A STUDY ON THE NATURE AND IMPACT OF CYBER CRIME ON WOMEN

By Ahesan Kabir

M. PHIL DISSERTATION

A STUDY ON THE NATURE AND IMPACT OF CYBER CRIME ON WOMEN

This Dissertation is Submitted to the Institute of Social Welfare and Research, University of Dhaka as Fulfillment of the Requirement for the Degree of Master of Philosophy (M. Phil)

M. Phil Researcher

Ahesan Kabir

Registration No: 65 Session: 2016-2017



Institute of Social Welfare and Research University of Dhaka Dhaka-1205

June 2021

A STUDY ON THE NATURE AND IMPACT OF CYBER CRIME ON WOMEN

Supervisors

Professor Dr. Mahbuba Sultana
Institute of Social Welfare and Research
University of Dhaka

Dhaka-1205

Institute of Social Welfare and Research University of Dhaka Dhaka-1205

Professor Dr. Sk. Tauhidul Islam

M. Phil Researcher

Ahesan Kabir

Master of Philosophy (M. Phil) Part- II
Registration Number- 65
Session: 2016-2017
Institute of Social Welfare and Research

stitute of Social Welfare and Researc University of Dhaka

Dhaka-1205



Institute of Social Welfare and Research University of Dhaka Dhaka-1205

June 2021

Dhaka University Institutional Repository
Pedication
I dedicate this dissertation to my mother Sabina Chowdhury, the Victims
of the Cyber Crime and the person whom I love most.
i



I hereby do solemnly declare that the work entitled "A Study on the Nature and Impact of Cyber Crime on Women" has been carried out by me and has not been previously submitted to any other institution for any other degree. The work I have presented does not breach any copyright. I further undertake to indemnify the University against any loss or damage from breach of the foregoing obligations.

.....

Ahesan Kabir

Master of Philosophy (M. Phil) Part- II Registration Number- 65

Session: 2016-2017

Institute of Social Welfare and Research

University of Dhaka

Dhaka-1205

সমাজকল্যাণ ও গবেষণা ইনস্টিটিউট

ঢাকা বিশ্ববিদ্যালয়

ঢাকা-১২০৫, বাংলাদেশ ফোন: ৮৮০-২-৫৮৬১৬৬১, ৯৬৭০৪১২, শিএবিএক্: ৯৬৬১৯০০-৭৩, এক্, ৮৪৮০ ফ্যাক্স: ৮৮০-২-৯৬৭০৪১২, ওয়োবসাইট: www.iswr.du.ac.bd ইমেইল: iswrdu.ad@gmail.com, info@iswr.du.ac.bd



Institute of Social Welfare and Research University of Dhaka

Dhaka-1205, Bangladesh Tel: 880-2-58616662, 9670412, PABX: 9661900-73, Ext. 8480 Fax: 880-2-9670412, Website: www.iswr.du.ac.bd E-mail: iswrdu.ad@gmail.com, info@iswr.du.ac.bd

CERTIFICATION OF THE SUPERVISOR

This is to certify that the M. Phil dissertation "A Study on the Nature and Impact of Cyber Crime on Women" is carried out by Ahesan Kabir as fulfillment of the requirement for the degree of the Master of Philosophy (M. Phil) under the Institute of Social Welfare and Research, University of Dhaka. It is a record of bonafide work carried out successfully under our supervision.

ofessor Dr. Mahbuba Sultana
Institute of Social Welfare and Research
University of Dhaka
Dhaka-1205

Professor Dr. Sk. Tauhidul am Institute of Social Welfare and Research University of Dhaka Dhaka-1205

Acknowledgement

As research is complex task, I had to receive, support, help and assistance from different persons. I am grateful to all those persons who provided me their logical support to carry on this research from beginning to revealing this final report.

First and foremost, praise be, to Almighty Allah who created all living things and is the true ruler of knowledge which he bestowed upon me without which no education or knowledge I would be able to attain for myself.

At the very onset, I express my deepest and sincere gratitude to my Mentors and research Supervisors Professor Dr. Mahbuba Sultana, and Professor Dr. Sk. Tauhidul Islam, Institute of Social Welfare and Research, University of Dhaka. Their scholastic and valuable guidance, suggestions, at all stages of my research have helped me to complete my research and prepare this report. Foremost Lam utterly in debt for the continuous support of my supervisors in terms of study and research, for their patience, motivation, enthusiasm, and immense knowledge. I must express my deepest gratitude to my Supervisor, Professor Dr. Mahbuba Sultana, whose invaluable support helped me in formulating the research questions and methodology rationally so that I conducted this study with perfection. Her feedback criticism pushed me to hone my reasoning and carried my work to a more significant level. I would also like to express my deepest gratitude to My Supervisor Professor, Dr. Sk. Tauhidul Islam, for his significant direction all through my Research and understanding the truest concept of case study which helped in analyzing the study findings in a required manner. He furnished me with the tools that I needed to choose the right direction and successfully complete my dissertation. Their guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my M. Phil study.

I would like to extend our heartfelt gratitude to the respondents who spontaneously have given their time and given interview with patience for obtaining data for the study. I wish to thank the authors and publishers whose works have been quoted for the study.

I like to express a special thanks to Merjem Popara Professor of Physics at High School of Mechanical Engineering, Sarajevo, Bosnia who has helped me reciprocally to understand different concepts correctly and carefully.

I finally would like to also express my gratitude to my mother who worked as my inspiration, guide and strength when I would feel down she always encouraged me to go on and carry out my research.

Ahesan Kabir

Master of Philosophy (M. Phil) Part- II
Registration Number- 65/2016-2017
Institute of Social Welfare and Research
University of Dhaka

Abbreviations and Acronyms

Shorten Form	Elaborated Meaning
BNWLA	Bangladesh National Woman Lawyers' Association
PTCL 143	Bangladesh Telecommunications Company Limited
CID	Criminal Investigation Department
CNN	Cable News Network
CTB	Cyber Tribunal Bangladesh
DOS	Denial of Service
DRU	Dhaka Reporters Unity
₁₆ M	General Manager
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technology
LGBTQ	Lesbian, Gay, Bisexual, Transgender, and Queer
114 S	Multimedia Messaging Service
NGO	Non Governmental Organizations
OECD	Organization For Economic Co-Operation and Development
PC	Private Computer
PP	Public Prosecutor
PTSD	Posttraumatic Stress Disorder
SMS	Short Messaging Service
SNS	Social Networking Site
SNW	Social Networking Website
T ₈₀ V	Technology-Facilitated Sexual Violence
UK	United Kingdom
UN	United Nations
UNICEF	United Nations Children's Emergency Fund
124A	United States of America
VOIP	Voice over Internet Protocol.
VPN	Virtual Private Network
123 VW	World Wide Web
YWCA	Young Women's Christian Association

Table of Contents

	Page No
Dedication	I
Declaration of Ownership	ii
Certification of the Supervisor	iii
Acknowledgment	iv
Key to Abbreviations	vi
Table of Contents	vii
List of Figures and Tables	
Abstract	
CHAPTER 1-INTRODUCTION	
1.1 Background	1
1.2 Statement of the Problem	1
1.3 Rationale of the Study	4
1.4 Objectives of the study	6
1.5 Operational Definition of the Key Terms	6
1.6 Construction of the Study	8
1.7 Scope and Delimitation of Research	8
CHAPTER 2-REVIEW OF RELEVENT LITERATURE	9-17
CHAPTER 3-CYBER CRIME IN BANGLADESH: A GENERAL ANALYSIS	
3.1 Narrowing Down the Term Cyber Crime	18
3.2 Classes of Cyber Crime in General	21
3.3 Characteristics of Cyber Crime	24
3.4 Cyber Crime Victims	25
3.5 Specific Cyber Crime and its Rate Occurring in Bangladesh	25
3.6 Range and Growth of Cyber Crime in Bangladesh	26
3.7 Reasons of Cyber Crime in Bangladesh	28
3.8 Laws Protecting Against Cyber Victimization	28
3.9 Consequences of Cyber Crime of Cyber Crime	29
CHAPTER 4-CYBER CRIME AGAINST WOMEN IN BANGLADESH:	AN
OVERVIEW	
4.1 Cyber Crime Specific to Women in Bangladesh	33
	vii

4.2 Vulnerability, Status and Demographic information of Women Who are Victims	35
4.3 Patterns of Women Cyber Victimization	36
4.4 Reason of Women Cyber Victimization	39
4.5 Legal and Structural Support Available to Women in this Regard	41
4.6 Psychological Impacts of Cyber Crime	43
4.7 Social Impacts of Cyber Crime	45
4.8 Economic Impacts of Cyber Crime	47
4.9 Death and Suicides Related to Cyber Crime	48
CHAPTER 5-METHODOLOGY OF RESEARCH	
5.1 Main Method	50
5.2 Research Area	51
5.3 Population and Unit of Analysis	51
5.4 Sample and Sampling	51
5.5 Data Collection Tool	51
5.6 Processing, Analysis and Interpretation of Data	52
5.7 Validity, Reliability and Generalizability	53
5.8 Ethical Consideration	54
CHAPTER 6- FINDINGS (CASE PRESNATATION)	
6.1 Presentation of Case of Cyber Crime Victims	55
6.2 Presentation of Cases of Support Agents	66
CHAPTER 7- FINDINGS AND ANALYSIS	
7.1 Findings and Analysis	75
7.2 Socio-Economic and Demographic Condition of Victims	75
7.3 Social Standing is Not Crucial Aspect of Victimization	77
7.4 Economic Condition is Also Not a Crucial Factor for Cyber Victimization	78
7.5 Offender Target Women who are Adults in Age Range	79
7.6 In Gender Ratio of Victimization Women are More Victims of Cyber Crime	80
7.7 Government's Awareness is not Adequate to Reduce Cyber Crime	81
7.7 Process of Filing Case is Unconventional and Difficult	82
7.8 Victims Face Legal Harassment from Filing Cases to Trail	83
7.9 The Process of Trail Is Lengthy in Cyber Crime Cases	84
7.10 Relatively Inadequate Investigative Personnel for Speedy Investigation	85
7.11 Victims Privacy is not Protected	86

7.12 Farticular Provisions for Women's Protection in Law is Unneeded	0/
7.13 Court Staffs are Involved in Corruption	88
7.14 Victims are Socially Discriminated, Distanced and Alienated	88
7.15 Victims are Blamed, stigmatized and Receive no Supported from the Society	89
7.16 All the Victims of Cyber Crime Suffer From Depression	90
7.17 The Victims Feel Anxious, Nervous Lose Their Self-Confidence as Aftermath	91
7.18 Insomnia is a Most Common Outcome of Cyber Victimization	92
7.19 Self-Harm and Suicidal Tendency Develops Among Victims in Severe Case	93
7.20 Cyber Crime Incurs Financial Loss for Victims and Their Family	93
7.21 The Victims Face Further Sexual Harassment Even After the Incident	94
7.22 Unsubstantial Role of NGOs in Awareness Raising on Cyber Crime Issue	95
7.23 Victims Don't Receive Proper Counseling and Guidance	95
7.24 Remarks	95
CHAPTER 8-DISCUSSIONS OF THE STUDY FINDINGS	
8.1 Discussion	96
8.2 Remarks	98
131	
CHAPTER 9-SUMMARY, RECOMMENDATIONS AND CONCLUSION	
9.1 Summary of the Research	99
9.2 Recommendations of the Research	101
9.3 Conclusion	102
	144
REFERENCES	104
APPENDICES	
Appendix – I	114
Appendix – II	116
Appendix – III	118

List of Table, Figures and Charts

		Page No.
Table	e 51 Suicide Attempts due to Cyber Crimes and Harassment in Bangladesh	49
Figu	res	
1.	Growth of cyber crime worldwide by year	27
2.	Wide distribution of Cyber Crime Specific to Women	34
3.	Growth of Cyber Crime Demographics on Gender Basis	36
4.	Psychological Impact of Cyber Crime on Women	43
Char	rts	
1.	Distribution of Cyber Crime Specific to Women	34
2.	People Who Seek Justice through Court and Law	42

Abstract

Title: A Study on the Nature and Impact of Cyber Crime on Women

Supervisors: Professor Dr. Mahbuba Sultana and Professor Dr. Sk. Tauhidul Islam

M.Phil Researcher: Ahesan Kabir

Keywords: Cyber Crime, Victimization, Women, Socio-legal Impacts, Cyber Space, World Wide Web, Nature of Cyber Crime.

Bangladesh has advanced toward digitalization which brought innovative control. Citizens are utilizing web and made life simple and comfortable. They investigate the questions and communicate with for all intents and purposes anybody, anytime, anyplace over the world. At the same time, be that as it may, it has a few negative sides as well. Cyber crime has developed as a major challenge confronting law authorization organizations within the nation, ladies and children stay at hazard. A call for modernization of the preventive, routine set up and prepared police faculty with information and abilities is for anticipation and control of cyber crime in of times demand. This paper tosses light on Cyber crime on women and administrative mediation measures. The general objective of this thesis is to distinguish the nature and affect of cyber wrongdoing on women and ways to making strides to their circumstance. Cyber Space could be an effective way for women to realize their rights, from getting to data, to communicating themselves freely and indeed anonymously. The defenselessness and security of women is one of the greatest concerns of any criminal and correctional law, but shockingly women are still defenseless in cyber space. Cyber crime against women is on at disturbing rise and it may posture as a major danger to the security of a individual as a entirety. The World Wide Web permits clients to circulate substance within the shape of content, pictures, recordings and sounds. The far reaching circulation of such substance is especially harmful for women. A few culprits attempt to slander women by sending indecent e-mails, stalking them by utilizing chat rooms, websites etc, creating obscene recordings where they are delineated in compromising positions generally made without their assent, spoofing e-mails, morphing of pictures for obscene substance etc. Other than these all in this research the readers will be presented with the driving cases to women being cyber victimized in Bangladesh and how they adapt with it and how distant was its affect.

CHAPTER 1 INTRODUCTION

1.2 Background

Women in Bangladesh are excessively focused by on the web and innovation worked with brutality and badgering. While the expansion of Information and Communication Technology (ICT) and developing web entrance are considered as sure markers of advancement in the country, however their connection with certain previous social-physiological settings related and lacking lawful assurances have prompted expanded digital brutality against women. As a rule, the type of this glaring infringement of common freedoms goes from digital following, vengeance pornography, cyber bullying, and savaging. Women are the essential beneficiary of hostile and regularly forceful lewd gestures and abusive messages in the internet from mysterious and counterfeit sources. Bogus and modified unclothed pictures of women alongside spam, sex-act recordings, assault dangers, and revolting recommendations have become the new standard of online media. Women are the essential beneficiary of hostile and frequently forceful lewd gestures and disparaging messages in the internet from mysterious and counterfeit sources. False and altered unclothed pictures of women along with spam, sexact videos, rape threats, and indecent proposals have become the new norm of social media.

"Justice is for all" that is stated in our constitution but most of the women of are victims of cyber crime in our country are being deprived from the formal justice and much needed facilities. Though for the ensuring of proper justice the governments and the Legal assistance organizations have taken various programs but it has not changed the present picture. Matter of fact is that only handful of the women get assistance from privatization in victim assistance. Majority of the women become victims of negligence, discrimination in the trail process. So for the development of the country introduction and implementation of new trend is necessary so that the rights of victims is ensured while offenders are brought under justice and thus resulting into prevention of cyber crime.

1.2 Statement of the Problem

Bangladesh could be a nation which is quickly creating scopes and keeping its pace with globalization. Progressive communication framework and digital innovation have made dramatic changes within the way we live. Within the final decade the Web has accomplished

significant development. The nation has gotten to be costumed to cyber world in each circle of its capacities. In Bangladesh the rate of web client is expanding quickly. Agreeing to BRTC there are almost 74,650,000 dynamic clients of web as of Walk 2018. With that Cyber Crime are continuously expanding within the nation. Cyber crime is wrongdoing that includes a computer and a network.

Offenses that are committed against people or bunches of people with a criminal rationale to intentioned hurt the notoriety of the casualty or cause physical or mental hurt, or misfortune, to the casualty straightforwardly or in a roundabout way, utilizing advanced media transmission systems such as Web (Chat rooms, emails, take note sheets and bunches) and portable phones e.g. SMS/MMS" (Halder & Jaishankar, 2011).

Since the quick increment of web and versatile innovation the women of Bangladesh are confronting a specific risk when they are associated to cyber space. The women in our nation are regularly getting to be casualties of vindicate porn, online bullying, online fakes and dark mailing. In spite of the fact that developed nations within the world such as U.S.A and U.K have strict enactment and back for dealing with cyber wrongdoings against women but Bangladesh have two out of date enactment and zero component for bolster for women who are casualties of cyber crime. At display the women in our society are most helpless in case of cyber wrongdoing (Attrill, & Fullwood 2016).

Definitions of most crimes committed in around the world in actual space are sexual orientation impartial; in spite of that fact a noteworthy number of violations are committed for the most part against women. There are certain cyber violations that are more likely to target women than their male partners. These can include cyber badgering, cyber stalking, morphing and disgusting distribution of profile, email/profile hacking, spoofing, cyber explicit entertainment counting to vindicate porn, web voyeurism, cyber maligning, cyber bullying, email badgering, cyber coercing, undermining, enthusiastic cheating by pantomime, insinuate accomplice viciousness through web and abetment of such offenses. Women's rights within the cyber space are mishandled in numerous ways in Bangladesh and utilize of web and portable phones to stalk, manhandle, threaten and mortify women is rampant (Supan's Article 2015).

The humility of women in our society is exceptionally simple to demolish as individuals continuously stigmatize and call names to women in any occurrence without comprehending the generally situation of a circumstance. The women casualties of spilled explicit entertainment are socially distanced and stigmatized intensely. The women in our nation are moreover fell casualties of online extortion and cyber stalking. There are many cases which are almost not reported due to fear of social alienation and stigmatization. As the majority of people in Bangladesh are not educated they quickly believe any rumour and false information they see online and while at it they brand a woman to be a person of bad character. There is case of many women not getting to marry due to their intimate pictures or videos have been posted in Facebook or at any internet site. Many women cannot take these hardships and commit suicide. Threat to leak pornographic videos on internet has become common tool for blackmailing now days. The psychological effect of cyber crime on a woman is another critical aspect to consider. Cyber crime as sexual crimes such as rape and sexual harassment has both short and long term effect on the psyche of women who are victim to such crimes. The psychological trauma can include guilt, embarrassment, self-blame, fear and terror, depression, anxiety, nightmares and becoming suicidal.

As cyber crime is a new form of crime the law enforcement agencies are not familiar with this in a professional way. When a cyber crime occurs the police have very limited idea on how to investigate it and provide proof to the court for conviction of guilty party. Although the police have modern cyber crime cell in each branch of their station but inexperience in this regard is proving efforts less fruitful. The modesty of women should be respected thoroughly but the matter of sorrow is that now a day's media of our country pays no respect to the confidentiality of women victims of cyber crime. The media show the faces of victims in camera and publish photos of victim in paper and online portals. This causes the whole country to know the identity of the victim leading to making her life hard for future ahead. Similar approach is also taken in police investigation and court proceedings as often male police officer and Judge go through the leaked video which in terms violets the privacy of the victim. At the same time there is no support center or mechanisms for such victims who in terms of seriousness is equal to victims of rape and sexual harassment which is a grave scenario in this country.

1.3 Rationale of the Study

Cyber Victimization of women have existed in Bangladesh for a long time since rise of Computer and web in our nation due to the nations long history of social segregation towards women, but the development have quickened after the 1990s primarily due to financial advancement in e-commerce and introduction of women to cyber world. Another perspective of Cyber Victimization of women is ceaseless relocation of individuals of rustic ranges to metropolitan regions particularly Dhaka. The population development rate of urban regions is three times higher (6-7%) than the national populace development of 2% per year. At display, around 20% (25 million) of the countries add up to populace of (129 million) live within the urban ranges. The individuals living in a Metropolitan region are associated to cyber world and dependent on it in an awfully huge amplify against those who live within the rural Bangladesh. So as a result there's a rise of cyber violations within the urban regions of the nation.

Although a large number of women become cyber victims each and every year but the matter of sorrow is that they don't get their legal rights and remedies. To cope with the emerging threat of cyber crime and harassment Bangladesh Government has initiated two laws. They are Digital security Act of 2018 and Pornography Control Act 2012. Bangladesh police has opened a Cyber wing to manage the expanding pace of digital danger. This wing of police so created is responsible for monitoring cyber crimes and tracking the criminals. Alongside Bangladesh police, Bangladesh Telecommunication Regulatory Commission is likewise attempting to direct and screen cyber crime. As to directive this commission also blocks inappropriate websites, blogs and Facebook accounts. But major problems of these two organizations are bureaucracy and lack of communication with the mass people (Maruf et al., 2010).

The unforgiving reality is Bangladesh Police or BTRC don't have the mechanical capacity to track down cyber hoodlums as well as to expel unlawful substance from Web (Mizanur Rahman Khan's Article 2018). Because of the inadequacy of BTRC and Bangladesh Police the cyber offenders take the advantage. In Bangladesh the circumstance of explicit entertainment is past resistance presently. Nearly 77% youngsters observe obscenity as a customary premise and in 78% cases the casualty could be a Woman (Manusher Jonno Foundation Report, 2014). Online pornography is on the rise each day and most of the times it is Women who are victims of pornographic contents as means of revenge. Sometimes the

victims face is edited with a nude background and spread through internet and social media sites. Upon spreading such videos and pictures catastrophe only follows the victim. Many women who cannot handle the pressure commit suicide.

The NGO's and other victim support service organizations provide a very little support for the victims of cyber crime. Most often it is seen that the organizations can't grasp the gravity of the situation of victims and in most other cases the victims themselves don't seek organizational help for being afraid of social context of Bangladesh.

The constitution of Bangladesh which is the supreme law of the state has ensured equal protection of laws to all the citizens and also ensured their right of life and liberty, freedom and movement. As indicated by Article 31 'To appreciate the assurance of the law, and to be treated as per law, and just as per law, is the natural right of each Citizen and Article 36 offers that: Subject to any sensible limitations forced by law in the public intrigue, each Citizen will reserve the option to move uninhibitedly all through Bangladesh, to live and get comfortable any place in that and to leave and return Bangladesh' (Constitution of Bangladesh, 1972). So the constitution itself has granted its citizens the right to fundamental freedom in every sphere of their life and it extends to cyber world too. A woman has the right to post, surf and browse internet freely and without any fear, but the practical situation is really different than the theoretical approach. The government has very least concern about this agenda and so development of protection of women's right in cyber world is very slow.

Lastly, armature investigation in this crime by police leads to the criminal being set free which causes the victims to live a life of shame in the society with alienated from the rest of the populace. A woman who is victim to cyber crime is seen to be stigmatized within her own family and when a criminal is set free this proves her critiques that the victims is a immoral person. This trend is now a common scene in the victim's social context.

The study will help the government to take necessary measures to ensure rights of the women who are victims of cyber crimes. As the government has largely failed to deliver the constitutional promise of protection and ensure socio-legal rights to women victims of cyber crimes this study will be an asset to make sure of the victims rights and develop their conditions. The study will also allow the general people to know about the conditions and challenges faced by the women who are victims of cyber crimes and will be helpful to change

the views of people of society and promote their aid in this regard. The proposed study is expected to draw the attention of Human rights organizations, human right activists, media, NGO and other personnel working for this agenda and also develop new policies for the betterment of victims of cyber crime.

1.4 Objectives of the study

The general objective of the study is to know the overall situation of nature and impact of the women cyber victimization in social context of Bangladesh. Under this general objective, the study would be conducted on the basis of following specific objectives:

- 1 To know the socio-economic and demographic information of the women who are victims of cyber crime.
- 2 To find out the social and legal challenges faced by the women victims of cyber crime.
- 3 To identify the after effects of cyber crime on women.
- 4 To find out the government and NGO's initiatives specific for the women victims of cyber crime.
- 5 To provide suggestions and recommendations for the prevention of cyber crime and improvement of the situation of women who are cyber crime victims.

1.5 Operational Definition of the Key Terms

Definition oriented towards the study is vital for the purpose of clarifying the terms frequently used in research. Its worth to mention that different key terms can be interpreted in different ways in case basis but its duty of a researcher to limit the scope of wide usage of different terms which is highly likely to be used often. So as to with that purpose the definition of different key terms are explained hence forth.

- Internet- For the purpose of this study the term Internet is the means of communication through which people connect with each other virtually such as Viber, Imo, Facebook Messenger, Whatsapp and others so on.
- Cyber Space- For the purpose of this research cyber space indicates a virtual space, which is spread across whole world and not bounded by particular territorial laws connected via internet where people share and exchange communication and information with means of various chat and applications such as Facebook, Messenger and so.

- Cyber Crime- Under this study cyber crime is any crime which occurs in cyber space.
 The examples of cyber crime are morphing, revenge porn, online fraud, hacking and many more.
- World Wide Web- World Wide Web is an information system of communication over internet used to access various websites.
- Victimization- Victimization under this study described as becoming a victim of cyber crime or the process of becoming a victim.
- Criminal/Offender- For the purpose of study all criminals and offender will be defined
 as any person who commits cyber wrong doings over cyber space.
- Women Victims- In this study women victims are indicated to those women who are victims of cyber crime.
- Law Enforcement agency- Law enforcement agency indicates in study to police, state
 prosecution and courts dedicated to reduce, minimize and prevent cyber crime while also
 facilitates women who are victims of cyber crime.
- Hacking- Hacking alludes to exercises that look to bargain computerized gadgets, for example, PCs, cell phones, tablets, and even whole organizations.
- Pornography- Under this study Pornography means and is defined as any sexual or elicit
 material circulated and distributed in cyber space or over internet.
- Socio-Legal- Socio- legal is the aspects and effects of certain activities in social and legal perspective.
- Digital Media- the term digital media is any type of media that utilizes electronic gadgets for dispersion. This type of media can be made, seen, altered and disseminated by means of electronic gadgets. Advanced media is generally utilized programming, computer games, recordings, sites, web-based media, and internet publicizing.

 Cyber Law - Cyber Law, otherwise called cyber crime law, is enactment centered on the adequate conduct utilization of innovation including PC equipment and programming, the web, and organizations.

1.6 Construction of the Study

This study is organized in nine chapters. Following this first chapter, the second chapter reviews the relevant literature in the field of this research, the third chapter, chapter hosts the theoretical framework related to cyber-crimes. The fourth chapter analyzes cyber crime against women in Bancladesh in a present context. The fifth chapter describers in details the methodology of the research. The sixth chapter presents the cases of victims and the support agents; the seventh chapter is the findings of whole research drawn from primary data. In the Chapter eight discussion of the study findings are presented and the final chapter contains the conclusions and recommendations.

1.8 Scope and Delimitation of Research

The scope of the study combines the current status of the cyber-crimes against women in Bangladesh. As the scope of cyber-crimes are numerous than any other forms of offences, so the researcher go through about the well-known offences which commonly occurring the Bangladesh and preventive measures of those crimes.

