



Contemporary Trends of Cyber Crime in Bangladesh: Regulatory Gaps and Way Outs

Submitted By

Masud Rana

ID: 221-38-062

LL.M. (Final)

Batch: DSC 2

Supervised by

Md. Safiullah

Assistant Professor

Department of law

Date of Submission

December 30, 2022

A Research Monograph Submitted in Partial Fulfilment of the Requirement for the Degree of LL.M. Program, Department of Law, Daffodil International University

LETTER OF APPROVAL

20th December, 2021

Md. Safiullah

Assistant Professor

Department of Law

Daffodil International University

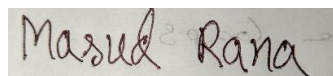
In Re: An Analysis on Contemporary Trends of Cyber Crime in Bangladesh: Regulatory Gaps and Way Outs

Dear Sir,

Most respectfully I beg to submit my Legal Research paper on “**Contemporary Trends of Cyber Crime in Bangladesh: Regulatory Gaps and Way Outs**” under your supervision. While conducting this Research monograph, I have tried my best level to make this research woke up to the mark and standard. I hope this work would fulfill your expectation and also the demand of the course.

I, hereby, do solemnly declare that the paper in dissertation has been carried out by me and has not been subject to any previous publication by any institution or organization. The work that I have presented is an authentic work and does not infringe any copyright

I, along with these lines, supplicate and hope that you would be sufficiently benevolent to this exploration paper for advancement.



Masud Rana

ID: 221-38-062

LL.M. (Final)

Phone: 01684413840

Email: rana38-062@diu.edu.bd

Department of Law

Daffodil International University

ACKNOWLEDGEMENT

Initially, before I start writing up the paper, I would like to express my gratitude towards some people around me for their unbound and generous support and encouragement during this project. First of all, I would like to carry millions of tons of gratitude to my supervisor Mr. Md. Safiullah for his close observation, assistance and cooperation throughout the project and also for cheering me up to be focused and issue centric. Again, I feel thankful to him for his valuable suggestions and corrections for which he spared his valuable time.

I am grateful to my family, especially to my wife who has always been a great support throughout my life.

I am also grateful to my mates who were and are with me during my legal studies.



Masud Rana

ID: 221-38-062

Department of Law


Daffodil International University

DEDICATION

I would like to dedicate this paper to my beloved parents whose dream is to see me as a fighter in the legal arena.

DICLARATION

This is hereby certifying that the Research Monograph titled " An Analysis on **“Contemporary Trends of Cyber Crime in Bangladesh: Regulatory Gaps and Way Outs** " has been accomplished by Masud Rana bearing ID No. 221-38-062 in partial fulfillment of the requirement for the degree of LL.M. Program at Daffodil International University. This Research Monograph has been carried out successfully under my supervision.



Mr. Md. Satiullah

Assistant Professor

Department of Law

Daffodil International University

ABSTRACT

In the age of the information society we live in, crimes committed using information technology (especially cybercrime) or those in which new technology plays an essential role are growing exponentially, and the fight against crimes committed via the Internet (not only cybercrime, but also cyber terrorism, cyber war, and other forms of cybercrime) represents a real challenge for the States, due to the unique characteristics of the means by which such crimes are committed. As a result, internet use has become an integral part of the lives of all educated people around the world. It connects a person sitting in a remote corner of their house or business to the rest of the globe via the information highway affectionately known as the web, cyber, and so on. It connects everyone to their office, banks, energy department, water works, transport services, markets, book stores, and friends from other countries, and it is ready to attack unsuspecting internet users with cyber attacks. In Bangladesh, cyber and technology-related crimes are on the rise. In Bangladesh, this is a critical issue. In the realm of information technology, it has already been observed that a bright threat has emerged. Recent e-mail threats to various individuals are an illustration of a handful of them. Cybercrime, on the other hand, is becoming a threat to the government itself. The broad and general goal of this study is to determine and define the nature of cybercrime, as well as the impact it has on those who utilize the Internet.

LIST OF ABBREVIATIONS

Abbreviation	Title
ACH	Automated Clearing House
ADC	Assistant Deputy Commissioner
Art.	Article
CID	Crime Investigation Department
CrPC	Code of Criminal Procedure
DIG	Deputy Inspector General
HCD	High Court Division
ICT	Information and Communication Technology
IGP	Inspector General of Police
IO	Investigation Officer
NGO	Non-Governmental Organization
NSA	National Security Agency
PCA	Pornography Control Act
RAB	Rapid Action Battalion
Sec.	Section
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UNDP	United Nations Development Programme
UNICITRAL	United Nations Commission on Internet Trade Law

Table of Contents

LETTER OF APPROVAL.....	ii
ACKNOWLEDGEMENT	iii
DEDICATION	iv
DICLARATION.....	v

CHAPTER 1

INTRODUCTORY

1.1 Introduction	1
1.2 Background of the Study	1
1.3 Statement of the Problem	2
1.4. Research Question	3
1.5 Objective of the Study	3
1.6 Scope and Limitation of the Study	3
1.7 Methodology of the Study	4
1.8 Justification of the Study	4
1.9 Tentative Work Plan	4
1.10 Conclusion	5

CHAPTER 2

LITERATURE REVIEW

2.1 Literature Review	6
2.2 Gap in the Existing Literature	10

CHAPTER 3

THEORETICAL FRAMEWORK

3.1Introduction	11
3.2 Classical Sociological Theorists	11
3.3 Modern Sociological Theorists	12
3.4 Post Modern Sociological Theorist	12

3.5 Others Theories	13
3.6 OPINION	13
3.7 Conclusion	14

CHAPTER 4

NATURE AND HISTORY OF CYBER CRIME AND ITS CLASSIFICATION

4.1 Introduction	15
4.2 Definition of Crime	15
4.3 Definition of Cyber Crime	15
4.4 Nature of Cyber Crime	16
4.5 Reason behind the Cyber Crime	16
4.6 History of Cyber Crime in Bangladesh	17
4.7 Classification of Cyber Crime	18
4.8 Different Types of Cyber Crime	19
4.9 Reasons of Cyber Crime	20
4.10 Current Situation of Cyber Crime in Bangladesh	21
4.11 Some New Dimensions AS Legal Remedy Against Cyber Crime	21
4.12 Conclusion	22

CHAPTER 5

DIGITAL SECURITY ACT, 2018

5.1 Definition	23
5.2 The Main Characteristics of Digital Technology	23
5.3 Critical Review of the Digital Security Act, 2018 from a Public Policy Perspective	24
5.4 Conclusion	26

CHAPTER 6

CONTEMPORARY TRENDS OF CYBER-CRIME IN BANGLADESH, REGULATORY GAPS AND WAY OUTS

6.1 Introduction	27
6.2 Cyber Crime Areas	27

6.3 Victims of Cyber Crime	27
6.4 Contemporary Trend of Cyber Crime	28
6.5 Regulatory Gaps	33
6.6 Way Outs	34

CHAPTER 7

RECOMMENDATION AND CONCLUSION

7.1 Recommendation	37
7.2 CONCLUSION	40

CHAPTER: ONE

INTRODUCTORY

1.1 Introduction

In this modern era crimes get the new dimension which defined as cyber-crime. Cybercrime is any criminal activity that involves ICT as the key-driving element for socio-economic development. But recent cyber-crime incidents arisen the controversies about the cyber security systems of Bangladesh. Government gives so much importance to combat cyber-crime taken many initiatives set up many institutions to control the cyber security, established cyber-crime tribunal, established regulatory body and others such institutions. Besides these initiative government initiatives have also some gaps and loopholes.

This study have focused on that gaps and loopholes besides the definitions, characteristics, existing laws, present scenario of cyber-crime in Bangladesh and also give some possible recommendations on the basis of different secondary sources, which may help to improve the cyber security systems in Bangladesh.¹.

1.2 Background of the Study

In 1820, the first cyber-crime was registered. The abacus, which is regarded to be the oldest form of a computer, dates from 3500 BC, which is not surprising. India, Japan, and China are three of the most populous countries in the world. The analytical engine of Charles Babbage, on the other hand, marked the beginning of the contemporary computer age.

Joseph-Marie Jacquard, a French textile producer, began producing looms in 1820. This gadget allows many steps in the weaving of specific materials to be repeated. Employees at Jacquard have expressed concern that their traditional jobs and livelihoods may be jeopardized as a result of this. They used sabotage to deter Jacquard from using new technologies in the future. This is the first time a cybercrime has been documented.²

¹Interpol.int. (2019).*Cybercrime / Cybercrime / Crime areas / Internet / Home - INTERPOL*. [online] Available at: <https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime> .

²Edwin H. Sutherland, *Principles of Criminology*, Second Edition, Philadelphia: Lippincott, 1934, page 3

Computers have gone a long way, with neural networks and Nano-computing promising to turn every atom in a glass of water into a billion-operation-per-second computer.³

Cybercrime is a modern-day problem that results from our increasing reliance on technology. Cybercrime has had a particularly devastating impact in an age when everything from microwave ovens and refrigerators to nuclear power plants is controlled by computers. The Citibank robbery is one of the most recent significant cyber-crimes. A total of \$10 million was unlawfully transferred from a bank to a Swiss bank account. The attack was carried out by a Russian cyber gang directed by Vladimir Kevin, a well-known hacker. The bank's security arrangements have been breached by the group. AO Saturn, a computer corporation based in St. Petersburg, Russia, is suspected of accessing Citibank computers using Vladimir's workplace computer. On his route to Switzerland, he was detained at Heathrow Airport.

1.3 Statement of the Problem

Cybercriminals are always looking for a quick way to generate a lot of money. They hack sensitive information from affluent individuals or wealthy entities like as banks, financial institutions, and financial institutions where large quantities of money travel every day. And apprehending such offenders is difficult. As a result, the number of cyber-crimes worldwide rises.

