, p.62.

[24] AFP, Submission 25, p.5.

[25] Md.Nahidul Islam and Md. Ahsan Habib, _Cyber Crime and the Impact of the Information and Communication Technology Law in the Legal System: Bangladesh Perspective', p-03. Available at: http://www.juristlawjournal.com/article2.pdf.last , last accessed on:10th July 2023.

[26] G Urbas and KR Choo (2008) Resource materials on technology-enabled crime, AIC, Canberra, p.83; AIC, High tech crime brief: Hacking offences, AIC, p.1.

[27] OECD (2008)Malicious Software (Malware): A Security Threat to the Internet Economy, OECD, p.10.

[28] OECD (2008) Malicious Software (Malware): A Security Threat to the Internet Economy, OECD, p.91; G Urbas and KR Choo, Resource materials on technology-enabled crime, AIC, Canberra,p.87;

[29] Ibid.

[30] Ibid, p.90.

[31] Ibid, pp.79-87.

[32] Md.Nahidul Islam and Md. Ahsan Habib (2016) Cyber Crime and the Impact of the Information and Communication Technology Law in the Legal System: Bangladesh Perspective',p-05.Available at: http://www.juristlawjournal.com/article2.pdf. Accessed on 10th July 2023.

[33] Ibid. p-06.

[34] AIC (2016) High Tech Crime Brief: More malware – adware, spyware, spam and spim, AIC, Canberra, p.1

[35] P Wood (2009) *A spammer in the works*, MessageLabs, Hong Kong, 2003, p.6; OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.27; cited in MessageLabs (2009)*The Dark Art of Spam*, Message Labs,pp.3-4.

[36] Ibid.p.6.

[37] Ibid.

[38] Ibid.

[39] Supra 28.

[40] Supra 26

[41] Supra note 32.

[42] Symantec Corporation (2009) Symantec Report on the Underground Economy Australian Bureau of Statistics, 2007 Personal Fraud Survey, ABS, Cat. No. 4528.0, 2007, p.8; Australian Government, Dealing with identity theft: Protecting your identity, Attorney General's Department (AGD), 2009, p. 4; Aus CERT, *Computer Crime and Security Survey*, Aus CERT, 2006, p.28.

[43] Ibid.

[44] Supra 32.

[45] Ibid.

[46] Ibid.

[47] Ibid.

[48] IBID.

[49] Ibid.

[50] Ibid.

[51] Ibid.

[52] Ibid.

[53] McAfee. (2006)McAfee Virtual Criminology Report: North American study into organized crime and the Internet. 2005, Available at: http://www.mcafee.com/us/local content/misc/mcafeena virtual criminology report.pdf. accessed on 5th march 2023.

[54] Reuters. Cyber crime is Getting Organized. 2006 Available at:https://www.wired.com/2006/09/cyber crime-is-getting-organized/.accessed on 2nd July 2023.

[55]Broadhurst, R. and P. Grabosky, (2005)eds. Cyber-crime: The challenge in Asia., Hong Kong University Press: Hong Kong

[56] 94 Aus CERT. Australian Computer Crime and Security Survey. 2006; Available at: http://www.auscert.org.au/images/ACCSS2006.pdf.accessed on 10th June 2023.

[57] IC3 Internet Crime Complaint Center. IC3 2005 Internet Crime Report. 2005; Available at: http://www.ic3.gov/media/annualreport/2005 IC3Report, pdf. accessed 0n 10th july.2023

[58] CNET Networks. IT Facts. 2006 ,Available at: http://blogs.zdnet.com/ITFacts/?cat=33. accessed on:20th July,2023.

[59] Rohde, L (2016) More Sophisticated Cyber Crime Costs UK Billions. 2005; Available at: http://www.infoworld.com/article/05/04/05/HNcybercrime 1.html. http://blogs.zdnet.com/ITFacts/?cat=33. accessed on:20th July,2023.

[60] CNN Money (2016), Record Bad Year for Tech Security. 2005. Available at: http://money.cnn.com/2005/12/29/technology/computer_security/index.htm. http://blogs.zdnet.com/ITFacts/?cat=33. accessed on:20th July,2023.