CHAPTER 2

REVIEW OF RELEVENT LITERATURE

Literature review assumes a critical function for social research. As suggested by Borge (1963), "The Literature review includes finding, perusing and assessing reports of exploration just as reports of easygoing perception and supposition that are identified with the people arranged examination venture". So it is difficult to portray the true significance of Literature review. Articles, Books, Cases, PhD papers are identified with the examination subject and significant wellspring of are included in literature review. In this paper, I have attempted to review the connected books, articles, examination and PhD paper to separate the idea, auxiliary data and recognize Knowledge Gap. Moreover, this examination is indicating Nature and Impact of Cyber Crime on Women in Perspective of Bangladesh. Literature review is inescapable and unavoidable for any research. It is key, basic and indispensable part to discover the Knowledge gap. It intensifies the extent of the researcher to investigate the essential information effectively and causes the researcher to accomplish the point and target of the examination significant viewpoints, segments, materials and applicable issues in this case with respect to the Nature and Impact of Cyber Crime on Women in Perspective of Bangladesh.

Elias Aboujaoude, Matthew W Savage, Vladan Starcevic, Wael O Salame, in their article "Cyberbullying: Review of an Old Problem Gone Viral" (2015), with objective to understand and gain an in depth knowledge of cyber bullying employed methodology of observation and data analysis of different search engines stated that the phenomenon of cybercrime or cyber violence encompasses a range of abuses perpetrated by and through digital means, including online harassment, cyber bullying, cyber dating abuse, revenge porn, and cyber stalking, types of cybercrime that often overlap and occur contemporaneous with offline violence. Studies suggest that women and girls and sexual minorities of all genders are more susceptible to online victimization. A significant proportion of females and sexual minorities are seemingly at higher risk of being victims of cyber bullying. Perpetrators are highly likely to be male. The easy accessible nature of the social media platforms, it seems to be an easier path to the bully-victim phenomenon than that in traditional bullying. A nonlinear relationship with age is recommended, however segment information by and large are fundamental. Going with psychopathology, including an inexorably entrenched connect to

suicidality, is normal. A few counteraction and the executives' approaches have been proposed to help forestall cyber bullying or alleviate its belongings.

In Sarah Bloom's article stated "No Vengeance for 'Revenge Porn' Victims: Unraveling Why This Latest Female-Centric, Intimate-Partner Offenses Still Legal, And Why We Should Criminalize It" (2016) the objective was to point out the devastating impact of revenge porn and the context of cyber harassment and intimate partner crimes and the problem of inadequate legal redress for victims of revenge porn. Here the main mythology employed was case study of women to conclude the objectives affirmation and as to such the article points to that women and young girls are disproportionately affected by technology-based harms. They are most frequent victims of revenge porn. Revenge pornography is a grievous offense, and if unregulated, its predominance will proceed. Casualties experience embarrassment, mental agony; dangers to their security, obliteration of their vocations, and a couple have even ended their own lives. So as to sufficiently rebuff the conduct according to the equitably improper act and damage caused, there should be a genuine criminal resolution legitimately tending to the issue. Revenge pornography casualties should not to be compelled to stand by as long as survivors of aggressive behavior at home, assault, and other intimate partner crimes needed to wait to see their wrongdoers vindicated through the law.

Vimala Balakrishnan in his article "Cyber bullying among Young Adults in Malaysia: the Roles of Gender, Age, and Internet Frequency" (2015) noted that the gendered nature of cybercrime represents a nascent frontier in the research community. Gender influences how cyber violence is perpetrated and experienced differently by men and women, boys and girls, and by sexual and gender minorities. The objective of the study was to indentify bullying activities over internet and to classify them in to age gender and internet consumer categories.

Nicola Henry and Anastasia Powell in the article "Technology-Facilitating Sexual Violence: A Literature Review of Empirical Research of Trauma Violence Abuse" (2016) noted Technology-facilitated sexual violence (TFSV) alludes to a range of behaviors where digital technologies are used to facilitate both virtual and face-to-face sexually based harms. Such practices incorporate online inappropriate behavior, sex and sexuality-based badgering, digital stalking; picture based sexual assault, and therefore the utilization of the employment of a carriage service to coerce a victim into an undesirable sexual act. this article audits the current status of data on these various measurements, drawing on existing

observational examinations. While there's a developing collection of examination into innovation encouraged damages executed against youngsters and youths, there's a shortage of subjective and quantitative exploration on Technology-facilitated sexual violence against grown-ups especially women. Besides, not many of the present examinations give dependable information on the character, extension, and effects of Technology-encouraged sexual savagery Preliminary studies, however, indicate that some harms, very similar to sexual violence more broadly, could also be predominantly gender-, sexuality-, and agebased, with young women being over represented as victims in some categories. This study gathers the experimental proof so far with regard to the commonness and sex based nature of Technology-encouraged sexual savagery against grown-ups and talks about the suggestions for strategy and projects, even as recommendations for future exploration.

Sheri Bauman and Angela Baldasare in "Cyber Aggression among College Students:

Demographic Differences Predictors of Distress, and therefore the Role Of The University" (2015) posits that previous victimization are often a risk factor for both future victimization and perpetration. While their review identified over 200 academic articles associated with cyber violence, significant gaps within the literature remain. Most of the research on cybercrime comes from developed countries just like the us, Canada, and Australia. Low and middle-income countries in Africa, Asia, and Latin America are notably absent from this literature. Insights from this review might not be applicable to those contexts where access to and ownership of devices, social norms around dating, and levels of offline violence vary widely. Since cyber violence is a component of the continuum of offline violence, rates of cyber violence will likely vary as rates of intimate partner violence and other sorts of interpersonal violence neutralize various countries. Given differences in income level, mobile ownership, and digital infrastructures regionally and internationally, the digital platforms for perpetration and prevalence of cyber violence victimization are likely to be similarly variegated.

Suvi M. Virtanen during this study titled "Fear of Cybercrime in Europe: Examining the consequences of Victimization and Vulnerabilities" (2017) utilizes aspects of Ferraro's risk interpretation model so as to look at how social and physical vulnerabilities and victimization experiences relate to fear of online crime using Euro barometer survey data. The study found the regression analyses show that individuals with prior cybercrime victimization experiences, women, and individuals with lower social station and lower confidence in their ability to use the net report higher levels of fear. Low social station and low confidence was

found to possess a big interaction effect with prior victimization experiences in reference to fear of cybercrime. Prior victimization experiences with online fraud appear to extend fear of cybercrime in low social station individuals quite other groups. Experiences with hacked accounts or cyber attacks also intensify the fear of these with low confidence quite those with a better amount of confidence. Overall, the results of this study indicate that social and physical vulnerabilities also as victimization have direct and indirect effects on fear of cybercrime, even as with traditional place-based crimes.

Jaspreet Singh's article "Violence against Women in Cyber World: A Special regard to India" (2015) indicates that the atrocities made against women are a violation of human rights and regular phenomenon. It's always takes new shapes time to time in Indian history. As time lapses and modernization facilitates, many feminists fought and raised voice against women violence and for his or her empowerment within the society, but there's no end of her vulnerable life and her exploitation. This paper presumes the cyber violence against women, how it's impacting their social life within the context of India. It points out the explanations and types of cyber-crime and explores some suggestions the way to cope up and control cyber-crime against women.

Alice Munyua in "Women and cybercrime in Kenya" (2015) show that cyber space and its attendant features of anonymity still influence both positively and negatively on social, economic, cultural, and political aspects of each society. Therefore, the cyberspace have provided secure tools and spaces where women can enjoy their freedom of expression, information and privacy of communication, an equivalent benefits of anonymity and privacy also reach those that employ ICTs for criminal activities and use the internet to commit violence against women. The utilization of mobile phones and internet to stalk, abuse, traffic, intimidate and humiliate women is palpable in developing countries including Kenya. The lack of specific cybercrime/cyber security legislation makes it even more difficult to punish those who use ICTs tools to conduct violence against women. In this study, the analysis of the Kenya Communications Amendment Act, enacted in January 2009, begins to deal with the problem; it does not explicitly deal with all cyber crime and cyber security issues on the person and specifically women. It also show with increased access to broadband, which will translate to increase in use of ICTs and the internet in particular, it is has become very urgent to ensure that policy and regulation is developed to address issues of cyber violence against

women. This study also attempts to provide evidence based framework to address cybercrime against women in Kenya and by extrapolation the East African Community Member states.

Natasha Kabir's study "Cyber Crime a new form of Violence against. Women: From the Case Study of Bangladesh" (2018) is concentrated on the present trend of cybercrime is basically dominated by the crime against the individual. These sorts of crime include cyber stalking, fake Id, nude pictures/videos, email hacking etc. People especially females are more susceptible to cyber-attacks. The study shows that numerous underage and minor girls and other female victims committed suicide after their private photos and videos were uploaded on the web. The paper are more emphasis on the question is how the various concerns of the government match up with the specialized security needs of their female citizens, who are the foremost vulnerable one this is often the time to initiate and being vocal against cyber-crime and being more protective on this crime and being aware against this crime as globally this crime is increasing and has become the most sustainable and devastating crime against state, individual, mass and last but not the smallest amount mental, socio-cultural and economic stability when the victims are the women.

Ruth Lewis, Michael Rowe and Clare Wiper in their article titled "Online Abuse of Feminists as an Emerging form of Violence Against Women and Girls" (2017) Posits that Abuse directed at visible and audible women demonstrates that cyberspace, once heralded as a new, democratic, public sphere, suffers similar gender inequalities because the offline world. This paper reports findings from a national UK study about experiences of online abuse among women who debate feminist politics. It argues that online abuse is most usefully conceived as a sort of abuse or violence against women and girls, instead of as a sort of communication. It examines the experiences of these receiving online abuses, thereby making a valuable contribution to existing research which tends to specialize in analysis of the communications themselves.

In reviewing Akancha Srivastava's "Indian Women at risk in the Cyber Space: A Conceptual Model of Reasons of Victimization" (2014) we found that Cyber crimes against women are on the raise and women are drastically victimized within the cyberspace. Some perpetrators attempt to defame women by sending obscene e-mails, stalking women by using chat rooms, websites etc, developing pornographic videos where women are depicted in compromising positions mostly created without their consent, spoofing e-mails, morphing of

images for pornographic content etc. The sex-offenders search for their victims on social network websites, and also on job or marriage websites where people post their personal information for better prospect. The revealing of private information has made women more a casualty of cyber crime. It's evident that victimization of women is resulting in cyber crime and contrariwise. While there are many instances where women in western countries are victimized, there's a raise of such victimization of women within the eastern regions like India and these women are relatively with less legal protection and that they are unique than their western counterparts. This paper attempts to seek out out the varied reasons behind the very fact on why Indian women are being victimized and a conceptual model of cyber victimization of Indian women is proposed.

In the article of Imam Fachruddin Deviana Mayasari, Rudy Kurniawan, Universitas Sriwijaya and Nabielah Agustin "Cybercrime Case as Impact Development Of Communication Technology that troubling Society" (2019) the main objective was to investigate cybercrime in society as a model of crime that develops because the advancement of Internet technology. Cybercrime becomes a practice which will create community behavior that's susceptible to conflicts and legal issues. The approach utilized in this writing is literature research; with knowledge analysis technique within the sort of content analysis with the aim of obtaining valid inference and may beer-examined supported its context. Individual actions within a community group are actions prescribed by norms, values, and social structures. The truth during this cybercrime as a simulation, as example of the creation of unprovoked real models or hyper-reality reality. Through the simulation model, humans are framed in one space, which is identified as real, albeit it's a pseudo or mere imaginary that the emergence of cybercrime as human practice publicly sphere is characterized as space without control, but on the opposite hand because without such control, so cybercrime becomes an anarchist space without rules and norms.

Adam M. Bossler, Thomas J. Holt and David C. May describes in "Predicting Online Harassment Victimization Among A Juvenile Population" (2011) Online harassment, which has also been referred to as electronic harassment, Cyber harassment and Internet harassment is often used as a general term to refer to other forms of cyber violence, including cyber stalking, cyber bullying, sexual harassment and revenge porn. The term online harassment itself comes up short on a uniform definition however will in general depict ("dangers or other hostile conduct focused on through new innovation channels e.g.,

Internet, text messaging") Different sources show that cyber harassment is characterized less by the particular conduct than its proposed impact on and the manner in which it is experienced by its objective. It is well known that anyone with an Internet modem may experience online harassment, prevalence data indicate that women, young girls, and LGBTQ (lesbian, gay, bisexual, transgender, and queer) individuals are more likely to be exposed to and be negatively impacted by it. A 2014 Pew study found that 70% of 18 to 24 year olds have experienced online harassment. Young women within this age group are particularly susceptible to online sexual harassment (25%) and physical threats (23%). Younger women are also more likely to experience invasions of privacy through the digital exposure of sensitive information and undergo online harassment for a prolonged period of time. The Youth Internet Safety Surveys (2010) found that 69% of the respondents who experienced online harassment were female and that an increasing percentage of aggressors online are female.

Thomas J. Holt, Sarah Fitzgerald and Adam M. Bossler in "Assessing the risk Factors of Cyber And mobile phone Bullying Victimization in a Nationally representative sample of Singapore Youth" (2016) proposed that during a survey among primary and secondary school students across Singapore, found female students were at increased risk for mobile phone harassment. This study used routine activity theory to inspect the connections between online behaviors, target appropriateness, and cyber and cell phone—based bullying victimization in a bin a nationally representative sample of youth from nine schools across Singapore. Key measures in every one of the three classes' admittance to innovation, online routine practices, and target reasonableness were huge indicators of the two types of bullying victimization. Specifically females and survivors of actual harassing were bound to encounter the two types of victimization. Admittance to innovation and online routine practices anticipated digital and cell phone—based bullying victimization in an unexpected way. These discoveries exhibit that routine activity theory is a feasible system to comprehend web based tormenting in non-Western countries, predictable with the existing literature on Western countries.

While reviewing Danielle Keats Citron's article titled "Law's Expressive Value in Combating Cyber Gender Harassment" (2009) it was apparent that the kinds of threats specifically leveraged against women and girls online also tend to require on a sexual component, with perpetrators threatening to rape their targets or disparaging the looks and

sexual desirability of their victims. This kind of gendered nature of online harassment has been referred to as cyber gender harassment cyber/online sexual harassment and technology related/cyber violence against women, the terms indicating that gender and sexuality may influence an individual's vulnerability to harassment. Researchers who gathered and analyzed secondary data on the utilization of sexist and misogynistic slurs directed at women and girls online through SNS like Facebook or Twitter found that engagement with anonymous sexist content promotes greater hostile sexism among users.

Wanda Cassidy, Chantal Faucher and Margaret Jackson within the article "Cyber Bullying Among Youth: A Comprehensive Review Of Current International Research And Its Implications And Application To Policy And Practice" (2013) described that most of the cybercrime literature collected in the review deals specifically with cyber bullying. Although cyber bullying has the most robust evidence base of the various cyber violence domains, with numerous systematic reviews and meta-analyses on the topic definitions and estimates of prevalence still remain inconsistent. Even the term cyber bullying is applied irregularly throughout the literature: electronic bullying, Internet bullying, cyber aggression, and online bullying have also been used to describe behaviors often captured under this term. One frequently cited definition of cyber bullying is "an aggressive intentional act carried out by a group or individual, using mobile phones or the Internet, repeatedly and over time against a victim who cannot easily defend him or herself". In a review of the cyber bullying literature, it is noted that girls are more likely to experience cyber bullying tactics like gender-based harassment and exclusion and suggest that the gendered nature of cyber bullying may impact girls' reputations more compared with their male peers. Some indicate that gender differences in cyber bullying are likely to vary across geographic regions and cultural groups, further signaling the necessity of more systematic international research in regions underrepresented in the digital literature. Cyber bullying has also been linked with a number of negative social and psychosocial consequences, including poor school performance, negative self-esteem, anxiety, depression, isolation, loneliness, stress, and suicidal ideation.

Danielle Keats Citron and Mary Anne Franks, in "Criminalizing Revenge Porn" (2014) explains Revenge porn represents another form of cyber crime, one with increasing visibility in the criminal and legal sector. Revenge porn, as it is sometimes referred as cyber rape, nonconsensual pornography, involuntary porn, or image based sexual abuse, is the publication of sexually explicit images or videos on an online forum without the consent of

the subject. Although revenge porn can be perpetrated by ex-partners using archived sexually explicit text messages, photographs or videos can also be accessed remotely through hacking and uploaded to a revenge porn website by a third party unknown to the victim. Revenge porn becomes even more threatening when images or videos are accompanied by the subject's personal information (e.g., name, address). There are almost no statistics on the prevalence of revenge porn. The Cyber Civil Rights Initiative conducted one of the only online surveys to document victimization. In a survey from August 2012 to December 2013, 22% of the respondents reported being revenge porn victims, 90% of whom were women (End Revenge Porn 2013). Over a period of 6 months, 139 revenge porn allegations were filed with police forces in England and Wales, with 10 of these victims being under the age of consent.

Harald Dreßing, Josef Bailer, Anne Anders, Henriette Wagner, and Christine Gallas in "Cyber stalking in a Large Sample of Social Network Users: Prevalence, Characteristics, and Impact upon Victims" (2014) describes that Cyber stalking definitions vary, although the practice is typically understood as "the repeated pursuit of an individual using electronic or Internet-capable device". While cyber stalking perpetrators may have had an intimate relationship with their victim, indicating some overlap between cyber stalking and cyber dating abuse, cyber stalking can also occur between strangers. Primary research and surveys conducted by working to Halt Online Abuse and Liz Claiborne Inc. indicate that cyber stalking perpetrators tend to be male and those women, non-heterosexual individuals and people of color are more vulnerable to incidents of cyber stalking. Victims are likely to know or have had a prior relationship with their perpetrator, indicating a possible connection among cyber stalking behaviors and cyber dating abuse. Finally, just as cyber stalking often occurs contemporaneous with in-person stalking, victims of cyber stalking are also at risk of being physically attacked by their stalkers.

Finally, all these literature reviews are relevant to my study. Most of those papers that I discussed above as a literature review focus on the nature and impact of Cyber Crime on Women Perspective of worldwide as well as Bangladesh. All those literature reviews help me to guide and select methodology, knowledge cap in my study. The focus of researcher while writing the thesis was that, the Bangladeshi women are still not open to immediately report the cyber abuse or cyber-crime.

CHAPTER 3

CYBER CRIME IN BANGLADESH: A GENERAL ANALYSIS

Over the last two decades the range of Information technology has widened and has become the centre line of today's global and technical Progress. Cyber World provides the users all the necessary information, fast communication and sharing platform making it the most indispensible source for information collection. With the innumerable advancement of cyber space, the crime by using internet has also grown in all directions. The cyber crimes now pose a great threat to individuals, organization and state. Cyber crime is a global phenomenon and women are the soft targets of this new form of crime. With that view this paper will explore the Cyber crimes and the online threat and vulnerabilities against women. Cyber-crime is at present the most alarming as a challenge for national and economic security. Various issues that are discussed in this Chapter are: Cyber Crime Classes of Cyber Classes of cyber crime Victims, Cyber crime in Bangladesh, its rate range and reason, Victim classes, related laws, agencies working against this, losses and prevention measures by the Bangladesh government and its effectiveness.

3.1 Narrowing Down the Term Cyber Crime

For the purpose of this study it is essential we narrow down the term cyber crime to develop a generalized idea. Crime and criminality is long associated with Human beings since the dawn of civilization. Concept of any sort of crime remains elusive and always tends to hide itself in the face of social development and growth. Cyber crime in specific is a new type of crime which has developed with the modern use of computers. With the expansion of modern use of computers, networks and cellular devices the domain of cyber space has increased and provided the scope for growth of cyber crime. The term cyber space is very closely related to cyber crime and criminality. In general sense cyber space is a space nonexistent in our real plane and is rather situated over the vast web link of networks through which we are connected to each other in Internet.

The term 'cyber space' was first used by William Gibson, now it is used to describe anything associated with computers information technology, the internet and the diverse online culture (Ratan, 2014, p.48). The virtual space in which all of Information Technology mediated communication and actions are taking place is often referred to as 'Cyber Space'. Cyberspace

is a space which cannot be spatially located. It is comprises of intangible objects, such as website, blog, social networks, email accounts, personal information and reputation. Cyber space can be understood as a global electronic village with in which instantaneous communication takes place and no geographical barriers limits its user from its access. (Rastogi, 2014, p.02) According to Webster's Dictionary, Cyberspace is an electronic system of interlinked networks of computer and other mediums which is considered as being borderless space providing access to information, interactive communication, and, in science fiction, a form of virtual reality (Pal Malik, 2010, p.71), And it is within the bounds of Cyberspace, Cyber Crime occurs.

Over the last few decades criminologists, technological analysts and social scientists have tried to draw a specific and general definition which will cover its range and diameters but sadly such could not be achieved because-

"Many criminological perspectives define crime on the social, cultural and material characteristics, and view crimes as taking place at a specific geographic location. However, this characterization cannot be carried over to cybercrime, because the environment in which cybercrime is committed cannot be pinpointed to a geographic location, or distinctive social or cultural groups. For example, traditional crimes such as child abuse and rape allow for the characterization of the attacker based on the characteristics of the crime, including determination of the social status of the attacker, geographic location within country, state, district, urban or rural residential areas, and so on. However, in the case of cybercrime, this characterization of the attacker cannot be done, because the Internet is "anti-spatial." As a result, identifying location with distinctive crime inducing characteristics is almost impossible in cybercrimes." (Jahankhani, Al-Nemrat and Hosseinian-Far, 2014, p.153).

Modern approach to crime is a functional approach (Nigam, 1965). Modern definition of cyber crime is provided by R. Nagpal from Asian school of cyber law who defines cybercrime as "any unlawful acts wherein the computer is either a tool or target or both" (Nagpal, 2018).

When the victim of cyber crime is an individual, the computer is considered as the tool and not the target. The main characteristics of these crimes generally involve less technical expertise as the damage done manifests itself in the real world. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal

action against the variants more difficult. Again when computer is used as a target select few with expertise commit them and nature of the crime is very professionally handled effecting, large servers are affected in order to gain information or economic advantage over the target.

On a socio-contextual note Debarati Halder and K. Jaishankar define cyber crimes as:

"Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)" (Halder & Jaishankar, 2011).

Unite Nations breaks down the term Cyber Crime into two categories and defined thus: "Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

Of course, these definitions are complicated by the fact that an act may be illegal in one nation but not in another." (Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders Report of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000).

So in light of the above discussions over the definition of Cyber crime we can draw a casual conclusion as to the nature of cyber crime and also develop a definition which covers all the grounds and provides insight for the study. With that object Cyber Crime can be defined as "Any illegal activity which takes place within the cyberspace involving a computer or modern means of communication tool to cause any injury or gain advantage over any individual or computer source whether it belongs to individual, groups or state is considered a cyber crime and such crime has practical social, psychological and economic consequences."

3.2 Classes of Cyber Crime in General

Another approach to gaining insight to cyber crime is to develop a classification which links offence with similar characteristics and into appropriate groups. Several ideas over the years have been developed over the years which indicate that there are only two general categories: active and passive computer crimes. An active crime is when someone uses a computer to commit the crime, for example, when a person obtains access to a secured computer environment or telecommunications device without authorization (hacking). A passive computer crime occurs when someone uses a computer to both support and advance an illegal activity (Jahankhani, Al-Nemrat and Hosseinian-Far, 2014, p.153). The following are various types of cyber crime which occurs within cyberspace- Financial Crimes, Cyber Pornography, Online Gambling, Intellectual Property Crimes, Email Spoofing, Cyber Defamation, Cyber Stalking, Data Diddling, Salami Attacks, Denial of Service Attacks, Virus/Worm Attacks, Trojans & Key loggers, Web Jacking, Email Frauds, Hacking (Gunjan, Kumar and Avdhanam, 2013, p.1-6).

Financial Crimes- Financial crime over the cyber space means gaining financial advantage over the victim by the offender by means of using cyber space as medium. This is the most common sort of crime now a day's occurring within cyber world and such crime involves cyber frauds, scams, money laundering, terrorist financing, fraud, bribery and corruption, market abuse and insider trading etc.

Cyber Pornography- Cyber pornography can be defined as pornographic material designed, published or distributed using cyber space as a medium. In Bangladesh however viewing pornographic materials are not considered as a crime but producing it is an offense under Pornography Control Act (Pornography Control Act). The most common form of this crime involves revenge porn. Revenge porn is a video or a picture which is made viral over the Internet in view to defame or extract revenge from the person or persons who are on that material. The victims of this crime are also very common now days and most widely are Women and teens. Such contains are always distributed over the net without the consent of victim (Keats, Mary and Franks, 2014, pp.345–392). It's also used for the purpose of blackmailing and exerting power and control over the victims (Bates, 2015).

Online Gambling-Online Gambling are gambling hosted by various websites and involve the transaction of a large amounts of money over the net and such money transactions are made

through various illegal channels and sometimes legal like PayPal and credit cards. This is illegal in Bangladesh although legal in some country.

Intellectual Property Crimes- With the expansion of the modern use of internet over the decade the cyber crimes related to Intellectual property are also growing. Cyber theft of Intellectual Property indicates stealing of copyrights, trade secrets, patents etc by using internet and computers. The most widely stolen Intellectual Property is Copyrights and trade secrets. For example, stealing of software, a unique recipe of a well-known dish business strategies etc. Usually, the stolen material is handed over for exchange of money to the rivals or others for further sale of the product. As a result it does huge loss to the company who originally created it. One of the major and most common forms of this breach is piracy. These days one can get pirated version of movies, software etc with ease and almost without even paying. The piracy results in a huge loss of revenue to the copyright holder. It is difficult to find the cyber thieves and punish them because everything they do is over internet, so they erase the data immediately and disappear within fraction of a second (Loza de Siles, 2015).

Email Spoofing- It is a form of email which is created with content having a fake or forged sender address. It's usually done to mislead or prank the receiver (Pandove, Jindal and Kumar, 2010).

Cyber Defamation- In the case of Sim v Stretch, proposed Lord Atkin proposed that 'a defamatory statement is one which injures the reputation of another by exposing him to 'hatred, contempt or ridicule', or which tends to lower him 'in the estimation of right-thinking members of society' (Asari, K.N. and Ismail Nawang, N., 2014). Cyber defamation is not a specific criminal offense, misdemeanor or tort, but rather defamation or slander conducted via digital media, usually through the Internet. It's done with the intention of defaming, hampering the reputation of victim which is propagated through digital medium and has a real life social, economic and Psychological consequences.

Cyber Stalking- Stalking in general means to 'pursuing stealthily' someone according to oxford dictionary. Cyber Space is a place where people have identities and persona. Cyber stalking is very common type of offense which occurs within cyber space. Cyber stalking means following an individual stealthily with or without letting that person know across the web by posting messages on the bulletin boards frequented by the victim, entering the chat-

rooms frequented by the victim, constantly bombarding the victim with emails etc (Borhanuddin, A.R.M., 2016). This type of cyber crime is frequent to women more than man. Cyber Stalking is also known as Cyber Harassment (Jahankhani, H., Nemrat, A.A. and Hosseinian-Far, A., 2014, p.159).

