Digital Criminality: An Ethnographic Perspective on cyber-crimes in Pakistan

By Sadaf Qayyum

Reg No: 02011913005

Department of Anthropology

Quaid-i-Azam University

Islamabad, Pakistan

2022

Digital Criminality: An Ethnographic Perspective on cyber-crimes in Pakistan

By Sadaf Qayyum

Thesis submitted to the Department of Anthropology, Quaid-i-Azam University Islamabad, in partial fulfilment of the Degree of Master of Philosophy in Anthropology

Department of Anthropology

Quaid-i-Azam University

Islamabad, Pakistan

2022

Formal Declaration

I hereby declare that this thesis titled 'Digital criminality: An Ethnographic perspective on cyber crimes in Pakistan' is the result of my individual research. Any ideas taken directly or indirectly from third party sources are appropriately indicated as such.

I also declare that this work has not been published or submitted to any other university/degree in a similar form.

I am solely responsible for the content of this thesis, owning the sole copyrights of it.

_____

Sadaf Qayyum

Islamabad, February 2022

Quaid-i-Azam University, Islamabad

(Department of Anthropology)

Final Approval of Thesis

This is to certify that we have read the thesis submitted by Ms. Sadaf Qayyum. It is our judgment that this thesis is of sufficient standard to warrant its acceptance by the Quaid-i-Azam University, Islamabad for the award of the Degree of M.Phil in Anthropology.

Committee:

1. Dr. Aneela Sultana
   Supervisor

2. Dr. Saif-ur-Rehman Saif Abbasi
   External Examiner

3. Dr. Aneela Sultana
   In-charge
   Department of Anthropology

Digital criminality: A Netnographic perspective on cyber crimes in Pakistan

BY

SADAF QAYYUM

Reg No: 02011913005

Approved by

_____

Dr Aneela Sultana(Head of Department and Supervisor)

External Examiner

_____

Endorsement

It is stated that the current research titled — Digital criminality: A Netnographic perspective on cyber crimes in Pakistan-submitted by Sadaf Qayyum, Reg No 02011913005, has been duely accepted and acknowledged by the Department of Anthropology, Quaid e Azam University, Islamabad. This thesis has been accepted in the pursuit of fulfilment of the partial requirement for the degree of Masters of Philossophy in Anthropology.

_____

Dr. Aneela Sultana

Head of Department,

Department of Anthropology,

Quaid e Azam university, Islamabad

Acknowledgements

All praises to Allah for blessing me with the strength and motivation for the completion of this thesis. This thesis was a result of consistent hard work but it could not have been initiated, carried through and completed successfully without the personal and professional support of many individuals. I am indebted to each of them for their particular contribution to the research. I want to appreciate the support of my friends, family and teachers. This research thesis would not have been possible without their constant support. First of all, I would like to thank Dr. Aneela Sultana for choosing to take me under her supervision. She provided me with an opportunity to work in the field of my interest and supported me in every way possible. Dr. Sultana's faith in me has led me to successfully complete this research in time. I would like to show gratitude towards my friends for the amount of love and emotional support they provided me with. I am highly indebt of my respondents who have opened up to me and provided me with the painful insights of their experiences. They generously took time out of their schedules to participate in my research and made this study possible. I would like to mention ' Gender Interactive Alliance (GIA)', an organization that helped me approach a few of my respondents. The executive director, Bindiya Rana, was very forthcoming in this regard. Most importantly, I would like to mention my Mamo, Muhammad Tahir, who provided me with the agency to independently work in the field of Anthropology and pursue my interest area. A special thanks to Ibrahim, Maryam, Mishayam and Summayya for keeping me motivated and believing in me. At the end, I would like to acknowledge myself for being consistent and passionate enough to have completed this research in time for the pursuance and completion of the degree of masters of philosophy in Anthropology.

Sadaf Qayyum

Dedication

This thesis is dedicated with affection and utmost regard to my beloved Mamo, ***Muhammad Tahir****, who has been my biggest support. He has played the role of a mother, a father, a brother and a friend. It was his unwavering support and unconditional love that has made me to be the person that I am today.*

List of Abbreviations

PTSD	Post traumatic stress syndrome
GIA	Gender Interactive Alliance
FIA	Federal Investigation Agency
LGBTQ	Lesbian, Gay, Bisexual, Transgender, Queer
GBV	Gender Based Violence
UN	United Nations
IT	Information Technology
VAWG	Violence Against Women and Girls
NR3C	National Response Centre on Cyber Crime
DRF	Digital Rights Foundation
PECA	Prevention of Electronic Crimes Act

ABSTRACT

With the rise of technological expansion, the world is changing at a rapid pace by disrupting the social fabric through manipulating the desires of a vast majority to pursue the false ideals of modernity and leaving the remaining half alienated and isolated waiting for their turn to get modernized. The concept of modernization by means of technology has long been debated and remains contested to the present day. Speculations of digital dictatorship to the doubts of intimate selves being exposed through massive digitalization indicate a bigger political, social and moral catastrophe that awaits mankind. This thesis is a qualitative study, which attempts to fill the gap left behind by generalized studies on digital crimes. This study focuses on the experiences of victims of cyber violence emanating from cyber crime and the socio-psychological impacts on the victims and their subsequent coping mechanisms. It seeks to explore the nature of cyber violence and possible motives of the perpetrators behind such crimes. In addition, it incorporates the victim's perspective on digital abuse and their coping mechanisms. The sample included men, women and trans-gender people from different backgrounds. The data was collected through digital fieldwork, using netnography as the main method of research. The research was carried out using the technique of semi-structured conversational interviews, that helped getting a better understanding of the topic at hand. The study's main findings indicate that digital world is brimming with crimes such as verbal abuse, stalking, threats and revenge pornography. In addition, crime syndicates such as beelas now operate through the internet. Economic crimes are also a major problem faced by numerous individuals. These crimes were identified and the resultant socio-psychological impacts were imminent. The victims faced social isolation, victim blaming, depression, anxiety and sometimes suicidal tendencies accelerated. The research also emphasizes the distinctive individual

experience and the coping mechanisms of victims. This research thesis concludes with certain recommendations provided by the victims coupled with the researcher's own analysis.

Table of Contents

List of Figures and Tables

1.Introduction

1.1 Setting the Research Context

"Unless and until our society recognizes cyber bullying for what it is, the suffering of thousands of silent victims will continue." ___**Anna Maria Chavez**

Crime is an unlawful and punishable offence inflicted to cause harm to someone. It includes numerous offences such as murder, rape, theft, and torture etc. The history of crime is as old as human existence is. However, it has shape shifted into various realms and has morphed into numerous perilous avatars. Among these shades of crime, Cyber crime has become a sharp edge of technology which has been fastidiously used to inflict pain, torture and agony to the victims. This evolution in crimes is primarily because of the human evolution in technology. As technology grew, humans got connected to each other and the contraction of time and space lead the world to become an interconnected virtual space. The virtual world has provided space for numerous positive and prosperous endeavours; however, at the same time, it has enabled the malignant elements of the society to grow robust. At this juncture, technology is the biggest blessing and an inevitable bane of the twenty first century.

In order to grasp an idea of what cyber crime is and how it affects people, one needs to define cyber crime first. Cyber crime can be defined as the crime committed on the internet using tools such as computer and smart phones. It is arduous to exactly draw a line as to what cyber crime is because new crimes surface quite often. In cyber crimes, a computer and a victim are involved and are identified as targets and victims. Computer can be a tool or a target. Simply put, when an offender uses it to target a certain victim it becomes a tool. Similarly, when an offender targets a

specific computer to access the data of that computer it becomes the target of that offence (Dashora, 2011).