[61] Internetnews (2006)Scammers Hooking Bigger Phish, available at: http://www.internetnews.com/stats/article.php/3642971. accessed on:21st April,2023.

[62] 100 Kshetri, N., (2009)Positive Externality, Increasing Returns, and the Rise in Cyber crimes. Communications of the ACM, **52**(12): p. 141-144. accessed on: 21st April,2023.

[63] United Nations (2016). About the United Nations: Introduction to the Structure and Work of the UN. 2007 ; Available at: http://www.un.org/aboutun/.accessed on:20th June,2023.

[64] 105 United Nations Office on Drugs and Crime (UNODC). About UNODC. 2007 [cited 2007 15 November]; Available of: http://www.unodc.org/unodc/en/about-unodc/index.html.accessed on20th June,2023.

[65] 106 UNODC(2016) United Nations Convention against Transnational Organized Crime and its Protocols. Available at: http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCe booke.pdf. accessed on: 20th March,2023.

[66] Mohay, G., et al., Computer and Intrusion Forensics. 2003, London: Artech House.

[67] United Nations (UN). Eleventh United Nations Congress on the prevention of crime and criminal justice. 2005 [cited 2016 16 December]; Available of: http://www.unis.unvienna.org/pdf/uniscp509e.pdf.

[68] International Telecommunication Union. ITU Toolkit for Cybercrime Legislation.2009 Updated on February 2010 [cited 2016 23 December]; Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itutoolkit- cyber crime-legislation.pdf. accessed on:10th April 2023.

[69] Ibid.

[70]asters, G. (2016)Global Cybercrime Treaty Rejected at U.N. 2010 Available at: http://www.scmagazineus.com/global-cybercrimetreaty-rejected-at-un/article/,68630/.

[71] 112 Computer Crime & Intellectual Property Section (CCIPS) at U.S. Department of Justice. (2005)The EU and its Institutions. 2005

[72] Ibid.

[73] Computer Crime & Intellectual Property Section (CCIPS) at U.S. Department of Justice.

(2007)International Aspects of Computer Crime.Available at.:.http://www.usdoj.gov/criminal/cyber crime/intl.html.accessed on 10th July 2023

[74] CoE Treaty Office (2010) Convention on Cyber crime CETS No.185: Status as of: 19/5/2010.

Available at : http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG. accessed on:5th March 2023.

[75]Privacy International. The Group of 8. 2004 [cited 20017 3 January]; Available of: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-65438&als[theme]=Cyber%20 Crime, accessed on:5th March 2023

[76]Interpol. Cyber-crime. (2007); Available at: http://www.interpol.int/Public/ICPO/FactSheets/FHT02.pdf. accessed on:5th March 2023

[77] Kirk, J. *Law Enforcement Lobbies Hard for ICANN Changes*. ComputerWorld 2010 [cited 2017 2 January]; Available of: http:/www.computerworld.com.au/article/340642/law enforcement lobbies hard icann changes/. accessed on:5th March 2023

[78] Ibid.

[79]Cyber Crime Strategy,UK Secretary of State for the Home Department, March 2010, P-12. [Cited 2016 20 December]; Available at: https://www.gov.uk/government/uploads/system/uploads/attachment data/file/228826/7842.pdf, accessed on:6th March 2023

[80] IC3 Annual Report 2009

[81] Cyber Crime Strategy,UK Secretary of State for the Home Department, March 2010, P-12. [Cited 2016 20 December]; Available of: https://www.gov.uk/government/uploads/system/uploads/attachment data/file/228826/7842.pdf ,accessed on:15th March 2023

[82] Ibid.

[83] Ibid.

[84] Ibid.

[85] Ibid.

[86] Ibid.

[87] Ibid, Sec:68(2)

[88] Ibid, Sec:82(2)(3)

[89] Ibid, Sec: 69(1)

[90] Ibid, Sec: 82(4)

[91] Ibid, Sec: 82,56,

[92] Supra nore 12.

[93] Congresswoman wants probe of 'brazen' $81M theft from New York Fed. accessed on:5th March 2023

[94] Korea Internet and Security Agency (2016) available at http://www.nida.or.kr/kisa/eng/englishver.html, accessed on : 11th November,2023.