Data Diddling- It is a kind of cyber attack which is conducted my altering the raw data before a computer processes it and then re-changing it as it was after processing is completed (Borhanuddin, A.R.M., 2016, p.4).

Salami Attacks-Objected towards financial gain in salami attack alteration is made in a system in such a small way that it would usually get unnoticed like in Ziegler Case wherein a logic bomb was introduced in the bank's system, which deducted 10 cents from every account and deposited it in a particular account (Bosworth, S. and Kabay, M.E., 2002, p.116).

Denials of Service Attacks- particular target of this attack are websites which are used for commerce. The victim website is flooded with more requests than it is equipped for hosting which cause it to crash. Distributed Denial of Service attack is also a type of denial of service attack, in which the offenders are wide in number and widespread (Dawson, E. and Raghavan, S.V., 2011).

Virus/Worm Attacks-Viruses and worms are programs that effect computers and systems through replication. The difference between two is the method of replication. Viruses usually attach themselves to a relative program of computer and affect the computer by altering or deleting files. Worms actually don't need host files rather they invade a system and make replication of themselves until the available space of computer dries out (Tiernan, R., 2004).

Trojans & Key loggers- Trojan horse is a program which is disguised as a genuine program and once installed it takes control for the creator a part or whole of the system. E.g. a Trojan was installed in the computer of a lady film director in the U.S. while chatting. The cyber criminal through the web cam installed in the computer obtained her nude photographs. He further harassed this lady. Key loggers affect the computer system same way as Trojan Horse but is directed towards getting keys and password of the computer.

75

Web Jacking- It is derived from hijacking but here the object of jacking is a website. In these kinds of offences the hacker gains access and control over the web site of another. He may even mutilate or change the information on the site (Borhanuddin, A.R.M., 2016, p.5).

Email Frauds- Email Fraud is a kind of fraud where the sender of the mail provides falsified information to the victim to gain monetary advantage over him or her (Kabir, A.E. and Chowdhury, S., 2017, p.421). For example – You won Coke lottery and to have that u have to send your account details to the General Manger (GM) is one of the most common email fraud frequent in Bangladesh.

Hacking- It is a method also a type of Cyber crime where the offender gains illegal and unauthorized access to computer and the offender makes some sort of alteration or modification to a computer system or network with a object to his personal gain Harassment [Jahankhani, H., Nemrat, A.A. and Hosseinian-Far, A., 2014, p.158]. It's one of the most studied type and method of cyber crime in cyber studies.

3.3 Characteristics of Cyber Crime

After the Classification of Cyber crime it is essential to identify the characteristics of cyber crime.

Firstly Cyber Crime is a product of modern technology so the people who have deep understanding of technology and internet are the ones who are offenders.

Secondly cyber crime is relatively easy to commit and get away with, it only involves a mean to access a system and takes few minutes or seconds to do what the offender intends also removing trace thereafter.

Thirdly, Cyber crime is not bound to geographical location so crimes can be conducted from one state to another without any inference.

Fourthly, Cyber crime is a crime that is from planning to execution conducted in cyber space which is not bound by laws of regular states.

Fifthly, it is extremely difficult to determine jurisdiction, collect evidence and prove the same in court of law in case of cyber Crime (Kabir, A.E. and Chowdhury, S., 2017, p.421-422).

3.4 Cyber Crime Victims

The victims of cyber crime are the people who are injured or suffer losses due to cyber crime. Bangladesh is a developing country which has adopted modern means of communication and the Government's commitment towards digitalization in all aspects has boosted the use of mobile communication and use of electronic media through computers. Now a day's people of Bangladesh apply to any job or schools, government tenders, pay taxes through internet. People are becoming more dependent on internet banking and mobile cash services. So with the expansion of communication technology there is an alarming rate of increase in cyber crime too. The victims of cyber crime in Bangladesh are particularly people who have little understanding about internet, Banks, Companies and mostly women.

According to Newspaper "More than 17,000 complaints were submitted to the ICT Division's Cyber Help Desk in the two years that it was open, an official from the division said. Among those, 70% of the complainants were women. More than 60% of women had faced some form of harassment on Facebook. About 10% of the victims had very serious allegations. Their images were stolen, merged with pornographic images and then released on the internet" (Dhaka Tribune, 2017).

According to another article in Daily Star the "rights of women in the cyber space are violated in many ways in Bangladesh and use of internet and mobile phones to stalk, abuse, intimidate and humiliate women is rampant. Women especially the young girls who have been newly introduced to the internet are comparatively inexperienced in cyber world, and consequently they are most susceptible to falling into the bait of cyber criminals and bullies. Morphing, cyber stalking and cyber pornography including revenge porn are the most common cyber crimes that target women in Bangladesh. These attacks against women are carried out to destroy their personal reputation, create fear for physical safety and also monetary losses" (The Daily Star, 2015).

3.5 Specific Cyber Crime and its Rate Occurring in Bangladesh

Cyber crime as seen in above discussion is not new phenomenon since the expansion of modern technology and it is classified into different categories. So not all the categories of cybercrime takes place in Bangladesh. Some are frequent while others are rare. According to a report published in the Daily New Nation 'Hacking, Theft, Cyber Stalking, Identity Theft, Malicious Software, Cyber Defamation, E-mail spoofing, Child soliciting and abuse,

Revenge Pornography, Denial of Service attacks are most frequent in Bangladesh (The New Nation, 2016.)

According to police Commissioner of Dhaka Charged with Cyber Security over 250 cases related to cyber crime are under investigation, about 400 are under trial, 45% of the cases are disposed through trial, 1417 cases where filed since 2012 to 2017 and only CID has a forensic lab to investigate where CID received over 1400 complaints during 2014-2017 alone (Dhaka Tribune, 2017).

So with the above discussion we can narrow down the understanding that cyber crime certain specific ones are frequent in Bangladesh and also from the statement made by commissioner of police it's more certain it's on rise and the country itself is not equipped to combat it.

3.6 Range and Growth of Cyber Crime in Bangladesh

With introduction of modern internet and computers in Bangladesh it has revolutionized how individuals now interact with each other. Over fifty million of people in Bangladesh are connected to internet over the span of four years and the popularity of using internet is growing rapidly.

The era of modern computing began with the discovery of analytical engine discovered by Charles Babbage. The growth of cyber crime since then increased and followed into historical event when The first instance of recorded cyber crime took place in 1820 when Joseph Marie's device allowed the repetition of a series of steps in the weaving of special fabrics causing fear among the employees that their livelihood were in danger. The employees then with intend to discourage use of machine to produce loom continuously sabotage the new technology.

Interpol as a first international organization dealt with computer crime and advocated for its penal legislation by holding conference and through their surveys. The OECD in Paris then in 1984 composed an expert committee to discuss their computer related crime and need for changes in their penal code. The committee proposed to constitute a common denominator between different member states. In 1985 Council of Europe appointed another expert committee in order to discuss the legal and procedural issues of computer related crime. A summary of all national legislation with liability for international acts only, was presented in

the recommendation of 1989. The UN adopted congress resolution o computer crime legislation at 8th U.N congress on the prevention of crime and the treatment offenders in Havana in 1990. Then UN's manual on prevention and control of computer related crime was published in 1994. By end of 90s all European countries adopted new penal laws which are related to computer related crime (Kabir, A.E. and Chowdhury, S., 2017, p.418-419). The word cybercrime was coined in the late 90s, as the Internet spread across North America (Ambrosi, A., Peugeot, V. and Pimienta, D., 2005). As the 20s hit the widespread of use computers begin with that professional hackers and cheaters spammed in cyber space and find ways to gain monetary or personal influence over the victims. In Bangladesh however the growth of cyber crime took a slow turn as modern internets development was popularized after 2005 and spread through the country with mobile internet and popularity of Facebook and growth of social network. The growth of cyber in Bangladesh took a rapid turn because of people being illiterate and simple minded. Majority of the victims was at the beginning were celebrities teenagers and illiterate people who are still learning the new means of technology. The government soon had to take measures in hand to indulge complaints in this regard so the information and communication technology Act of 2006 was enacted which was amended in 2012. In the year 2017 government again took initiatives to reenact law in this regard by passing Digital Security Act, 2018. By this time cyber criminals have caused sufficient amount of monetary and moral damage and it's on the rise. Even the national bank of Bangladesh was hit and millions of Dollars were transferred from bank to casinos in Philippines by the hacker and the government is unable to bring it back. So cyber crime is now a national threat for Bangladesh (Dhaka Tribune, 2016). CyberEdge Group conducted a survey called 2020 Cyberthreat Defense Report the results they found year wise are given

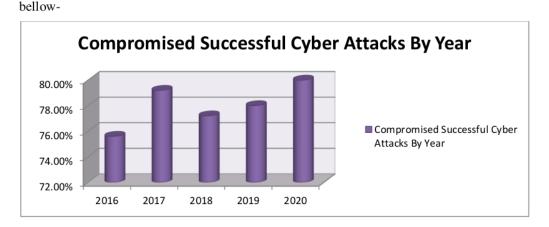


Figure-1 Growth of cyber crime worldwide by year

3.7 Reasons of Cyber Crime in Bangladesh

In general the main reason for cyber crime is the vulnerability of computers. Offenders target rich and easy targets because their privacy is easy to access, they are negligence and the data related to the crime can be easily destroyed. So, Loss of evidence has become a very common & obvious problem which paralyzes the system behind the investigation of cyber-crime.

The reasons for the growth of cybercrime rate against women can be categorized into two folds legal reasons and sociological reasons.

Legal reason can be understood as Crime of any nature is actually objected as to its growth depending on the question on how much easy is it to be committed and get away with. As it stands Bangladesh is actually developing at a fast speed in cyber world and day by day the number of regular users of internet is also increasing. The legislation which actually governs the safety of people over the net is Digital Security Act, 2018 which is full of procedural gaps and as the nature of cyber crime provides little scope for deductive work and investigation offenders are more eager choose to commit cyber crime over actual crime in physical world. The most alarming problem arises when the offender removes his or her trace from internet and also in determining jurisdiction. Also Bangladesh still has no machinery to prove or use digital evidence as there is no Digital forensic lab.

Again for social reason we find that most of the cybercrimes remain unreported due to the hesitancy and shyness of the victim and her fear of defamation of family's name. Many times women consider that she herself is accountable for the crime done to her. The women are more vulnerable to the danger of cybercrime as the perpetrator's identity remains anonymous and he may constantly threaten and blackmail the victim with different names and identities. Women fear that reporting the crime might make their family life difficult for them; they also question whether or not they will get the support of their family and friends and what the impression of society will be on knowing about them. Due to these fears women often fail to report the crimes, causing the spirits of culprits to get even higher (Jeet, S. (2012).

3.8 Laws Protecting Against Cyber Victimization

There are several laws that work in prevention of cyber crime in Bangladesh. The laws that regulate the press are the Printing Presses and Publications Act, 1974 and the Indecent Advertisement Prohibition Act, 1964. The laws that govern media are the Bangladesh Television Authority Act, 2001 and the cinematography Act, 1918. Whenever a law relating

to cyber space is passed there are two concepts of constitutional law that is most frequently brought into question and these are right to privacy and freedom of expression. In actuality these two rights sometimes come into conflict with each other as it's seen when the omitted Information Communication Technology Act, 2006 was in acted, there formed two opinion regarding the enactment of the law where one sect of the critics actually explained that this law is necessary to protect cyber space and individuals right to privacy but critiques who were majorly formed of journalist and media personality argued on this law to be curtailing their right to freedom of expression as the section 57 of the act was generalize in nature and allowed scope of case to be brought against any individual (Kabir, A.E. and Chowdhury, S., 2017, p.51-366).

At present the two main laws which protects individual in cyber space are Pornography Prohibition Act, 2012 and newly enacted Digital Security Act, 2018. The object of Pornography Prohibition Act, 2012 is to prevent pornography production and people posting pornographic materials over the internet.

It's the Digital Security Act, 2018 which is actually law of procedure and substantive governing people's behavior and providing security to people on cyber space in Bangladesh. This law is objected to combat cyber crime of all forms. The act provides for the establishment of Digital security agency, Digital Forensic Lab, Digital Security Council and from sections 17-48 provides punishment of cyber crime of different types and nature. The act also provides procedure for investigation trail and international assistance in later parts (Digital Security Act, 2018)

3.9 Consequences of Cyber Crime of Cyber Crime

In a somewhat conservative society like Bangladesh, the effects of cyber violence against women are not limited to the victims. They have a chain reaction on their families and eventually tear a hole in our social and moral fabric. This section is delved to consequences of cyber crime. Whenever a crime takes place its natural that some consequences will follow with it and cyber crime is no different. Cyber crime has in general consequences which may expand to socio-economic, psychological and biological in nature. In narrow sense this includes loss of life, tarnishing the reputation of victim, loss of employment, social stigma, loss of money, Post Traumatic Stress Disorder, depression, loss of social status.

Loss of life indicates suicides which are directly resulted from commission of a cyber crime in this regard. It is seen in many cases that the victims of cyber crime is humiliated in society and in family and ridiculed among his or her peers where strong minded somehow bear the pain but weak willed people actually pick up the easy way to commit suicide. Its reported in a research conducted by BNWLA in 2014 showed that the victims of suicide resulted directly due to cyber crime was around 24 in the year 2014. Again the most common consequence of cyber crime is tarnishing the victim's reputation which is sometime planed by the offender. The victims of every cyber crime are seen somehow suffering from PTST. Sometimes many victims lose their job because their employers think they working in that establishment will hinder the organizations reputation. This results more monetary losses to the victim and further more he or she is further stigmatized in the society where they live. These consequences sometime have short time or long time effect on the psyche of the victim. Furthermore those who associate with the victim are sometime face alienation or isolation (BNWLA Report 2014 p 145-173).

CHAPTER 4

CYBER CRIME AGAINST WOMEN IN BANGLADESH: AN OVERVIEW

"The growth of the internet has come the growth of cyber-crime opportunities"

Sinrod Reilly, 2000

Cyber crimes can be conducted against Individuals, organizations and Government. Cyber crimes committed against individual may include various crimes for instance transmission of obscene messages, harassment of anybody with the utilization of a computer like e-mail, cyber-bullying revenge porn and cyber-stalking. The second category of Cyber-crimes is that of Cyber-crimes against organization or all sorts of property. These crimes include illegal and unauthorized computer trespassing, and transmission of important and critical information outside the organization which can lead to a great loss to the organization. The third category of Cyber-crimes relate to Cyber-crimes against Government which is popularly known as Cyber Terrorism. This chapter is actually directed to gain an insight and understanding the nature of cyber crime on women in general.

Cyber crime against women or as it can be called violence not only causes physical injury, but it also undermines the social, economic, psychological, spiritual and emotional well being of the victim as well as the perpetrator and the society as a whole. It is accurate to say that this kind of violence is a major contributor to the ill health of women. Moreover, cyber violence doesn't need to be experienced on to leave an impression.

The term 'cyber' is used to capture the different ways that the Internet magnifies, exacerbates or broadcasts the abuse (Dean, 2017). In many ways cybercrime is the same as other types of violence against women, whether it is physical abuse or sexual assault. In that violence is wielded as a tool to control and have power over women, to maintain men's dominance over women, and to reinforce patriarchal norms, roles and structures.

Usually, it has serious consequences on women's mental and physical health, including their reproductive and sexual health. These include depression and suicide, amongst others. Many sorts of verbal and psychological abuse appear relatively harmless initially, but they expand and grow more menacing over time, fairly often gradually and subtly. As victims

adapt to abusive behavior, the verbal or psychological tactics can gain a strong 'strongpoint' in victims' minds, making it difficult for them to recognize the severity of the abuse over time. These physical and mental health outcomes have social and emotional squeal for the individual, the family, the community and the society at large.

Over both the short term and future, women's physical injuries and mental trouble either interrupts, or ends, their educational and career paths resulting in poverty and economic dependence. Family life usually gets disrupted, which also features a significant effect on children, including poverty (if divorce or separation occurs) and a loss of religion and trust within the institution of the family. These squeal not only affect the quality of life of individuals and communities, but also have long-term effects on social order and cohesion. For example In India, one incident of violence translates into the women losing seven working days. In the USA, total loss adds up to 12.6 billion dollars annually and Australia loses 6.3 billion dollars per annum (Hindustan Times, 2005).

Main problem with this kind of violence is that most of the cybercrimes remain unreported due to the hesitancy, strong feeling of shame and shyness of the victim and her fear of defamation of family's name.

Women usually fear that reporting the crime will probably make their family life difficult for them. They also question whether or not they're going to get the support of their family and friends and what the impression of society are going to be on knowing about them. Due to these fears women often fail to report the crimes, causing the spirits of culprits to urge even higher. Nearly 1 / 4 (23%) of the women surveyed across sixty seven countries said that they had experienced online abuse or harassment a minimum of once, starting from 16% in Italy to 33% in the US. Alarmingly, 41% of girls who had experienced online abuse or harassment said that on a minimum of one occasion, these online experiences made them feel that their physical safety was threatened. Over half (59%) of girls who'd experienced abuse or harassment online said it came from complete strangers (www.amnesty.org, 2017). In a somewhat conservative society like Bangladesh, the consequences of cyber violence against women aren't limited to the victims. They have a chain reaction on their families and eventually tear a hole in our social and moral fabric. All impacts of cyber-violence against women can be divided in four groups: psychological, social, economic and physical. In continuation of this research, each of these four types of impacts will be discussed. This

chapter will also examine what are the status of women who are victims of cyber crime their reason for being such and legal and structural support available to them in this regard.

4.1 Cyber Crime Specific to Women in Bangladesh

The expansion use of computers and the internet has facilitated the path for people to keep in touch across the globe worldwide. However, the methods that enable the independent flow of information and Data across the world also give rise to an alarming risk of being in potential victim of high indecent and irresponsible behavior. The Protection and safety of girls is one among the foremost prioritized concerns of each criminal and penal law, but a matter of sorrow and practical regret is that women are still vulnerable in cyber space. Cybercrime against women is on the increase and is at already during a stage that gives a serious threat to the safety of an individual as an entire. The web allows users to share and send information within the sort of text, images, videos and sounds. The widespread circulation of such content is especially harmful for women. In recent years, there are numerous reports of women receiving unsolicited emails which frequently contain obscene and obnoxious language (Agarwal, N. and Kasuhik, D.N., 2014).

Bangladesh is taken into account together of the only a few countries that have enacted ICT Act 2006 then Digital Security Act, 2018 to combat cyber-crimes. This Act widely covers the commercial, economic crimes and Crimes against State. But still issues regarding women still remain untouched.

Social Networking and other websites are created and updated for a few helpful purposes, yet they're lately likewise be utilized to flow hostile substance too. Individuals who post personal information about themselves on job and marriage websites or social networking websites are often at the receiving end of 'cybercrime'. Women and minors who post their contact subtleties become particularly powerless. Amongst the varied cyber-crimes committed against individuals and society at large, crimes that are specifically targeting women are- Cyber stalking, Harassment via e-mails, Cyber Bullying, Morphing, Email spoofing, Cyber Defamation, Revenge pornography (Agarwal, N. and Kasuhik, D.N., 2014). The subsequent chart is summarized from multiple statistical data from the courtesy of statista.com provides a view of specific cyber crime on women.

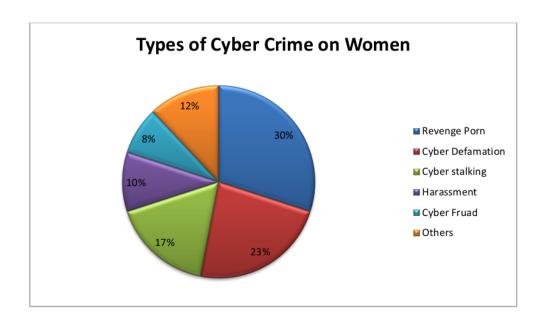


Chart-1: Distribution of Cyber Crime Specific to Women

Another Figure from statista.com with more comprehensive and detailed view is given also.

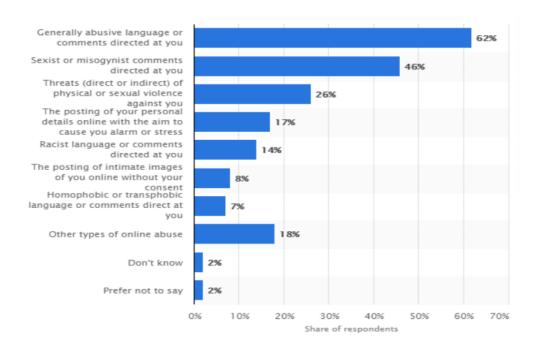


Figure-2: Wide distribution of Cyber Crime Specific to Women

4.2 Vulnerability, Status and Demographic information of Women Who are Victims

After determining the specific cyber crimes which are conducted particularly against women it's essential to gain an insight to the status and some idea about the demography of women who are the victims of this sort of criminal activity. With the lapse of time consumer of internet in Bangladesh is increasing very fast through mobile; by the end of April, 2018 the total number of internet subscribers has reached to 85.918 million. Among the subscribers who use internet 93% of them access it through mobile and the existing number of people using mobile phones have crossed more than 150 million. As natural and expected result use of internet and mobile phones, social media platforms has been increased, 29 million registered Facebook users where 86% use Facebook from their mobile devices. At least one third of the subscribers of mobile phones and internet are women (BTRC Report., 2018).

In Bangladesh, specifically young women are more likely to face severe online abuse that is sexualized and violent than men these kinds of abuse, it is seen women often make formal report of harassment, abuse, and violence originated from online spaces. Study conducted in this regard points that, 73% of women internet users have reported cybercrime (Zaman, S.T., Gansheimer, L., Rolim, S.B. and Mridha, T., 2017). As of December, 2017 the government's Information and Communication Technology Division's Cyber Help Desk has received more than 17,000 complaints, 70% of complainants were women. In 78% of these cases related with digitally manipulated images with pornographic materials, the victim is found to be a woman. It may be noted that, almost 77% of the country's teenagers watch pornography on a regular basis (Report on Porn Addicted Teenagers of Bangladesh, 2014). Bangladesh National Woman Lawyers' Association pointed that harassment was and is ever remained a problem and monitoring and enforcement of the guidelines were poor, which sometimes prevented women from attending school or work (BNWLA., 2014).

Often it is seen women who social media accounts have become targets of hacker. The offenders usually upload fake, undressed pictures of the victim to victimize them. Also, lewd messages are sent from victims account to her contacts (i.e. Facebook friends) to undermine and dishonor the victim.

"Cyber Crime Awareness Foundation a NGO working on raising awareness about crimes in digital space revealed that women aged between 18 and 30 years constitute the highest

percentage of cyber-crime victims at 73.71 percent. The study findings were revealed during a roundtable discussion at Dhaka Reporters Unity (DRU) auditorium in the capital. The findings highlights once again the vulnerability of women in Bangladesh no matter where they go, what they do, how they dress and speak and cyberspace is no less a place for them to be abused than anywhere else" (Cyber Crime Foundation Report, 2019).

In most cases, the form of this glaring violation of human rights ranges from cyber stalking, revenge porn, cyber bullying, and trolling. Women are the primary recipient of offensive and often aggressive sexual advances and defamatory messages in cyberspace from anonymous and fake sources. False and altered unclothed pictures of women along with spam, sex-act videos, rape threats, and indecent proposals have become the new norm of social media (Mahmud, F., 2018).

According to report of Cyber Crime Foundation the following findings show the Gender based effect of cyber crime in comparison to growth from 2018-2019. (Cyber Crime Foundation Report, 2019).

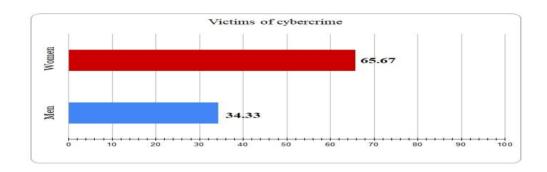


Figure-3: Growth of Cyber Crime Demographics on Gender Basis

4.3 Patterns of Women Cyber Victimization

Women within the SNWs are victimized in several patterns by the abuser who are often a private or maybe a bunch of people. The victimization type differs on the premise various factors, for instance, on the basis of the victim's sexuality, her ideologies, her legal status, her profession and professional commitments, the regularity of her participation in some chosen groups, the language she may use, her popularity within the groups etc. Again, the

abuser may be both male and feminine. Similarly, the offences are often either sexual or non sexual in nature. In most cases male harassers attack the victim for sexual purposes like morphing, using the image for pornographic purposes, cyber stalking etc and non sexual purposes like harassment and bullying. Female perpetrators however, victimize the victim mainly for ideological differences, hatred or for taking revenge. Such attacks might not be sexual in nature. Supported the above criteria the typology of the offences against the women victims within the SNWs is framed as follows:

Cyber verbal abuse by groups of perpetrators expressing hatred: Citron best describes this as "cyber mob attack" where a female member of the SNW could also be attacked by a bunch of perpetrators both within the community wall and also in her own message board.

Cyber defamation targeting the individual self: Emotional breakups may lead the male member to spread lies about the female member to other members through his own posts, community walls etc.

Cyber stalking: the female member is stalked altogether the groups she joins, her friends' walls are constantly watched for seeing her posts, her own write ups and her activities online Morphing: the images of the female members are taken from the private albums and that they are morphed for pornographic purposes by using parts of the photographs, for instance, the top or up to breast.

Cloning: Cloned profiles or fake profiles of female victims are created by stealing the private information of the female member. The cloned profile presents the first profile in such a fashion that folks are duped. The cloned profile then asks the buddies of the first member to become his/ her friend and crack the privacy of other members besides using the first member's information for evil purposes. Female members within the popular SNWs like Facebook, MySpace often face this problem.

Cyber obscenity: The victim's photograph is employed, morphed and distributed within the internet with obscene postures. The harasser can also post messages using obscene languages to her wall. Cyber obscenity also can be practiced by way of hacking the profile of the feminine member. Then the first photographs posted within the mentioned profile are morphed and therefore the profile name and knowledge also because the morphed

photographs are wont to send obscene messages to the "friends" of the first profile owner and also to wider audience.

Hacking: Particular targets are chosen and their profiles are hacked. Their personal information is employed for evil purposes. The harasser may even distribute open invitations for having sex with the profile owner at her home address.

Cyber harassment: this might include constant messaging to the profile's wall or personal email id which is shown within the profile, regular peeping in as a visitor and leaving messages in her wall, continuously sending request for friendship, joining groups where she is member and constantly posting messages disagreeing together with her, etc.

Virtual rape: this is often a violent sort of cyber victimization where the targeted woman is haunted by a harasser. He either posts constant messages like "I will rape you", "I will tear you up" or "your internet identity are going to be f...ed off" etc, or particular community members may "mob attack" the targeted female with such words which successfully generates more enthusiasm among other unrelated members to discuss the victim's sexuality. The profile owner then becomes a hot topic for erotic discussions, vulgar names etc.

Banning a female member and restraining her from expressing her views: This generally happens during a male dominated group or community where the moderator or owner or group members may victimize the targeted female member by banning her for her own feminist ideologies even through the group or the community could are created for letting people express their own ideologies. The rationale might be that the bulk of the group could also be pro feminist or some individual members dislike the straight forwardness of the female members in discussing the issues of girls in everyday world.