Actually, I'm going to try to figure out the current trend, regulatory gaps, and ways out of cyber-crime.

³Encyclopedia Britannica.(2014). *cybercrime / Definition, Statistics, & Examples*. [online] Available <https://www.britannica.com/topic/cybercrime> .

1.4. Research Question

- a) What are the complexity in taking legal action against offenders of cyber-crime?
- b) What are the regulatory gaps regarding this problem?
- c) Is there any way outs to solve this problem?

1.5 Objective of the Study

The objectives of this paper includes-

- a) To ensure the cyber relief.
- b) To remove the complexity in taking legal action against offenders.
- c) To identify the problems in identification of offenders.
- d) To analysis the existing law relating to cybercrime.
- e) To make some recommendation for preventing cyber-crime.
- f) To identify the regulatory gaps and solve the problem as soon as possible.

1.6 Scope and Limitation of the Study

There are a number of observations that must be made as regards the scope and limitations of this research. Firstly, this research will focus on the regulatory gaps and way outs of cybercrime. Although this thesis also deal with the previous history of the cyber-crime and existing law of cyber-crime. Secondly, this thesis will provide, prior to discussing national law and case-law. Finally a limitation of this research which needs to be mentioned that because of knowledge and capability, things this study may not fully represent the picture of cyber-crime.

1.7 Methodology of the Study

This is a combination of qualitative research. I have collected all the information from secondary sources like books, articles of referred journals in national and international arena, periodicals, magazines, newspaper. Collected data therefore I analyzed systematically to achieve the objective of the research.

1.8 Justification of the Study

It is hoped that this study will make a significant contribution to the concept of cybercrime. It will help policymakers, lawmakers and researchers learn about the problems and possibilities for reducing cybercrime. The results of this survey are intended to help the government improve existing laws relating to information and technology security in Bangladesh.

As the study relates to the current situation or the current possibility of cyber-crime and its prevention, as well as the effectiveness of the law, government action, public awareness and respect for the law, which is a matter of daylight, it deserves. Some outstanding significance. This will be a new combination for researchers, as far as is known, no research has been done on this subject in Bangladesh yet. It is to be hoped that this recent issue can be considered as an important and valuable resource for workers in this regard. The results of the research will be helpful for people, especially for those who are concerned and interested in this field.

1.9 Tentative Work Plan

The research monograph contains eight different chapters preferred with the view to state the purpose of the paper plainly and in an extensive manner. In the first chapter it is the Introductory chapter which consists of introduction, background of the study, statement of the Problem, research question, objective of the study, justification of the study, methodology of the study, scope and limitations, conclusion and Structure of the Research Monograph. In the second chapter, the chapter illustrates the concept of literature review. In the third chapter, the chapter illustrates the concept of theoretical framework. In the fourth chapter, the chapter illustrates the idea of the nature and history of cyber-crime and its classification. In the fifth chapter, this Chapter talks about The Digital Security Act 2018. In the sixth chapter, the chapter has formulated the contemporary trends cyber-crime in Bangladesh, and also defined regulatory gaps and way outs. In the seventh chapter, this chapter talks about the recommendations and finding. In the eighth chapter it is the final chapter this chapter talks about the conclusion.

1.10 Conclusion

Cybercrime is unquestionably the most recent and difficult-to-control sort of crime. However, the difficulties does not preclude us from taking necessary measures to combat cyber-criminals. We must cultivate morals and ethics in our personal and community life because law alone is insufficient. Because our youth are prone to misdirection, they must be properly guided and cared for. The government must take all necessary precautions to avoid any cyber-attack that could harm human life. The government's vital tasks include maintaining constant watch and strengthening countermeasures. Ordinary people must likewise exercise caution when accessing computer systems and online resources. Hopefully, our increased awareness and unwavering fight against cybercrime will be successful.

Basically, there hasn't been any big cybercrime in Bangladesh yet. The growing reliance on and widespread use of computer and information technology by financial institutions such as banks, insurance companies, and other non-governmental entities raises the risk of cyber-crime in this country. For years, computers have been used in Bangladesh to perform crimes such as falsifying certifications and documents, while attacks on computers or computer systems are extremely rare.

CHAPTER TWO

LITERATURE REVIEW

2.1 Literature Review

In Bangladesh, the concept of cyber law is relatively new. There are only a few books on cyber law in the Bangladeshi market. The Penal Code of Bangladesh is one of the books I've acquired, and I've also read our country's ICT law. As a result, I have to rely on the internet to complete my paper. I visit numerous websites and gather a great deal of useful information from them. I use the public library to gather information on a few occasions. However, I was unable to locate any books on cyber law there. As a result, it is becoming increasingly difficult for me to obtain knowledge on cyber law from public libraries, as our public library's collection is inadequate. To construct this research paper, I presented a critical examination of the concerns, and the study aims to cover practically all of the scenarios that affect its evaluation, as well as a recent report and some past years on legal education and cyber-crime in Bangladesh, with particular offered remedies. To complete this research paper, I will need to gather two sorts of information: the definition of cyber crime and specific features of cyber-crime in Bangladesh. Preliminary data was acquired from a variety of sources, including legal authorities, experienced individuals, and others who had conducted research on the same topic. Secondary data was gathered from a variety of books published by a variety of knowledgeable researchers from both public and private universities, as well as certain websites. To conclude my research report, I merged these two forms of information. I also included observations, opinions, and recommendations from many authors in my research paper.

Concerning the Nature of Cybercrime According to Borhanuddin A.R.M in his web Article Cyber Crime and Bangladesh Perspective,

Cybercrime is regionally unrestricted and occurs in an electronic or virtual environment, whereas traditional crimes occur largely in the regional and actual world. More fundamental considerations concerning the nature of cybercrime, such as whether it is a criminal infraction, a civil wrongdoing, or torture, are posed. The nature of the occurrence will determine the answer. All computer violations are now deemed criminal charges, according to the enactment of the ICT (Information and Communication Technology) Act of 2006.

In His Book "Introduction to Computers, Fifth Edition," Peter Norton Spoke on The History of Cybercrime, Saying,

The last cybercrime was registered in 1820!" These abacus, hence is regarded in stay that oldest since its an computer, dates from 3500 BC, which is not surprising. India, Japan, and China are three of the most populous countries in the world. The analytical engine of Charles Babbage, on the other hand, marked the beginning of the contemporary computer age. In 1994, First Virtual, the first online bank, was established. This has given hackers a lot of opportunities. Cybercrime was gradually getting traction. The first internet wiretap, similar to a phone wiretap, was received by the confidential serving also the Drug Enforcement Agency (DEA) in 1995. The Drug Enforcement Administration was capable in closed under an business that was sale illicit cells phone cloning technology. In Bangladesh, thither has done an rapid increment on cyber offense, also law enforcement officials also finding it extremely difficult to deal with this technical crime.⁴

"In 2014, The Daily Star Published a Report on the Present State of Cybercrime in Bangladesh, Which Stated,

Bangladesh, which lacks natural resources, is attempting to build its economy by using the ICT industry. Many countries have taken convenience its that potential afford with ICT in developing a principle structure, establishing guidebook, also building an nationwide ICT trick as part of a larger nationwide improvement scheme in recent years. Bangladesh aspires in make information and communication technology (ICT) a significant engine of socioeconomic development. The current government has proclaimed Vision-2021, which states that by 2021, the country would be digital and have a per capita income comparable in an middle-income country. However, that administration, as well as various stakeholders, worthy assess the extent to which the continuation in the internet also various the networks on transform the country in an digital country may result in increased crime.

⁴ bdnews24.com publish a report on 2018 about the title " Bangladesh -making-digital-security-act-to-tackle-cyber-crimes".

5.The Information and Communication Act, of 2006

6.S.Ghosh, and E. Turrini. A Multidisciplinary Analysis. Springer-Verlag Berlin Heidelberg, 2010.

Borhanuddin A.R.M. Published Cyber Crime and Bangladesh Perspective, Which is Available Online.

"In 2008, a tiny hacker named Shahimirza from Bangladesh penetrated RAB's website. He further revealed to the authorities which he was hacked no sole that RAB website, however also the websites of other national governments. And he has long hacked the private and international site. He has hacked 21 websites in total, including army websites.

The Following Report Was Published on the Dailystar.Net/Archive Website: Cyber criminals have stolen \$400 million in election-related assets in the United States. The Pentagon's network was hacked in June 2007. RAB's website was recently hacked by four students from a private technological institute in Bangladesh. On June 23, 2009, RAB detained JMB IT head Rajeev, who acknowledged to downloading explosives information from the Internet, translating it into Bengali, and sending it to Mizan.Bashar (The Dailyster), "which is a big problem for our national security."

In His Book "Cyber Law in Bangladesh," Ahmed Dr. Zulfiquar Presents The Results of the ICT Act as Follows:

1. There is a lack of public awareness and implementation,
2. The law ignores intellectual property rights entirely, with no provisions for patenting copywriting, trademarking, or electronic data and information. The law is silent on the rights and obligations of domain names, which are the initial step in e-commerce.
3. A police officer investigating a cyber crime must have relevant skills: according to section 80 of the ICT Act 2006, police officers must be at least an inspector's rank.
4. Any crime committed in violation of this Act will be investigated by the police. This provision should be changed to require that the Inspector of Police and above have adequate ICT knowledge (e.g., a diploma or bachelor's degree in an ICT-related subject or relevant training in this field).
5. Section 54 of the Criminal Procedure Code and Section 80 of the Information and Communications Technology Act of 2006: Section 80 of the ICT Act 2006 rewrites section 54 of the Criminal Procedure Code of 1898, giving police more authority. In Bangladesh's legal system,

police empowerment is referred to as a "black legislation." Whereas it is a pressing problem that Section 54 be repealed, the ICT Act has reintroduced measures that are old wine in new bottles. Countries like Bangladesh are blindly applying the Criminal Procedure Code on the Internet, despite the fact that it is a distinct medium than the actual world.