There are certain types of internet-related crimes that are defined by United Nations. United Nations office on crime and drugs define numerous clusters of digital crimes: i) offences against the confidentiality, integrity and availability of computer data and systems; ii) computer-related offences; iii) content-related offences; iv) offences related to infringements of copyright and related rights (UNODC).In a general division, cybercrime is described as having digital space-dependent offences, digitally-enabled offences and, as a specific crime-type, online child sexual offence and abuse. This classification encompass a broad spectrum of digital offences perpetrated by numerous individuals using cyber space as a tool to further their malignant agendas. Social media is now a vector for youth violence and it has morphed the landscape for aggressive behaviour (Peterson & Densley, 2017). This electronic aggression takes up numerous forms of cyber violence that not only violate victim's personal space but also leave them with traumatic experiences. The perpetrators of cyber violence are mostly those who do in person violence and are now using social media as a tool to further their violent endeavours. Terror groups, hate groups, illicit sexual service seekers, paedophiles and sexual predators can equally access their potential victims. The perpetrators of cyber violence have added new forms of violence that occur exclusively online. (Peterson & Densley, 2017). Some authors view this cyber violence or offences as "old wine in new bottles" (Grabosky, 2001).

Studies suggest four types of cyber crimes that exist in cyber culture: deception/theft, pornography, violence and cyber trespass (Peterson & Densley, 2017). In this particular research the researcher is taking up the realm of 'cyber violence', the term introduced by Holt (Holt, 2021). This research narrows down to the aspect of cyber violence that is inflicted upon women,

trans-genders(Gender fluid orientations) and men. This includes cyber dating experience, cyber harassment, blackmailing, revenge porn and other kinds of psycho-symbolic violence. The violence against women is usually termed as cyber violence against women and girls(Cyber VAWG).

Cyber security threat has seen exponential rise in the past ten years. Cyber violence has been defined as “the use of computer systems to cause, facilitate, or threaten violence against women and girls that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering, and may include the exploitation of the individual’s circumstances, characteristics or vulnerabilities. The internet has provided ample opportunity to stay anonymous, while simultaneously allowing deep access into the privacy of its users. "This violence has further increased exponentially during the Covid-19 crisis." (Dorokhova, vale, Laçí, & Mahmutovic, 2021). It happened because the world went under a lockdown and people had ample time at their hands to indulge into the digital world.

Similarly, it can be understood by relating it to the fact that domestic violence is most often linked to the use of digital ways to stalk, track and harass female victims. Through cyber space, the victim of domestic violence can often be further pressurised, intimidated, controlled, followed, harassed and bullied into compliance through technological means. The consequent harm this causes to the victims is witnessed at emotional, psychological and often physical levels. More than often, the victims feel trapped and find no safe space to retreat. This predominantly adds to feelings of despair, humiliation, and fright in victims of domestic violence, intimate partner cyber harassment furthermore is “demonstrably a strong and unique predictor of both depression and PTSD, even in the absence of physical violence.” (King, 2017).

Cyber violence can lead to the further perpetration of transnational crimes with serious human rights implications. Connections made in cyberspace and the use/abuse of social media networks are among the most commonly used tools for human traffickers to entrap victims into sexual exploitation schemes through various manipulation tactics.

1.2 Statement of the Problem

Undoubtedly, the phenomenon of Cyber crime has been explored at large in literature. It has been studied under different perspectives. From online child abuse to sexual harassment of women, violating trans people, threatening men, verbal abuse and stalking etc.

The many forms of cyber violence stem from the fact that these crimes are often culturally accepted practices. These violent practices emanate from the inherent supremacy of patriarchal structures existing in society, which not only affect women and trans people but also men . The violence that is directed against an individual because of one's gender, affecting them disproportionately, must be deemed gender-based violence (GBV).

Cyber violence, in its most rampant forms, includes direct violence in the form of digital or online harassment; online sexual abuse or offence; digitally perpetrated defamation; cyber stalking and surveillance/ tracking; hacking; impersonation; identity theft; photographs based abuse; Blackmailing; Revenge porn; cyber bullying and many other forms of abuse. (Dorokhova, vale, Laçí, & Mahmutovic, 2021)

There is no doubt that the phenomena of cyber violence has been explored in literature from various perspectives. However, there are the dimensions, contexts, and specific corners that are left unexplored. Most often, the researchers deal with cyber crime as an act of crime committed

only by strangers while completely ignoring the fact that many a time the perpetrators are intimate partners, lovers or family members. The use of digital platforms for abuse can range from online violence, verbal abuse, (sexual) harassment, sexting, revenge-porn, image-based abuse, stalking and tracking, all the way to human trafficking and child sexual exploitation and abuse. Cyber violence thereby also acts as an enabling tool leading to the perpetration of a variety of further crimes, with serious human rights consequences; for instance, crimes of passion, use of revenge porn to destroy their social image and prestige etc.

This research aims at studying cyber crimes which are specifically related to women. It offers an advanced perspective as to how women and trans-genders and men in Pakistan get violated digitally. It looks into the tools and most often used types of cyber violence against individuals. In addition, This study explores the social and psychological impacts of cyber violence on the victims and how they adapt using certain coping mechanisms.

Pakistani has a heterogeneous but very closed culture where incidents like these are stereotyped and discouraged to be talked about. In closed societies, cultural barriers often prevent individuals to take up space and discuss taboos. The specific cultural values often determine nature of the crime and how people deal with it. (Kottak, 2015). This study tends to unfold this phenomenon in a purely Pakistani context. It positions different genders in the cultural context and then delves into further exploring the nature and impacts of digitally facilitated crimes and inflicted violence against individuals.

At the end, this study seeks to expound upon the possible solutions to this digitally-facilitated violence including victim's perspective in a context specific to Pakistan.

1.3 Research Questions

Taking into account the aim of this research, the Researcher has formulated two research questions:

1. What are the experiences of victims of cyber violence emanating from cyber crime?

2. What are the socio-psychological impacts on the victims and their subsequent coping mechanisms ?

1.4 Research Objectives

1- To explore the nature of cyber violence and possible motives of the perpetrators behind such crimes.

2- To understand and highlight the social and psychological impacts of cyber violence on individuals.

3- To incorporate the victim's perspective on digital abuse and their coping mechanisms.

1.5 Significance of the Study

A plethora of various researches have been conducted on the issue of cyber crime or digital offences, internationally and locally. All these researches ponder upon various aspects of this crime. It is high time that these crimes are operationalized to understand the nature and facets of cyber violence emanating from cyber crime in Pakistan.

This research would plays its part in achieving this understanding. It holds significance as it would add another perspective to the already existing research.

First of all, it aims at fulfilling the gap in the existing literature that encapsulates cyber crimes and its consequent impacts on people. This research thesis also provides an emic perspective into the very phenomenon of cyber violence inflicted through cyber crimes. In addition, this research provides with a reflexive context to let the readers grasp the possible biases of the researcher. This reflexivity would help other researchers to grasp a less value-laden view of the said topic.

Previous researches quantify the phenomenon of cyber violence into a crime based on the use of technology. These researches fall short in addressing the subjective experiences of cyber crime victims and the coping mechanisms used to pacify the torture. This research not only adds a subjective element but also a native Pakistani perspective to it.

This research delves into the details of social and psychological impacts of the said phenomenon and provides with an overview of how the victim scope with this. It uses different case studies to show the experiences of different genders and age groups. It provides a detailed, in-depth perspectives of the cyber crime victims and documents their experiences along with the provision of reflexive subjectivity.

This thesis research holds significance because of the fact that it is a Netnography and uses the same technology to access the victims which is used to inflict offence on the victims. Netnography is an effective tool to understand and unfold the crimes in digital spaces. It lays out a framework for future reference as well. Additionally, it can be used as a reference in the contexts of cyber bullying, cyber violence and cyber crimes.

It would also be helpful in policymaking on cyber crimes, as it adds a subjective perspective of the victims and addresses their privacy concerns.