Cyber Bullying and Name Calling: The harasser may constantly bully the target within the SNW, both in her wall and within the groups or communities where either he or she is member. Albeit this is often a gender neutral cyber offence, women are most chosen targets for his or her sexuality, emotional breakups or maybe violence. The ex spouse or the ex lover constantly bully the lady to vent out his anger publicly.

Cyber flirting generally starts when miscreant sends the victim obscene songs, videos or messages.

Domestic violence and cyber flame: As mentioned above, separated partners may take up SNWs to vent out their anger against the feminine member. In such cases the ex-partner starts bullying the lady first then provokes her to possess "online fights".

Impersonation and cheating: SNWs give wide options for creating profiles under pseudo names, hiding one's real age, sex and other information. Further, the creation of multiple profiles of an equivalent individual using different email ids is additionally possible within the SNWs, this provides the chance for mischief mongers to impersonate and entertain female members'. The harasser drags the victim in an emotional relationship and she or he is inspired to share her secrets, and even have erotic chats with the harasser. When the victim finally pressurizes to satisfy him face to face, either he blackmails the victim or cheats the victim. However, impersonation and cheating can even happen for financial issues in the SNWs as well. The harasser may promise the victim some online or offline monetary gain by showing his fake credentials and there by later on dupe the victim.

Blackmailing and threatening: This happens due to the easy availability of the personal information of the women members in the SNWs. "Jilted lovers", ex spouses, mischief mongers and stalkers may threaten and blackmail the woman for various reasons which may even lead to shut down the profile of the female member. This can even have an offline effect where miscreants may physically threat and blackmail the woman with her secrets that she may have shared with her friends in groups or communities (Karuppannan, J. and Halder, D. 2009).

4.4 Reason of Women Cyber Victimization

Every human action has rationality and by the principle of rationality every human action has a reason even if the action taken may seem irrational. So crime is an illegal action taken by the offender which causes harm to the victim and thus is intentional and motive driven. Cyber Crime is a crime committed in cyber space targeting individuals to gain some sort of advantage over him/her. Among the key motives of such cyber-crimes against women are defaming the victim; revenge; compelling the victim for physical relation; blackmailing for money; physiological torture; ego and power trips; the obsession for love and emotion etc. To

summarize why the women are most preferred target of cyber crime following things are to be taken into consideration.

Firstly, the main reason for cyber crime against women is to exert power and control over them. It is seen in most cases similar to sexual offense cyber offender's usually target women in cyber space to have control over her real life. Cyber stalking and revenge pornography can be explained by this notion. Rational choice theory in this case suggests that individuals, which would be cyber stalkers, freely choose to commit a crime after determining the prospective rewards against the potential risks (Mullins, 2007). Routine activities theory can also be integrated with rational choice theory because routine activities theory proposes that any person will commit a crime if there is a motivated offender, suitable target, and absence of guardians capable of preventing the offense from successful commission. Usually it is seen in most cases the offenders in these cases are among known acquaintance of the victim. The offenders usually target victim who they can get monetary sexual or any other benefit (Mustaine, E. E., and Tewksbury, R. 1999).

Secondly, Cyber crime against women in 70% cases is committed due to revenge as a motivational force. It is seen in majority that a jealous husband or lover usually post intimate pictures and videos over the net to defame or cause damage to the reputation of the women who ended the relationship (Dhaka tribune, 2019).

Thirdly, Cyber crime is easy to commit and get away with and through it the offender can actually cause real life damage to the victim.

Fourthly, Women of Bangladesh are still simple minded and very trusting so cyber offenders actually present them with irresistible offers which they often think as real and fell in their trap.

Fifthly, the accounts of women in social media are less secure especially in case of Bangladeshi women and are easy to be targeted by professional criminals.

Sixthly, there is little social awareness among the women regarding their privacy and safety in internet and there is no promotional awareness neither from government nor from private sectors in this regard to create awareness which makes women more vulnerable.

Seventhly, most of the cybercrimes remain unreported thanks to the hesitancy and shyness of the victim and her fear of defamation of family's name. Many times women consider that she herself is accountable for the crime done to her.

Eighthly, in Bangladesh the legal and legislative support available to women in this regard is generalized and not specific like certain laws enacted to protect women only such as Women and Children Repression Act, 2006. The provisions of New Digital Security Act, 2018 have no specific section which covers women's safety in cyber space and there are a lot of provision in the Act which is not implemented yet. This makes proving cyber crime to court and ensuring justice almost impossible. The present investigation system is not equipped with technology which can in proper way finish a case in favor of victim and at the same time there is no digital forensic lab to gather Intel on this regard. All of these factors motivate and encourage offenders to commit cyber crime against women because they believe and are sure they can get away with the offense.

4.5 Legal and Structural Support Available to Women in this Regard

Women in Bangladesh are disproportionately targeted by online and technology facilitated violence and harassment. While the expansion of Information and Communication Technology (ICT) and growing internet penetration are considered as positive indicators of development in the country, but their interaction with certain pre-existing social-physiological settings related and inadequate legal protections have led to increased cyber violence against women. Women are the primary recipient of offensive and often aggressive sexual advances and defamatory messages in cyberspace from anonymous and fake sources. False and altered unclothed pictures of women along with spam, sex-act videos, rape threats, and indecent proposals have become the new norm of social media.

A proverb goes 'Prevention is better than cure'. For prevention of numerous cyber crimes it is better to initiate advanced technological actions. These are technological precautionary affairs for prior prevention. We will rather try to find out the legal and other remedies and their lacking available in Bangladesh for curing the alleged cyber crimes. A cyber victim in Bangladesh has a better opportunity to get the proper remedy under the ICT Act, 2006. This statute is the first that door open for the lawful remedy of numerous cyber crimes in Bangladesh. Through this statute it is being tried to locate all the probable grounds of cyber crime frequently occurring at present and which might occur in future as well like damaging

any computer or computer system, hacking, spreading viruses and false information, causing defamation through the internet, changing the source code, stealing or damaging any text, audio, video documents etc. then the government enacted pornography control act, 2012. And on 2018 the government enacted Digital security act, 2018. However from past to present there is been no special provisions of law which covers only woman's security on net (Maruf, A.M., Islam, M.R. and Ahamed, B., 2014).

Structural support for women in this regard is still too low, there are NGO; s along with police special wing of cyber crime is working at this regard. But still the support only exclusive to women are not sufficient. Some this NGOs involve Bangladesh National Women's Lawyer Association, Cyber Crime Awareness Foundation, Ain O Salish Kedra etc.

Another aspect of this crime is although in Bangladesh there is Digital Security Act, 2018 but people and victims tend to attain justice is really marginal. The following chart from The Report of Cyber Crime Foundation gives an exact view in this matter.

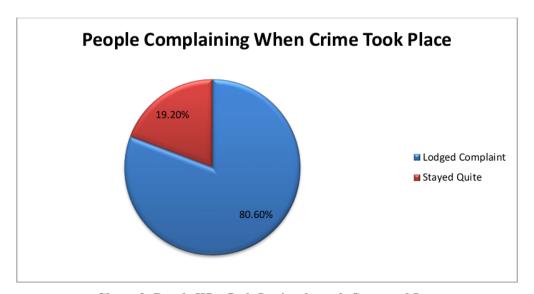


Chart- 2: People Who Seek Justice through Court and Law.

When the respondents were asked the reason why they don't seek formal justice about 23% said they wanted it kept secret, 22.7% didn't knew the procedure, 19.3% were afraid of hassle of procedure and 16% truly believed that they will never get justice (Cyber Crime Foundation Report, 2019).

4.6 Psychological Impacts of Cyber Crime

Psychological harm is recognized as a form of violence and is clearly defined as a human rights violation under international law. According to a survey taken by Symantec, the Norton Security Company, people have identified their top emotions after falling prey to a cybercrime as angry, annoyed, cheated, upset, and frustrated, among other associated terms that are expected in the aftermath of such an event.

The Human Impact, which represents the first large-scale study to examine the emotional impact of cybercrime, shows that victims' strongest reactions are feeling angry, annoyed and cheated, depressed and in many cases, they blame themselves for being attacked. Many believe that 'faceless' criminals are the main perpetrators of cybercrime and nearly of users surveyed don't expect cybercriminals to be brought to justice (Norton.com, 2016). As a result, many victims fail to take action as far as reporting and working to remedy the damage done. The following chart is a representation of human emotions occurring after cyber crime is taken place by courtesy of Norton.com.

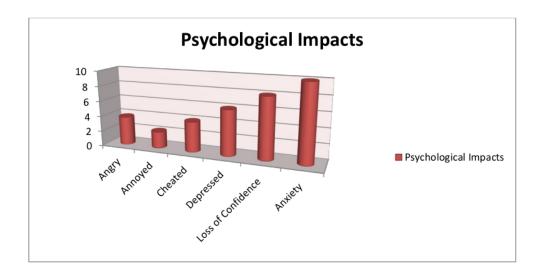


Figure-4: Psychological Impact of Cyber Crime on Women

The most prevalent impacts are psychological impacts, which are felt by most women who experience cyber-violence. In the survey which was done for sixty seven countries all over the world, (www.amnesty.org, 2017) 65% of the women reported experiencing some sort of psychological impact, ranging from the most common, anxiety and damaged self-image (with

roughly half and 43% of respondents respectively), to the most extreme, thoughts of suicide and engaging in self-harming behavior (10% of respondents). These impacts are apparent in the famous self-published stories of Daisy Coleman, Annmarie Chiarini and Savannah Dietrich who describe experiencing all of the above and other psychological impacts (Jessica West, 2014).

These forms of violence also impacts on women's capacity to move freely, without fear of surveillance. It denies them the opportunity to craft their own identities online, and to form and engage in socially and politically meaningful interactions.

The psychological impact of online abuse can be devastating. For psychiatrist Muriel Salmona, cited in a report from the High Council for Equality of the French government, these forms of violence impact on women's mental health and physical health that can last long term and cause avoidance and control behaviors, accompanied by anxio-depressive disorder, sleep disorder, and can damage social, emotional and sexual life (Mariel Salmona, 2017). UNICEF furthermore announced in 2014 that the risk of suicide attempt is 2.3 times higher for a victim of cyber harassment compared to non-victims.

- Across all countries 61% of those who said they'd experienced online abuse or harassment said they'd experienced lower self-esteem or loss of self-confidence as a result.
- More than half (55%) said they had experienced stress, anxiety or panic attacks after experiencing online abuse or harassment.
- About 63% said they had not been able to sleep well as a result of online abuse or harassment. Three-quarters (75%) in New Zealand reported this effect.
- Well over half (56%) said online abuse or harassment had meant that they had been unable to concentrate for long periods of time. (UNICEF., 2014)

Only 3% of women don't think it will happen to them, and nearly 80% do not expect cybercriminals to be brought to justice. It is resulting in an ironic reluctance to take action and a sense of helplessness.

Despite the emotional burden, the universal threat, and incidents of cybercrime, people still aren't changing their behaviors – with only half (51%) of adults saying they would change

their behavior if they became a victim. Even scarier, fewer than half (44%) reported the crime to the police. There are consistent findings that victims tend to have lower self-esteem than their peers who are not victims. These results could be explained by the fact that the experience of being a victim decreases one's self-esteem or that those with low self-esteem are more likely to be targeted as victims (Houbre, Tarquinio and Lanfranchi, 2010).

Cybercrime victim explained, "I was emotionally and financially unprepared because I never thought I would be a victim of such a crime. I felt violated, as if someone had actually come inside my home to gather this information, and as if my entire family was exposed to this criminal act. Now I can't help but wonder if other information has been illegally acquired and just sitting in the wrong people's hands, waiting for an opportunity to be used" (Security, n.d.).

In terms of consequences, research has regularly found that experience with both bullying and cyber bullying contribute to a host of maladaptive emotional, psychological, behavioral, and even physical problems. These include, but are not limited to: anger, self-pity, depression, anxiety, eating disorders, and chronic illness (Borowsky, Taliaferro and McMorris, 2013). Minor and moderate forms of school misbehaviors and violence have also been associated with cyber bullying in recent years (Hinduja, S., and Patchin, J. W., 2010).

4.7 Social Impacts of Cyber Crime

The social consequences for women are often very severe, particularly if their entire community is involved with the cyber-violence. For instance, within the case of Daisy Coleman, her brother and she were bullied in class. She was suspended from her cheer leading squad, her mother lost her job, her family was forced to maneuver back to Albany and their range in Maryville was burned down. Likewise for the 33-year-old woman whose ex-partner solicited men on the net to come rape her, she also removed of her community, and therefore the affects were felt by her whole family as her children had to change schools. (BuzzFeed News, 2013).

In a somewhat conservative society like Bangladesh, the results of cyber violence against women aren't limited to the victims. They have a sequence reaction on their families and eventually tear a hole in our social and moral fabric.

Cyber Bullying as Gender-based Violence Online Survey found that 3.3% of girls responded that that they had to maneuver out of their community as results of cyber-violence. a standard social impact of cyber-violence is isolation from friends and family. It's common for several victims that ex-partner posts things about them on Facebook and a few of victim friends and family, including siblings, stopped chatting with them. They believed whatever attacker had posted on Facebook. This is often one among the foremost commonly reported social impacts with 28% of girls responding that they experienced isolation from friends and family as results of cyber-violence.

Isolation from friends and family is extremely serious for women, and therefore the threat of exposing information that would potentially cause women's friends and family to show against them is taken very seriously by women. Often women will adjust to their abuser's threats so as to avoid such repercussions. Usually abuser knows how afraid female is of her circle of relatives checking out about her work, for instance as an escort in order that they use that to coerce her to possess sex with him on demand.

The most common social impact reported by women is withdrawing from online activity, with 40% of girls reporting that they need experienced this as an impression of cyberviolence (Jessica West, 2014). Having experienced abusive relationships within the past, most of the women are avoiding using social media and online platforms so as to stay themselves safe. They're very scared of the likelihood of individuals online using their personal information against them, violating their privacy and becoming the victims of bullying and violence. However, avoiding online activity to stay safe also mean that they're overlooked of online social networks and therefore the significant amount of socializing that takes place online in our society. Therefore, the important social impact of withdrawing from online activity is usually social isolation.

Cyber violence and hate speech online against women can have a long-term effect on women's reputations and may damage the livelihoods of girls. Consistent with the 2014 Pew research facility report on cyber abuse, a few third of the people (men and women) who experienced physical threats and sustained harassment felt their reputation had been damaged. Overall, 15% of those who have experienced online harassment said it impacted their reputation.

Furthermore, by pushing women out of cyber space's, due to fear of victimization or retaliation, cyber violence punishes women counting on the net for a living, within the cases involving intimate partner violence, image-based sexual assault, the victim's current or future employment status are often compromised by privacy attacks and private information released online.

Many studies show the negative impact of cyber-violence on female performance, including reduced concentration, school avoidance, isolation, lower academic achievement and better risk of faculty problems (Hinduja and W. Patchin, 2007). Greater frequency and intensity appear within the group of perpetrators/victims, and that they feel less safe at college, have lower self-esteem and have more suicidal thoughts (Hinduja and W. Patchin, 2008). However, other research indicates no such differences.

4.8 Economic Impacts of Cyber Crime

Cyber-violence against women can have serious and detrimental economic impacts for women also, particularly nonconsensual distribution of images and revenge porn. Women can even lose their jobs over things that get posted about them on the web, and with the impossibility of ever completely erasing things from the web, revenge porn images and defamation can haunt women forever, keeping them from being hired for brand new jobs or advancing in their current job (CNN, 2014). It also has an impression on the economic health of girls and their family, their communities and societies.

Around 13% of girls reported some impact on their job (losing their job, being unable to advance in job or being unable to seek out a replacement job) (Jessica West, 2014). Interestingly, a big number of girls (10%) reported that their credit rating was damaged as a result of online abuse.

Regarding cyber violence happening within the context of intimate partner violence, researchers have estimated the value related to responding to technology-based victimization "to \$1,200 compared to \$500 for survivors of non-technological abuse" (YWCA, 2017). Cyber violence and hate speech online have a physical and psychological impact that demands reparations, having a price, both at individual and society level. Some costly consequences of cyber violence against women include: chronic physical conditions and loss

of anticipation, psychological state conditions (e.g. depression, anxiety, post-traumatic stress disorder, attempted suicide) that demand future treatments; sexual and sexual health issues, sometimes hindering women's reproductive health; drug abuse and associated crimes; social isolation and solitude; lost wages; reduced participation in society; and individual and public expenditure on medical protection, judicial and social services.

Also, there's a comparatively new sort of cybercrime. It came up just a few of years ago. It's called ransomware, and within the essence it's a cryptovirology attack gaining a fast popularity among cybercriminals. By entering a cryptovirus during a user machine with, as an example, a computer virus attack - cybercriminals can lock the user's screen or encrypt vitally important data on the pc discs or connected databases, then demand a ransom to return computer status/data back to normal.

These attacks becoming more frequent and make serious danger as they will cause loss of business or personal data privacy, confidentiality, and security, also as substantial reputational and loss. Paying ransom may be a two edge sword, because the same cybercriminals can repeat this attack again. There was a mention within the media that the worldwide economy loss reached a mark of 1B\$ a year thanks to ransomware attacks.

49 Death and Suicides Related to Cyber Crime

The relationship between cyber bullying and suicide has continued to grow in recent years (Goldblum et al., 2014). Bullying victims were 1.7 times more likely and offenders were 2.1 times more likely to have attempted suicide than those not involved in bullying. Similarly, cyber bullying victims were 1.9 times more likely and offenders were 1.5 times more likely to have attempted suicide than those not involved in cyber bullying. Finally, cyber bullying victimization was more strongly related to suicidal thoughts and behaviors than school bullying victimization (Hinduja and W. Patchin, 2010).

These findings have been duplicated in more recent work and in general cyber bullying victimization tends to be a consistent covariate of suicidal ideation, although possibly mediated by depressive symptomatology (Luis Jasso Medrano, Lopez Rosales and Gámez-Guadix, 2017).

Not only do girls and women who experience cyber-violence against women sometimes face thoughts of suicide and attempt suicide, but sometimes they also complete their suicide attempt, such is in the tragic stories of Rehtaeh Parsons and Amanda Todd.

Consequently, it leads to shattering the victim's career, education and social life. Some victims take the route of drug addiction while some choose to end their lives. Only in a handful of exceptional cases do we see the victims recover from such a tragedy.

From 2010 to 2014, Bangladesh National Woman Lawyers' Association identified a total of 65 reported suicide attempts by female victims of violence. It also reveals that on an average, every year there are 11 suicide attempts by women due to cyber violence. By contrast, in 2008 this number stood at 8 revealing a sharp increase in the trend. Needless to mention, the official statistics is just the tip of the iceberg. The number of unreported cases far outweighs the reported ones. The following figure shows the statistics of Suicide attempts due to cyber harassment to grasp the reality and importance of the situation (Survey on Psychological Health of Women, 2014).

Year	Suicide Attempts
2011	10
2012	17
2013	21
2014	32

Table-1: Suicide Attempts due to Cyber Crimes and Harassment in Bangladesh

CHAPTER 5

METHODOLOGY OF RESEARCH

The methods segment depicts actions to be made to examine and exploring a research problem and the reasoning for the utilization of specific methodology or procedures used to recognize, select, measure, and break down data applied to understanding the issue. There are two research methods in social research one is Qualitative and another is Quantitative. Along with certain similarities the both styles differ from another in significant ways. Each method has its strengths and limitations, issues where it is most efficient and provides understandings which leads to discovery of new facts in social science. This chapter hosts the total representation to the methodologies which are used in this study.

5.1 Main Method

The present study is conducted through qualitative research approach. As method case study is selected through which the cases of women who are victims of cyber crime and also support agencies in this regard is studied, analyzed and interpreted for the research findings. In this study, data is collected through semi-structured interview schedule which are analyzed and interpreted by using descriptive techniques.

Qualitative approaches are utilized across numerous academic disciplines, focusing especially on the human components of the social and natural sciences. Qualitative methods are best for researching many of the why and how questions of human experience, in making a decision for example; and have a strong basis in the field of sociology to understand government and social programs. Qualitative research is widely used by political science, social work, and education researchers. Since this research is objected primarily on understanding the nature and impact of cyber crime on women in Bangladesh the justification of choosing qualitative research and case study for it can be derived from the observation of scholars in this field —

According to Merriam (2009) "Qualitative researcher are interested in understanding the meaning people have constructed, that is, how people make sense of their world and experiences they have in the world"

According to Parkinson and Drislane (2011), "Qualitative research is research using methods such as participant observation or case studies which result in a narrative descriptive account of setting or practice. Sociologists using these methods typically reject positivism and adopt a form of interpretive sociology."

5.4 Research Area

The Dhaka City is selected as the area of study to find victims of cyber crime and also to select relevant support agencies for the study.

5.3 Population and Unit of Analysis

In this study the women who are victims of cyber crime, law enforcement officers and agents of victim support agencies are taken as population and each of these persons are considered as the unit of analysis.

5.6 Sample and Sampling

Selection of sample and sampling is a significant part of the research. Statistical representation is not deciding factor in sample size in this study rather size that was sufficient to provide required data in lieu to the objective of the research was deciding factor of sample size. In the study non-probability purposive sampling technique was adopted in selection of respondents. Neuman (2000) provides justification to selection of such sampling technique when three conditions are met. First, when a researcher decides to choose a case that is especially informative; second, when selecting members of a difficult to reach specialized population; and lastly, when a research tends to identify cases for in-depth investigation. So from the study area 5 female who are direct victims of cyber crime and 3 law enforcement and support agency representatives (2 male and 1 female) are selected. As the nature of study being sensitive, the reason for choosing purposive sampling is the researcher can use his experiences to select sample that will be the most useful or representative for the study.

5.5 Data Collection Tool

The data was collected through face to face interview with the respondents. A semi-structured interview schedule is used and both open and closed ended questions were designed. Following the semi-structured interview guide more information from the respondents were collected and respondents have understood more about the importance of the study and took it into a great concern. Interviews were conducted in Bangla because it is assumed that the

respondents are comfortable in answering the questions in their native language since they had to talk about a sensitive issue. Then they were for the purpose of research transcribed in verbatim style to English. Semi-structured interview guide allowed me to ask extra question about their feelings and share their opinion also. Semi-structured interview guide covered themes of respondent about their life style, thinking, sufferings, experiences and perspectives also. To ensure accuracy secondary data was collected from different journals, papers, books, literatures, official documents and internet.

5.9 Processing, Analysis and Interpretation of Data

Qualitative analysis is very tedious and demanding measure. Qualitative data comprise of words and perceptions, not numbers. Similarly as with all data, examination and interpretation are needed to bring order and comprehension. Neumean and Kreuger (2003) mentioned that "qualitative analysis does not draw on a large well established body of formal knowledge from mathematics and statistics. The data are in the form of words, which are relatively imprecise, diffuse and context based, and can have more than one meaning. So, researcher analyzes data by organizing it into categories on the basis of themes, concepts or similar features and develops new concepts, formulates conceptual definitions and examines the relationships among concepts."

Therefore the information was collected through the semi structured interview in verbatim style, has been complied for qualitative analysis. Qualitative data have been condensed through classification or categorized through coding. This was done because qualitative coding is an integral part of data analysis. In the perspective qualitative data analysis we know that it is deferent from quantitative analysis and less about statistical analysis and closer to raw data. Qualitative analysis does not draw on an established body of formal knowledge from mathematics and statistics. The data are consisting of words, which are relatively imprecise, diffuse and context-based and can have different meaning. So data was analyzed by organizing it into categories, ideas, concepts or similar features and develops new concepts from connections and examines the relationships among the concepts. This study, firstly data from the study area was edited. Then it have been classify and categorized then coded according to the characteristics and then coded data was analyzed and it was presented through Electronic print.

5.10 Validity, Reliability and Generalizability

Validity, in qualitative research, alludes to whether the discoveries of a study are true and certain. True as in the study discoveries precisely mirror the circumstance and certain as in research discoveries are upheld by the proof. To that note Robert L. Barker (1995) defines validity as "the concept concerned with the extent to which a procedure is able to measure the quality it is intended to measure". There are two fundamental sorts of Validity, one is internal which refers to the legitimacy of the measurement and test itself and other is the external validity referring to the capacity to generalize the discoveries to the objective populace. I have used both criteria in my study which have helped me to ensure the qualitative inquiry such as differentiation and explication as primary and demonstration of authenticity and integrity as second criteria. By these criteria I have added aptness of the tools, data and process in my study. I have found actual results of my study through validity. To increase the validity as much as I could as first triangulation, second triangulation; as well documented check trail of materials and process, multidimensional analysis, respondents verification. I have tried to validate my study also by maintaining prolong engagement and persistent observation of my respondents and i have build up rapport to my respondents.

Validity means' having establishment dependent on truth' while the term reliability is most firmly identified with idea of consistency. The objective of data collection is to collect data that is 'reliable data'. The data will be the same overtime and place. "Reliability of research according to (Wiersma, 2000) concerns the reliability and consistency of the methods, conditions and results. Reliability is a necessary characteristic for validity. Essentially reliability and validity establish the credibility of the research". I have used reliability to find out the accurate results of my study. By designing the data, evaluating and analysis the findings and arbitrating the standard of my study: I have ensured reliability in my study. Reliability has also assisted me to ensure the analytical procedures of my study.

To generalize is to claim that what is the case in one place or time, will be so elsewhere to in another time. The goal of qualitative work isn't to sum up over a populace. Rather a qualitative approach tries to give understanding from the respondent's point of view. From the findings of my study and after careful consideration of other examination of same nature previously conducted in this field i can say that this study can be generalized in whole of the selected issue while it was being conducted to when it reach its final outcome.

5.8 Ethical Consideration

The researcher has asked for verbal consent from each respondent. The aim and purpose of the researcher was clearly explained to every respondent. The researcher has tried his level best to ensure and maintain values, norms and ethics of the research. Respondents" rights to confidentiality was be secured and maintained to the best of knowledge.

CHAPTER 6 FINDINGS (CASE PRESNATATION)

A case study is a definite investigation of a particular subject, like an individual, group, place, event, organization, or phenomenon. Case studies are regularly utilized in social, educational, clinical, and business research. There are total 8 cases in this research which is divided into two parts; among them 5 are the cases of women who are victims of cyber crime and 3 are case narrative of people who are engaged in facilitating curative and preventive services to the women victims of cyber crime. This chapter widely presents their narrative as they described.

6.1 Presentation of Case of Cyber Crime Victims

This segment is exclusive to describe the detailed case presentation of victims of cyber crime along with their own narrative in different aspects. They are identified as A, B, C, D, E

Case-1

"A" is a 24 year old woman, currently living in Dhaka. She belongs from a 5 member family where she is the eldest daughter. The family is believers of Muslim faith. Her education status is B.S.S. She manages her financial needs well before the incident through money from her family and private tuitions which she taught students of schools. Her educational cost is minimal because she studied in Government College. Every one according to her was very nice to her until the incident of cyber crime took place.