6. Fundamental Rights Violations: We all know that the Constitution is a country's supreme law. Every citizen of Bangladesh has the right to freedom of opinion, conscience, and expression, according to Article 39 of the country's constitution. However, Article 57 of the ICT Act has usurped these rights, which is in direct violation of Bangladesh's Constitution. Everyone has the right to criticize the executive in Western countries such as the United Kingdom and the United States.

Bdnews24.Com. (2018) Publish a Very Important Report that,

In the coming days, cybercrime will be the most major crime.' The government was aware, according to the law minister, that the new law could cause new controversy in the country. "If the new law is passed, sections 54, 55, 56, and 57 of the ICT Act can be repealed and replaced with the new law to avoid redundancy," he explained. He went on to say that the new regulation will not be "unfair" to reporters.

Cyber crime is on the rise in Bangladesh, as the country's internet penetration rises. ICT legislation solves the problem, but it also draws criticism, particularly in Article 57, which some claim essentially limits freedom of speech and expression. The disclosure of false, obscene, or defamatory information in electronic form is illegal under Section 57 of the Act. Any offense is punishable by a minimum of seven years in jail and a maximum of fourteen years in prison under this section of the ICT Act. The maximum fine that can be imposed is taka 10 million.

‘The Daily Star (2018) Publish Another Important Report on Digital Security Act, 2016 that, According to BLAST (Bangladesh Legal Aid Services and Trust), the cyber crime tribunal has

registered 520 cases where the number of female victims was 90. Out of 520 cases, 326 cases have been disposed of in the mentioned period.⁵

The most important thing that we must need to review is about „ Digital Literacy „, as well as preventive measures through awareness campaign at the root level. These days number of people can afford digital devices and do have accessibility on the internet which mostly covers Facebook. However, people are still now not that much well informed about digital literacy and that must be regarded with proper action and requirements. In Bangladesh, till now people perceive Facebook as the internet where they are not well informed and aware of the privacy settings and security because of a language barrier which has been mostly written in English. This context must be regarded as one of the important issues due to the safety and security as well as awareness through digital literacy.

2.2 Gap in the Existing Literature

The Women and Child Abuse Suppression Act of 2000 punishes 'sexual harassment' with any indecent gesture, whilst Article 14 makes it illegal to reveal a victim's identify in the media.

The High Court of Bangladesh interpreted "sexual harassment" in the workplace and in educational institutions to include specified forms of online discourse in both the public and private sectors in its 2009 verdict in **BNWLA v. Government of Bangladesh**. In the absence of legislation adopted by Parliament, this ruling contains 11 directions that are binding on everyone.

Surprisingly, the cybercrime legal system now prioritizes defamation of the Prime Minister and the President over women's protection. Most cases and complaints have been decentralized and based in Dhaka, rather than having effective mobile courts in remote, rural areas and suburbs. Most victims do not want to go to the police, who may be hesitant to handle such a case; in such circumstances, a reference to the High Court's sexual harassment guidelines and existing law may be beneficial. For fear of embarrassment and/or future police harassment, most women, married or unmarried, do not seek legal assistance.

⁷ Ellery Roberts Biddle, "Bangladesh's ICT Act Stoops to New Lows," Global Voices Advocacy, 20/07/19,<http://bit.ly/1O1Lxy9>

⁸<http://www.thedailystar.net/law-our-rights/cyber-crimes-70592>

CHAPTER: THREE

THEORETICAL FRAMEWORK

3.1 Introduction

Cyberspace, according to internet theorists, offers close and instant interaction between geographically distant individuals, allowing for new sorts of associations that lead to cybercrime and cyber deviance. Simply described, cyber- offense is an offense which is aided or promised through that use its an calculating machine, network, or physical instrument. Computers on devices can act as criminals' agents, collaborators, or targets. It afford receive space on a single calculating machine otherwise in different virtual or non-virtual environments. It is acknowledged that the existing legal definition of cybercrime differs greatly across the legal system.

3.2 Classical Sociological Theorists

The real contribution of comte's (1865) positive philosophy to social and political philosophy is his positive philosophy. Positive thinking is the final stage of his intellectual development, according to him. In his philosophy, positivism is founded on logic and objectivity. Analysis, testing, and observation have received less attention. According to him, positivity is not only accountable for societal reformation, but it is also unavoidable. Creating a new society and social structure is critical.⁶

1. Durkheim 1893 (1933) underlines that as society and industrialization progressed, labor division became not only significant but also unavoidable. Labor specialty is related with the Department of Labor. Society becomes more efficient as a result of the division of labor, which contributes to social progress. Many new vocations and ideas are born as a result of progress.

2. According to Pareto (1961), each person engages in both logical and illogical behavior. In reality, everyone tries to rationalize unreasonable behavior. He also believes that every social occurrence has two sides: reality and form. Where the former refers to the thing's true significance, and the latter to the way the event manifests itself in the human mind. He refers to the first as the

9. Crozier, B. *A Theory of Conflict*. Hamish Macmillan, London, (1974).

10. Thomas, Douglas and Loader Brian, *Cybercrime Law Enforcement, Security and Surveillance in the Information Age*, Routledge, London. (2000), Pg 8.

purpose and the second as the thematic aspect. He also believes that all of a person's activities have two ends: one is the goal and the other is the goal.

3.3 Modern Sociological Theorists

1. According to Marton (1938), the gap between permissible aims and means causes pressure. In today's society, success is predominantly defined by material accomplishments and social status. Individuals in a heterogeneous economy like India must choose their own route and work hard to make a living. As a result, career and employment opportunities are highly competitive. Marton applies the theory of denomination to the study of deviant conduct in various communities. Success is undoubtedly regarded considerably more than virtue in today's society.

2. Beck (1992) coined the phrase "risk society" to describe the present environment. New modern and technologies bring with them dangerous societies. Both aspects exist in today's world. Beck coined the term "reflective modernity" to describe the new or improved but still new developing form. In the West, there has been a customization process.

3.4 Post Modern Sociological Theorist

Emotion and passion have made their appearance in postmodern society. The downsides of technology are now well acknowledged in the modern period. Individualism was significant in modern civilization, but in the post-modern age, collectivism or group was emphasized.

1. According to Boudrillard (1984), symptoms used to stand for something real, but now they refer to themselves a little more. The postmodern world is built on the distinction between what is genuine and what is artificial. There is a clear distinction between the indicators and reality.⁷

2. According to Jameson (1991), postmodernism is usually associated with a radical break. "Culturally influential," he said of the new style. The four aspects are crucial to postmodern society, according to Jameson.

11. Denning, Dorothy ER, *Information Warfare and Security*, (1999) Pg 166

12. Comte, *A General View of Positivism*; Trubner and Co, Cambridge University press, August (1865)

In a modern culture dependent on reproductive technology, particularly electronic media such as television, computers, and the internet, impressions are formed.

3.5 Others Theories : Other theories bolster the above-mentioned sociological idea. The theories that follow look at crime, deviant behavior, and people's transitions from physical to virtual space and back.

1. Social control theory and cyber crime: The attempt to manage the behavior of a group or members of a society according to set rules is known as social control. As a result, there exist limits, either internally or externally imposed.

2. Social Education Theory and Cyber-crime: Individuals learn abnormal behavior, according to Tarde (1903), and it is not physiologically inherent.

3. Space Transition Theory: Jayashankar (2008) suggested the "Space Transition Theory" to explain the conduct of people who carry their compatible and inconsistent behavior into physical and virtual space. A virtual area allows a person to express his sentiments and even his wrath toward another individual.

3.6 OPINION

Space Transition Theory” is an explanation about the nature of the behavior of the persons who bring out their conforming and non-conforming behavior in the physical space and cyberspace (Jaishankar 2008). Space transition involves the movement of persons from one space to another (e.g., from physical space to cyberspace and vice versa). Space transition theory argues that, people behave differently when they move from one space to another. The postulates of the theory are:

1. Persons, with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position.

2. Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cyber crime.

3. Criminal behavior of offenders in cyberspace is likely to be imported to Physical space which, in physical space may be exported to cyberspace as well.

4. Intermittent ventures of offenders in to the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape.

6. Persons from closed society are more likely to commit crimes in cyberspace than persons from open society.

3.7 Conclusion

Alarming changes in the social environment are thought to be the cause of contemporary society's dynamic nature. New social changes result from the introduction of new cultural aspects into society. A sophisticated culture of networking and informational pervades today's society. Many changes in the social structure have resulted from the information technology revolution.

CHAPTER FOUR

NATURE AND HISTORY OF CYBER CRIME AND ITS CLASSIFICATION

4.1 Introduction

The majority of us are familiar with the different characteristics of the internet and the services it provides, but only a few of us have seen or are aware of its drawbacks. A cyber-crime is any crime or criminal conduct that involves the use of a computer or network as a target or tool. In everyday language, it simply implies using a computer to harm someone, a corporation, or a country.

In the world of technology, cybercrime is on the rise. On the World Wide Web, criminals profit from the personal information of Internet users. They scour for black market products also services in bought and sold. These until there is entry on the most secret administration information. Individuals, property, and government are the three basic categories of cybercrime. Depending on the category, the sort of process employed and the level of complexity differ.

4.2 Definition of Crime

An offense is a law that is committed otherwise excluded inside infraction its an public act, is prohibited otherwise ordered; Violation or infraction its certain universal claim or ought the rest each an entire people, to consider an people. Its overall social potential, as distinct from a civilian injury. Now computer crime is “a crime, such as cheating via the Internet that requires wisdom otherwise usage its calculating machine technique. It is also called cyber-crime.