1.6 Operationalization of the Key Yerms

This research includes certain concepts which are an essential part of this research thesis. These key concepts or terms used in the study are first conceptualized and then operationalized down below:

1.6.1 Cyber Crime

Cyber crime[1] can be defined as a criminal activity (such as fraud, theft, or distribution of child pornography) committed using a computer especially to illegally access, transmit, or manipulate data. Cyber crime is the most advance and perhaps the most perplexing bane among the witches' brew of problems brought about by the cyber world. “Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime” “Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime” (Dashora, 2011).

In this particular research thesis, the term cyber crime tends to encompass the technology-facilitated crimes perpetrated to inflict violence, offence, psychological, emotional and symbolic trauma to women, trans-genders and men. These crimes may take up physical form subsequently.

1.6.2 Cyber Space

The world of twenty first century is replete with technology. These technologies have created a new frontier, commonly known as “cyberspace.” The term “cyberspace” first appeared in

[1] Merriam-Webster. (n.d.). Cybercrime. In *Merriam-Webster.com dictionary*. Retrieved November 28, 2021, from https://www.merriam-webster.com/dictionary/cybercrime

Neuromancer, a science fiction novel, by William Gibson (1984) who referred to it as a consensual hallucination (Berson, 2008). It describes an intangible, nonmaterial location or dimension created by computer systems to which people gain access, allowing them to communicate with one another via e-mail or engage in research etc. The movement involved in this type of activity requires pressing keys on a keyboard, moving a mouse, or voice commands. Some computer programs consist of games that are designed to give the user an experience that resembles physical reality; in virtual reality, for instance, the user is presented with feedback affecting the sensory systems such that occurrences in cyberspace feel real. (Chisholm, 2006).

This research determines cyber space as text messages, phone calls, emails, and social media apps(Instagram, Twitter, Facebook, snapchat, VChat, Signal, Telegram, Skype, and Tiktok, etc). Any technological tool which can be used to inflict harm to victim is taken under the umbrella of Cyber space.

1.6.3 Cyber Violence

Cyber violence is usually understood as a completely separate phenomenon to 'real world' violence, when in fact it is more appropriately seen as a continuum of offline violence. For example, cyber stalking by a partner or ex-partner follows the same patterns as offline stalking and is therefore intimate partner violence , simply facilitated by technology. Studies substantiate this continuum: a UK study of cyber stalking found that more than half of cases involved a first encounter in a real-world situation. Similarly, data from the 2014 survey shows that 77 % of women who have experienced cyber harassment have also experienced at least one form of sexual or/ and physical violence from an intimate partner; and 7 in 10 women (70 %) who have

experienced cyber stalking , have also experienced at least one form of physical or/and sexual violence from an intimate partner . (EIGE, 2019)

In this Research, Cyber violence is taken up as a phenomenon of inflicting trauma to individuals online. This violence can be exclusively digital or it can stem from in-person violence and merge into cyber space; for instance, uploading videos of torture and abuse on the internet. This would add to the already caused physical, psychological, emotional and symbolic trauma. It further deteriorates the emotional state of victims. This research aims at encapsulating the experiences and coping mechanism of victims.

1.6.4 Cyber Criminals

In general view cyber criminals are identified in literature. These perpetrators of cyber crimes constitute of various categories. This division may be justified on the basis of the object that they have in their mind. The following are the category of cyber criminals: Children and adolescents between the age group of 6 – 18 years; organised hackers; professional hackers; and Discontented employees. (Dashora, 2011).The delinquent behaviour pattern in children emerges to try and know about things and to put on a cool label. On the other hand, organised hackers try to achieve a certain set objective which might be politically, sexually, economically or fundamentally motivated. The Pakistanis are said to be one of the best quality hackers in the world. The NASA as well as the Microsoft sites is always under attack by the hackers. Similarly, professional hackers are those whose only motivation is money. Discontented employees include those people who have been either sacked by their employer or are dissatisfied with their employer.

This is a broader definition and categorization of digital criminals; however, the context used in this research is quite different. This research thesis takes up criminals whose sole purpose is to inflict harm and danger to individual subjects. They can be organised hackers, family members, friends, co-workers, Beelas(in case of Trans people) and to name a few.

1.6.5 Cyber Culture

Cyber culture[2] is defined as, "A set of shared attitudes, practices, and goals associated with the world of computers and the Internet." (Meriam Webster). Unlike societal culture, Cyber culture is very fluid and rapidly changing. However, it does include certain shared attitudes, practices and goals. Personalities, applications, websites, digital contact portals and data bases make up cyber culture. This research incorporates the general behaviour and attitudes of cyber citizens towards the content and activities in cyber space.

1.6.6 Cyber Citizen

Cyber citizens[3] are generally called 'Netizen'. Neitzen are active participants in the online community of the Internet (Meriam Webster). This study takes up cyber citizens as all those individuals who engage in the cyber world in any form. Anyone having contact with the internet and is an active member of the cyber community is a cyber citizen. It includes both victims and criminals.

---

[2] Merriam-Webster. (n.d.). Cyberculture. In *Merriam-Webster.com dictionary*. Retrieved November 28, 2021, from https://www.merriam-webster.com/dictionary/cyberculture

[3] Merriam-Webster. (n.d.). Cybercitizen. In *Merriam-Webster.com dictionary*. Retrieved November 28, 2021, from https://www.merriam-webster.com/dictionary/cybercitizen

2. Literature Review

This chapter of the research thesis expounds upon the core variables of the said topic from existing literature to further develop a theoretical and analytical understanding of the research framework. This literature starts off with the basic understanding of core ideas through literature and then goes toward the historical placement of the topic. This chapter provides with a general orientation of cyber crimes first and then it takes up the case of Pakistan. It further delves into the history of Cyber violence against women, men and trans-genders.

2.1 Crime

In Lexicon, the term crime comes from the Latin word 'crimen' which means offence and refers to a wrong-doer. Crime is usually defined as an offence against public. It includes all acts of violence perpetrated to inflict harm to people and t violate laws of the state. These acts are highly denounced by the society and are legally admonished by the state structure. Violations such as these are punishable under law in the form of imprisonment or fine. These violations or offences include: murder, rape, theft, and failure to pay taxes etc. Usually, it is considered that criminal behaviour is deviant and antisocial in nature (Thotakura, 2014). Various societies define crime in a different light and a unique perspective. Crimes follow a continuum from a legal end to an illegal end, where culture determines the nature of illegal crimes branding these acts of crimes as 'folkways' and 'mores' and then goes on to decide the punishments as well (Kottak, 2015). For instance, cultures stereotype certain behaviours and then those behaviours are deemed unacceptable. It may result in abandoning, ousting, name calling, pressurising and branding as deviant. On the other hand, there are crimes which come under the legal umbrella but are not punishable: crimes under self-defence.

As per research, no individual is born a criminal; however, the situations around an individual determine if they would become criminals. There are several causes which make an individual turn into a criminal. Then primary precursors of crime include social, psychological, biological and geographical causes. (Klimczuk, 2015). Social cause might include, family disorganization, upbringing of the individual, defective education, hype created by media, drinking and drug use, unhappy marriages and dowry system, family planning, and social disorganization etc (Thotakura, 2014). Similarly, the economic cause of crime include: poverty, unemployment, rapid industrialization and urbanization etc. The psychological causes are intellectual weakness, mental diseases, and inherent personality flaws etc. In addition, there are certain biological precursors such as age, gender, hormones, etc. (Klimczuk, 2015)

2.1.1 Types of Crimes

There are numerous types of crime based on the medium or subject which is being affected, crimes include personal crimes (murder, assault, sexual assault), property crimes(burglary, theft, arson fires, automobile theft, vandalism), victimless crimes(prostitution, illegal gambling, illegal drug use), white-collar crimes, organized crimes, juvenile delinquency, Computer crime (cyber crime, cyber terrorism, cyber warfare, harassment on the internet, spam, internet fraud), Violation of public safety (disorderly conduct, driving under influence of drinks and drugs, terrorism) (Thotakura, 2014). All these types of crime are prevalent in the society and humanity faces a witches' brew of problems emanating from these crimes. Among all these types, the only matter of concern for this thesis research is cyber crime.