"A" was studying in a college in Dhaka before this she was raised in her native hometown situated in Barisal district. When she graduated H.S.C, she came to Dhaka for her honors and after coming to Dhaka she made new friends and through her friend she meets a boy and started a relationship with him. The boy eventually captured digital materials of their intimate time. After that the boy started cheating on the victim to which she confronted and broke off her relationship with the boy. In revenge the boy released the sensitive content on internet. The incident according to victim's narrative is as follows-

"I got into a relationship with a boy who was studying in engineering in a private university. As I dated him we shared intimate moments and when he cheated me and broke off with him he released those on internet. I even begged him, that off from the website but he denied and said something in slang and I deserved it".

She thinks government in the issue of cyber crime is aware but she is not satisfied as there are no specific provisions in law that safeguards the rights of women as she stated:

"About my victimization or women victimization government I think doesn't have any particular policy or law separate for women which makes it difficult in access to justice because our cases are handled typically as ordinary which is disappointing because women has more to lose in defamation then male in our society"

She faced extreme social problems like being isolated, bullied and criticized among her peers and society. She even faced difficulties in her family and got little support suffered social alienation and discrimination, she felt ashamed because of people around her being judgmental to the incident and blaming her, and to that she said:

"the social problem I have faced, first there was problem of gossip in my college and among my peers... upperclassmen and some started calling me with worse names ... this news traveled to my family and I got heavy threats of stopping my education and scolding from my family side particularly from my father". People will often judge me as some kind of prostitute or worse".

She faced many difficulties in legal issues such as the local police stations refused to take her case which made her worried more and to that from her statement as she stated:

"I would like to tell that there is no legal assistance in Bangladesh rather there is legal harassment. After the incident I along with some of my friends did go to police they refused to lodge any case and rather asked me to file a GD so they can see what they can do... Some said to contact a higher up connection if I had any among my friends or family"

The Victim had immediate and long lasting deep rooted psychological trauma such as nervousness, anxiousness and self harm, which she described by herself as:

"I was depressed, nervous, anxious, humiliated and worst suicidal. I wanted to end my lifogeveral occasions but I had some same age people looking for me so I survived. I really don't want to talk about those nightmares"

This case was classified as a case of revenge pornography and it is still in trail before cyber tribunal situated in Dhaka.

Case-2

"B" is a 34 year old female living with her husband who is a government employee along with her two kids. She is in faith a Muslim and her educational qualification is MS. She comes from a well-off family and has good social standing. She has no financial crisis. She met on net a woman who claimed to be a Syrian refuge who is in need of assistance. One day the victim got a random call from a person claiming to be a customs officer that she has received a parcel and she has to pay taxes as in parcel there is money in Euros. He blackmailed the victim to deposit money in a particular bank account and when victim deposited the said money they turned off all communication and ran away with the money. The victimization according to victim "B"s narrative is as follows-

"One day I got a call have a parcel in my name from Amira and in that parcel there is about 10,000 euro which is now laundered money and I have to pay taxes so it can be white money or I will be charged with money laundering. He said they will give me a account and I have to deposit 725850 Taka in that account as VAT and Excess duty then with that receipt I have to come to customs office and show my voters id card as proof and sign some papers so I can clear. I somehow managed the money and deposited it on the said bank. After that when called him I was shocked that the number was completely off I tried to message Amira but her account was deactivated".

She faced harassment from her relatives and she kept the things under the wraps in fear of social criticism and to that end she stated:

"The major social problem I faced was that I was blamed and ridiculed by my husband's side and in laws when they heard it. We hid this fact from the society in fear of people gossiping and ruining our reputation future down on mud".

Victim found the process of courts to be lengthy and she didn't found help in local police stations to which she commented:

"...My case is still on trail so it's almost one year of the crime actually taking place so the delay in process and getting justice is a definite issue for me... when we contacted local Thanas they said they can't do anything but they said out of respect to my husband they advice us to talk to CIDs cyber crime division".

As limited people know about her victimization so she didn't get any help from her society. But her regular life changed and she faced financial consequences which she states as:

"Regular life changed in a way that I was blaming myself and it affected all of my regular activities. I could not sleep well at night it also effected for some time in my health. A huge amount of sum was taken away in fraudulent way and then the whole process involved many costs of travels, lawyers fee etc. So it was a very traumatic and expensive experience".

The victim also suffered long term psychological issues which she describes:

"I was blaming myself and self guilt was killing me. I suffered from depression and anxiety of what is going to happen next. I lost trust on people. I became insomniac and I was treated with a psychologist... I felt complete insecurity after cyber crime happening to me".

The Victim wasn't aware or heard of NGOs working dedicated to this issue and didn't seek help from any to this she said:

"No I didn't got myself involved with any organization nor we got any voluntary help".

This case is common form of online fraud and the offender here targeted women because they tend to believe that women are easy targets. The case is pending for witness testimony before the cyber tribunal. The victim is yet to receive any formal remedy.

Case-3

"C" is a female who lives with her family in Dhaka city. She is 19 year old girl who passed her H.S.C examination. She is of faith Muslim. She had no prior social and financial problem before the cyber crime incident. She was supported by her family for education and Health. The case of her victimization according to her narrative is as follows-

"My case is against my ex-boyfriend. We meet in a co-educational college after my S.S.C. He somehow managed my contact number and used to call me at first I would avoid him then after some time I get used to talking to him. On issue of his birthday he invited me and made physical contact with me under influence of drug. When I got well I said I will not stay with him in fury he circulated that video of that moment on the Whatsapp group of college".

Regarding awareness about cyber crime, herself and government's awareness the victim seemed confused but she said she didn't felt that the awareness through promotional activities were enough as she in this regard notes:

"I don't know Government may be aware but I never saw any warning...Hmm.. Like they say smoking is bad for health. Before this case I only heard about cyber crime in class 8 book".

The victim was worried for delay in filing of her case as she said:

" ... the case took....like like 3 months right? Mom? to get started that made me worried and sad...".

According to her she faced many social problems and discrimination in her school, among her own relatives and neighborhood:

"... Many social problems I faced among them was shame to show my face... People called me with bad names as it's my problem especially my class mates...in college ...among relives and in neighborhood to whoever who heard or seen that video. They think sin is mine ...I am bad girl".

About legal issues she didn't know much her mom was the person who took care of that but victim felt uncomfortable sharing and revising her story of victimization as she said in this regard:

"that everything is known by my mom...I don't know 79 ything.. but I felt uncomfortable coming to court and in front of people... It's not that I wanted this to happen to me".

The Victim "C" didn't get any help or encouragement from her society rather her regular and personal life was adversely affected by the occurrence of cyber crime which we find in her own words when she described her issues on this regard:

"Except from my cousins and mom I didn't get anything from anyone let alone society...everything changed in my regular life I can't sleep ... I can't believe I curse myself and I lost trust feel ashamed I can't go to college thinking about it. Life is complete changed. I can't go back to being what I was before".

On the note of Psychological problems the victim claimed she is extremely depressed and insecure which is noted from her following response:

"I was completely depressed and tells on and still I am. I worry what will happen and how all will go away.....I don't feel I have security at all and don't even believe this will go even in future".

Except from Police and the Prosecution the victim didn't get any help from and other governmental or NGOs which she clearly said:

"Except for police and government lawyer I didn't get any extra support"

This case also introduces another situation of revenge pornography. The victim and offender is both students and in their early teenage. This case is in trail before the cyber tribunal. This case points out a burning issue of cyber crime which can affect any age group on attaining majority.

Case-4

Victim "D" is a 20 year old female who lives in a slum situated in Dhaka with her family of six. In faith she is a Hindu (Santan) preacher and she is uneducated. To support herself she used to work in a local garment factory. According to her own statement their whole family is poor where her mother works as house aid and her father sells vegetable. She doesn't have enough support for education or health. On this note the victim stated:

"We live in slums we have a lot of financial problem, I work in garments to support my family.... My brothers are small they can't earn... My mother is working in house as servant and my father works selling vegetables in van."

The Cyber victimization of "D" is as flows as she described-

"... how to say ... I feel extremely shy talking about this. I worked at garments not far away from my house. While working there I met a boy and he proposed me one day and said he wants to marry me. As we were supposed to be married he made physical contact with me several times and after some time he cheated on me when I confronted him he in revenge released recording of our intimate moment"

Victim herself didn't know what type of offense it was which we found in her dialogue as:

"I don't know what crime it is police did it all by themselves so after coming to court and talking to prosecutor sir I understood its cyber crime".

The victim "D" still faces social consequences and in past she faced more which can be concluded from her own narrative as:

"A lot of social problem I faced ... also I faced in family I couldn't show my face...."

According to victim she after the cyber crime incident is still being sexually and verbally harassed and facing social discrimination in finding job and everywhere and to that she commented:

"Unknown people would call me night and day and ask dirty things. People even bother my mother and father with calling names like sl*ts mom and dad..... I still am suffering because garment owners won't even give me job".

The Victim according to her faced no legal harassment of any sort but she didn't get any social support also w to which she stated:

```
"No I didn't ... But.... I didn't get any support from anyone.."
```

The victim's regular life dramatically changed and she still according to her suffers which we found in her answer as:

```
"My everything was and still is destroyed... I don't have work...I have nothing... My family suffers, they are ashamed and ashamed of me and so much more I can't even sav..."
```

The victim had immediate deep psychological effect and she tried to take her life, to that end she still suffers and feels insecure as she explained:

```
" ... I tried to hang myself but I instead took sleeping pills and was taken to medical after that everyone calmed down and said I am not guilty... my whole life is still insecure ... "
```

As state agent police and prosecution is helping her in her case and she didn't get any assistance from any NGOs:

```
"Police caught him that's the best facility for me .... I am happy at least for that...." No I didn't got any help from any NGO"
```

As a victim she is unaware of her rights and what kind of support she is entitled to because according to her:

```
"No I didn't get any facility so I don't know".
```

Despite being poor or belonging to a working class the victim here suffered the same consequences as earlier studied cases. This gives us the pen picture view of the class and status neutrality of the nature of cyber crime.

Case-5

In this case Victim "E" was a married women and she divorced her husband due to cheating which resulted in her being victim of cyber crime. She is a 32 year old female who lives now with her family consisting of four members where she is second daughter. She is educated to B.B.S. and she has no financial crisis. Her family is of Muslim belief and she got well support for health and education from her family. Before interviewing her although I expressly said all information will be kept secret and confidential she still was reluctant to give an interview. Then the prosecutor of cyber tribunal requested on my behalf then she agreed to give us a brief summary of her case. As she said:

"Please try to understand talking about this incident is painful to me and my family and I would prefer if I don't have to tell but since the prosecutor sir made a request and it's for a research I will briefly say about the incident".

Her case according to her narrative is precisely mentioned below-

"... I was married the accused of this case and it was fixed by my family... later months passed and I somehow in concrete found evidence that once he was married before and he still has many affairs. I am really a peaceful person I simply left his house and filed for a divorce explaining all to my family. When he got notice of divorce he did tried to convince me back but I didn't wanted to spend my life him... Then he circulated our intimate video in many platforms which I don't want to say".

The victim beliefs that there is progress in field of cyber crime in government's activity and according to her the state agents helped her. She has only regard for the process being lengthy as to this issue the victim said:

There is an Act called Digital Security so I think our government is doing progress..... prosecution and police are very helpful but the process is little lengthy and I do have to say case like this should be little bit handled with sensitivity.

Then on regard of governments awareness affecting the cyber crime she added:

"Of course it effects and I think it should improve more but I am not expert..."

The Victim blames herself more than lack of government's activity and to that end her conversation was brief as:

"I don't know actually... maybe it's just my naivety or stupidity not governments fault at all".

The victim has become a subject of gossip and is being harassed in sexual advances after the video of her was circulated along with that she is also alienated by the friends and on that note she described:

"...Firstly... I am having divorce and we all know how people think about divorcee...and then this video did circulated among my friends and neighborhood so I am having extreme problem because I know people are saying... they are judging. Most annoying is I am getting threats and slang advances from unknown numbers".

The victim didn't face any legal issues because her uncle was a lawyer but she claims of the court process being bad and bribery among the court staff and them siding with accused more as she explained:

"No for me legal issue was not problem...but trust me the court process is really bad and there is bribery among the court stuffs... They seem to side with accused because he bribes them..."

On note of her psychological issues the victim "E" is depressed, insomniac and she has symptoms of less self esteem which she explained:

"I am mostly divested psychologically because this left a scar permanent of the life and I will pay rest of my life I know that and there is no escape.... I am depressed ... I can't sleep... I often feel would my suffering if I died".

The victim is uncertain of her future and this incident left her regular life in complete turmoil as she narrates herself in following:

"Regular life definitely changed... Behavior in family changed..... I am anxious, nervous I blame myself stay locked in my 140 m.. I think my life is destroyed... Or it can never be as it used to be before... I don't know what can I or what to do next..."

The victim got all the support law provided her with but nothing special as being a women and got no support from any other Government or NGOs:

"I got all the government support which law provides me nothing special for the part of being women". And on note of NGOs "No.." was her answer.

The victim wished for social support which she claims she didn't got, she expected mental support and non-judgmental attitude towards the victims particularly her as she exclaimed:

"I don't know how to answer... maybe a little support from society.. non judgmental attitude would help".

This case can be identified as classic example of revenge pornography by former partner. This is also a form of partner abuse completely driven by the motive of revenge and defimation. The case is in cyber tribunal pending to be tired.

6.2 Presentation of Cases of Support Agents

These cases which were collected from advocates and support agencies don't describe any particular cases rather they are taken to solidify the claims of victims and to understand the nature and impact of cyber crime. As these persons regularly handle victims they have an expert views of present trends and situation and they supposed to shed light on things which remains untold or which has been missed. The main reason for studying case of expert is to ascertain their valuable insight to draw a casual conclusion and to develop recommendations and plan on how to combat and prevent cyber crime.

Case-1

"X" is a 50 year old male who works for prosecution in Cyber Tribunal Bangladesh. He is a veteran lawyer in this line of work and deals regularly with many victims of cyber crime directly. His interview statements on different aspects are as follows-

Regarding government's awareness level regarding the issues of cyber crimes and women victimization he said that government that government is over all not only exclusive to women is aware of the issue, he describes:

"Not particularly regarding women but overall the government is really aware about cyber crime issue regarding making and implem [43] ing laws. Thanks to government there are tribunal and specific laws for cyber crime. The trail process of cyber offense is very fast. Over [47] the awareness level is very satisfactory. First there was the Information Communication Technology Act, 2006 then the government enacted Digital Security Act, 2018 and from there on government has to with the object digital Bangladesh been working and till now with forming partnership with different NGO's ran in 247 schools cyber awareness program. At the same time Government is running promotional broadcast in television channels and radio for that reason almost majority of people is aware of this law."

He also explained how laws protect citizens in general and against heinous crimes of morphing the advocate also made remarks on the procedure of cases which are cognizable and which are not to which he stated:

"This also covers Morphing of pictures and attacking on ones religion. At present the definition of defamation given in Digital Security Act, 2018 is the same as sections 499 of the Penal Code but occurring in cyber space. Because this section 25 and 26 of the Act is non-cognizable that's why the case must be filed as petition case in cyber tribunal or in Thana only as GD and after investigation of GD with the permission of the Tribunal."

On the note of if there is any specific provision in law that exclusively protects women he said, there is not and provided a picture how women are more victims of cyber crime as she states:

"No in new Digital Security Act, 2018 there is no specific provision for women. But Harassment to women is very easy in online so it's noted that the cases involve more than women than male in case of cyber defamation. There is sexual harassment online for women, online blackmails, and pornography. In the tribunal almost 45% of cases the victim is women".

For further awareness raising activity in this issue of cyber crime present awareness of government is according "X" is enough and women need to be self-aware to which he said-

"The present awareness of government is act 74 ling to me is enough in terms of legal issues. But women themselves need to be aware of their rights and responsibilities in cyber space. They should do this for their own protection".

On asking if the government is negligent or lack of awareness or in structure affecting your activities to deal with cyber crimes and women victimizations cases "X" Said:

"No government is not negligent in this regard they are doing their best and implementing laws which is needed and required, so the people should do everything to upheld and follow the law...... the lack of structure in government is that there is only one tribunal in Bangladesh and there are few police only CID of the police who has a forensic lab and are equipped with investigation of these cases."

Respondent "X" identified two main legal problems faced by a victim of cyber crime are:

"The main legal problem is that some of the sections of the law is non-cognizable so they can't file cases in conventional way. People not filing cases in fear of hassle are also another legal problem".

On the issue of cyber crimes that occur specifically to women and their social problems X stated:

"In Bangladesh the main cyber crimes in my experience which occur only to women are morphing, hacking of ID, Pornography for revenge, Cyber Defamation, harassment bullying and Cyber fraud. While most are the cases of defamation and revenge porn are major among these all. The social problem faced by women is social stigmatization, alienation and pressure from their family on not filing any case."

According to "X" he and the judge present at the Cyber tribunal both had formal training to develop specialized knowledge on how to prosecute and try these sorts of cases by government:

"Yes I along with the honorable judge of cyber tribunal have undergone training from government from U.S.A".

"X" although dealing with Cyber crime Vitim on regular basis had no concrete idea of the victim's psychological issues but he did affirmed that there have been several cases of suicide relating to cyber crime occurrence to which he said:

"We don't get to interact with victims much outside of court so it will be difficult to answer but still in my experience I have seen them depressed, low in self confidence, anxious and suicidal in few cases and there have been many cases of suicide related to cyber offense".

In regards to cyber crime issue affecting the women victims' more than male victim "X" said:

"Yes cyber crimes tend to affect more women than male because it's easy to ruin the honor and modesty of women more than males."

"X" suggested the kind of initiatives that can be more fruitful to women victims of cyber crime and their whole betterment as follows:

"Women themselves need to be ware of them not to share sensitive pictures, videos and information on vast internet and even to their intimate partners. We all should be respecting laws and governments policies at the same time we should respect ourselves as human being. For overall betterment I would like to suggest that women be aware of their modesty and what they share in Facebook and other social media on what they share and how much they share And more specialists and knowledge should be developed in this sector as world is now more dependent on online transactions."

After careful consideration of the various aspect of the respondent's narrative various aspects which needed to be shed light into came to clarity. Various important and crucial aspects and concepts were discussed in this case which was useful and valuable to this research.

Case-2

"Y" is a 30 year old male who works at Cyber Crime Awareness Center, a NGO which is dedicated to work with the social dilemma of cyber crime. It is situated in Dhaka. They have conducted research work before on overall cyber crime situation in Bangladesh. On the selected research of mine he gave interview on various aspects of that are presented bellow-

Regarding government's awareness level on the issues of cyber crimes and women victimization "Y" believes government to be very negligent. He added that the government awareness raising and promotional activates are not up to the mark to which his comment:

"Cybercrime and women victimization these are two separate separate issues first of all I would like to say the government is really negligent in issue of Cyber crime there are laws which should protect everyone in internet but sad reality is that it's so inefficient in the issue women in this regard who are most vulnerable in internet. The government has no special provisions of law or no special awareness raising programs regarding women specific".

On Suggesting to me the type of awareness the government needs to deal with cyber crimes and women victimizations cases "Y" said:

"Situation knowledge based special program should be adopted in dealing with the issue of cyber crime which happens in internet or in platform which is not a real but this occurrence can be controlled because every crime arises from human action so it is possible control human action. At the same time primary and secondary education should include how to protect oneself in cyber space and these should be primary factors in controlling the crime of this nature".

On the issue of lack in governmental structure affecting activities to deal with cyber crimes and women victimizations and According to "Y"s opinion the victim suffer for government's negligence cases he stated:

"The lack of government in structural efficiency is another issue on its own after the law of digital security passed only one Tribunal which is situated in Dhaka was established and people from whole country have to travel to Dhaka just to file complains and cases in this regard. With one Tribunal in my opinion it is impossible to ensure justice or do any significant change in present situation. Normal police don't have the knowledge or skill to deal with situations of cybercrime so they cannot entertain the cases local Thana."

According to "Y" as the process and without availability of conventional means the victims face legal problems also:

"The main legal problems faced by women are firstly normal process of cases don't apply to the situation of cyber crime in Bangladesh and police in local Thana don't in most cases take immediate action. There are limited scopes of legal aid in this situation so all the expenses are usually born by victim which makes it difficult in sustaining the case in long run".

According to him the following types of cyber crime are prevalent in cases specifically to women:

"In my experience I have seen women specifically being victim of revenge porn, picture morphing and cyber harassment and online fraud mostly. In school, college and university level we see there are online trolling, bullying, harassment and deflation happening more".

"Y" claims he on his own intent he went through official training to provide the victims assistance:

Yes I have under gone specialized programs before I involve 119 yself in this line of awareness and assistance organization. If I myself don't have special knowledge I don't think I will be of any use in this line of work".

"Y" affirmed that there is no law that deals with the social problems of victims which arise after cyber crime is taken place and he added that the victims face deep psychological traumas which is similar to victims of sexual assault and offense that renders affect and extend to victims regular life:

"No there is no special law in dealing with social problems of women in cyber crime related issue. In Bangladesh the social problems are never addressed by any laws in the first place. After a crime takes place the life circle of victim changes drastically. They are more afraid to trust people and it takes almost years to again re-integrate them in society".

According to "Y" on gender ratio women suffer more cyber violence then males to which he quotes a statistic from the research which his organization conducted:

"In our last study in 2018 we found that almost 52% of the victims of cyber crime are women so this number does undoubtedly show a clear picture of the gender specific occurrence."

"Y" voices his opinion that NGOs can play any role to help the women victims of cyber crime to which he explains:

"The NGOs in this sector can play a huge role in awareness raising, promoting measures and prevention of crime through victim hardening. First of all specialized NGOs can play a vital role in policy making. In Bangladesh there are a lot of NGOs who are oriented to women's right these NGOs can provide victim handling, counseling, reintegration, support and legal assistance to destitute women who are victims of cyber crime".

In the end for betterment of women and improving their situation "Y"s recommendation were:

"Women themselves are responsible to most degree to keep them safe in this regard. They should defiantly be aware of what they share and how much control they give 34 themselves to others in cyber space. For overall betterment of this situation I would personally like to posit that the cyber space is vast more diverse and vast than the whole Bangladesh so for any country not only Bangladesh it's impossible to regulate for everyone on what happens and to provide security to all. People need to be self aware and especially women need to be aware of incoming dangers lurking in the web. Law enforcing agencies should be more efficient in their line of work to provide speedy remedies to victims and government should deal with this situation with experts of this field so they have better control of this situation".

The respondent pointed out in his narrative various deformations on existing system which aided in identification and analysis of various crucial concerns.

Case-3

"Z" is a 36 year old female advocate who works in Bangladesh National Woman Lawyers' Association. On the issue of cyber crime against women she said her organization dealt only few in comparison to other criminal cases but in her experience she gave the following responses to different aspects of cyber crime against women-

In regard to governments awareness on the issue of women cyber victimization "Z" said:

"I should say the public authority is really thoughtless in issue of Cyber crime ...terrible in all actuality it's so inefficient in the issue women in such way and the public authority has no remarkable plans of law or no uncommon care raising ventures as for women".

On account of any specific provision that protects or provides remedy to women in Digital security act her response was:

"There a 54 laws which safeguards individual from computerized crime these laws are the Digital Security Act 2018 and Pornography Prohibition Act 2012 and as said under the watchful eye, it's a general law and isn't for protective for women".

She also things the governments negligent or less awareness is accelerating the women cyber victimization and to that extent she claims:

"The government in my view is truly careless about specialized issue like cyber crime. As a researcher even you feel... One or two laws can provide insurance to the stakeholders? They require legitimate advancement in certain social issues which needs to be diminished essentially".

In lack of governmental facility she pointed that co-ordination between public- private sector is a hindrance to solving the situation to a better one and also people's personal conduct is equally responsible, so her views are:

"We large 115 iled to tackle cyber crime effectively, by not having the option to build up multidimensional public-private coordinated efforts between law enforcement agencies, the data innovation industry, data security associations and internet companies."

"Z" Posited that due to Governments negligence the victims suffer economically, psychologically and legally to that end she quotes:

"Yes.. surely they do suffer with finance and significantly psychologically through the who process"

"Z" also explained that they have limited interaction with victims out of work but those victims coming to them tell them their own suffering:

"We have little interaction out of our work with clients or victims so I am not sure... but they do tell that they have many social problems like stigmatization and blames..."

"Z" told that she didn't have any special training and the scope of the training in Bangladesh is low:

"I am afraid I didn't get any... and the scope of learning in this regard is really small".

While working with her few clients "Z" Described them to have the following psychological challenges:

"I gave few of my clients counseling too and among them I noticed heavy self blame... guilt, shame ... depression which is most common and in some suicidal tendencies".

"Z" like previous interviewees also said women are more victims to cyber crime then males are as to that she quoted:

"Yes.. as far as I know to best of my experience... I have seen very few males filing for cyber crime when I go to tribunal myself...."

She thinks both the government and NGOs role in this matter is not sufficient and there is a lot of room to expand to which she described:

"No... I think more awareness is needed than more laws" And "these things are really technical so majority of NGOs seem to only be focused on what they are used to deal with till now... we do what we can... "

Providing her suggestion about the appropriate implementation of laws pertaining to women victims of cyber crime she said:

"I don't consider implementation of laws just will make the circumstance of women in such manner any better. There is hypothesis of prevention yet that goes up until this point. Beside this in my perspective two things should be possible initially existing laws ought to be all the more clear and direct to which individuals can discover solution for. Also, besides the laws ought to give some level of additional assurance to women in view of them being more sufferers in this matter."

"Z" recommended for the overall betterment of the situation of women victims of cyber crime the following:

"Women should keep an eye out for insignificant/fake telephone/email messages. They should not react to email messages that request individual data. They should be mindful of false Websites used to take individual data also; women should pay regard for protection strategies on Websites and in programming, Guard email address and consistently use strong passwords. They defiantly should not share personal things like topless photographs or something to that effect even with their spouses".

At the end of this section it tends to be said that case study is a method for finding the obscure things into notable limits. In my study, it has been documented the history of the cyber crime which the victims faced and then a comprehensive expert opinion were drawn from the advocates who are dealing with the crime of this sort with their oral description. With that all it can very well be said that this chapter has covered all the concerning subjects and objectives of my study. As a researcher it has enabled me to examine data of specific respondents and finally to draw finds in following chapter.

CHAPTER 7 FINDINGS AND ANALYSIS

Demographic information suggests that there is a rapid increase with daily basis in online usage and activity. Recent pandemic and rapid digitalization has made the people more dependent on internet based activity and with that there is an alarming raise in cyber crime. But in actuality women are most significant victims of cyber crime for many reasons. Cyber crime is not only a national but also a global challenge as well. Gradually, this issue has become prominent and affective measures must be taken to control activities in cyber space. This chapter is the total presentation of my research findings and analysis of data of my study.

7.1 Findings and Analysis

I have collected from my 5 cases who are women victims of cyber crime they are categorized with letters A, B, C, D, E and 3 cases of advocates or support agents categorized as X, Y, Z, who are working with this issue through Semi-structured interview.