4.3 Definition of Cyber Crime

This level it's the fallen part in embodied offense also cyber crime will increase significantly inside this subsequent something years. These is an issue who demand per stay acknowledged, with merchandise also administration which a predominant also extremely heavier threats on cyber safety. Cybercrime afford be widely define namely an offender action involved fact technique infrastructure, with unauthorized entry (disallowed entry), unauthorized interference, information tampering (disallowed, malicious, removal, degradation, change alternatively tampering with calculating machine information), Fraud (theft), also electric bunk. Includes everything to

download invalid song documents per theft lot its plunk to online bank calculation. Cybercrime further covered nonfinancial crimes, namely as made also distribution against going various calculating machine alternatively posting secret merchandise fact going this Internet. ⁸

4.4 Nature of Cyber Crime

The Internet was advanced, that founders its the Internet was little notion which the Internet can be abuse because offenders activity. However that reality this is occurrence fairly also broadly around that universe. Currently these query is how this crimes could be behavior medium some common and great method. Whether we take an deeper look, this willpower prove as thither is not much other among seemingly usual offense also cyber offense. This primary limiting rank of distinction is that means by which crime occurs. Conventional crimes occur primarily in the regional and real earth, however cyber-offense is regionally limitless also occurs on a global that is a electric otherwise unearthly any one. Whatever more main query is moved about that physical its cyber-offense, if that is an offenders offense alternatively an citizens wrongdoing otherwise torture. This reply will dependent going that temperament its the incident. Following this passage of the ICT (Information and Communication Technology) Act, 2006, whole calculating machine offenses mentioned is currently considered offenders offenses.

4.5 Reason behind the Cyber Crime

There is a lot because wherefore cyber-offenders commit cyber-crimes; The main ones are mentioned below:

1. For recognition
2. For fast rupee.
3. On war an because same gratitude that trust.
4. Less costs its online work the rest in worldwide reach out.
5. Caught with act also application agencies is low efficient and also costly.
6. Recent opportunities per make juridical work usage technological masonry.

13.gethackingsecurity. (2019). *Cyber Crime : History and Evolution*. [online] Available at: <https://gethackingsecurity.wordpress.com/2019/06/22/cyber-crime-history-and-evolution/>

14.ibid

7. Government investigations and criminal trials are rare.
8. Measure any concrete regulator.
9. Deficiency its reporting also the value,
10. Disadvantage to consolidation.
11. Narrow media cover.
12. Corporate cyber-offenses is committed aggregately also no with individuals

4.6 History of Cyber Crime in Bangladesh

Cyber-offense has an small yet very eventful story. In addition to a grand reading near itself, watching that story its cyber-offense will pay individuals and society that chance in eliminate mistakes dressed on the bygone. The last registered cyber offense occurred on 1820! Not surprisingly, that abacus, hence is medium in stay that oldest schedule its an calculating machine, dates from about 3500 BC. In India, Japan and China. This latter computer age, anyway, start gladly Charles Babbage's analytical instrument. This maiden online bank called First Virtual was opened in 1994. This has opened up many chance to hacker. Cyber-offense was gradually gaining popularity. In 1995, that confidential worship also Drug Enforcement Agency (DEA) received these premier Internet Wiretap, much choice an phone Wiretap. DEA was capable in closed under an institution that was sale invalid cells phone cloning furniture. This is a keen arise on cyber crime on Bangladesh also act application agencies in Bangladesh seem to be search that verily tough in handle this technological offenses. Cyber-offense there is meanwhile happened an matter of anxiety on Bangladesh, both in the personal and universal sectors. Over the past decade, the private and public sectors have revolutionized this usage its technological advances. The rest in disallowed interference in that method, the institution loses big amount of secret news resulting in huge monetary damage. That there is meanwhile done marked the monetary organization on particular are among that maximum threaded entities on cyber crime which simultaneously reflects on private lifetime. Whatever improvement associate there is begun work on whom in equipment cyber-offense also improvement efficient communication.⁹

15. Peter Norton, *Introduction to Computers*, Fifth Edition, (Career Education) 2019, p. 23

16. Rashid Hamidur, *Internet History of Bangladesh*, <http://ezinearticles.com/?Internet-Historyof-Bangladesh&id=2327010>,

4.7 Classification of Cyber Crime

In the system, there also numerous sorts its cyber-crime. We can categorize them into four broad groups, as described below:

Individuals Level Crimes

Transmission of Child Pornography, vexation its anyone usage an calculating machine, namely as follows email, cyber abasement, hacking, obscene expression, email cheat, net unjust claim, contaminated anthology, kidnapping, delivery, posting, Phishing, deposit cards bunk, also publicity its indecent components, with software confidentiality, are examples its cybercrimes committed against individuals. The potential harm to an individual from such a crime is immeasurable.

Crime Against Property

Other arrangement its cybercrime is cybercrime versus whole types its wealth. This offenses covered calculating machine destructive (destruction in other people's wealth), intellectual wealth offenses, threats, salami assault. Such crimes are General on monetary organizations otherwise because that motive its committing monetary offense. A significant peculiarity its these kind on crime is the correction is therefore short the it is not usually noticed.

Crime Against Organization

Cybercrime versus formations is that third category in cybercrime categories. Cyber terrorism is an type its offense on these department. This expansion in the internet there is revealed which cyberspace is existence utilized with people also band in exert pressure on universal administration as like well as scare a country citizens. While an human individual, fracture among an administration and martial program, the offense becomes terrorism.¹⁰

Crime Against Society

18. Borhanuddin A.R.M, *Cyber Crime and Bangladesh Perspective*, Available Online: <http://www.scribd.com/doc/3399476/cyber-crime>, 19.. Lecturer, Department of Law, Britannia University, Comilla-3500, Bangladesh and M. Phil Research Fellow under the Faculty of Law, Chittagong University, Bangladesh.

20. Anon, (2019). [online] Available at: <http://www.thedailystar.net/archive.php?date=2014-09-06>, last visited 25.07.2019.

Cybercrime against society is the fourth category of cybercrime. Fraud, cyber terrorism, online jacking, young peoples pornography, financial crime, illicit article disposal, net unjust claim, cyber ban, information trafficking, salami attacks, also argument bomb kinds is whole with in these category. There were crimes involved. Computers, lofty-multiplication search engine, also typographer could be usages in made fake money remark, tribute impressions, also mark sheets, in various substance.

4.8 Different Types of Cyber Crime

Credit Card Fraud

All you have to do is kind the credit card numbers on the seller's www page because online transactions. Whether electronic trading is not protected, credit card number can be theft with hackers which may abuse the card in disguise as credit card owners. Millions its rupees can be misused through computerized bank account fraud. In whatever suit, man have been arrested also others have been accused with theft also abusing credit card numbers.

Online Gambling Millions of websites offer online gambling, which is often regarded as the primary method of money laundering. These sites may be linked to drug trafficking, though this has not been confirmed.

Cyber Defamation

Cyber defamation occurs when someone defames someone else using a computer and/or the internet. It has the potential to destroy a person's personal image as well as a company's, bank's, or organization's reputation.

Salami Attacks

The Financial Crimes Commission employs salami attacks. The essential goal here is to adjust something so minor that it will go unnoticed in every circumstance." A bank staffer, for example, may program bank servers to deduct a little sum from each customer's account. This illicit debit may go unnoticed by the account user, yet it earns a bank staff a large sum of money each month.

Data Diddling: A computer can do data diddling by modifying the provisional information right before running also then change that again later that processing is finished. When private firms computerize their systems, government agencies may fall victim to data debugging programs.

4.9 Reasons of Cyber Crime

In her article that definition its act, Hart wrote, "People are weak, hence that regulation in act is needed in protection their." In that context in cyberspace, we may be country which calculating machine is precious, also which that regulation in act is required to protect also protection their versus, cybercrime. This follow is something on this causes because the calculating weakness:¹¹

Easy to Access

The challenge with preventing unwanted access to a computer system is that every break is due to complex technology rather than human error. Covertly planted logic bombs, cotter loggers which theft entry code, improved voice recorder, Retina painter, and other devices which can trick the biometric system also breach the firewall could be used in found around an variety of safety measures.

Complex:

The mankind intellect is flawed, also this is improbable in avoid making mistakes at any point. This lack of access to computer systems is exploited by cyber thieves.

Loss of Evidence

Because all data is deleted on a regular basis, evidence loss is a very prevalent and evident concern. The criminal justice system will be crippled if more information is gathered beyond regional lines.

Impact of Cyber Crime

Victims of crime may lose precious items. Security, tranquility, money, also wealth is probably the most fundamental standard, as them help in satisfy a variety of desires. Financial loss,

21. <http://www.thedailystar.net/archive.php?date=2014-09-06>, last visited

22. Borhanuddin A.R.M, Cyber Crime and Bangladesh Perspective, Available Online: <http://www.scribd.com/doc/3399476/cyber-crime>,

intellectual property theft, and a loss of consumer confidence and trust are all possible outcomes of a single successful cyber-attack. Cybercrime has a wide range of effects on society, both online and offline. Identity theft can have a long-term impact on hunting its cyber-offense.