2.2 Cyber Crime- A Genesis

Having expounded upon the details of crime and its types, the research must now move towards understanding the concept of cyber crime in detail.

As technology is advancing, an advancement in criminal opportunity in the form of cyber crime has surfaced. Cyber crime is distinguished from traditional crime because of the involvement of digital space in the form of computer and internet. Cybercrime is an extension of existing criminal behaviour alongside some novel illegal activities. Cybercrime includes attack on information about individuals, corporations, or governments. These attacks are perpetrated on the visual persona or body of the victim, hence, sabotaging their virtual identities. (Dennis, 2019)

It is difficult to have any precise definition of cyber crime; however, the general definitions of term cyber crime are as follows:

The oxford Dictionary defined the term cyber crime as "*Criminal activities carried out by means of computers or the Internet*."[4]

"Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime"[5]

"Cyber crime means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them"[6]

[4] ://www.oxforddictionaries.com/definition/english/cybercrime (Accessed on 8th July, 2021)
[5] http8 http://cybercrime.org.za/definition (Accessed on 8th July, 2021)
[6] http://www.naavi.org/pati/pati_cybercrimes_dec03.htm (Accessed on 8th July, 2021)

Dr. Debarati Halder and Dr. K. Jaishankar define cybercrimes 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)*. (Chaubey, 2012). Cyber crime is not novel to the world. It includes any criminal activity which undertakes the medium of information technology gadgets such as computers or internet. Cyber crime is one the most prevalent and insensitive crimes in numerous parts of the world . Not only the criminals are causing magnanimous losses to the society and the government but are also able to conceal their identity to a great extent. There are number of illegal activities which are committed over the internet by technically skilled criminals. Taking a wider interpretation it can be said that, Cyber crime includes any illegal activity where computer or internet is either a tool or target or both. (Dashora, 2011)

2.3 History dateline of Cyber Crime

Year	Agenda
1834	French Telegraph System crisis
1870	Switchboard Hack
1878	Early Telephone hackings
1903	Wireless Telegraphy sending insulting Morse code messages discrediting the invention.

1939	Military Code breaking during WWII
1940	First Ethical Hacker , Rene Carmille, finds out that the Nazis are using punch-card machines to process and track down Jews
1955	Phone Hackers
1957	Joy bubbles -the U.S.'s first phone hacker or "phone phreak."
1962	Allan Scherr — MIT sets up the first computer passwords, Allan Scherr made a punch card to trick the computer into printing off all passwords
1969	RABBITS Virus — An anonymous person installed it on a computer at the University of Washington Computer Centre. It is thought to be the first computer virus.
1970-1995	Kevin Mitnick, the most-wanted cybercriminal of the time.
1971	Steve Wozniak and Steve Jobs — Steve build a

	blue box designed to hack into phone systems
1973	Embezzlement — A teller at a local New York bank used a computer to embezzle over $2 million dollars.
1981	Cybercrime Conviction — Ian Murphy, aka "Captain Zap," hacks into the AT&T network. He is the first person convicted of a cybercrime.
1982	The Logic Bomb — The CIA blows up a Siberian Gas pipeline without the use of a bomb or a missile by inserting a code into the network and the computer system in control of the gas pipeline.
1984	US Secret Service — The U.S. Comprehensive Crime Control Act gives Secret Service jurisdiction over computer fraud.
1988	The Morris Worm — Robert Morris creates what would be known as the first worm on the Internet
1988-1991	Kevin Poulsen -the manhunt for a hacker
1989	Trojan Horse Software - destructive program masquerading as a benign application.

1994	Data stream Cowboy-a password “sniffer” installed onto networks
1995	Vladmir Levin — Russian software engineer hacked into Citibank’s New York IT system and did fraudulent transactions
1998-2007	Max Butler — hacked U.S. government's websites
1999	NASA and Defense Department Hack-Systems were shut down for three weeks.
1999	The Melissa Virus — A virus infects Microsoft Word documents, automatically disseminating itself as an attachment via email
2000	Mafiaboy — 15-year-old Michael Calce, attacked Amazon, CNN, eBay and Yahoo!
2002	Internet Attack — By targeting the thirteen Domain Name System (DNS) root servers
2003	Operation Cyber Sweep — The U.S. Justice Department announces more than 70 indictments and 125 convictions or arrests for phishing, hacking, spamming and other

	Internet fraud as part of Operation Cyber Sweep.
2003-2008	Albert Gonzalez —a Shadow Crew that stole and then sold card numbers online
2005	Polo Ralph Lauren/HSBC –card information was stolen during a security breach at a U.S. retailer (Polo Ralph Lauren).
2006	TJX — A cybercriminal gang stole 45 million credit and debit card numbers from TJX
2010	The Stuxnet Worm — A malicious computer virus called the world's first digital weapon is able to target control systems used to monitor industrial facilities. It is discovered in nuclear power plants in Iran, where it knocks out approximately one-fifth of the enrichment centrifuges used in the country's nuclear program.
2010	Zeus Trojan Virus — An Eastern European cybercrime ring stole $70 million from U.S.
2009-2013	Roman Seleznev —hacked into more than 500 businesses and 3,700 financial institutions in

	the U.S
2013-2015	Global Bank Hack —Russian-based hackers gained access to sabotage more than 100 institutions around the world.
2013	Credit Card Fraud Spree — In the biggest cybercrime case filed in U.S. history
2014-2018	Marriott International — A breach occurs on system and the thieves steal data on approximately 500 million customers.
2014	eBay — A cyberattack exposes names, addresses, dates of birth, and encrypted passwords of all of eBay's 145 million users.
2016	Democratic National Committee emails are leaked to and published by Wiki Leaks prior to the 2016 U.S. presidential election.
2017	Equifax, one of the largest U.S. credit bureaus, got hacked, exposing 143 million user accounts.
2018	Dubsmash - The popular video streaming platform discovered 161.5 million user records were placed for sale on the dark web. Records included details like name, email address, and

	encrypted passwords.
2019	- Alibaba - A telemarketing employee privately obtained 1.1 million pieces of data including Alibaba client contact information and leaked it. - Facebook - Information relating to more than 530 million Facebook users got exposed by an unknown hacker including phone numbers, account names, and Facebook IDs.
2020	- Sina Weibo - 538 million users' information stolen from Sina Weibo, the Chinese equivalent of Twitter, and circulated on the dark web. -Fire Eye, a prominent cyber security firm, announced they were hacked
2021	-Colonial Pipeline - a ransom-ware attack -Accenture crisis, when a ransom-ware gang breached Accenture's networks, encrypted files and demanded $50 million to avoid having their encrypted files sold on the dark web.