The schedule of interview followed Semi-structured guide and style which enabled me to covered themes of respondent about their life style, thinking, sufferings, experiences and perspectives. It also helped me to get adequate answer to complex questions and finding most effective analysis of these different aspects. I have presented here on sections along all the findings which came through my study.

7.2 Socio-Economic and Demographic Condition of Victims

The socio-economic and demographic section provides an ample view of the social condition and economic status of victims. It enables the researcher to know if the respondents have adequate education, social and economic support. Demographics show us the age range and the ratio of gender based violence. For any social research it is a mandatory condition to have a background history of the victims and agents as well, which has been studied as case. In terms of women being more popular target for cyber offenders Respondent "X" said-

"Women are more likely to be harassed in cyber space because they trust people easily, and they are easy targets for offenders because they can easily be blackmailed, and they often remain silent for the sake of their honor".

Respondent "Y" also agrees in this case as according to him our social norms and practices allow the victims to be blamed and after any of these sorts of crime victims are the one who lose their social standing and support, on this note he stated:

"Of course women and teenagers are the biggest target of gain for the offenders due to its mostly seen they are careless about their cyber protection, they if someone blackmails them try to compel them; they become submissive and it's highly due to our social structure".

We have on the course of our study found that victims are majorly belonging from good economically sustained families. Also religion or caste doesn't effect in victimization. When interviewed Victim "A" said:

"Yes I belong form a family which has good social reputation, and from my childhood I never had to suffer economically in any regard. I am Muslim by faith"

Victim "B" agreed to this matter and she thinks offenders mostly target women who have good socio-economic condition. She said:

"My husband works for government, we have respected and we are stable economically and for that reason I think I was targeted for this heinous act".

But we when interviewed Victim "D" found that she are a poor garments worker and she is of Hindu Religion. She believes that cyber crime can take place anywhere to any one despite their socio-economic condition. It can sometimes be pure revenge driven.

"I have no money... and the offender gains nothing from the offense except for being in power and control of my life... I don't think people's social or economic status matters. Cyber crime is often revenge motivated simple."

Analysis of the Socio-Economic and Demographic Condition of Victims

Socio-economic and demographic information of a study of this nature is vital in gaining the insight to the life of the victims and certain factors of related to such affects the main outline of the research. This is one of the objectives of my research and to sum it up after studying all the cases, listening from experts from this fields and from the different narratives of victims

themselves I conclude that cyber criminals actually do target the population of women more than their counterpart. At the same time although Some of the nature of cyber crime can be often be driven by economic gain or targeting women who belong from family of good social standing but it is also matter of fact that most cyber crime are sometimes driven purely from the hatred and revenge from offenders perspective. So in that sense I deduce that cyber crime actually is a crime which cannot be defined or confined within the dimensions of socio-economic status, rather it is a crime which is neutral in nature but also gender specific.

7.3 Social Standing is Not Crucial Aspect of Victimization

On the issue of social standing I like to posit the criteria on which it is measured. For finding the social standing of the victims I took into consideration their family background and education/Job to reach a conclusion. I let the victims describe their social position and to which Victims A, B, C and E claimed to be from families who have good standing on society. All of them were educated from minimum H.S.C to highest MS. They had enough support from their family on health and other issues. As for profession most of them were students others where housewives. According to Victim "C":

"I am a Student and since my childhood I never seen our family to suffer economically. We are respective Muslim family in our locality."

Victim E also said that both their father and in-laws where from good family standing in their perspective society. But she can't believe that her educated Husband would do something like this to her. According to Victim "E"

"Both my family and his they are equally respective in their own regards, we had no shortage of anything... I really can't believe despite having everything in life my ex-husband did this to me".

However Victim "D" claimed to be very poor and lived in slum, she only had primary education till class 5 and is a garment worker. According to Victim "D":

"We live in slums we have a lot of financial problem, I work in garments to support my family.... My brothers are small they can't earn.. My mother is working in house as servant and my father works selling vegetables in van. ..."

From this we can also conclude one thing that cyber crime is not class specific or it's not like the offenders only target the victims with well social standing.

The respondents X, Y, and Z all are perspective professionals who are well informed about cyber crime and has a history of dealing cases relating to cyber crime victims. Of them two are advocates and one is NGO employee. They too agreed to the claim that in case of cyber crime victims' personal background is neither a factor nor offenders background.

Analysis of the Social Standing is Not Crucial Aspect of Victimization

For the sake of neutrality and also reliability I conducted study of victimization of both people of well social standing and those who belong to by existing norms as lower class as well and to have a neutral effect to the outcome that cyber crime is not exclusively a social class driven crime. I found that cyber crime in majority of cases is completely passion and revenge driven offense to affect the women in most if not all cases. Even the nature of this crime in this manner is accepted by and arrived by respondents "X" has he said that majority of cyber crime cases in court are completely revenge driven.

7.4 Economic Condition is Also Not a Crucial Factor for Cyber Victimization

On findings relating to the economic condition we uncovered all the victims except from Victim "D" had good economic support and capability. Victims A, B, C, and E can through spouse or family support their basic needs according to their own description. According to victim "A":

"I had good support economically from my family and also from the private tuitions which I would do".

In agreeing to this Victim "B" also said that her husband works as government officer and they have well of standing in society and she claims that he victimization happen because of economically driven situation to which she exclaimed:

"I think since my Husband works as government employee the offenders thinking we have good finances targeted us."

But on courser of research we found Victim "D" and she is extremely poor but despite that she still was porn to being a cyber crime victim. On explaining economic condition Victim "D" said:

"We have a lot of financial problem, I work in garments to support my family...we don't have enough to support education... with my earning trying to educate one of my two brothers..... I didn't have a smart phone even..."

But despite the fact of good economic condition and to worse cyber crime did take place in life of all victims. So we can also deduce that cyber crime is not always economically motivated crime.

Analysis of Economic Condition is Also Not a Crucial Factor for Cyber Victimization

Offence and economic condition are two paradigms that are always looked and researched into together. In my case I tend to find a link between the economic condition and women cyber victimization the result came into from victim testimony as cyber crime is a crime of passion and mostly conducted on emotional grounds than gaining financial advantage. The result indicated around 80% of victims who belong to family and status of good economy were victimized but also the 20% who are poor and don't even have means to support their family were also victimized which tends to revel the economic un-biasness of this offense.

7.5 Offender Target Women who are Adults in Age Range

The age range is a crucial finding in my research as conducting interviews and from victim testimony it came out that cyber offenders target teenagers and mature women more. As it stands from Victims A to Victim E the minimum age was 19 year old maximum 36. So it can be determined that the victim age range is roughly around 18-40 years old. On this note respondent "X" who has most experience in dealing with cyber crime said:

"The accused or offenders target women who are mature, due to causes like revenge when they have relationship with them and victims marry someone else".

In affirming to "X" respondent "Y" also came to same conclusion that cyber criminals actually target mature women who has face to lose in society and whom they can compel to have sexual favors. According to "Y":

"Cyber offenders target mature women from whom they can easily gain control and favors more through blackmail and other means".

From this statement we can also deduce cyber crime is motivated most often by revenge.

Analysis of Offender Target Women who are Adults in Age Range

The present study concluded into the finding that 100% of the women who are victims of cyber crime are indeed mature women. As earlier established cyber crime in Bangladesh hence in generalization in whole world in circumstance of women are majorly driven from gaining control and power over them and in sense of refusal the sensitive contents are leaked to defame the target or victim. The offender in this manner heavily target women who have some status to loose and they are mature to have sexual and other gain from them. So after thorough analysis I came to conclusion that the majority of women who are victims of cyber crime are mature women whose age range from 18-40 years in life span.

7.6 In Gender Ratio of Victimization Women are More Victims of Cyber Crime

Gender ratio is among the most important reason and objective of my study. Gender ratio is a ratio that indicates of certain phenomenon to be happening over gender based. In simpler term whether cyber victimization takes place more to Females or males in our society at present. To this Respondent "X" Stated:

"Harassment to women is very easy in online so it's noted that the cases involve more than women than male in case of cyber defamation. There is sexual harassment online for women, online blackmails, and pornography. In the tribunal almost 45% of cases the victim is women".

And Respondent agreed to statement of "X" and on this regard "Y" said:

"In our last study in 2018 we found that almost 52% of the victims of cyber crime are women so this number does undoubtedly show a clear picture of the gender specific occurrence".

So from the above clear and statistical statement from Respondents "X" and "Y" it can undoubtedly be said that women are more victimized in case of cyber crime then males.

Analysis of in Gender Ratio of Victimization Women are More Victims of Cyber Crime

The Gender ratio of victimization of any criminal activity indicates the gender dependent variable of a particular offense being conducted. To that end the present study tried to gain insight on the notion whether the women are more prone to cyber victimization or not. From this query I conducted interviews to the support agents and all of them where distinctively clear on their stand from their personal and professional experience that women are most vulnerable to be a victim of cyber crime then their counterpart. As modesty of women in Bangladesh is easy to condemn the victims are mostly women in terms of cyber crime. These findings give me a crucial aspect to present under my present objectives.

7.7 Government's Awareness is not Adequate to Reduce Cyber Crime

On the issue of Governments present awareness I asked question to all of my respondents. There is wide range of responses from various respondents. The gist of the responses is that government presently is aware of cyber crime issue and they have enforced laws for sanction the offenders but according to victims and advocates this is not enough. Another aspect which came out of inquiry about this issue is that the laws which are introduced by government are the Digital Security Act, 2018 and Pornography Control Act, 2012. But in none of those Acts has any specific provision for women. On this regard-

According to Victim "A":

"About my victimization or women victimization government, I think doesn't have any particular policy or law separate like Women and children repression Act which makes it difficult in access to justice"

According to Victim "B" Government is very aware of the situation although the situation according to her it can improve:

"I am sorry I don't know about laws that much. But I think the initiative of government is good but it can always be better."

But the most practical description came from Respondent "Y" who said:

"Cybercrime and women victimization these are two separate separate issues first of all I would like to say the government is really negligent in issue of Cyber crime there are laws which should protect everyone in in internet but sad reality is that it's so inefficient in the issue women in this regard who are most vulnerable in internet. The government has no special provisions of law or no special awareness raising programs regarding women specific".

This was also corroborated by Respondent "Z" who stated:

"The public authority has no remarkable plans of law or no uncommon care raising ventures as for women unequivocal".

Analysis of Government's Awareness is not Adequate to Reduce Cyber Crime

The present finding revealed that the government of Bangladesh is actually not unaware of the issue of cyber crime they are very well informed and to meet both ends numerous laws with sanction have been passed but despite that the activity of the government according to our respondents is not up to the par and there is still a lot more ways to go for governmental activity to reduce cyber crime or completely or effectively prevent it. The study outcome into the finding of government need to address the issues regarding cyber crime from expert hands on approach.

7.7 Process of Filing Case is Unconventional and Difficult

Most of the Victims found the filing of the case under Digital Security Act, 2018 or for cyber crime to be full of hasselious process. Victims said the case filing is completely different and also difficult. And with affirming victims claims support agents also described the process to be unconventional and difficult. The statement of Victim "A" is as she narrated her experience:

"One of the officers said they don't have power to take on this case. Some said to contact a higher up connection if I had any among my friends or family and through them I should contact CID of police to have some visible action taken against the offender".

Most of the Victims said similar things so to ascertain that fact we also asked respondents X, Y, Z, and all of them to confirm that it's a challenge due to process of law and due diligence. To this Respondent X said:

"The main legal problem is that some of the sections of the law are non-cognizable so they can't file cases in conventional way".

Analysis of Process of Filing Case is Unconventional and Difficult

After careful consideration of all responses of respondents I was able to deduce and conclude that the nature of cyber crime is in itself different than other criminal activity and to which special laws were enacted and under this special law only cyber tribunal and CID of police had power to make cases and issue warrants. This curtailed the victim's right to make cases into local Police stations and made the whole process troublesome and difficult for majority of sufferers. When a offense takes place its better if the victim or the effected party can go to police and ask for immediate help which is not the case for cyber crime victims and this an major outcome of this study.

7.8 Victims Face Legal Harassment from Filing Cases to Trail

The victims especially women facing cyber crime they have to also face different legal harassment from process till end of a case by closing judgment. Firstly the process is difficult to start as we found earlier. Then there is only one tribunal in whole Bangladesh so people from all over the country have to come to Dhaka to file a Case in tribunal. This process involves money, time and mental stability which often victims don't posses. The government might support criminal cases for free but these factors harass the victims and their family further. The exclamation of Victim "A" gives us a picture of suffering and pressure of the nature of legal harassment as:

"I would like to tell that there is no legal assistance in Bangladesh rather there is legal harassment. After the incident I along with some of my friends did go to police they refused to lodge any case and rather asked me to file a GD so they can see what they can do."

According to respondent "Y" even the scope of investigation is limited as there is only one Digital Forensic lab in whole Bangladesh which also adds to victims' legal suffering. To which he said:

"The main legal problems faced by women are firstly normal process of cases don't apply to the situation of cyber crime in Bangladesh and police in local Thana don't in most cases take immediate action. The case needs to be filed in Cyber Crimes Tribunal and it is only one in capital so people come around from whole the country just to file their complaints. Secondly only CID of police branch has the digital lab and means of investigation of cyber crime".

Analysis of Victims Face Legal Harassment from Filing Cases to Trail

In Bangladesh in many previous studies and reviewed articles I had this assumption that there is a delay in process of legal suits and cases and to find out if there is any delay in cyber crime cases I throw questions to all the victims and the support agents and to that the outcome came as the victims around 60% faced legal harassment by police or by process itself. This notion was further elaborated and affirmed by Respondent "X" "Y" and "Z" who from their professional stand point and legal expertise admitted that yes the process of filing cases tend to harass the victims. I found that due to this reason many cases go without being reported also.

7.9 The Process of Trail Is Lengthy in Cyber Crime Cases

Almost every victim respondent and support agents admitted to the trail process being lengthy and said it takes quite some time to get any cases closure whether justice is served or not from victims perspective. Some of the respondents are waiting almost a year just so they can start witness testimony. Due to thinking about these lengthy processes of time many victims refrain from even complaining and their cases go unreported. To affirm this claim I mentioned two statements from respondents "X" and "Z".

According to Respondent "X":

"Although after file of a case we try our best to give speedy remedy to the victims but sometimes delay is caused in investigation and witness testimony. People not filing cases in fear of hassle are also another legal problem".

And according to Respondent "Z":

"Just because of one tribunal and one Forensic lab actually the scope of investigation is limited and delays the process of courts in a length, as in many cases the police report are given after one or more year of time depending on the nature of offense. There are limited scopes of legal aid in this situation so all the expenses are usually born by victim which makes it difficult in sustaining the case in long run".

While I was interviewing the victims I noticed their frustration and unease about this particular issue.

Analysis of the Process of Trail Is Lengthy in Cyber Crime Cases

The Respondent "X" who is a prosecutor and Respondent "Z" who provides legal assistance to the victims both accepted that the process of cyber crime to dissolve takes a huge span of time. The obvious reason for this is lack of investigative personnel, delay in trail, delay in witness summoning and delay in investigative reports. I while conducting my interviews observed that this has built a frustration and tension within the victims. The victims psyche is affected directly from this aspect and finding. The women who are wronged actually seek some sort of solace and comfort when the offender is brought under justice but delay in that actually discourages and diverts their attention to seek justice.

7.10 Relatively Inadequate Investigative Personnel for Speedy Investigation

For investigation and investigative purpose only the cyber wing of CID police with their training and equipment can investigate Cyber crime in Bangladesh. And they all have limited personal to make a speedy and effective investigation as the cyber crime is a crime committed in cyber space its most frequent than any crime and to even occur it just may take less than a minute. So lack of personnel is a problem which the victims ultimately suffer from. To this Respondent "Z" relates:

"If a victim comes to us we either direct them to cyber wing of CID or we ask them to file a CR case from our agency if they want. In cases of CID although I think they are really performing well but they eventually run out of investigative officers to give a swift investigation report". The claim of "Z" that lack of investigative personnel is accepted and affirmed by Respondent "X" who works for the prosecution and on that note the effect is described by him as:

"One tribunal in Bangladesh and there are few police only CID of the police who has a forensic lab and are equipped with investigation of these cases. Often it makes difficulty in process and investigation and also for being only one tribunal people have to come from out of Dhaka to file cases here".

Analysis of Relatively Inadequate Investigative Personnel for Speedy Investigation

Any investigative works efficiency and speed depends on the number of investigating personnel. The abundant the available investigators are the more speedy and efficient the investigation will be. Cyber crime is a crime which involves special knowledge while investigation of any crime of this nature. Though my study from various victims account and agents account I found that only the CIDs cyber wing conducts the investigation of cyber crime through whole Bangladesh. This wing only consists of few investigators and thus it is creating far reaching negative consequences in ensuring justice.

7.11 Victims Privacy is not Protected

Every victim respondent themselves said that they felt unease to explain, share or show sensitive content to a male police personnel, a male judge and a male prosecution. Some exclaim that the thought of these videos, pictures will be seen again as evidence by other males makes them nervous, anxious and very shamed. We find this theme common among all the respondent victims' statements to this "A" one of my respondents said:

"I felt uneasy sharing everything and from thinking even police and other man will see those pictures".

In affirmation of this victim "C" also was buzzard by the fact of male investigative personnel, male prosecution and Judge will go through her sensitive content. She said on this note:

"I felt uncomfortable coming to court and in front of people who went through those."

Victim "E" also agreed that the thought of anyone watching those contents even if for the purpose of investigation bothers her heavily and to that end she described her feelings as:

"I felt the offence being repeating as I went along trail and process thinking the whole thing will be seen and viewed by others".

Analysis of Victims Privacy is Not Protected

The privacy in regards to explicit and sensitive content of women should be addressed with utmost caution and care. In most cases I found that the victims claim that they felt uneasy to narrate and thinking the male investigative personnel, prosecutor and judge will go through those to view it as evidence. To them it was same as repeating the offense itself and these finding needs to addressed immediately to ease further discomfort to the victims.

7.12 Particular Provisions for Women's Protection in Law is Unheeded

Regarding if there is any special provision of law in the new Act or law particularly dedicated to women we actually enquired respondents "X" "Y" and "Z" and all of them affirmed there is no special provision of law under both Digital Security Act, 2018 and Pornography Prohibition Act, 2012 specially for women victims neither in process or in penalty. To this Respondent "Y" sated:

"There are laws which protects individual from cyber crime these laws are the Digital Security Act 2018 and Pornography Prohibition Act 2012 and as said before it's a general law and is not for exclusive for women".

"Z" also made the same conclusion as she said about this provision and laws in following:

"There a 54 laws which safeguards individual from computerized crime these laws are the Digital Security Act 2018 and Pornography Prohibition Act 2012 and as said under the watchful eye of it's a general law and isn't for protection only for women. There are general arrangements of laws, who is entitled under the sections can get remedies."

Analysis of Particular Provisions for Women's Protection in Law is Unheeded

I came to conclusion of this finding on account of respondent "X", "Y" and "Z"s response to my direct question in this regard and then i myself went through the Digital security Act to

find out and detriment the truth of this claim and the claims where affirmed to be true in this regard as there is no particular provision in the cyber law that exclusively deals with women cyber crime issue. The law is general and deals with certain cyber crime for all who can claim remedy under it.

7.13 Court Staffs are Involved in Corruption

Lastly some of the victims on note of assuring privacy alleged that there is a tradition of bribery among the stuff of court and she also claimed its offender sided. The respondent "E" said:

"Trust me the court process is really bad and there is bribery among the court stuffs.. They seem to side with accused because he bribes them".

Victim "D" Also made exact same claim in broader sense though as she said:

"Court and Justice in Bangladesh side with person who has money in my case the offender as he has money to throw around"

Analysis of Court Staffs are involved in corruption

Among the victims who I interviewed around 40% bluntly claimed that the staff of court are involved in various corruption activities like bribery and taking money from the offenders to give them necessary information. This causes frailty and defect in the justice system which promises to ensure justice to anyone who is entitled under it despite their status and race.

7.14 Victims are Socially Discriminated, Distanced and Alienated

Majority of my study victims faced social distancing and isolation from society into some bizarre group. Some of the respondents in fear of this happening even took precautions so no one in her social group finds out about the crime actually happening. According to victim respondents the social structure of Bangladesh provides for this kind of behavior and its not the offenders rather victims' are the one who are afraid to come through and ask for help. In support of this argument Respondent "D" said:

"A lot of social problem I faced... I faced in family I couldn't show my face.... Unknown people would call me night and day and ask dirty things. People even bother my mother and father with calling bad names about me".

Victim "C" also said the same when she described her account of experience:

"Yes I was alienated within my class within my society and everyone would label me as some sinner or untouchable object not even as a person."

Respondent E said of her suffering in the flowing lines:

"I am Judged and then again judged and then I am isolated from people everyone thinks to be normal".

The attitude of victims' society alienating and distancing is also accepted and mentioned by the experts in this fields. All the support agents who I interviewed them all agreed that victims face heavy isolation as she is herself a disease.

Analysis of Victims are socially Discriminated, Distanced and Alienated

Social discrimination is characterized as sustained inequality between individuals on the basis of illness, disability, religion, sexual orientation, or some other proportions of variety. In the cases the discrimination is faced by the victims and on the basis of them being cyber victimized. They were isolated and alienated as they themselves are the wrongdoer. These themes of social problem I find to be exact from each respondent and Respondent "D" was selected as representation from them. Every single case study victims said they have been discriminated, called with bad name at and lastly their family or supports even suffered from social backlash.

7.15 Victims are Blamed, stigmatized and Receive no Supported from the Society

Along with being discriminated socially we found in our investigation that victim blame is another theme which all the victim respondents share in common in every single case. Victim blame is not actually a new theme it occurs within society continuously no matter the subject matter is when there is a crime the people in our society educated or uneducated always blame the victim for their victimization and this finding is outcome of many earlier studies in crime science and social science.

The best description of Victim blame with common voice among the Respondents came from Respondent "C" as she said:

"yes..I was blamed in many ways..in school..among relives, my classmates and in neighborhood to whoever who heard or seen that video. They think sin is mine

Social stigma is the term given when a person's social, physical or mental condition influences other people's views of them or their behavior towards them. The respondents of my study claimed that they were socially stigmatized and it had consequences on their job, even on their family and reputation for future. According to Respondent "D":

"Unknown people would call me night and day and ask dirty things. People even bother my mother and father with calling bad names. I still am suffering because garment owners won't even give me job... and supervisors of garments would ask me to do same for them and they will give me work..."

Analysis of Victims are Blamed, stigmatized and receive no Supported from the Society

The victims in their interview astonishingly all of them said that they are blamed for their own victimization. They are blamed by their families and peers they are stigmatized by any person who knows about the incident. Some of the victims faced backlash from their family and relatives. They are ridiculed and their neighbors gossiped and stigmatized their life further. In the end all of the victims agreed to one notion that they received zero help from the society rather they faced further pressure of judgmental attitude. Some victims where alienated in family. This finding gave me the precise description about the social aftermath of attitude towards victims.

7.16 All the Victims of Cyber Crime Suffer From Depression

Depression or major depressive disorder is most common but serious medical illness that negatively affects how a person feels, the way they think and how they act. Among the major findings of psychiatrical condition of respondents who are victims of cyber crime I noted that all of them claimed that they are completely depressed about their life and surroundings. Some of the respondents shout even professional help but while some try to cope up with it. Depression is most common outcome in our finding for our study while I gathered data among the respondents.

The depth can be understood from Respondent "A" statement as she state that:

"I will answer this in short I was depressed, nervous, anxious, humiliated and worst suicidal. I wanted to end my life so ral occasions but I had some same age people looking for me so I survived. I really don't want to talk about those nightmares".

Respondent "B" said that she too was depressed and worried about what happens next, to which she said:

"I was complexly depressed and worried about how to make everything as it was. I felt stupid and I wanted my suffering to end, hoping time will go back."

Victim "C" was depressed enough that she needed psychological aid from professional and it affected her education, to which she described:

"Depression got me so much that I received medical aid and i could not study for more than 5 months."

Analysis of All the Victims of Cyber Crime Suffer From Depression

My study revealed that all of the victims who were victimized suffered from depression which affected their regular life and rendered them unable of many activities which might be essential to them. Some of the victims' suffered health and educationally. In some victims the amount of depression was so high that they needed medical help to cope up with that. Depression is a psychological disease that directly effects health triggers other psychological traumas and this was an important finding in regard to impact of cyber crime on women.

7.17 The Victims Feel Anxious, Nervous Lose Their Self-Confidence as Aftermath

Anxiety and nervousness is another psychological impact of cyber crime. Majority of the respondents claim that after they were victimized they now feel anxious and nervous about every single choice they make in their regular life which is also a part of their post-traumatic stress disorder. It makes the afterlife of the victims extremely difficult and contributes to further psychological distress. According to Respondent "C":

79
"I don't feel I have security at all, I am anxious and nervous all the time and I don't even believe this will go even in future".

Losing confidence: it can be a feeling of something gradually going away from an individual, being eroded. When someone loses confidence it can feel like they are losing themselves: like they have gone into hiding from themselves. Sometimes losing confidence is slow; other times losing confidence is sudden. Another revelation as my study findings is that all of the respondents', who are subject of this study, lost their self confidence drastically to the point where there is nothing left. They described the feeling as a feeling of nothingness. To deduce this finding I quote the expression of Respondent "A" where she stated:

"I could not concentrate in my studies and it took well effect in my result of that year too. I was ashamed to go in public to think who have viewed that video and they will indentify me. I felt unseen eyes on me and I felt often that I will faint from this all pressure. I felt unwanted in group discussions and talks. I would always remain in some sort of trance and I lost my repute in no time".

Analysis of Victims Feel Anxious, Nervous Lose Their Self-Confidence as Aftermath

I found through conducting interview and victims claimed that all of them feel anxious about their future. They were constantly nervous even while I was conducting my interview and they state they completely lost their self confidence and trust on people. This is also a psychological impact of being cyber crime victim and an important addition to clearing our objective to know their impacts of cyber crime on women.

7.18 Insomnia is a Most Common Outcome of Cyber Victimization

Insomnia is a sleep disorder in which you have trouble falling and/or staying asleep. The condition can be short-term or acute and can last a long time or chronic. It may also come and go. Most of the respondents of my study after the cyber victimization developed Insomnia and they claim they are having extreme difficulty for this reason. According to Respondent "E":

"I am depressed ... I can't sleep... I often feel would my suffering if I died ... I am currently patient to psychologist by the way".

Victim "D" agreed and said:

"Yes it's been a long time since I had a good night sleep and I wonder if I will ever have that back."

Analysis of Insomnia is a Most Common Outcome of Cyber Victimization

Through my research and various victim's interview expression and dialogues I found that all the victims suffered from lack of sleep. Some where diagnosed to have insomnia a condition of sleeplessness and they are receiving medical aids to sleep. This is yet another impact of cyber crime which I identified common in all victims.