4.10 Current Situation of Cyber Crime in Bangladesh

Bangladesh, which lacks natural resources, is attempting to build its economy by using the ICT industry. Many countries have taken benefit in that potential afford with ICT in developing an principle structure, establishing guidebook, also building an nationwide ICT trick namely portion in a larger nationwide improvement scheme in recent years. Bangladesh aspires on make information and communication technology (ICT) a significant engine of socioeconomic development. The current government has proclaimed Vision-2021, which states that by 2021, the country would be digital and have a per capita income comparable to an medium-revenue state. However, that administration and various stakeholders worthy be aware which the continuation of the Internet also various networks in transform these state in an digital state may result in increased crime..¹²

4.11 Some New Dimensions AS Legal Remedy Against Cyber Crime

Technical defenses are unquestionably superior to legal remedies for preventing high-tech crime, but they are always vulnerable to being destroyed because they are not permanent. Those with more advanced technology than we possess have the ability to breach the security barrier at any time. As a result, legal and other associated remedies are required to combat the aforementioned predicament. In addition to existing remedies, the state may implement new efforts similar to those used by something its that universal most advanced high-tech states. Let's have a look at some of their characteristics:

Constitutional Safeguard

Bangladesh is a state where the constitution reigns supreme. That Constitution serves as a mother, protecting and insuring the claim also responsibilities its both that country and this man.

23. <http://www.thedailystar.net/archive.php?date=2014-09-06>,

24. Chowdhury Iqbal Ahmed, Department of Sociology, Shahjalal University of Science and Technology, Sylhet-3114, Bangladesh. E-mail: Iqbal_chy@yahoo.com

25. Borhanuddin A.R.M, *Cyber Crime and Bangladesh Perspective*, Available Online :<http://www.scribd.com/doc/3399476/cyber-crime>,

Constitutional measures versus cybercrime may lead to a national mood that is more effective in comparison something various formation or juridical redress. The means of enacting such a provision could be by constitutional amendment.

Special wing of Police

To secure a peaceful cyber cloud in a digital Bangladesh, we must provide law enforcement authorities with training and technology. Cybercriminals are not adversaries of any one country or region; rather, they are the world's shared enemy.

Cyber Crime Agency by Government

Given the current state of internet use and the rise in cyber-crime in Bangladesh, the government may consider establishing such bodies. The value of such agencies is that they will be able to undertake multifaceted tasks such as improving internet infrastructure, maintaining ISPs, repairing internet costs, combating cyber attacks, and so on.

4.12 Conclusion

Thus, while violent and property crime rates have dropped significantly, other types of crime continue to rise alarmingly, according to police statistics. The hate survey concludes that economic, social and political factors are more responsible for changing the nature and type of crime than geographical, seasonal and criminal justice factors. Although thither is an deficiency its accurate crime statistics also empirical research to the causes its offense crim

CHAPTER: FIVE

DIGITAL SECURITY ACT, 2018

5.1 Definition

Digital technology is providing new opportunities every day, all around the world; recent ways in work, the game, transaction, also communicate. We are encompassed by digital identity also information that must be shared across networks gladly other person, devices, also organizations. As more in this gadgets become attached, they will be able to assist us in accessing a range of services, such as communication, payment, and government. The advantages are clear, but there are also safety concerns. Personal, corporate, and

government information, as well as personal identity, are presumably at risk.

5.2 The Main Characteristics of Digital Technology

Media Integrity

Information saved in analog format cannot be replicated except loss of quality. This worse that copy becomes as more copies are made. Digital data, on the other hand, does not degrade as much as it is reproduced. Movie, video, music, and audio materials, for example, can be replicated and distributed in digital format with the same high quality as the original.¹³

Media Integration

The inability of many traditional systems to merge several media kinds is a key drawback. For example, a telephone can only broadcast and receive sound. Similarly, you can expect a character on television to respond to your inquiries. It is, however, simple to connect media with digital data. Interactive sound with video or graphics with video can be created in this way.

Flexible Interaction

26. What is Digital Security? (n.d.). Retrieved December 10, 2021, from <https://www.gemalto.com/companyinfo/digital-security/digital-security-markets>

27. Global Investigative Journalism Network » Digital Security. (n.d.). Retrieved December, 10, 2021, from <https://gijn.org/digital-security/>

28. B. (2019, July 27). What is Digital Security?, from <https://www.justaskgemalto.com/en/what-is-digital-security>

The digital realm allows for a wide range of interactions, from one on one meetings to one to a lot broadcasting, also everything in within. Furthermore, this exchanges could be simultaneous also tangible period.¹⁴

5.3 Critical Review of the Digital Security Act, 2018 from a Public Policy Perspective

The Digital Security Act 2018 was approved by the President on 08 October 2018. This is the 46th law of 2018. The law was enacted to confirm nationwide digital safety also to legislate acts on digital offense detection, prevention, repression, also justice. And various concerned problems .Under that act, there is a 13-member National Security Council, chaired by the prime minister. The law provides for imprisonment of 7 to 14 years and a fine of taka 25 lakh to taka 1crore.

The vision of the Awami League (AL) government led by Prime Minister Sheikh Hasina is to build a digital Bangladesh. In this case, information technology gets the highest priority. In this recent age of science and technology, information and communication technology (ICT) is providing many benefits, but at the same time it is also bringing some problems like cyber-crime. In these circumstances, the implementation of such laws is essential to ensure national digital security through the prevention or control of digital crime. The primary motive its these Act is in protect the lives also property of the nation and the public from cyber-crime (Digital Security Act 2018, 2018).

Before verifying the Digital Security Act (DSA) 2018, some necessary sections should be highlighted. Section 8 of DSA 2018 states that the concerned Director General (DG) may honor the Bangladesh Telecommunication Regulatory Commission (BTRC) to retrieve any information or block any platform if he deems it harmful. In response to the BTRC, the government will receive instantly work in transportation and block that harmful subject matter reported Bangladesh: New Digital Curry Laws Put Dangerous Restrictions on Freedom of Expression, 2019).

Article 21 provides austerities for the liberation war, the spirit of the liberation war, the father of the nation, the national an them and any kind of propaganda against the national flag. However, what is meant by consciousness of liberation war has not been properly defined. This law. Article

29. The Information Age/Notes.(n.d.), from https://en.wikibooks.org/wiki/The_Information_Age/Notes#5

25 deals with the disclosure or distribution of offensive, false or threatening information or data. It also includes tarnishing the image also fame its that country otherwise spreading confusion. This

Section annoys all investigative reports directly in the media. Corruptors will have the opportunity to intimidate journalists by claiming that reports have attacked them (Why the editorial board opposes the Digital Security Act,2019).This clause makes it almost improbable in publish any negative description related a corrupt person. Again, there is ambiguity about the reading confusion in this section. Since it does not provide a clear definition of confusion. Instead of being helpful, the media has become a weapon of harassment. This clause does not even clarify what the image or reputation of the state is. This could hinder writing about deaths, disappearances, or extrajudicial killings in custody, as state forces such as the police, RAB, and similar agencies are involved.¹⁵

DSA 2018 also takes action against any publication or broadcast that hurts religious values and religious sentiments, but the term religious sentiment is highly undefined. There can be plenty of explanations for hurting religious feelings. This will avoid journalism analysis in the society. This section may be used to harass journalists (Review Digital Security Act: TIB, 2019)

Article 29 of DSA 2018 relates to the disclosure and distribution of defamatory information. Article 31 deals with crimes and punishments for deteriorating law and order (Analysis of the Draft Digital Curry Bill, 2018). Article 32 relates to offenses and penalties for breach of official privacy. It is nothing more than a heinous legacy of colonial law. At the time, it was protecting the British administration from any kind of accountability (Why the editorial board opposes the Digital Curry Act,2019). This section directly contradicts the Right to Information (RTI) Act. Article 43 is the most heinous article, which deals with search, seizure and arrest without warrant (Hasan, 2019).It allows principle in enter any premises, search and network, seize computers also servers, and make arrests on suspicion. Threats of arrest without a warrant will create panic among journalists and activists. The most dangerous aspect of this clause is that law enforcement agencies can shut down

30.The Daily Star.(2019). *Digital Security Act, 2016*. [online] Available at: <http://www.thedailystar.net/opinion/interviews/how-does-it-affect-freedom-expression-and-the-right-dissent-1305826last>

a newspaper or TV station or an online news portal by confiscating its equipment and systems (Analysis of the Draft Digital Security Bill, 2018).

Thus, the above discussion proves that DSA has many fundamental flaws. Although the government tries to show that this law is for crime prevention and security, the reality is different. DSA is about controlling digital media. This law regulates media operations, censors various relevant subject matter also rheostat media liberty and liberty of speech. By violating freedom of speech, it is constantly violating the constitution (Bangladesh: New Digital Security Act imposes dangerous restrictions on freedom of expression, 2019).

The law gives government officials unlimited powers. It should be noted and highlighted that the policy should not be thematic. A subjective policy can be misinterpreted and misused. However, this law is somewhat vague. Appropriate definitions are not provided where necessary. DSA only creates an environment of fear and panic. Prior to the Digital Security Act 2018, ICT was 2006. It was used for the same purpose to control the media, journalists, activists and others. Under Section 57 of the ICT Act, they were done. Now, the same things can be done by the misuse of DSA 2018.

The awesome feature of DSA 2018 is that it gives a lot of power. Police often allow arrests without a non-bailable warrant. This indicates that the law is protecting journalism under police control. of the 20 sections, 14 are non-bailable, five are bailable and only one can be negotiated (Hasan, 2019). The minimum penalty is one year imprisonment, and the maximum penalty is life imprisonment, but mostly between four and seven years (Digital Security Act 2018, 2018)

5.4 Conclusion

In concluding remarks, it can be said that the Digital Security Act of 2018 has violated the citizens Freedom of speech is a constitutional right. Although this law speaks in protection that spirit on the liberation war, the DSA itself violates the spirit of our liberation war. DSA 2018 against the principles of democracy and democratic governance. The DSA is nothing more than an obstacle to independent journalism. This is in conflict with the Right to Information Act.