Table 1 (Herjavc, 2021)

2.4 Types of Cyber Crime

Cyber crime comes in numerous shapes and forms, the use of computer or technology as a tool for orchestrating unlawful acts spread across a spectrum including various types. It usually involves a conventional crime that is morphed into a digital crime by using informational technology(IT). A few types of cyber crimes are discussed below:

2.4.1 Cyber Pornography

The Oxford Dictionary defines Pornography as "*printed or visual material containing explicit description or display of sexual organs or activity intended to stimulate sexual excitement*".[7]

Further, the Black's law dictionary defines Pornography as "*Lewd and lascivious materials depicting erotic images, designed to arouse sexual desire*".[8]

In simple words, cyber pornography can be described as using the cyber space to create, display ,spread, import or publish pornographic or lewd content. It all started off with the advent of information technology and internet, that allowed easy access to everything. The subsequent cyber space, created as a result of internet, supplanted most of the traditional pornographic content with digital pornography. There is no legal definition of pornographic content. It is loosely defined primarily because of the culturally distinct understanding of obscenity. Each culture has a different understanding of what is sexually or morally right and wrong. There is no uniform standard. Numerous things are branded obscene and banned in certain cultures; whereas, the same things are celebrated in other cultures. (Chaubey, 2012). Obscenity and pornography are different but related terms. Obscenity is defined as culturally inappropriate display of nudity

[7] https://en.oxforddictionaries.com/definition/pornography

[8] https://dictionary.thelaw.com/pornography

and lewdness, primarily determined by cultural norms and values. On the other hand, pornography is an agenda based content creation for inciting sexual pleasures. It has taken up the form of an industry. Porn industry in undisputedly one of the largest industries in the world. According to BBC, 37% of the internet is made up of pornographic material as per a report published in 2010. Covid-19 and the global lockdown has increased the consumption of pornography up to 95% in some counties such as Spain. The overall consumption of pornography saw a huge increase in this period. [9]

There is a thin line between the entertainment industry and using cyber space as a tool to inflict harm to people in the form of child pornography, revenge porn or doctored pictures. Blackmailing, threatening and to name a few. Child pornography is defined as, "*any portrayal, by whatever methods, of a child occupied with genuine or mimicked express sexual exercises or any portrayal of the sexual parts of a kid for principally sexual purposes.*' (Arora & Sharma, 2018). Similarly, revenge pornography, or coerced/non-consensual usage of sexually explicit material, has introduced a new form of cyber crime. In the pursuit of this offence, the perpetrators target the sexual bound integrity of the victims by making one's private or sexually explicit content public. Resultantly, the victim's sexual integrity and identity is gravely affected. (Šepec, 2019).

2.4.2 Stalking Through Computer

Stalking refers to behaviour of harassing or threatening the other person, often obsessively. Among numerous types of stalking, on is called Cyber Stalking. It is an extension of physical form of stalking; however, it transcends into the cyber world where identities are then

[9]Zattoni, F., Gül, M., Soligo, M. et al. The impact of COVID-19 pandemic on pornography habits: a global analysis of Google Trends. Int J Impot Res (2020). http://sci-hub.tw/10.1038/s41443-020-00380-w

compromised. In cyber stalking the internet, e-mail, chat rooms etc. are used to stalk another person. It includes harassment through e-mails. It is very similar to harassing through letters. For instance, former boy/girl friend sending mails constantly sometimes emotionally blackmailing and also threatening . This is a very common type of harassment via e-mails which also includes sending pornographic images and obscene messages. Similarly, making of false accusations or statements of fact (as in defamation), monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information that may be used to harass. (Dennis, 2019). Stalking is a continuous process, which includes a number of actions, each of which may be entirely legal in itself. According to Professor Lamber Royakkers , *"Cyber stalking is the repeatedly harassing or threatening of an individual via the internet or other electronic means of communication. A cyber stalker is someone with amorous and/or sexual motives who constantly harasses someone else electronically: via the bulletin board, chats box, email, spam, fax, buzzer or voice-mail. Stalking generally involves the constant harassment or threatening of someone else: following a person, appearing at someone's house or workplace, making harassing phone calls, leaving written messages or objects, or vandalizing someone's property. Because the stalking activities are so diverse and have to be seen in their connection it is difficult to give a precise description of stalking.*" [10]

Sometimes the offender doesn't invade the private space of the victim but harasses her through the global medium publically. For example, posting the phone numbers and email address of the victim on porn sites and publicising morphed photos of the victim on cyber space and threatening them. Perpetrators often chase the activity and followers of a specific person, might hack accounts, post false information and lewd stuff. Stalking is as old as humanity itself;

[10] http://www.sociosite.org/cyberstalking_en.php

however, it has shape shifted into the new cyber world. Erstwhile, it was done th ugh accessing former friends, employees and acquaintances turned nemesis etc. Since the advent of IT, the reach of stalkers is widened. Anyone can cyber harass anyone beyond time and space. Most of the stalkers are the dejected lover's, ex-boyfriends, colleagues, who failed to satisfy their desire and wants to harass the victim. Most stalkers are men and most victims are women. The common reason behind the cyber stalking is rejection in love or one sided love, harassment, revenge and show off by the offender. (Chaubey, 2012).

2.4.3 Cyber Terrorism

Cyber-terrorism refers to specified and targeted efforts made with the intention of terrorism. It is an emerging threat that has the potential to cause serious damage. Cyber-terrorism is often associated with loss of life, perpetrated through intimidation or coercion that is brought about by cyber-terrorism.[11]

2.4.4 Hacking

Hacking is among one of the most dangerous and grave cyber crimes. It refers to getting into another's computer without permission. Gaining unlawful and unauthorized entry into a computer belonging to another is hacking. It is equivalent to phone-tapping. Hackers see the weakness in the target computer programme and then find ways to enter and access therein. (Goldsmith & Brewer, 2014)

2.4.5 Defamation

It is an act of imputing any person with intent to lower the person in the estimation of the right thinking members of society generally or to cause him to be shunned or avoided or to expose

[11] Dr. Sirohi M. N., Cyber Terrorism and Information Warfare, Alpha Editions Delhi

him to hatred, contempt or ridicule. Cyber defamation is not different from conventional defamation except the involvement of a virtual medium.

2.4.6 Trafficking

Trafficking may assume different forms. It may be trafficking in drugs, human beings, arms weapons etc. These forms of trafficking are going unchecked because they are carried on under pseudonyms. For instance, a racket was busted in India where drugs were being sold under the pseudonym of honey. (Chaubey, 2012)

Such and numerous other types of cyber crimes are highly prevalent in today's society. Having said that, this research would now move towards understanding cyber violence against different subjects.

2.5 Cyber Crime against women

In 2015, APC developed the following definition of technology-related violence against women as encompassing:

> *Acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information and communication technologies (ICTs), such as mobile phones, the Internet, social media platforms, and email* (APC, 2018).

There are various forms of cyber Violence against women and girls(VAWG), including, but not limited to, cyber stalking, non-consensual/revenge porn, gender-based slurs and harassment, slut-shaming[12], unsolicited pornography, sextortion[13], rape and death threats, doxing[14], and

[12] The action or fact of stigmatizing a woman for engaging in behaviour judged to be promiscuous or sexually provocative.
[13] The practice of extorting money or sexual favours from someone by threatening to reveal evidence of their sexual activity.
[14] Doxing is the act of revealing identifying information about someone online, such as their real name, home address, workplace, phone, financial, and other personal information. That information is then circulated to the public — without the victim's permission.

electronically enabled trafficking. Among these the most prevalent are cyber stalking, cyber harassment and non-consensual pornography.

Cyber stalking is chasing someone through means of email, text (or online) messages or the internet. It involves repeated incidents, which may or may not individually be innocuous acts, but combined undermine the victim's sense of safety and cause distress, fear or alarm. For instance, sending emails, text messages or instant messages that are offensive or threatening, posting offensive comments about the respondent on the internet. (Impe, 2019)

Similarly, cyber harassment would include unwanted sexually explicit emails, text messages, Inappropriate or offensive advances on social networking websites or internet chat rooms, threats of physical and/or sexual violence by email, text messages, hate speech, meaning language that denigrates, insults, threatens or targets an individual based on her identity (gender) and other traits (such as sexual orientation or disability). (Al-Nasrawi, 2021) On the other hand, Non-consensual Pornography, also known as cyber exploitation or 'revenge porn', involves the online distribution of sexually graphic photographs or videos without the consent of the individual in the images. The perpetrator is often an ex-partner who obtains images or videos in the course of a prior relationship, and aims to publicly shame and humiliate the victim, in retaliation for ending a relationship. However, perpetrators are not necessarily partners or ex-partners and the motive is not always revenge. Images can also be obtained by hacking into the victim's computer, social media accounts or phone, and can aim to inflict real damage on the target's 'real-world' life (such as getting them fired from their job). (Impe, 2019)