7.19 Self-Harm and Suicidal Tendency Develops Among Victims in Severe Case

I found out that self-harm and suicidal tendency is common among the victims. The victims as established earlier in above sections develop different psychological disorders and in trance of that they often cause physical harm to themselves. This finding is also supported by earlier research in this field. The symptoms may vary but about half of my respondents hurtled themselves bodily in some way and tried a failed attempt of suicide. Their justification for that is shame, self guilt, depression and they wanted the suffering to end. To this note Respondent "D" give me a horrific statement in which she quotes:

"Once I tried to hang myself but I instead took sleeping pills and was taken to medical after that everyone calmed down".

Victim "A" said that she also tried to kill herself and ham herself to wich she described:

"I was so hopeless that I cutted my nerves and tried to kill myself to ease my suffering."

Analysis of Self-Harm and Suicidal Tendency Develops Among Victims in Severe Case

Around 20% of my respondent victims once tried to harm themselves or commit suicide to cope up with the situation. This provided me with the ultimate finding that in worse cases cyber crime can drive victims to commit suicide.

7.20 Cyber Crime Incurs Financial Loss for Victims and Their Family

Along with other issues material issue of financial loss also occurs when a cyber crime takes pace and its seen victims are cheated a lot of money by the offenders or victims have to pay for their suffering and justice. In this sense victim pays for her suffering means the victim goes through medical treatments and psychological guidance which comes off their own wallet which if the incident never took place they would not have to go through. Again financial loss also occurs for filing suits and hiring lawyers and again victims have to bear

that or their family does which is outcome of cyber crime. The feeling of financial loss I found in respondent "B"s voice as she voiced out:

"A huge amount of sum was taken away in fraudulent way and then the whole process involved many costs of travels, lawyers fee etc. So it was a very traumatic and expensive experience".

The victims also suffer negative effects on their job and some lose them due to the incident. Further if a victim's incident is flush out too much they further suffer back lass of no one giving them employment. Around one third of the respondents actually faced this problem and it was captured perfectly by respondent "E" as she narrated her experience:

"...I still am suffering because garment owners won't even give me job... and supervisors of garments would ask me to do same for them and they will give me work..."

Analysis of Cyber Crime Incurs Financial Loss for Victims and Their Family

I have found that victims who used to have jobs they easily lose their jobs and means of supporting themselves after commission of cyber crime. Some victims are targeted for financial gain and when their money is fraudulently taken they also suffer directly financially. Lastly the whole process of cyber victimization is cost effective from filing case to travel expenditure and expense of medicine all involves cost which would not arise if they were not victimized. This finding reveled the economic aspect of cyber victimization.

7.21 The Victims Face Further Sexual Harassment Even After the Incident

In many cases the victims faced further sexual harassment after their sensitive content got public. This section is best described by Respondent "D" and according to her:

"Unknown people would call me night and day and ask dirty things. People even bother my mother and father with calling names".

Victim "E" also had similar experience to which she narrates:

"First I am having divorce and with this incident unwanted people are making advances to me thinking I am an easy target."

Analysis of the Victims Face Further Sexual Harassment Even After the Incident

In the study I found due to their sensitive content being spread the victims faced further sexual harassment even after the victimization as many people think that are persons of bad morale and they will welcome unwanted advances.

7.22 Unsubstantial Role of NGOs in Awareness Raising on Cyber Crime Issue

With the lack of Specialized NGOs in dealing with victims it's also established that the role of NGOs in awareness raising is also very limited. The issue of Women cyber victimization is not a priority of the NGOs and we establish this fact from wording of Respondent "Z":

"Even though I myself work in a NGO but I think the extend of help in this regard is not enough and it should be more..... These things are really technical

7.23 Victims Don't Receive Proper Counseling and Guidance

As the number of NGOs and private organizations who support victims of cyber crime is scares the counseling of victims are also lacking in a huge way and I have drawn this conclusion from the statement of Respondent "Z" as she said:

Victim counseling is a part of working in a NGO but we are not equipped with dealing with victims of cyber crime. I on personal basis do victim counseling when I feel they need it.

7.24 Remarks

At the end of this chapter I would like to say the mentioned above are all the findings which were collected on the journey of this research. I tried my best to keep the experiences of cyber crime victims and the support agents as best as they have said for the sake of reliability and validity. The study findings are not end of a study rather from this finding, I as a researcher hope future generation will conclude to develop more mature hypothesis and draw more variant of conclusion than I have done.

CHAPTER 8 DISCUSSIONS OF THE STUDY FINDINGS

The council of Europe defines Cyber Crime as the utilization of computer systems to cause, facilitate, compromise, and threaten violence or to commit savagery against individuals that outcomes in, or is probably going to bring about, physical, sexual, mental or financial mischief or enduring and may incorporate the abuse of the person's conditions, attributes or weaknesses. European Institute for Gender Equality in 2017 conducted a research on Cyber violence against women and girls. Research shows that one of every three women have encountered a type of viciousness in the course of her life, and regardless of the moderately new and developing phenomenon of internet connectivity, it is assessed that one out of ten women have effectively already experienced a form of cyber violence since the age of 15 (European Institute for Gender Equality, 2017).

8.1 Discussion

Cyber Crime is a Disruptive, Impulse-Controlled, and Conduct Disorder that has a great impact on individuals and societies. But there is limited scope to prevent Cyber Crime. People have no knowledge how to protect themselves in cyber space. Even majority of law enforcement officers and investigators have no academic training to conduct a proper investigation or collect definite evidence to penalize the offender. Awareness level is very low to develop victim hardening environment. Depression, stress, sleeping disturbance, obesity, depression and other psychological problems are the main psychological outcome which is affecting women who are the victims of cyber crime. Specific interventions have not been introduced for recovering the victims.

Actually there is no permanent eradication for Cyber Crime. So, people of the society as well as government should take initiative to prevent this offense as to minimum as they can. Governments have to also formulate policy, law which is relating to women who are the most vulnerable group and prevent of Cyber Crime also in general. Plan should be implemented as well as resources should be allocated to prevent Cyber Crime as early will possible.

Many earlier study and my study findings has showed that Cyber Crime is not a curse for only the victims, but also their family members have to suffer with them badly. Government is trying to take initiatives to formulate policy and trying to implement strategies but these strategies need to be specific and well formulated in consultation with people who are pioneer in this field.

Findings of my study revealed that Cyber Crime is a socio-legal issue. So it needs to be addressed by the People of society to change their mindset and also make them aware of consequences of Cyber Crime. Strategies and their implementation have to introduce to prevent findings of my study revealed that Cyber Crime is a socio-legal issue. Strategies to prevent Cyber Crime should be focusing, to improve lack of awareness of people of society, lack of knowledge of Law enforcers, lack of cyber forensic experts, victim counseling and support facilities which are the contributing factors of Cyber Crime. Halder, D., and Jaishankar, K. (2011) In "Cyber Crime and the Victimization of Women: Laws, Rights and Regulation" showed An Action Plan to face the Challenge of cyber crime.

Cyber crime is damaging the youth and mature females gradually by incident basis. Many women have tried to take their own life out of shame and self-blame which is common outcome of Cyber Crime. It damages the mental health of victims. Insomnia is very much related to Cyber Crime. Social awareness, proper training, psychotherapy can prevent this. Government should allocate resources to address the people of Cyber Crime. My study showed that my respondents have Trauma- and Stressor-Related Disorders. Government has to introduce national Cyber Crime plan to prevent Cyber Crime. A study Cyber Crime in Asia Pacific Region has revealed that due to urbanization, industrialization extended families turned into nuclear families is the reason increase of cyber crime in both being criminal and in being victims. Cyber Crime is one of victims are suffering from deep psychological impacts. They need counseling and proper car as support. This report also showed that by proper awareness promotion, online activity maintenance and well early age teaching can prevent the Cyber Crime. Dissertation showed that Cyber Crime has dramatic effects on the lives of the people. My respondents are suffering many problems due to impact of cyber crime social, financial and also legal issues of Cyber Crime. Facilities are very poor to provide the women deserving justice to Cyber Crime, but have no choice that they have to depend on government facilities but government haven't enough facilities to prevent Cyber Crime.

My study also showed that respondents cannot do their own daily task. They have so many mental problems. But they have no one to support them properly. Even her family members don't know the how to empower them or in some cases it's seen that family members are against the victims. Through the discussion of above literature I get the ordinary miserable scenario of women who are victims Cyber Crime. Most of my respondents have same situation. At the most crucial part of life, they are helpless in society. A women before cyber crime enjoys respect honor modesty but the situation changes drastically after being victim to cyber crime. Modernization, urbanization, Economic hardships, declining social values, growth of web based activity; changes of the culture are also responsible for this situation. This altering environment is being created many socio-economic, psychological and legal problems of women. They are suffering from vicious diseases like Cyber Crime.

It is world-wide problem. It is the reason of changes of individual behavior and life circle change. Unknown information has been revealed by doing 8 case studies by qualitative research in my dissertation. Most of the Cyber Crime people are between 18 and above 30. All of them suffered many psychological traumas like sleeping problems, nervousness, sadness, depression and many other physical problems when they tried to harm themselves. Social distance and stigma are responsible to the deprived and encouragement to offenders of Cyber Crime. The sign and symptoms are varied from person to person of Cyber Crime because family background, life standard are not some of the people. My respondents are some common behavior like that- Restlessness Aggression Agitation, Phantasm, few of my respondents has lost the work and they have lost their family bondage. My participant's family relationship is being weaker than before. Due to Cyber Crime, my respondents are unable to communicate with others. They cannot response properly. As a result their family members have to suffer by many problems. Most of my respondents want to forget their past which is hunting them. They are often confused what to do and how to do. They are remained puzzled in all time. My respondents use negative words rather than positive words. They like to say no rather than yes. Besides family members, government and communities have to take steps to cure Cyber Crime from the society.

8.2 Remarks

Cyber crime is a curse on modernization and digitalization. As a conclusion to this chapter it can be said that on gender ratio women are mostly affected by Cyber Crime. Many respondents have so much life ahead and potential and yet they are suffering many problems as well as fighting legally against cyber crime. Collective sate wise and globally steps should be taken to prevent this viciousness.

CHAPTER 9

SUMMARY, RECOMMENDATIONS AND CONCLUSION

Cyber crime and women through this research and many more done before this research ever come to existence has no doubt raised an alarm that this matter now at this age of time needs to be addressed with utmost importance. The internet is a vast unexplored world which is receiving each day new inhabitants and it's on rise not on decline and as to such half of that number consists of women who are more affected by crime conducted in this space. The law makers, researchers, policy makers software companies social networking sites all must take into consideration of the fact that women's privacy and protection needs to be upheld with a priority basis. In the following outline I have indicated a summary of my research and recommended some ideas which might change the picture of present scenario at least for Bangladesh if not globally before finally concluding my thesis.

9.1 Summary

The purpose of this study was to show the nature and impact of cyber crime on women particularly in the scenario of Bangladesh. It was a qualitative research. The main method employed in this research was case study, that looked at how cyber crime on women is more prevalent on gender ratio, the long term and short-term consequences the victims suffered from, the nature and types of cyber crime which are frequent to women, the socio-legal aspects as after math of the offense. Dhaka was selected as the study area. Participants were asked various questions on face to face interview for the study and professionals who are working with issues of cyber crime were also interviewed. The schedule of interview followed Semi-structured guide and style which enabled the researcher to covered themes of respondent about their life style, thinking, sufferings, experiences and perspectives.

The research was conducted firstly giving a brief idea on the problem and the research objectives. To ascertain those objective relevant books, articles, newspaper articles, prior research on the same field and all relevant existing materials were reviewed. The review all affirmed the problem that cyber crime is a new and major threat and females are most targets of these types of offenses. Formal literature reviews are a basic examination of a subject and are a scholarly necessity as well as fundamental when arranging a research project and for

setting research discoveries into setting. Understanding the scene in which a researcher is working will empower him to make an important commitment to the research field.

Findings of my study uncovered that Cyber Crime is a socio-legal issue. So it should be tended to by the People of society to change their mindset and furthermore make them mindful of outcomes of Cyber Crime. Techniques to forestall Cyber Crime ought to centered, focusing, to improve lack of awareness of people of society, lack of knowledge of Law enforcers, lack of cyber forensic experts, victim counseling and support facilities which are the contributing variables of Cyber Crime. Cyber crime is harming the Youth and females progressively by episode premise. Numerous women have attempted to end their own life out of disgrace and self-guilt which is regular result of Cyber Crime. It harms the emotional wellbeing of victims. Sleep deprivation is a common issue identified with Cyber Crime. Social awareness, proper training, psychotherapy can prevent this. Government ought to assign assets to address individuals of Cyber Crime. My study showed that my respondents have Trauma-and Stress or-Related Disorders. Government needs to formulate public Cyber Crime plan with forestall Cyber Crime. My investigation likewise showed that respondents can't take care of their own day by day task. They have such countless mental issues. The finding revealed that the victims have nobody to help them appropriately, even victims' relatives don't have a clue about how to enable them or sometimes it's seen that relatives are against the people in question. I found out in course of this research that Cyber abuse or the cybercrime goes unreported as Bangladeshi women lack the necessary awareness of such offences. The biggest problem of the cyber crime lies in the modus operandi and the motive of the cyber-criminal. Many websites and blogs provide security tips for the safety of women and children while using internet.

But still the cyber-crime against women is on the rise. Modernization, urbanization, Economic difficulties, declining social qualities, development of online based activity; changes of the way of life are additionally liable for the present circumstance. This altering environment is being created many socio-economic, psychological and legal problems of women. Cyber crime is world-wide problem. It is the reason of changes of individual conduct and life circle change.

9.2 Recommendations

Digital Security Act, 2018 defines some cyber-crimes and their punishments but all these are mostly dealing with the economic and financial issues. Issues straightforwardly influencing women and the children are nowhere examined in the Act. Typical cyber crimes against women like cyber stalking, morphing, blackmailing and email spoofing are not considered as offences in the act. These are the problems affecting the women at large and once they aren't protected or prevented by the statute, this loophole encourages the cyber criminals or stalkers to pursue with these shameful activities. As a researcher from the findings and with observation of surrounding also in depth study the recommendations to improve the present picture of women Cyber Victimization are flows-

- a) To reduce and prevent cyber-crime against women, or to be precise, to protect their modesty being outraged through the means of internet, the Bangladeshi legal system needs to come up with some amendments in the present statutes, both in Digital Security Act, 2018 as well as Penal Code, to define and punish for such activities affecting the women at large.
- b) It is the right, as well as the duty of victims of cyber crime, or of any kind of crime, to report it so that necessary actions can be taken, offenders can be punished, and so further crime rate can be decreased.
- c) Victims are silent, bear all embarrassments, and thus, they and the society need to change their approach and pre set mindsets. They don't understand that offender deserves that punishment, not the people in question. There is always a fear in their minds of being a source of fun and embracement in the society which prevents them to ask for their justice and that needs most addressing from social stand point.
- d) Crime not being reported, and unfortunately gives rise to the crime rate, as the fear of being caught or punished vanishes from the minds of offenders. So to all women don't be a liability on the society, always is an asset, and for offenders or people, who use internet before thinking about committing any offence, think about its consequences. "Prevention is better than cure".
- e) Along these lines, every one of the net clients, particularly women, who are more inclined to be the casualties of cyber crime, ought not to share their own data to public and in Social Networking locales like Facebook; they ought to keep up as far as possible on their data and photographs. They should take care in adding outsiders in their friend list. The less open their private data and photographs will be; the more protected they are, behind the screens.

- f) If any cyber crime happens against them, they should immediately report it to the cyber cell of police which is under CID and ask for immediate actions.
- g) Police Personnel should be increased who are specially trained and equipped with dealing with cyber crime.
- h) Government victim support centers should be opened for psychological and moral support of victim
- i) For Bangladeshi Legal system, as well as Bangladeshi justice delivery system effective laws should be enacted through required amendments in the present statutes that can tackle such issues of cyber crime against women and can provide for deserved punishments to the offenders.
- Cyber Tribunal in each district is of times need as the present Act provides scope of such.
- k) The Judges and the prosecution of such tribunal should be properly trained to entertain and try these cases.
- Internet security is of imperative significance and should be dealt with to ensure every victims or potential victims protection.
- m) Equity conveyance ought to be expedient and successful. Present law shouldn't cause injustice form being conveyed. There is no advantage of delay, because according to William Edward Gladstone "Justice delayed is justice denied."
- n) To forestall and stop crime, some exacting moves should be made. Those activities ought to be quick and compelling. These actions should have a part where promotional activities to raise awareness are included.

9.3 Conclusion

In Bangladesh where the general public peers downward on the women and the law doesn't even as expected perceive cyber crimes. The central issue of cyber crime lies in the usual methodology and the persistence of the cyber criminal. The police, judiciary and the investigative agencies need to keep up to date with the most recent improvements in online applications so they can rapidly recognize the genuine culprit. It is the job of the legal system and regulatory agencies to stay up with the Technological turns of events and guarantee that more current advances don't become devices of abuse and provocation. Governments can take authoritative estimates that guarantee common freedoms; particularly women' privileges are secured online similarly as they are in physical spaces. Legislation shouldn't just protect users; however, it should also educate and inform all groups on the way to exercise their

communication rights. Simultaneously, Individuals should become aware both on the online and offline; realize how to take careful steps in the internet and look for plan of action if their privileges are disregarded. Nonetheless, a few changes are as yet required, for example, digital wise adjudicators and more digital council in each locale. Cyber crimes, for example, morphing, e-mail spoofing do-not have a moral backing in society and hence are taken lightly. This carries us to the main part where social headway is required, individuals need to perceive the privileges of others and acknowledge what comprises a wrongdoing. They should learn not to meddle with the private existences of others; regard towards women in the public eye needs to increment. This must be done if youths are instructed since early on, to regard women with the modesty and privacy they deserve. Consequently, to counter cyber crime against women in Bangladesh, stricter reformatory changes are required as well as an adjustment in training framework is a colossal necessity. Such change can't emerge out of inside a solitary square of society however individuals, government and NGOs and so on need to cooperate to deliver such changes. Women themselves must be trained to take preventive measures, such as caution in posting their and their friends and family's photos and clips on the web; they should be alert in speaking with outsiders on the web, and ensuring passwords and other fundamental data which may be bargained with the women's security and protection. Women Internet users in Bangladesh are required an expanded consciousness of upgrading security settings in person to person communication destinations as a preventive measure. In this manner, there is a pressing need of carrying mindfulness and awareness among women to be cautious while utilizing social networking sites and also a proper guidance if somehow, they face cybercrime then they will raise their voice against it. There is also an alarming requirement for knowledge and technical enhancement for prevention of woman harassment in Bangladesh.

REFERENCES

A.M. Maruf A.M. el at. (2010). Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies. The Northern University Journal of Law, Vol. 1, pp 112-113.

Aboujaoude E, Savage M, Starcevic V, Cyberbullying: Review of an Old Problem Gone Viral, Journal of Adolescent Health 2015, Volume 57, Page 10–18.

Agarwal, N. and Kasuhik, D.N. (2014). CYBER CRIMES AGAINST WOMEN. *GJRIM*, 4(1), pp.38–39.

Agarwal, N. and Kasuhik, D.N. (ibid.,)

Akancha Srivastava, Indian Women at Risk in the Cyber Space: A Conceptual Model of Reasons of Victimization, International Journal of Cyber Criminology (IJCC) ISSN:0974 – 2891 January, June 2014, Volume 8 (1): Page 57–67.

Alam, N. (2016). The great Bangladesh cyber heist shows truth is stranger than fiction. *Dhaka Tribune*. 12 Mar.

Alice Munyua, Women and cybercrime in Kenya, 2015.

Ambrosi, A., Peugeot, V. and Pimienta, D. (2005). *Word Matters: Multicultural Perspectives On Information Societies*. C & F Éditions.

Asari, K.N. and Ismail Nawang, N. (2014). Cyber Defamation: A Comparative Analysis of the Legal Position in Malaysia and the United Kingdom.

Attrill A. & Fullwood C. (2016) Applied Cyberpsychology Practical Applications of Cyberpsychological Theory and Research. London: Macmillan Publishers Limited.

Balakrishnan V. Cyberbullying among Young Adults in Malaysia: the Roles of Gender, Age, and Internet Frequency, Computer Human Behavior 2015, Volume 46, Page 149–157.

Bangladesh National Women Lawyer Association Report. (2014). Dhaka: BNWLA, pp.145–173.

Bauman S, Baldasare A., Cyber Aggression among College Students: Demographic Differences, Predictors Of Distress, And The Role Of The University, Journal Of College Student Development (2015). Volume 56, Page 317–330.

Bloom S. No Vengeance For "Revenge Porn" Victims: Unraveling Why This Latest Female-Centric, Intimate-Partner Offenses Still Legal, And Why We Should Criminalize It. Fordham Urban Law Journal 2016 Volume 42, Page 233–289.

BNWLA. (2014). Survey on Psychological Health of Women. Dhaka: Bangladesh National Women Lawyers' Association.

Borhanuddin, A.R.M. (2016). Cyber Crime and Bangladesh Perspective. Available at: https://www.academia.edu/4488760/Cyber_Crime_and_Bangladesh_Perspective [Accessed 16 Mar. 2020].

Borhanuddin (ibid., p.4)

Borhanuddin (ibid., p.5)

Borowsky, I.W., Taliaferro, L.A. and McMorris, B.J. (2013). Suicidal Thinking and Behavior Among Youth Involved in Verbal and Social Bullying: Risk and Protective Factors. *Journal of Adolescent Health*, 53(1), pp.S4–S12.

Bossler AM, Holt TJ, May DC, Predicting Online Harassment Victimization Among A Juvenile Population, Youth & Society, Sage Journals 2011, Volume 44, Page 500–523.

Bosworth, S. and Kabay, M.E. (2002). *Computer Security Handbook*. 4th Edition ed. New York: John Wiley & Sons, Inc, p.116.

BTRC Report. (2018). [online] Dhaka: Btrc. Available at: http://www.btrc.gov.bd/sites/default/files/paper_files/BTRC_English%20Annual%20Report %202017-18.pdf.

BuzzFeed News. (2013). *Daisy Coleman Publishes A Personal Essay About Her Sexual Assault*. [online] Available at: https://www.buzzfeednews.com/article/alisonvingiano/daisy-coleman-publishes-a-personal-essay-about-her-sexual-as [Accessed 13 Mar. 2020]

Cassidy W, Faucher C, Jackson M., Cyber Bullying Among Youth: A Comprehensive Review Of Current International Research And Its Implications And Application To Policy And Practice. Sage Journal, Volume 34, Page 575–612.

Citron DK, Franks MA, Criminalizing Revenge Porn, Wake Forest Law Review 2014, Volume 49, Page 345–391.

Citron DK. Law's Expressive Value in Combating Cyber Gender Harassment. Michigan Law Review 2009. Volume 108, Page 373–415

CNN, B.D.K.C., Special to (2014). *Opinion: Make "revenge porn" a crime in U.S.* [online] CNN. Available at: https://edition.cnn.com/2013/08/29/opinion/citron-revenge-porn/index.html [Accessed 13 Mar. 2020].

Constitution of Bangladesh 1972, Art. 31.

Cyber Crime Foundation (2019). Cyber Crime Foundation Report.

Dawson, E. and Raghavan, S.V. (2011). An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks: Critical Information Infrastructure Protection. 2011th ed. New Delhi: Springer.

Dean, M. (2017). *The Story of Amanda Todd*. [online] The New Yorker. Available at: https://www.newyorker.com/culture/culture-desk/the-story-of-amanda-todd [Accessed 25 Apr. 2019].

Dhaka Tribune. (2019). *Rise in cybercrime worries women*. [online] Available at: https://www.dhakatribune.com/cybersecurity/2019/04/01/rise-in-cybercrime-worries-women [Accessed 7 May. 2020].

Digital Security Act. 2018.

Drebing H, Bailer J, Anders A., Cyber stalking in a Large Sample of Social Network Users: Prevalence, Characteristics, and Impact upon Victims, Cyberpsychology, Behavior, and Social Networking 2014, Volume 17, Page 61–67.

European Institute for Gender Equality (2017). Cyber violence against women and girls. *EIGE's publications*, pp.3–5.

Goldblum, G., L. Espelage, D., Chu, J. and Bongar, B. eds., (2014). Youth Suicide and Bullying: Challenges and Strategies for Prevention and Intervention. *Oxford University Press*.

Gunjan, V. K., Kumar, A. and Avdhanam, S., 2013. Survey of Cyber Crime in India. In: 2013 15th International Conference on Advanced Computing Technologies (ICACT). [online] Rajampet, India: IEEE, pp.1-6. Available at: https://ieeexplore.ieee.org/document/6710503> [Accessed 7 March 2020].

Halder, D., & Jaishankar, K. (2011). Cyber Crime and the Victimization of Women: Laws, Rights and Regulations. Hershey Pennsylvania USA: IGI Global.

Haque, M.M.R. (2016). Cyber crime and cyber law in Bangladesh. Daily New Nation. 16 Jul.

Henry N, Powell A., Technology-Facilitating Sexual Violence: A Literature Review of Empirical Research of Trauma Violence Abuse, Sage Journals 2016, Volume 19, Page 1–14. Hinduja, S. and W. Patchin, J. (2007). Offline Consequences of Online Victimization: School Violence and Delinquency. *Journal of School Violence*, 9(3), pp.89–112.

Hinduja, S. and W. Patchin, J. (2008). Cyberbullying: An Exploratory Analysis of Factors Related to Offending and Victimization. *Deviant Behavior*, 29(2), pp.129–156.

Hinduja, S. and W. Patchin, J. (2010). Bullying, Cyberbullying, and Suicide. *journal of the International Academy for Suicide Research*, 14(3), pp.206–221.

Hinduja, S., & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. Archives of Suicide Research, 14(3), 206–221.doi:10.1080/13811118.2010.494133

Hindustan Times. (2005). '70% married women abused'. [online] Available at: https://www.hindustantimes.com/india/70-married-women-abused/story-YFOmB1vNqQVnfP29313NfN.html [Accessed 12 Mar. 2019].

Holt TJ, Fitzgerald S, Bossler AM, Assessing The Risk Factors of Cyber And Mobile Phone Bullying Victimization In A Nationally Representative Sample of Singapore Youth, International Journal Of Offender Therapy And Comparative Criminology 2016, Volume 60, Page 598–615.

Houbre, B., Tarquinio, C. and Lanfranchi, J.-B. (2010). Expression of self-concept and adjustment against repeated aggressions: the case of a longitudinal study on school bullying. *European Journal of Psychology of Education*, [online] 25(1), pp.105–123. Available at: https://www.jstor.org/stable/23421679?seq=1 [Accessed 12 Mar. 2021].

Jahankhani, H, Al-Nemrat, A & Hosseinian-Far, A 2014, Cybercrime classification and characteristics. in *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Cyber Crime and Cyber Terrorism Investigator's Handbook, Elsevier Inc., Physics. https://doi.org/10.1016/B978-0-12-800743-3.00012-8

Jahankhani, H., Nemrat, A.A. and Hosseinian-Far, A. (2014). Cyber crime Classification and Characteristics. In: F. Bosco, A. Staniforth and B. Akhgar, eds., *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Amsterdam, Netherlands: Elsevier Science, p.159.