CHAPTER: SIX

CONTEMPORARY TRENDS OF CYBER-CRIME IN BANGLADESH, REGULATORY GAPS AND WAY OUTS

6.1 Introduction

Cybercrime is defined as any illicit behavior in which a computer is used as a device, a destination, or otherwise both. E-crime is another term for cybercrime. E-crime refers to crimes committed with the use of a computer or other form of information and communication technology. This is a criminal action carried out through the use of a calculating machine also that Internet. These might range from downloading pirated songs to theft of millions of dollars from other people's online accounts. Cyber-offense is a term that refers to illegal action that takes place on a computer or through the Internet. Some of them are illegal in various nations, while others have a murky legal position.

6.2 Cyber Crime Areas

Cybercrime is the fastest-growing type of crime. Criminal networks are increasingly utilizing the Internet's speed, advantage, also anonymity to carry out a diversity of their offenders' operations which pose a threat to people all over the world. New cybercrime trends emerge on a regular basis, with the global economic impact estimated to be in the billions of dollars. Cyber offense encompasses a wide perimeter in actions that could be split into two groups. A computer network otherwise instrument is that destination of a cybercrime. Virus and denial-of-service attacks are examples of such crimes, as is the use of computer networks to carry out other criminal actions. Crimes against minors, financial crimes, and even terrorism are examples of such crimes.

6.3 Victims of Cyber Crime

Unfortunately, as technology advances, cyber-crime will become more prevalent in 2019. According to the 2018 Cyber Security Violations Survey, 43% of firms had experienced a cyber-security breach in the previous year. California alone has lost more than 4.214 billion dollars due to cybercrime in the United States. VPNs are increasingly being utilized to protect people's online privacy (check out the best VPNs here). Despite the fact that most people are aware of the dangers of clicking on a link or opening an email, statistics show that attacks are on the rise. As technology

advances, so do hackers; the globe is falling behind in the fight against cybercrime, which is frightening. Every day in 2017, 780,000 records were lost.¹⁶

According to the Economic Impact of Cyber Crime report by McAfee (February 2018) Cybercriminals are quick to adapt. Malicious behavior on the Internet is at an all-time high. The figures are on a monthly or annual basis, not daily! Cybercriminals are always coming up with new and dangerous ways to target their victims. Payments and transfers from and to cyber criminals have become more understandable since the introduction of bitcoins. Every day, over 24,000 fraudulent mobile apps are blocked.

6.4 Contemporary Trend of Cyber Crime

- Bangladesh bank heist.
- Threatening to pm sheikh Hasina in 2004
- The international war crimes tribunal is embroiled in a skype scandal.
- Hacking the Brac Bank Bangladesh
- Inserting porn to the website of Bangladesh national parliament

To violate user privacy, cybercriminals are employing more sophisticated and scalable methods, and they're succeeding. In 2017, two billion data records were hacked, with just 4.5 billion records breached. Here are the top cyber security concerns for 2019, as well as a rising trend for 2020.

Advanced Phishing Kits

Every second, four new malware samples are developed. Because most phishing sites are only online for four to five hours, phishing remains one of the most successful attack vectors. Phishing attacks are reported by only 17% of users, and thus is considered a low-risk activity. As a result,

31. Goodman, Marc D, Why the police don't care about computer crime. Harv. J L and Tech. (1996) pg . 465

32.D. L. Shinder. Scene of the Cybercrime: Computer Forensics Handbook. Syngress Publishing, Inc, 2002.

33.. Khan, Dr. Borhan Uddin, Introduction to Cybercrime, Kamrul Book House, Dhaka, 2014

only 65% of all URLs are now rated trustworthy. This puts a strain on both the consumer and any business, especially those with an internet presence.

Due to the large number of new phishing kits available on the Dark Web, we believe that 2020 will be remembered for advanced phishing attacks. Only people with rudimentary technical skills can use these kits to carry out their own phishing assaults. Phishing will become a more serious attack strategy as more tools become available.

Remote Access Attacks

Remote attacks are growing more sophisticated as well as increasing in quantity. Crypto jacking, which targeted cryptocurrency owners, was one of the most common types of remote access attacks in 2018. The threat of enclosure devices is another common sort of attack, Remote access assaults are one of the most popular attack routes in a connected home, according to our Threat Intelligence database. Because these devices typically have open ports and must be redirected to an external network or the Internet, hackers target PCs, cellphones, IP cameras, and Network Connected Storage (NAS) devices

Attacks via Smartphones

Unsafe surfing is one of the most popular attack vectors on cellphones (phishing, spear phishing, malware). According to RSA, mobile platforms account for more than 60% of online fraud, and mobile apps account for 80% of mobile fraud rather than mobile web browsers.

This is a big threat because most individuals use their phones to make financial transactions or manage sensitive data outside of the security of their home network. Because users often save all of their data on their phones, and cellphones are now used for two-factor authentication - one of the most extensively utilized cybersecurity techniques - the security risk grows if the device is lost or stolen.

Vulnerabilities in Home Automation and the Internet of Things

The consumer Internet of Things (IOT) business is predicted to grow to more than seven billion devices by the end of 2020, according to Gartner. Because a large percentage of IOT devices lack a user interface, many users do not consider them to be a flaw. This can make it difficult to figure

out what kind of data the gadget collects or controls. IOT devices, on the other hand, are collecting more than just useful user data. They could be used by attackers or tools to launch a distributed denial-of-service (DDOS) assault. Because focusing on security would drastically increase production and maintenance costs, IOT devices are not designed to be secure.

Online Child Sexual Exploitation Material

Online child sexual abuse material, or CSEM, and self-produced explicit material, or SGEM, is increasingly being tracked by police. "While the majority of CSEMs are still shared via peer-to-peer networks, more extreme aspects are increasingly being found on the Darknet," according to the research. Online CSE remains a particularly difficult format.

Payment Card Fraud

In the recent year, almost every EU member state has reported skimming attacks, but Europol maintains that the geo-blocking mechanism has helped to limit such attacks in Europe. Despite this, the research claims that "skimmed card data is often exchanged on the dark web and cashed out in places where EMV deployment is sluggish or non-existent."

"Toll fraud" (the avoidance of tolls) and "card-not-current" fraud, which largely targets the EU's transportation and retail sectors, are two other major types of fraud. According to the research, many EU countries have "increased access to points of sale and abuse, as well as a rise in the creation of phony companies to profit from compromised information."¹⁷

Crypto Jacking

Attacks on cryptocurrencies that leverage bandwidth and processing power to attack computer users are becoming more widespread. "While this is not unlawful in some situations," according to the research, "it does generate extra cash streams, which pushes attackers to infiltrate reputable websites in order to exploit their users' computers." Actual crypto mining malware has the same effect, except it can cripple a victim's computer by using all of its processing power. Crypto mining malware is projected to become a regular, low-risk revenue stream for cybercriminals due to the availability of such attacks and attack tools, according to Europol.

Bit Coin Popularity

Despite increased interest in virtual currencies like as Monroe, which promises greater privacy and can be mined without the requirement of highly specialized tools - including systems for malware

34. Singh; The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006

35. BBC News, Hacking: A history, 27.10.2000, available at: <http://news.bbc.co.uk/1/hi/sci/tech/994700.stm>.

36. <http://www.bdlawdigest.org/cyber-crime-a-new-menace-in-modern-era/>

victims - Europol believes Bitcoin has become a "significant cryptocurrency cyber crime investigation."

Social Engineering

Europol cautions that social engineering - cunning - attacks will be simple, inexpensive, and effective. "Phishing via email is the most popular kind of social engineering," according to the research, "although viewing (by telephone) and smashing (via SMS) are less common."

"Criminals use social engineering to accomplish a variety of objectives, including obtaining personal data, hijacking accounts, stealing identities, initiating illegal payments, or persuading victims to engage in any activity that is against their interests, such as money transfers or personal sharing. Taken annex Data," he continued.

Spam and RDP Attacks

According to Europol, the number of automated attack toolkits designed to target vulnerabilities in commonly used software, such as the Windows operating system or plug-ins like Flash and Java, is constantly reducing. In order to obtain access to targeted networks, attackers are increasingly relying on "spam, social engineering, and remote desktop protocol (RDP) brute-force."

New Life for Old Tricks

The Europol report also serves as a reminder that many sorts of criminal activity never die; they simply evolve to fit the present environment.

Fraudsters operating outside of West Africa - and other regions - have, for example, been altering their assault tools and strategies, including developing more complex business email compromise schemes, according to the research.

According to the research, "several old scams, such as technical support scams, advanced fee fraud, and romance scams, still result in a significant number of victims." Due to the seriousness of the damage, phishing remains a significant concern, according to Europol. Such attacks are possible. "A successful effort may be enough to expose a whole firm," it argues, even if only a small percentage of victims click on the bait.

Legal Instruments Related to Cyber Crime

In Bangladesh, there are insufficient laws to prosecute cyber offenders. Bangladesh's courts have enacted the "Bangladesh Information and Communication Law 2006." (as amended in 2009). This

Act's Section 57 (1) provides for a ten-year sentence, with or without a fine. The institution of a special tribunal known as the "Cyber Tribunal" is stated in Section 6 of the same statute.

The perpetrators of such cybercrime could be identified, but they could not be stopped or punished. It hasn't yet rewarded any sort of retribution. It has become nearly impossible for a judge to identify and punish both the perpetrator and the offender due to a shortage of skilled professionals to assist the court.

Under Section 82 of the aforementioned Act, there is only one Cyber-Tribunal in Dhaka City. None of the perpetrators have yet been found guilty by the tribunal. Until a district court cyber tribunal is established, the Sessions Judge has the authority to try such offenses under Section 64 of the Act.

Bangladesh has a statutory organization called the Bangladesh Telecommunications Regulatory Commission (BTRC) that monitors cyber security, but it has yet to deliver on its promise. It has the authority to set up mobile courts with the assistance of other government authorities in order to expedite the prosecution of such offenses.

Present Practices to Combat Cyber Crime

When it turns to focus on the present practices to combat cyber-crime it refers the existing investigation practice, trial procedure & cyber Appellate tribunal.