'Cyber violence against women is an act of gender-based violence perpetrated directly or indirectly through information and communication technologies that results in, or is likely to

result in, physical, sexual, psychological or economic harm or suffering to women and girls, including threats of such acts whether occurring in public or private life, or hindrances to the use of their fundamental rights and freedoms. Cyber violence against women is not limited to but includes violations of privacy, stalking, harassment, gender-based hate speech, personal content sharing without consent, image-based sexual abuse, hacking, identity theft, and direct violence. Cyber violence is part of the continuum of violence against women: it does not exist in a vacuum; rather, it both stems from and sustains multiple forms of offline violence.'[15]

2.6 Cyber Crime Against Men

Cyber crime against men is a phenomenon relatively less discussed; however, they face similar crimes in cyber world. These crimes include hacking, intellectual property rights infringement, stalking, harassment, bullying, data theft, denial of service attack, and cat fishing etc (NR3C,FIA). During a September 2020 survey it was found that 43 percent of male internet users in the United States had claimed to have been harassed online, more so than their female counterparts. The most common type of online harassment experienced by male online users was offensive name calling, whereas women were more likely to encounter sexual harassment than men.[16]Harassment often indicates personal or physical characteristics; political views, gender, physical appearance and race are among the most common. Men face offensive comments, threats to tarnish their honour, financial abuse and identity theft etc. (Pew, 2017)

[15]Opinion on combatting online violence against women, European Commission Advisory Committee on Equal Opportunities for Women and Men, April 2020

[16] https://www.statista.com/statistics/333954/us-young-internet-users-online-harassment-experiences-gender

2.7 Cyber Crime Against Trans Genders

Trans-gender is a term widely used to address cross-dressers, eunuchs, gay/lesbian, Hijra/moorat, male-woman, inter-sex and trans-sexual people.[17]

Trans people all around the globe face multitude of types of violence that includes structural, institutional, societal, and direct violence. Structural violence is inscribed in the very social structures in which trans people live, produced and maintained by ideologies of gender and sexuality and relationships of power that collude to restrain agency. One major reason is Transphobia, which can be institutional, reflected in policies, laws, and institutional practices that discriminate against transgender people. It can be societal, which is reflected in rejection and mistreatment of transgender people by others. Finally, it can manifest in interpersonal transphobic incidents and hate crimes specifically targeted at trans people. (Fedorko, 2016). Having established the grave reality of transphobia translating into different forms of violence, the research needs to expound upon internet facilitated violence against trans-genders. This online offence includes offensive comments and name-calling, targeted harassment, verbal abuse and threats, as well as sexual, sexuality and gender based harassment and abuse. Sexual, sexuality and gender-based harassment and abuse refers to harmful and unwanted behaviours either of a sexual nature, or directed at a person on the basis of their sexuality or gender identity. According to Pew Research, Trans people face almost the same harassment as do women, and in some cases even more. Digital harassment and abuse, however, affects these people psychologically and socially subsequently cementing the marginalization of an already marginalised group.

[17] https://genderinteractivealliance.wordpress.com/trans-gender-education

2.8 Cyber Crime in Pakistan

Digital harassment and cyber-bullying are rampant in Pakistan and the number of cases being reported is perpetually increasing. (DRF, 2020). The report identified 2,023 cases or 146 calls every month during 2019. Among these fifty seven percent of the complaints were women and thirty percent were me. Most of the cases reported were from Punjab. It doesn't, in any case, implies that people in other provinces do not face digital crimes. However, less reporting rate and lack of awareness contributes to the availability of myopic data. The demographic genesis of these complaints included women, men and transgender. Majority of complaints were between the ages of 21 and 25. Cyber harassment and bullying was reported on whatsapp, facebook and instagram. According to, Nighat Dad, the executive director of DRF, a research and advocacy NGO, said the organization witnessed an exponential increase in the number of cases since the corona virus pandemic and the consequent lockdown this year. “In the months of March and April, we saw an increase of 189 per cent as compared to January and February,” she said. (DRF, 2020). In 2016, Pakistan’s parliament passed the Prevention of Electronic Crimes Act (Peca), a law to curb online crimes, extremism, hatred and harassment etc. However, this law is far from bearing fruit. Reports are usually ignored and the victims face structural discrimination. Implementation of Peca is the responsibility of FIA, specifically the cyber crime wing of FIA. The unfortunate thing with this wing is that it potentially lacks human resource. In a country of 34 million internet users, the cybercrime wing has a team of only 500 individuals. Until 2018 there were only two women in the cybercrime help desk staff. (Gossman, 2020)

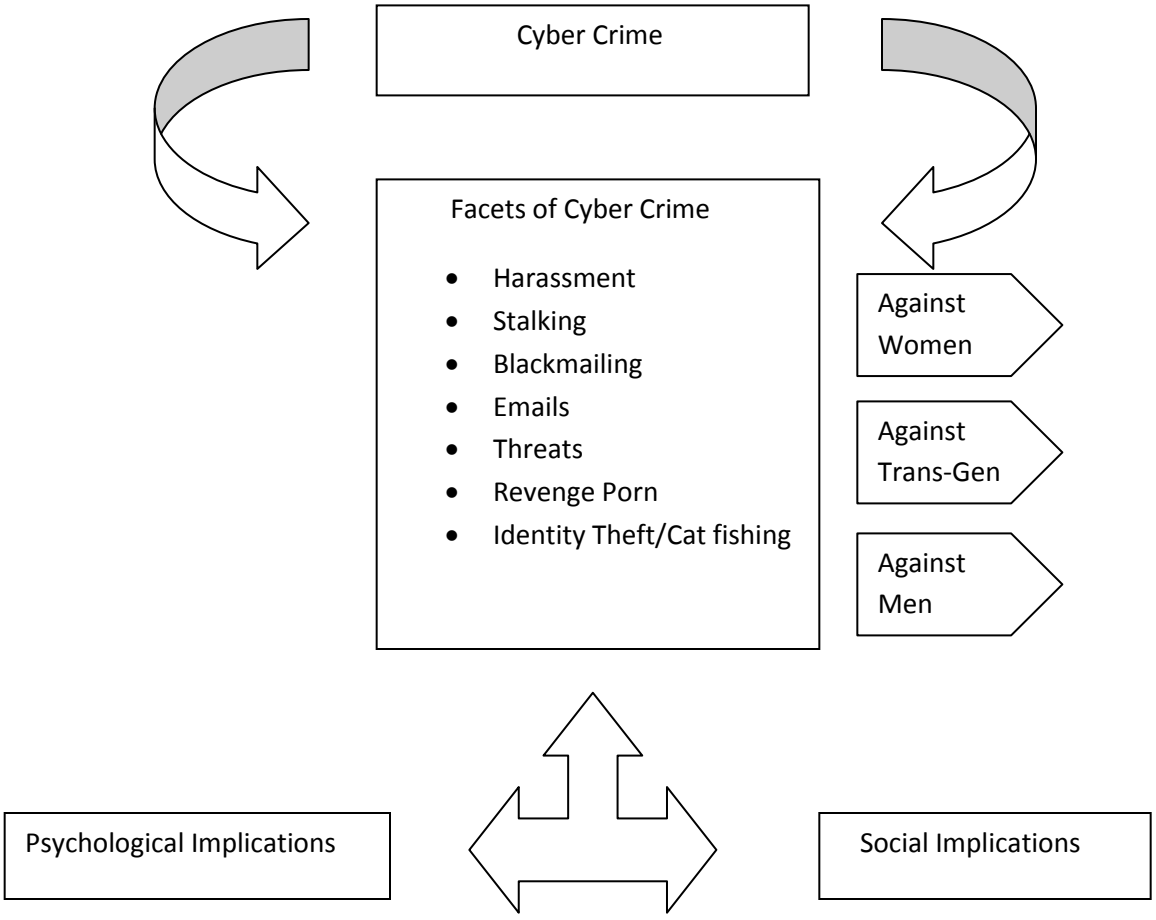
Digital crimes affect all three categories: men, women and trans people. However, women and trans people are most likely to be affected more. For instance, two trans person was gunned down by unidentified men in the khyber paktunkhwa province. They went to perform on an