Jahankhani, H., Nemrat, A.A. and Hosseinian-Far, A. (ibid. p.158)

Jeet, S. (2012). Cyber crimes against women in India: Information Technology Act, 2000. *Elixir Criminal Law*, 47, p.8892.

Jessica West, J. (2014). Cyber-Violence Against Women.

Kabir, A.E. and Chowdhury, S. (2017). *Media and Cyber Laws in Bangladesh*. 1st ed. Dhaka: Sufi Prokashoni, p.421.

Kabir, A.E. and Chowdhury, S. (ibid., p.418-419)

Kabir, A.E. and Chowdhury, S. (ibid., p.421-422)

Kabir, A.E. and Chowdhury, S. (ibid., pp.55-366)

Karuppannan, J. and Halder, D. (2009). Cyber socializing and victimization of women. *Temida*, 12(3), pp.12–14.

Keats Citron, D. and Anne Franks, M. (2014). Criminalizing Revenge Porn. *Wake Forest Law Review*, 49(2), pp.345–392.

Khan MR. (2018) 'Law Enforcement To Determine Accuracy of News', Prothom Alo 22 May. Available at: https://en.prothomalo.com/bangladesh/Law-enforcement-to-step-up-control-of-media (Accessed: 10 November 2019).

Lindsay M, Booth JM. Messing JT, Experiences of online harassment among emerging adults: Emotional reactions and the mediating role of fear, Sage Journals 2016, Volume 31, Page 1–22.

Loza de Siles, E. (2015). Cybersecurity and Cybercrime: Intellectual Property and Innovation. *Landslide*, 8(2).

Luis Jasso Medrano, J., Lopez Rosales, F. and Gámez-Guadix, M. (2017). Assessing the Links of Sexting, Cybervictimization, Depression, and Suicidal Ideation Among University Students. *Archives of Suicide Research*, 22(1), pp.1–12.

Lynn Bates, S. (2015). "Stripped": an analysis of revenge porn victims' lives after victimization. [Thesis] Available at: https://summit.sfu.ca/item/15668 [Accessed 11 Mar. 2020].

M Cairul Basrun Umanailo, Cybercrime Case as Impact Development Of Communication Technology that Troubling Society, Internation journel of scientific and technology research volume 8, issue 09, September 2019.

Mahmud, F. (2018). CYBER-CRIME AND THE VULNERABILITY OF THE FAIRER GENDER. [online] FinTech Magazine. Available at: http://www.fintechbd.com/cyber-crime-and-the-vulnerability-of-the-fairer-gender/ [Accessed 20 Apr. 2020].

Manusher Jonno Foundation. (20011) *Manusher Jonno Foundation Annual Report*. Available at: http://www.manusherjonno.org/who-we-are/annual-reports/index.php?Key=44 (Accessed: 11 November 2019).

Marcus Gillespie, B. and Richard Giardino, J. (1998). Explaining the Importance of Operational Definitions to Students. *Journal of Geoscience Education*, 46(5), pp.427–432.

Marczak, M., & Coyne, I. (2010). Cyberbullying at school: Good practice and legal aspects in the United Kingdom. *Australian Journal of Guidance and Counselling*, 20(2), pp.182–193.

Mariel Salmona cited in Haut Conseil à l'Egalité (2017), "En finir avec l'impunite des violences faites aux femmes en ligne: une urgence pour les victimes", available at http://www.haut-

conseilegalite.gouv.fr/IMG/pdf/hce_rapport_violences_faites_aux_femmes_en_ligne_2018_0 2_07.pdf

Maruf, A.M., Islam, M.R. and Ahamed, B. (2014). Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies. *Northern University Journal of Law*, 1, pp.112–124.

Mullins, C.W. (2007). Book Review: Barkan, S. E. (2006). Criminology: A Sociological Understanding (3rd ed.). Upper Saddle River, NJ: Pearson/Prentice Hall. 657 pp. *International Criminal Justice Review*, 17(3), pp.239–240.

Mustaine, E. E., & Tewksbury, R. (1999). A routine activity theory explanation for women's stalking victimizations. Violence Against Women, 5(1), pp.43-62.

Nagpal, R., 2018. What Is Cyber Law And Why Do We Need It?. [online] Medium. Available at: https://medium.com/@rohasnagpal/what-is-cyber-law-and-why-do-we-need-it-9e9a9b956b1a#:~:text=Cyber%20crime,An%20interesting%20definition&text=computer%2 Orelated%20crime%20i.e.%20violations,specifically%20prohibited%20by%20criminal%20st atutes. [Accessed 7 March 2020].

Natasha Kabir, Cyber Crime a New Form of Violence against Women: From the Case Study of Bangladesh, 2018.

Nigam, R., 1965. *Law Of Crimes In India"*, *Principles Of Criminal Law (Vol.1)*. 1st ed. New York: Asia Pubication House, p.36.

Norton.com. (2016). *Norton*. [online] Available at: https://us.norton.com/internetsecurity-emerging-threats-personal-impact-cybercrime.html.

Pal Malik, K. (2010). Computer & Information Technology Law p-71. Available at: http://14.139.13.47:8080/jspui/bitstream/10603/188293/9/09_chapter%201.pdf [Accessed 2020 Feb. 3].

Pandove, K., Jindal, A. and Kumar, R. (2010). 'Email Spoofing.' *International Journal of Computer Applications* (0975 – 8887), 5(1), p.27-29.

Pornography Control Act 2012. Available at: Bangladesh Official Gazette Registered No: DA-1 [Accessed 8 Mar. 2020].

Rabbi, A.R. (2017). Women biggest victims of rising cyber crimes. *Dhaka Tribune*. 21 Sep. Rastogi, A. (2014). Cyber *Law- Law of Information Technology and Internet*. New York, US: Lexis Nexis p-2.

Ratan, J. (2014). Cyber Laws & Information Technology p- 48

Report on Porn Addicted Teenagers of Bangladesh (2014). Dhaka: Manusher Jonno Foundation.

Ruth Lewis, Michael Rowe, Clare Wiper, Online Abuse of Feminists as An Emerging form of Violence Against Women and Girls, *The British Journal of Criminology*, Volume 57, Issue 6, November 2017, Pages 1462–148,

Security, H.N. (n.d.). *Help Net Security, Author at Help Net Security*. [online] Help Net Security. Available at: https://www.helpnetsecurity.com/author/helpnet/ [Accessed 12 Mar. 2019].

Singh J, Violence against Women in Cyber World: A Special Reference to India, International Journal of Advanced Research in Management and Social Sciences (ISSN: 2278-6236)

Singh Jaspreet, Violence against women in cyber world: a special reference to India, 2015

Supan, MHQ. (2015) 'the Cyber Crimes: Are Women the Main Target?', The Daily Star, May 20. Available at: www.thedailystar.net/law-our-rights/cyber-crimes-70592 (Accessed: 10 November 2019).

Supan, Q.M. (2015). CYBER CRIMES: Are women the main target? Daily Star. 15 Mar.

Supan, Q.M. (Ibid.,)

Survey on Psychological Health of Women. (2014). Dhaka: Bangladesh National Women Lawyers' Association.

Tiernan, R. (2004). Business & Technology: E-mail viruses blamed as spam rises sharply. *The Seattle Times*. 18 Feb.

UNICEF FRANCE (2014), Ecoutons ce que les enfants ont à nous dire, Consultation nationale, available at https://www.unicef.fr/sites/default/files/userfiles/Consultation_2014.pdf

United Nations, 2000. Tenth United Nations Congress On The Prevention Of Crime And The

Treatment Of Offenders. Vienna: UN, pp.161-174.

Virtanen SM, Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities, 2017.

Winchester, C.L. and Salji, M. (2016). Writing a literature review. *Sage Journals*, 9(5), pp.308–312.

www.amnesty.org. (n.d.). *Amnesty reveals alarming impact of online abuse against women*. [online] Available at: https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/.

YWCA. (2017). *Technology and gender-based violence*. [online] Available at: https://www.ywca.org [Accessed 19 Mar. 2020].

Zaman, S.T., Gansheimer, L., Rolim, S.B. and Mridha, T. (1AD). Legal Action on Cyber Violence against Women. : *Bangladesh Legal Aid Services Trust*. 2017 Dec.

Appendix - I

Semi-Structured Interview Guideline Victim

Institute of Social Welfare and Research University of Dhaka Dhaka -1205

Research Title- A Study on the Nature and Impact of Cyber Crime on Women

INSTRUCTIONS

Kindly respond to all the quarries NB. All information will be kept Confidential.

A. Demographic and Socio-Economic Information about the Respondents.

- a) Name:
- b) Father/Husband's Name:
- c) Age:
- d) Address:
- e) Sex:
- f) Religion:
- g) Total family members:-
- h) Types of family:
- i) Educational status:
- j) What types of social and financial problems do you face?
- k) Do you get enough economic support for your education and health?
- 1) What type of behavior do you get from the people around you?

B. The awareness for government with the issue of cyber crime and women victimization.

- Tell me your thoughts on our governments awareness with the issue of cyber crime and women victimization
- 2. Tell me if you found any type of awareness in government activities in your issue?
- **3.** Do you think the governments' awareness level affect the cyber crime issues and women victimization?

4. Tell me in your opinion the if lack of government's awareness responsible for cyber crime issues and women victimization and if it is how

C. Identifying the social and legal problems faced by the women victims of cyber crimes.

- 1. Describe the social problem do you face after the cyber crime took place
- **2.** Explain to me if you are facing any discrimination in society after victimization and if the answer yes then how.
- 3. Explain if any of legal issues did you face after the victimization.
- **4.** Tell if you face any legal harassment or impediment after victimization? If yes then how?
- Describe the amount of support you get from your society during dealing with cyber crime case

D. Identifying the after effects of cyber crime on women

- Please describe the changes you experienced in your regular life as the after effect of cyber crime.
- **2.** Please describe the difficulties that you faced in your personal life after cyber victimization.
- 3. Please describe if you had psychological effect after you were victimized.
- **4.** Tell if you felt insecurity in self after the cyber crime issue.

E. Government and NGO's initiatives specific for the women victims of cyber crime.

- 1. Have you got any government support after victims of cyber crime?
- Explain in detail the types of government facilities have you got after victims of cyber crime.
- 3. Explain if you got any NGO support in dealing with victimization and to what extend.
- **4.** Tell me if you felt facilities enough to help you get out of your problems and the kinds of assistance got and you need for overcoming you problem

F. Suggestion and recommendation for the women victims of cyber crime to increase their standard of support.

- Suggest according to you the initiative can help improve the social structure in this
 regard.
- 2. What kinds of help does the government can provide you achieve a better life?

Appendix – II

Semi-Structured Interview Guideline

Law Enforcement and Advocate of cyber crime and women victimization

Institute of Social Welfare and Research

University of Dhaka

Dhaka -1205

Research Title- A Study on the Nature and Impact of Cyber Crime on Women

INSTRUCTIONS

Kindly respond to all the quarries NB. All information will be kept Confidential.

G. Demographic and Socio-Economic Information about the Respondents.

- m) Name:
- n) Father/Husband's Name:
- o) Age:
- p) Address:
- q) Sex:
- r) Educational status:

H. The awareness for government with the issue of cyber crime and women victimization

- In your opinion please explain the government's awareness level regarding the issues of cyber crimes and women victimization.
- Suggest to me the type of awareness the government need to deal with cyber crimes and women victimizations cases.
- Please tell me if you think the government is negligent or less aware in regarding to this issue and if the government is responsible to what extent.
- Explain if there is any lack in governmental structure affecting your activities to deal with cyber crimes and women victimizations cases.
- Give me your opinion if victim suffer for government's negligence if any and how and extent of the suffering.

I. Identifying the social and legal problems faced by the women victims of cyber crimes.

- 1. Give us your experience account of main legal problems faced by a victim of cyber crime
- Give us your experience account of social problems do the victims face after cyber crime issues.
- 3. Please explain the extent of your help solve the victims legal problems.
- 4. Do you get any official training to provide the victims legal and to overcome their legal problems?
- 5. Please describe the legal complexities that the victims face after cyber crime issues.
- 6. Are there any laws to solve the social problems of the victims after cyber crime issues? If 'yes' and explain?

J. Identifying the after effects of cyber crime on women

- Describe your experience regarding psychological issues women face during dealing cyber crime issues.
- Explain the depth of change in the lifestyle of the victims of cyber crime and the type of complexities women face in their personal or family life after cyber crime issue.
- 3. Does cyber crime issue affect the women victims more than male victim? If 'yes' then how?

K. Government and NGO's initiatives specific for the women victims of cyber crime.

- 1. Do you think the initiatives of the government capable enough to help victimized women?
- 2. In your opinion explain if NGOs play any role to help the women victims of cyber crime.
- 3. Please provide as suggestion the kind of initiatives that can be more fruitful to women victims of cyber crime.

L. Suggestion and recommendation for the women victims of cyber crime to increase their standard of support.

- Provide your suggestion about the appropriate implementation of laws pertaining to women victims of cyber crime.
- 2. How does the government provide legal assistance to the women victims of cyber crime?
- Give us your recommendation for the overall betterment of the situation of women victims of cyber crime.

Appendix - III

Later of Approval for Interviews

সমাজকল্যাণ ও গবেষণা ইনস্টিটিউট

ঢাকা বিশ্ববিদ্যালয়

ঢাকা-১২০৫, বাংলাদেশ ছোন: ৮৮০-২-৫৮৬)৬৬৬১, ৯৬৭০৪১২, শিএবিএছ: ৯৬৬)৯০০-৭০, এছ, ৮৪৮০ ফ্যাক্স: ৮৮০-২-৯৬৭০৪১২, গুমোবসাইট: www.iswr.du.ac.bd ইমেইল: iswrdu.ad@gmail.com, info@iswr.du.ac.bd



Institute of Social Welfare and Research University of Dhaka

Dhaka-1205, Bangladesh Tel: 880-2-58616662, 9670412, PABX: 9661900-73, Ext. 8480 Fax: 880-2-9670412, Website: www.iswr.du ac.bd E-mail: iswrdu.ad@gmail.com, info@iswr.du.ac.bd

																٠		٠									

To Whom It May Concern

This is to certify that Ahesan Kabir, is conducting M.Phill study under our supervision at the Institute of Social Welfare and Research. University of Dhaka, titled "A Study on the Nature and Impact of Cyber Crime on Women".

Ahesan is required to collect some information and interview some of the officials of your organization to understand the above mentioned field. He will certainly meet at your convenience and will maintain confidentiality and integrity in this regard.

If you have any questions regarding his work, we will certainly endeavor to assist in clarifying his work.

Thank you very much for your nice cooperation.

Sincerely Yours,

(Dr. Mahbuba Sultana)

Professor

Institute of Social Welfare and Research

University of Dhaka

E-mail Id :mahbubaiswr@gmail.com Mobile Number: +8801614-990330 Slam.

(Dr. Sk. Tauhidul Islam)

Professor

Institute of Social Welfare and Research

University of Dhaka

E-mail Id: sktauhidul@du.ac.bd Mobile Number: +8801678052628

A STUDY ON THE NATURE AND IMPACT OF CYBER CRIME ON **WOMEN**

ORIGI	INAL	.ITY	REP	ORT

28%

SIMILA	ARITY INDEX	
PRIMA	ARY SOURCES	
1	www.liebertpub.com Internet	1030 words -3%
2	nls.academia.edu Internet	792 words -2%
3	www.genderit.org	758 words -2%
4	docs.manupatra.in Internet	412 words — 1 %
5	www.bwss.org Internet	407 words — 1 %
6	www.europarl.europa.eu	345 words — 1 %
7	www.researchgate.net	344 words — 1 %
8	ijless.kypublications.com Internet	245 words — 1 %
9	docplayer.net Internet	229 words — 1 %

10	journal.lawmantra.co.in Internet	214 words — 1%
11	www.kictanet.or.ke	211 words — 1 %
12	tiikm.com Internet	208 words — 1%
13	www.snmorcollege.org.in	195 words — < 1%
14	www.scribd.com Internet	194 words — < 1%
15	www.tandfonline.com Internet	173 words — < 1 %
16	citeseerx.ist.psu.edu Internet	159 words — < 1%
17	papers.ssrn.com Internet	156 words — < 1%
18	banglajol.info Internet	149 words — < 1 %
19	drrajivdesaimd.com Internet	147 words — < 1 %
20	www.ijstr.org Internet	146 words — < 1%
21	www.amnesty.org	140 words — < 1 %

teresas.ac.in

22	Internet
11	

$$128 \, \text{words} \, - < 1 \%$$

127 words —
$$< 1\%$$

123 words
$$-<1\%$$

121 words
$$-<1\%$$

112 words
$$-<1\%$$

ropositorii unios bu

repozitorij.unios.hr

$$106 \text{ words} - < 1\%$$

105 words
$$- < 1\%$$

$$104 \, \text{words} \, - < 1 \, \%$$

www.fintechbd.com

101 words
$$-<1\%$$

$$_{89 \text{ words}}$$
 $< 1 \%$

34	www.essay.uk.com Internet	Dhaka University Institutional Repository 85 words — < 1 %
35	en.wikipedia.org	81 words — < 1%
36	jlsr.thelawbrigade.com Internet	79 words — < 1 %
37	www.helpnetsecurity.com Internet	78 words — < 1 %
38	s1.securityweek.com	77 words — < 1%
39	www.japss.org	77 words — < 1%
40	acadpubl.eu Internet	73 words — < 1%
41	www.dhakatribune.com	73 words — < 1%
42	id.123dok.com Internet	71 words — < 1%
43	pt.scribd.com Internet	66 words — < 1%
44	www.herodebeauvais.com	64 words — < 1 %
45	www.cybercrimelaw.net	62 words — < 1 %

46	"Cybersecurity, Privacy and Freedom Protection in the Connected World", Springer Science and Business Media LLC, 2021 Crossref	60 words — <	1%
47	www.garph.co.uk Internet	58 words — <	1%
48	www.feeleminds.com Internet	57 words — <	1%
49	qa-platforms.com Internet	54 words — <	1%
50	www.amnesty.ca Internet	52 words — <	1%
51	dspace.daffodilvarsity.edu.bd:8080	50 words — <	1%
52	uir.unisa.ac.za Internet	50 words — <	1%
53	Aboujaoude, Elias, Matthew W. Savage, Vladan Starcevic, and Wael O. Salame. "Cyberbullying: Review of an Old Problem Gone Viral", Journal of Health, 2015. Crossref	47 words — < Adolescent	1%
54	en.prothomalo.com Internet	45 words — <	1%
55	blog.ansi.org Internet	44 words — <	1%
56	stars.library.ucf.edu	42 words — <	1%

57	www.iosrjournals.org	42 words — < 1 %
58	pdfs.semanticscholar.org	41 words — < 1%
59	ijmr.net.in Internet	40 words — < 1 %
60	feministkilljoys.com Internet	39 words — < 1 %
61	unswlawjournal.unsw.edu.au Internet	38 words — < 1 %
62	www.saulibrary.edu.bd	37 words — < 1 %
63	go.gale.com Internet	36 words — < 1 %
64	documents.mx Internet	34 words — < 1 %
65	lijden-jesse.pw Internet	34 words — < 1 %
66	www.itu.int Internet	34 words — < 1 %
67	repository.au.edu Internet	33 words — < 1 %
68	lawsheet.wordpress.com	32 words — < 1 %

69	www.scribbr.com Internet	32 words — < 1 %
70	inba.info Internet	31 words — < 1 %
71	researchspace.ukzn.ac.za Internet	30 words — < 1 %
72	www.ijcrt.org Internet	30 words — < 1 %
73	LexisNexis Publications	29 words — < 1 %
74	tasued.edu.ng Internet	29 words — < 1 %
75	easystudy.info Internet	28 words — < 1 %
76	www.cybercrimejournal.com Internet	28 words — < 1 %
77	Adina Michael-Titus, Patricia Revest, Peter Shortland. "EPILEPSY", Elsevier BV, 2010 Crossref	27 words — < 1%
78	www.science.gov Internet	27 words — < 1 %
79	Dostoevsky, Fyodor. "Crime and Punishment (First Edition) (Norton Critical Editions)", W. W. Norton & Company Publications	26 words — < 1 %

80 hdl.handle.net

$$_{26 \text{ words}}$$
 $< 1\%$

81 www.digital4n6journal.com

 $_{26 \text{ words}}$ - < 1%

82 en.unionpedia.org

 $_{25 \text{ words}}$ – < 1%

vitak.files.wordpress.com

 $_{25 \, \text{words}}$ - < 1 %

www.legalservicesindia.com

 $_{25 \, \text{words}}$ - < 1 %

85 tnfwl.com

 $_{24 \text{ words}}$ - < 1 %

article.sapub.org

 $_{23 \text{ words}}$ - < 1%

london.northumbria.ac.uk

 $_{23 \text{ words}}$ - < 1%

88 sfx.library.newschool.edu

 $_{23 \text{ words}}$ - < 1%

89 www.mondaq.com

 $_{23 \text{ words}}$ - < 1 %

90 www.wave-network.org

- 23 words < 1%
- Shofiqur Rahman Chowdhury, Haris Abd Wahab, M Rezaul Islam. "The role of faith-based NGOs in social development: Invisible empowerment", International Social Work, 2018

92	docshare.tips Internet	22 words — <	1%
93	www.7consultancy.in	22 words — <	1%
94	www.experts.scival.com Internet	20 words — <	1%
95	Sameer Hinduja, Justin W. Patchin. "Connecting Adolescent Suicide to the Severity of Bullying and Cyberbullying", Journal of School Violence, 2018 Crossref	19 words — <	1%
96	dspace.uta.edu Internet	19 words — <	1%
97	nectar.northampton.ac.uk Internet	18 words — <	1%
98	vitamin-health-online.co.uk Internet	18 words — <	1%
99	"Ethical Considerations and Challenges in Geriatrics", Springer Science and Business Media LLC, 2017 Crossref	17 words — <	1%
100	Kudrat E Khuda Babu, Md. Ahsan Ullah. "Cyber legislation and cyber-related legal issues in Bangladesh: inadequacies and challenges", Intern Journal of Electronic Security and Digital Forensics		1%

101 aiirjournal.com

Crossref

 $_{17 \text{ words}} - < 1\%$

102	link.springer.com Internet	17 words — <	1%
103	repozitorij.unizg.hr	17 words — <	1%
104	Rebecca Ong. "Confronting online social aggression in Hong Kong: A wake-up call", International Journal of Law and Psychiatry, 2017	15 words — <	1%
105	W. Lawrence Neuman. Social Research Methods: Qualitative and Quantitative Approaches, 5e, 2003 Publications	15 words — <	1%
106	ise.ait.ac.th Internet	15 words — <	1%
107	satheeshgnair.blogspot.com Internet	15 words — <	1%
108	img.tapuz.co.il Internet	14 words — <	1%
109	lawyersnjurists.com Internet	14 words — <	1%
110	tel.archives-ouvertes.fr	14 words — <	1%
111	Holt, T. J., S. Fitzgerald, A. M. Bossler, G. Chee, and E. Ng. "Assessing the Risk Factors of Cyber and Mobile Phone Bullying Victimization in a National Representative Sample of Singapore Youth", Interest		1%

Journal of Offender Therapy and Comparative Criminology, 2014.

Crossref

112	www.officesoon.com Internet	13 words — <	1%
113	www.pwc.co.za Internet	13 words — <	1%
114	creativecommons.org Internet	12 words — <	1%
115	krazytech.com Internet	12 words — <	1%
116	www.learncram.com Internet	12 words — <	1%
117	www.studymode.com Internet	12 words — <	1%
118	www.journalcra.com Internet	11 words — <	1%
119	www.truecrit.org	11 words — <	1%
120	M Rezaul Islam, M Shamsuddoha. "Socioeconomic consequences of climate induced human displacement and migration in Banglades International Sociology, 2017 Crossref	10 words — < h",	1%
121	dr.ntu.edu.sg	10 words — <	1%

	Dhaka University	Institutional Repository
122	dspace.bracu.ac.bd Internet	10 words — < 1 %
123	dspace.lboro.ac.uk Internet	10 words — < 1 %
124	globalforexcoin.com Internet	10 words — < 1 %
125	repository-tnmgrmu.ac.in	10 words — < 1 %
126	www.fropper.com Internet	10 words — < 1 %
127	www.nvidiadefect.com Internet	10 words — < 1 %
128	Fardaus Ara. "chapter 48 Cyber Crime Against Women and Girls on Social Sites in Bangladesh", IGI Global, 2020 Crossref	9 words — < 1 %
129	core.ac.uk Internet	9 words — < 1 %
130	journal.unnes.ac.id Internet	9 words — < 1 %
131	pure.royalholloway.ac.uk	9 words — < 1 %
132	www.citethisforme.com Internet	9 words — < 1 %

Mark Lacy, Nayanika Mookherjee. "'Firing cannons to kill mosquitoes': Controlling 'virtual streets' and 8 words - < 1%

the 'image of the state' in Bangladesh", Contributions to Indian Sociology, 2020

Crossref

134	N Varma T, Khan D A. "Information technology and e-risk of supply chain management", African Journal of Business Management, 2015 Crossref	8 words — <	1%
135	airwebworld.com Internet	8 words — <	1%
136	archiveofourown.org Internet	8 words — <	1%
137	bspace.buid.ac.ae Internet	8 words — <	1%
138	collegecounseling.org	8 words — <	1%
139	currentliner.com Internet	8 words — <	1%
140	dsc.duq.edu Internet	8 words — <	1%
141	www.apc.org Internet	8 words — <	1%
142	www.broadwaymag.com Internet	8 words — <	1%
143	www.claasfamily.com Internet	8 words — <	1%

144 www.fareham.gov.uk

		8 words — <	1%
145	www.hrw.org Internet	8 words — <	1%
146	www.metafilter.com Internet	8 words — <	1%
147	www.primeuniversity.edu.bd	8 words — <	1%
148	www.slideshare.net Internet	8 words — <	1%
149	www.state.gov Internet	8 words — <	1%
150	Kimberley R. Allison, Kay Bussey, Naomi Sweller. "Fair Game: The Effects of Target Identity, Attack Topic and Role-Relevance in the Judgement of Onli Aggression", International Conference on Social Me Society, 2020 Crossref		1%
151	nrl.northumbria.ac.uk Internet	7 words — <	1%
152	"Intelligent Data Analytics for Terror Threat Prediction", Wiley, 2021 Crossref	6 words — <	1%
153	Ashiquddin Mohammad Maruf, Md Rabiul Islam, Bulbul Ahamed. "Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies", University Journal of Law, 2014	6 words — < Northern	1%



Balsing Rajput. "Cyber Economic Crime in India", Springer Science and Business Media LLC, 2020 Crossref $_{6 \text{ words}}$ - < 1%



Debarati Halder, K. Jaishankar. "chapter 4 Women's 6 words — <1% Rights in the Cyber Space and the Related Duties", 6 IGI Global, 2012

Crossref

EXCLUDE QUOTES

OFF

EXCLUDE MATCHES

OFF

EXCLUDE BIBLIOGRAPHY ON