Investigation Procedure:

A police officer not below the rank of an Inspector of Police shall investigate any offence under this act, according to Section 80 of the ICT Act, 2006. Our ICT Act allows cops to make arrests without a warrant.

Bangladesh Computer Security Incident Response Team is one of the new institutions, units, and groups established by the government to speed up the investigative process. To combat cybercrime, Bangladesh Police has established specialist cybercrime police stations, a Cybercrime Investigation Bureau (CCIB), a Cyber incident response team, and a "cyber-crime investigation cell" and a "IT Crime Forensic Lab."

Trial Procedure:

According to section 70, the cyber tribunal's trial procedure shall be consistent with Chapter 23 of the Code of Criminal Procedure, 1898 (trial procedure by the Court of Sessions). According to Section 71, the accused will not be granted release unless the Government is given the opportunity to present its case on the grounds of bail.

Section 72 states that after the witness or evidence examination is completed, the hearing tribunal must render its decision within ten days, which may be postponed for ten days. The tribunal must issue a decision within six months of the matter being filed, according to section 73. If the judge fails, he or she must submit a report to the High Court explaining the reasons for the delays.

Cyber Appellate Tribunal:

The government is required by section 82 to create one or more Appellate Tribunals to be known as the Cyber Appellate Tribunal. It will be made up of the following elements: - Two Members, a Chairman (appointed by the government) (appointed by the Government).

No original jurisdiction would be granted to the Cyber Appellate Tribunal. It will only hear and decide appeals from the Cyber Tribunal's ruling and judgment. It has made a final decision.

6.5 Regulatory Gaps

Inappropriate designs for increasing awareness about cyber-crime and also lack of the proper application of that design is first regulatory gap. Governments have no specific project to increase awareness about cyber-crime.

The existing legislations are remain silent about various intellectual property rights like copyright, trademark, patent right of e-information and data.

Lack of appropriate department or authoritative body that will have regulatory overseeing power which can safeguard personal and sensitive data. BTRC is such regulatory body but it just focus on the selected issues like national security issues.

The existing traditional cyber defenses such as anti-virus software are ineffective against new threat vectors.

Power to arrest without warrant can be used for arbitrary arrest or for political purpose.

The judges and lawyers are not enough experts to deal with cyber-crime cases.

Existing legislations focused on e-commerce & m-commerce but remain silent about electronic payment of any transaction.

There is no project or campaign held in our country like, Stay Safe Online, Stop... Think... Connect campaign by which all the users get to know, how users of all levels of sophistication can establish and improve their protection profiles in cyberspace.

Inappropriate application of economic framework for cyber security is one of the major regulatory gaps.

There is no separate cyber Security Council exists in Bangladesh.

The existing cyber organizations don't update their org-charts identifying role, even the developing work of the website of government Digital Security agency still in progress.

There are some good initiatives designed through the existing legislations but nobody knows the proper procedure of practice to achieve the goals.

There is no direct provision in Bangladesh to deal with financial frauds in cyber-crime-related law.

Legislations which address specific types of criminal activity are not enough to tackle the problem of cyber-crime.

Existing legislation made emails as an evidence which is conflicting with the country's Evidence Act, that does not recognize as email as evidence.

Bangladesh is not party to any international treaty on cybercrime.¹⁸

6.6 Way Outs

- Workshops and free advertisements might be organized by the government to raise public awareness.

37. Ahmed Dr. Zulfiquar; Cyber law in Bangladesh; (National law Book Company Dhaka, 2009); Page: 110

38. Chapter 23 of the Code of Criminal Procedure, 1898

- Recognizing cyber world crimes and illiteracy should begin at the grassroots level, with institutions, computer centers, schools, and individuals.
- NGO's should work on such project, and they can assist the government. They can also work for the victim.
- To prohibit cyber criminals from committing cybercrime in Bangladesh, the government should implement a cyber law.
- Governments should improve contact with the world community, for example, by becoming parties to various cyber treaties and conventions and adopting cost-effective efforts from global communities to improve cyber security.

Ways to Deal With Cyber Crime

To combat cyber risks, both government and non-government groups must take a coordinated strategy. The ICT department of our government has already taken some measures in this direction. That isn't enough, though. Hackers and intruders find ways to invade our privacy, mess with our sensitive data, and occasionally do long-term damage to a country like ours. We shall recommend measures for concerned agencies to consider in dealing with cyber security in this document.

A. Invest in the Security Aspect of the Butcher: Given the rise in cyber crime in Bangladesh, it goes without saying that a considerable portion of the country's budget should be allocated to improving cyber security in both the commercial and public sectors. The government of Bangladesh has invested taka. 40 crore in the ICT Department to establish a Cyber Security Branch . At the same time, businesses in the private sector should be urged to invest in cyber security.

B. Legal Framework :Our government has passed various laws to prevent cyber attacks and to stop digital harassment.

C. Seminars and Training: Our government has enacted a number of regulations to combat cyber-attacks and online harassment..

D. CERT Group Formation: Computer Emergency Response Team (CERT) is an acronym for Computer Emergency Response Team. This team's job is to deal with any urgent catastrophic crisis caused by a cyber attack. In the guise of BDCERT , the government of Bangladesh has provided us with CERT help 24 hours a day, seven days a week. Each organization and organization must

establish its own CERT. The International Conference on Advanced Communication Technology is a gathering of experts in the field of advanced communication (ICACT)

E. Cyber Security Strategies: Every company should have a strategy in place to combat cybercrime and, if necessary, take prompt action. The National Cyber Security Plan should guide this strategy.

6.7 Conclusion: We have to consider the economic capability, efficiency and availability of resources of our country. The government has almost It has dominated and invested heavily in the ICT sector.

CHAPTER: SEVEN

RECOMMENDATION AND CONCLUSION

7.1 Recommendation

Bangladesh is a country where the constitution reigns supreme. The Constitution serves as a mother, protecting and insuring the rights and responsibilities of both the state and the people. Constitutional measures against cybercrime may lead to a national mood that is more effective than any other organizational or legal remedy. A constitutional amendment may be the best method to put such a provision in place.

The government may also establish a cyber law company, given the existing state of internet usage and cyber-crime in Bangladesh. Such agencies will be valuable because they will be able to do a variety of activities, including developing Internet infrastructure, maintaining ISPs, resolving Internet costs, and combating cyber attacks

To defend against e-mail fraud, behavior through e-mail, and publishing defamatory or illegal photos, the Bangladesh Police has a specific division called the "Anti-Cyber Crime Division," which is led by the Deputy Commissioner of Police. However, due to a shortage of trained personnel, the department has been unable to meet public demand. Due to the plaintiff's disappearance, the case could not be launched. By becoming a plaintiff, there is no way to assume state accountability.

Cyber lawsuits are rarely resolved due to the need on technological experts and experienced lawyers and judges. To handle such matters, judges, lawyers, and specialists must be trained.

Because ordinary people are frequently exposed to cyber attacks and millions of computers are destroyed, public awareness is just as vital as technical precautions. So, if it is feasible to raise public awareness about the nature, potential barriers, and countermeasures to threats, it will be easier to battle cyber criminals and safeguard the virtual world.

Do not respond to an email message that requests personal information. Email messages will not be used by legitimate businesses to identify your personal information. If you have any doubts,

call the company or type the company's site address into your web browser. You should not click on the links in these messages because they will take you to a false or malicious website

Keep passwords safe and don't use the same password for all of your online accounts. If users notice symptoms soon after their data has been stolen, the repercussions of identity theft and online crime can be considerably mitigated.

Regularly review your bank and credit card statements. Many institutions and businesses now employ fraud prevention systems that necessitate unique purchase patterns. Pay attention to web site and software privacy policies. Before providing your personal information with an organization, it is critical to understand how they will gather and utilize it.

A stranger should not disclose personal information over e-mail, chat, or a social networking site if they do not know them. You should avoid sharing photos to strangers over the internet because the phenomenon of photography is being abused or changed on a daily basis. All citizens should use updated anti-virus software to defend themselves against virus attacks.

To avoid fraud, a person should never enter their credit card or debit card information on an insecure website. Parents should always keep a watch on the sites that their children visit in order to prevent any form of harassment or abuse from minors. Internal business networks must be physically protected from web servers hosting public sites. To govern the information on the sites, it is best to utilize a corporate security tool. Legislators must pass strict statutory laws that protect citizens' interests. The IT department should issue certain instructions and notices to protect computer systems, as well as enact more stricter regulations to combat cyber-crime.

A separate cybercrime protection law should be implemented right once to adequately regulate cybercrime.

The victims of cybercrime must receive complete justice through compensatory remedies, and the perpetrators must be given the maximum kind of punishment so that it can apprehend the perpetrators of cybercrime.

Some Recommendations From The ongoing Discussion are Attached Below for Proper Consideration

The findings from this study have led the authors to recommend a holistic approach to deal with cybercrime. The proposed holistic and collaborative approaches comprise of three categories

namely: legal, strategic and technical perspectives in predicting, preventing, identifying, and responding against cybercrimes.

Legal Perspective

- i. The Government of Bangladesh should have cybercrime laws for dealing with cybercrime and there should be collaborations of different stakeholders (i.e. within organization, national wide and worldwide).
- ii. High penalties should be enforced for cybercrime committed and for those who do not report the incident of cybercrime.
- iii. Training and awareness to citizens, organizations, the Government and public in general regarding the collection of digital forensics evidences; and how to report cybercrime. culprits must face the harshest punishment possible in order to catch cybercriminals.

Strategic Perspective

- i. The Government should revise the National ICT policy to accommodate new ICT developments in the industry.
- ii. The organizations/Government should have Internet usage and security policies in specific
- iii. Standards and procedures should be enacted with regard to usage of information systems in cyberspace.