event and when they were preparing to leave they were shot dead. Their peers tried to protest and those people were then digitally harassed by rape threats, threats of amputation and even murder. The most common practices of digital harassment in Pakistan include, hate speech, doxxing, accessing private data, cyber bullying, cyber stalking and revenge porn etc. (Hamara Internet(DRF), 2015). The physical abuse bills have undoubtedly provided with some air; however, digital abuse is condoned as something trivial or insignificant. The misogyny[18] ingrained in the society is unraveling in the form of hidden faces behind computers perpetrating offence against women and trans people. Here, cyber harassment is meant to include a variety of online actions: cyber stalking, bullying, trolling, intimidation, blackmail, extortion, revenge porn, and the invasion of privacy. Side by side with "real-world" violence, there is technology-related violence against women (VAW) as well — and it's now growing to epidemic proportions. (Mohsin, 2016). The most grim reality about these crimes are that they are silent killers and lead the victims toward psychological intimidation and emotional distress. Cultural constructs such as 'honour' is one of the reason that women shy away from seeking legal help and suffer in the psychological agony, which sometimes translates into physical harm in the form of suicide and self perpetrated harm emanating from anxiety and depression.

Digital abuse against men is relatively less sexual but sometime it can be sexual in nature. Men usually face identity theft, corporal or money theft, blackmailing, stalking, professional abuse etc. However, the reporting rate of crimes against men is very low. It is because usually men tend to ignore these things as trivial owing to their patriarchal prejudices.

[18] hatred of, aversion to, or prejudice against women
https://www.merriam-webster.com/dictionary/misogyny

2.9 Conceptual Framework



Fig# 1

3. Research Design and Locale

3.1 Research Methodology

The research methodology acquired to carry out this specific research thesis is qualitative. Qualitative research is a type of research where researcher collects detailed accounts of data and then interprets that data to find out subjective realities, meanings and general view of life of the specific research sample (Bernard, 2006). It is a type of methodology that lets the researcher delve into the subjectivity and relativity of people's perceptions of different events. Qualitative method is considered as backbone of anthropology. As anthropological studies highly focus on in-depth and first hand data. It involves looking subjectively into non numerical data. Qualitative data can also be said as taking deep, quality look at a certain phenomenon. It is primarily exploratory research, which is used to gain an understanding of underlying reasons, opinions, and motivations. It provides insights into the problem and helps in developing ideas or hypotheses for potential quantitative research. Qualitative Research is also used to uncover trends in thoughts and opinions, and dive deeper into the problem. Qualitative data collection methods vary using unstructured or semi-structured techniques. It makes use of numerous tools to achieve the result. Some common methods include focus groups (group discussions), individual interviews, and participation/observations (Battalan, 2019).

Qualitative research methodology is the most appropriate methodology in this case because crime and deviant behavior cannot be understood quantitatively. One can efficiently quantify the rate of these crimes but can never expound upon the underlying reasons and consequences . Hence, qualitative methods, techniques and tools were used to collect, analyze and interpret data.

3.2 Research Methods and Techniques

A number of methods are applied to gather the data. as the data in qualitative research requires multi-dimensional approach a number of methods are to be applied so as to get accuracy and emic perspective (Bernard, 2006).

3.2.1 Netnography- Digital Ethnographic Perspective

This research uses netnographic research design for the collection of data For data. Netnography is a research that is conducted in cyber space in the realms of technoculture. Netnography redefines anthropological methods to present an ethical and detailed ethnographic research so as to understand the phenomena of cyber world. It seeks to combine archival and online communications work, participation and observation, with new forms of digital and network data collection, analysis and research representation (Kozinets, 2014). It's a qualitative, explanatory research methodology that puts to use traditional in-person ethnographic research methods in anthropology to investigate technocultures and cyber communities based on computer-mediated communication. The data gathered for this research thesis was solely extracted using internet and cyber space. It was collected through computer-mediated observations and participation, as well as mediated interviews with key informants.

This technique helped the researcher gather adequate amount of data to satiate the requirement of the research at hand.

3.2.2 Rapport Building

Rapport building is a very important aspect in the process of data collection. It adds credibility to the answers. It is the first and foremost step to initiate data gathering, interviewing and probing. It helps building a trustful and comfortable relationship between the respondent and researcher

and provides with the opportunity to interact and become a part of a particular social setting. It can help get first hand, reliable data. For this research the researcher gave her introduction and explained the contents of research and ensured the respondents about their privacy. In addition, the researcher had to add the respondents to her private social media profiles. The researcher also shared her personal details and experiences to build trust with the respondents. Another technique that was put to use included the free flow of speech. Respondents were given the agency to freely talk about their experiences while the researcher kept quiet for sometime.

9.3.2 Interview Guide

Interview guide is a tool that helps the researcher gather its respective data and answer to all the queries. it consists of semi structured questions covering almost every aspect of the research inquiry (Bernard, 2006). Before heading into the field, an interview guide was created, and a pilot study was undertaken to test the research guide The interview guide was prepared in the light of relevant literature and was used to gather the required data from targeted sample. Interviews were conducted from all three of the social units considered as part of the study. The interviews were conducted in the safe spaces of their own comfort i.e., whichever social platform they preferred. They were taken on video whatsapp calls and audio calls as per their own preference. The questions were asked multiple times in a different manner so as to proof check the reliability of data. In addition, the researcher built an open-ended interview guide which was morphed accordingly during the interview, which allowed the researcher to expunge that added personal bias or sticking only to a pre-determined list of questions.

3.2.2 Participant Observation

This research put to use the most important tools of ethnography: participant observation for the collection of data for this research thesis. It was used as the main tool to carry out the research

process. This digital fieldwork lasted for approximately ninety days . This field work was carried out by observing people, comments and opinions on social media. Analyzing content that described experiences of cyber crime victims on instagram and youtube. For this study, participants were observed by putting to use the researcher's own social media accounts. Theses social media platforms offer free browsing and access to numerous people. It allows to view, comment and share the content of others. For the purpose of observation of verbal abuse or other such offences comments were thoroughly observed.

3.2.3 Use of Key Informants

Key informants are usually cultural specialists and are valuable sources of data collection in qualitative research. These cultural experts have knowledge, information, access and societal respect which allows them to act as bridge between researcher and respondents. (Bernard, 2006).The key informants for this research was Dr Abdullah and Pawan Parhar, and Bindiya Rana. These people made it possible for the researcher to access numerous respondents. These were the people who allowed me to have a direct access to the respondents and respondents trusted them enough to give interviews. However, their role was helpful only in accessing and they did not remain present throughout the process.

3.2.4 In depth Semi Structured Interviews

In-depth interview is an effective method to have a descriptive insight of the study. Researcher chose this method in addition to case study so as to strengthen the validity of research. In-depth interview is a dialogue between the researcher and the sample (Emerson, 2012). In depth interviews were conducted along with participant observation to collect the maximum data and include numerous people in it. It provided the researcher with an extensive account of how and what happened and what did they do to cope up with the consequences. The number of people

interviewed was predetermined; however, it saw a slight change. The researcher could not find more than two male respondents, hence, the change in the number of male interview respondents. Interviews were thoroughly conducted to saturate the research data. A total fifteen in-depth interviews were conducted. These interviews provided with clarity and deeper insight. Audio calls helped the respondents to feel safe. None of the respondents agreed to record the calls, hence, no recordings were made. In addition, except for a few, all names used in this research are supposed to protect the identity and privacy motivated anthropological ethics. The language used to conduct the interviews was primarily Urdu because the respondents were comfortable as such. The interview time ranged from 60 to 90 minutes each. These interviews were then transcribed and analysed later in order to squeeze out all the relevant data.