Technical Perspective

- i. Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised.
- ii. Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a task. When prompted for a root or User Account Control (UAC) password, ensure that the program asking for administration-level access is a legitimate application.

Discussion Cybercrime analysts point out that although pornography is not considered illegal across the world, but in Bangladesh it is one of the predominant computer crimes. There is already evidence of the existence of illegally hosted pornographic websites with local content. In Bangladesh, Nowadays youths are increasingly using cyber cafes as their dating places.

Bangladesh is not safe from cybercrime The government statistics for cybercrime are not remarkable, but district judges have been empowered to try cases in reference to the penal code

and code of criminal procedure. The limited number of cybercrimes apprehended is confined to email threats.

Bangladesh is in danger Cyber terrorists are very expert. It is not possible for the normal police to arrest them. Cyber warfare is a complex aspect of the modern war, but it is not a new feature. It has been called by various names in the past - intelligence and electronic warfare.

Use of internet in bad intention There are two sides of a coin. Similarly internet also has advantages and disadvantages. Internet can be used as a mass destructive weapon. By using internet terrorist can destroy one country. Various names in the past - intelligence and electronic warfare.

7.2 CONCLUSION

Cybercrime is more prevalent than any other type of crime. To combat this crime, both laws and technological advancements are required. Many people in Bangladesh, a developing country, are unaware of this deadly crime. There can also financial loss in addition to personal loss. National security is jeopardized by cybercrime. Bangladesh has several laws in place around the world to prevent this horrific crime, but we have no control over cyberspace, which allows us to perpetrate this heinous crime.

By the completion of this survey, we will have a better understanding of the current level of cyber crime in Bangladesh, as well as the criminal laws in place to combat it.

These disparities in calculating machine technicality around the globe are posing a challenge for countries attempting to combat cybercrime. Because cybercrime knows no geographical or political boundaries, and many computer systems are freely accessible from anywhere on the planet, domestic solutions are ineffective. It's also difficult to compile accurate cyber crime statistics because an unknown proportion of offenses go undetected and unreported. It is also costly to develop and maintain security and other protective measures. Computer fraud and embezzlement schemes frequently target international financial organizations. Organized crime and terrorist groups are also employing modern computer technology to avoid detection by the

government and carry out violent attacks. As a result, the development of cyber criminal law that applies to both domestic and international audiences is a perpetual ups and downs battle.¹⁹

While technological progress is to be commended, it has also brought with it a slew of new obstacles. To meet these issues, the Internet need security-related characteristics. Countries should aim to strike a balance between maintaining the free flow of information and opinions while also protecting and safeguarding individuals. As the world community is accountable for reviewing such rules, Jahankhali urged the global digital community to take steps to evaluate and preserve cyber law in order to achieve efficient and socially acceptable Internet use. The effective fight against cybercrime necessitates increased, quick, and efficient international criminal cooperation. On the topic of the judiciary, Brenner proposed that a country's judiciary's "territorial idea" be enlarged to allow a country to decide whether the perpetrator's action occurred in whole or in part on the judging country's territory. Brenner goes on to say that governments should examine their evidence gathering and analysis systems to see whether they can incorporate obscure evidence from cybercrime rather than traditional crime, which generates genuine evidence. In order to resolve the matter of jurisdiction in an intelligent and rational manner, courts must also comprehend the technical elements of the Internet and generate well-established precedents. Indeed, the efficient employment of criminal sanctions and administrative measures to prevent cybercrime has been discussed.

Wherever possible, Internet users should be encouraged to share the burden of maintaining personal information privacy. In addition, children should be taught computer policy in schools so that they are aware of the dangers of cybercrime. With the advancement of technology, there is a chance that new forms of cybercrime will emerge. As a result, new cyber laws need be enacted to address this rapid shift. Furthermore, as computer technology advances, IT security workers, financial services personnel, police officers, prosecutors, and the judiciary should receive ongoing research and training. Finally, when it comes to the preservation of basic human rights and the necessity for successful cybercrime prosecution, a balanced approach is the way to go.

39.Cassim, F. (2019).*Formulating specialised legislation to address the growing spectre of cybercrime: a comparative study*. [online] Scielo.org.za. Available at: http://www.scielo.org.za/scielo.php?pid=S1727-37812009000400004&script=sci_arttext&tIng=en

BIBLIOGRAPHY

Books

1. Dudeja VD, Cyber Crime and Law Enforcement, Commonwealth Publishers, 2003.
2. Jody R. Westby, International Guide to Combating Cybercrime, American Bar Association, 2003.
3. Victoria Roddle, The Ultimate Guide to Internet Safety, Lulu Press, 2008.
4. Janczewski, Lech, and Andrew M. Colarik, (eds.), Cyber warfare and Cyber Terrorism, IGI Global, 2008.
5. Grabosky, P.N., Virtual criminality: Old wine in new bottles?, Social and Legal Studies, (2001), (10:2), pp. 243-249:243.
6. Goodman, Marc D. "Why the police don't care about computer crime." Harv. JL & Tech. 10 (1996): p. 465
7. Kamal, Mohammad Mostufa, et al, Asian Social Science 8.15 (2012), titled: "Nature of Cyber Crime and Its Impacts on Young People: A Case from Bangladesh": p.171.
8. Hasan, Md Mehedi. Nilakas-duronto.blogspot.hk. N, titled:'Nil Akas: Cyber Law And Its Weakness: Bangladesh Perspective'. .p. 2011,
9. Butani, Anita, Bryan Chao, and Nineteenth Annual Session, "Commission on crime prevention and criminal justice." (2002).
10. Parsons, Talcott ,Theories of Society; Foundations of Modern Sociological Theory , The Free Press of Glencoe ,Illinois.(1961).
- 11.. Halim Abdul, Siddiki N E. *The Legal System of Bangladesh after Separation,(1st ed.), Dhaka: University Publications .(2008).*
- 12.Zulfiquar Ahmed. *A Text Book on Cyber Law in Bangladesh, 1st ed , Dhaka: National Law Book Company .(2009)*
13. Naughton J. A Brief History of the Future: The Origins of the Internet. London:. , *Phoenix (1999).*
14. Karzon, Sheikh Hafizur Rahman, Theoretical and Applied Criminology, Palal Prokashoni, Dhaka, 2008, page-411-418
15. Yar, M., The novelty of "cybercrime": An Assessment in Light of Routine Activity Theory, European Society of Criminology, 2005, page 407-427

Statutory Laws

1. The Information and Communication Technology Act, 2006.
2. The Penal Code Act, 1860 .
3. The Digital Security Act, 2018.
4. The Bangladesh Telecommunication Control Act, 2001.
5. The Pornography Control Act, 2012.
6. The Code of Criminal Procedure, 1898.

Journals/Article

1. Mohammad Mahabubur Rahman, Cyber Space: Claiming Conceptual and Institutional Innovations..
2. Shakila Yeasmin Suchana, Cyber crime in ‘Digital Bangladesh’ published in Daily Star on.
3. Stein Schjolberg and Solange Ghernaoui-Hélie, A Global Protocol on Cybersecurity and Cybercrime, Cybercrime data, 2009.
4. Sam Lumpkin, Senior Security Architect, 2AB, Inc, ‘Internet Security and Cyber Crime’.
5. A.R.M. Borhanuddin (Raihan), Department of Law, Dhaka University, ‘Cyber Crime and Bangladesh Perspectiv.
6. Hasan, R. (2019). Digital Security Bill passed. Retrieved from <https://www.thedailystar.net/politics/bangladesh-jatiya-sangsad-passes-digital-security-bill2018-amid-concerns-journalists-1636114>
7. Bangladesh: New Digital Security Act imposes dangerous restrictions on freedom of expression. (2019). Retrieved from <https://www.amnesty.org/en/latest/news/2018/09/bangladesh-newdigital-security-act-imposes-dangerous-restrictions-on-freedom-of-expression/>
8. Analysis of the Draft Digital Security Bill. Centre For Law And Democracy (2018)
9. APWG (Anti Phishing Working Group) pg 1 Phishing Activity Trends Report :Jan 2005,

at<http://www.antiphishing.org>

10. Cha, A. (2005), Police find that on Ebay some Items are a realsteal, 8 January, retrieved from<http://www.duluthsuperior.com/mid/duluthsuperior/10597328.htm>.

11. Zimmer, E. and Hunter, D. (1999) , 'Risk and the Internet :Perception and Reality ' retrieved fromwww.copacommission.Org/papers/webriskanalysis.pdf16.

12. Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No. 4, 2001, page 889

13. Virginia Journal of Law and Technology, Vol. 9, 2004

Internet Websites

1.<https://www.researchgate.net/publication/33408930-Crime-in-Bangladesh>

2.[https://www.scribd.com/document/327150100/Cyber Crime Theoretical Framework](https://www.scribd.com/document/327150100/Cyber-Crime-Theoretical-Framework)

3. <http://cs.etsu-tn.edu/gotterbarn/stdntppr/stats.htm>

4. <http://trusecure.com/html/tspub/whitepapers/crime.pdf>

5. <http://securityfocus.com/vulns/stats.shtml>

6. http://cfr.org/publication/15577/evolution_of_cyber_warfare.html

7. <http://theatlantic.com/magazine/archive/2010/02/cyber-warriors/7917/>

8. http://en.wikipedia.org/wiki/cyberwarfare#cite_note-41

9. <http://www.thedailystar.net/archive.php?date=2014-09-06>

10. Why the Editors' Council opposes the Digital Security Act. (2019). Retrieved from <https://www.dhakatribune.com/bangladesh/2018/09/28/why-sampadak-parishad-opposesthe-digital-security-act>

11. Review Digital Security Act: TIB. (2019). Retrieved from <http://www.dailysun.com/printversion/details/306160/2018/05/03/Review-Digital-Security-Act:-TIB>.