3.2.5 Focus Group Discussion

Focus group discussion refers to a discussion when the target population is asked to have discussion about the research topic. This is characterized by anonymity and consent. People engage in candid discussions about their views and experiences. The group discussion is led by a person called a moderator or facilitator. This person asks open-ended questions that the group then discusses. This discussion produces qualitative data about the topic, which then can be analyzed by the researcher.

3.2.6 Probing

Qualitative researchers yearn to get a grasp of the deeper meaning and what the respondent actually means. The understanding of the deep structure of conversation can be achieved through the process of probing, which allows the researcher to get maximum information out of any respondent. This research required probing and it was done so as to extract further explanation from the participants wherever they seemed hesitant. However, due to audio call as the primary

method of interview, the researcher could not rely on non verbal cues. The researcher had to ask and use the *huh-huh, hmmm, bilkul* probe to get the answers. In certain cases researcher had to take the lead to get the respondents talking and sometimes she had to stop some respondents from diverting. The researcher listened to the respondents carefully and paid full attention to whatever and however they said.

3.2.7 Digital Field Notes

Field notes were used to supplement the data in this investigation. Field notes were transcribed throughout each interview and major points were highlighted so as to simplify data analysis. According to Bernard (2006) field notes are of four kinds: diary, jotting, log, field notes proper and formal methodological, descriptive and analytical notes to record and analyze every crucial detail. The quality and quantity of field notes depend on the type of research, method of data collection, and research circumstances. During my fieldwork, I made notes of everything I observed notable for this research. Since I could not note everything during interviews, I had to interact with respondents, make them feel comfortable, and keep the conversation going; therefore, I made field jottings on the spot to jog my memory later on for details. I had a notepad with me all the time whenever I was observing the digital spaces. I asked all my respondents at the start of interviews if I can write this information, and I asked for their permission again to write when they told me something sensitive which could cause them trouble. I also made descriptive notes by transcribing these interviews, which helped me with my analytic notes. I made themes for my analysis from those descriptive notes. Consequently, it led to coherent, organized, and meaningful findings for this research to analyze.

3.3 Data Collection and its Challenges

Data collection is an extensive and nerve testing deal. As a researcher, I had to face numerous challenges in the collection of data. There were some expected but some unexpected challenges which lead to the delay of research. First of all, it is a very sensitive topic and people avoid talking about such incidents openly. Secondly, accessing the respondents was really difficult in the earlier phases. I planned on approaching Federal Investigating agency (FIA) for data but it remained inaccessible. I had to stop, re-plan my research multiple times. I had to opt for two other organizations: Gender Interactive Alliance(GIA) and Digital Rights Foundation(DRF). GIA helped me getting most of the trans gender respondents. Another challenge that I faced here was the non responsiveness of some the respondents. These respondents were accessed primarily through snowballing.

In my experience, the victims of digital abuse consider themselves vulnerable and hence, prefer to refrain from engagement. They would start by narrating an abuse story of someone they know. They would never accept the grotesque details at first. However, the interview unfolded numerous stories. Throughout the research, I had to take lead by sharing my own personal experiences with the respondents to get them to open up about their own experiences. This build a better and safe environment for them to talk. Unlike women and men, most of my trans gender respondents were open to talk to and they wanted to be heard. Their responses were, however, abrupt and complaining. They deviated from the issue at hand and started how in general they are marginalised in the society.

3.4 Data Analysis

Data analysis is the process of systematically applying statistical or logical techniques to describe and illustrate, summarize and recap, and evaluate the data gathered from the respondents. Qualitative research calls for collection of data which is then analysed to extract the underlying meanings. Collection of relevant data and then coding it is the most significant part of qualitative research. The codification of data is a process of categorising data into different thematic divisions or clusters (Bernard, 2006). In short, data analysis is breaking down the data into its constituent parts to better understand it. The acquired data was sourced through semi-structured interviews, which were predominantly conversational in nature, observation and digital field notes. This data was used to codify different themes, which eventually took up the form of thematic analysis. I chose thematic analysis because it would best suit this research thesis. Thematic analysis helps to arrange the raw data in a systematic form and adds symmetry to the research. It would allow the reader to understand and comprehend what actually the research was able to extract and how is it significant (Braun & Clarke, 2012).The interview results are presented and analyzed in themes. Themes are observed by addition to being important fragment of ideas or perspectives that, when viewed separately, are often irrelevant. Each theme is followed a analysis in relationship to the literature and cultural context. Hence, interpretive approach is used to view the data in its entirety. A more specific approach would be qualitative content analysis. It helped me in understanding and interpreting the data acquired in cyber space.

3.5 Sampling

Sampling is one of the most significant processes included in ethnographic research. It identifies the elements or the group of people to be studied. It implies different sampling techniques to

chose the best possible sample, that would further the research process. It also adds to the validity of the outcomes of research.

3.5.1 Sampling Technique

This research is characterized by non-probability sampling in general, and a mixture of purposive sampling, convenience sampling and snowball sampling in particular. This sampling technique includes individuals with specified feature that may or may not exist in all members of the population of a certain locale. Mostly researchers are also bound by time and management of resources. Non probability sampling in this research is applied because I have outlined certain fixed pre-requisites for the sample. Non probability sampling was the most suitable option for the researcher. Purposive sampling allows to find individuals who can reflect and share experiences related to research. The researcher jots down the outcome or purpose he/she would want the informants to serve and then strives to find those respondents (Bernard, 2006). On the other hand, convenience sampling and snowball sampling depends on the availability of individuals. In convenient sampling, respondents are chosen as to anyone available fulfilling the specific research profile. Snowball sampling was used because it is a very sensitive topic. This was specifically helpful in case of trans genders. Respondents referred to other victims hence providing more respondents.

3.5.2 Sample Size and Uniting

The initial sample size for the interview was to be kept Forty. However, later during the field work it was revealed that it was difficult to access people fitting that specific profile. It included all three genders and did not draw a line on age. A lot changed during fieldwork because of the sensitivity of the topic. I had to adjust and gather whatever I could. A sample of twelve women, eight men, and eight Trans genders were interviewed.

3.6 Demographic Profile of the Sample

Demographics		*Number of Respondents 28*
Age	18-25	16
	26-45	10
	46-56	2
Gender	Women	12
	Men	8
	Trans Genders	8
Marital Status	Married	4
	Unmarried	16
	Trans-people	8
Educational Background	Matriculation	3
	Intermediate	3

	Bachelors	12
	Masters	10
Occupation	Administration	3
	Business men	1
	Organizations owner	2
	Students	11
	Teacher	3
	Makeup Artist	2
	Public figure/bloggers	2
	Jobless	4
Residence	Islamabad	12
	Rawalpindi	9
	Karachi	4

	Bahawalpur Lahore	1 2

3.7 Reflexive Mirroring of the Research Thesis

Reflexivity is a very important part of Anthropological research which illuminates the researcher's own reflections on the research. Anthropological reflexivity is an influential and coherent ethnographic practice that critiques descriptive and realist modes of ethnographic representation (Dominy, 2018). Reflexivity allows the reader to understand the researcher's social positioning and personal views. It helps in making the research as bias-free as it can. Reflexivity moves anthropology from an empirical and observational methodology to a recursive epistemology that reveals its methods, collaborates with its interlocutors in the construction of knowledge, and attends to narrative and literary forms of representation in ethnographic writing. It started off with Malinowski and Boas and then saturated by others such as Victor Turner and Clifford Geertz. It called for being present in the situation while limiting the researcher's own biases. They emphasized that researcher's own values and biases must not outweigh what actually is happening. It would make the data less reliable and more value-laden. Hence, to avoid the data being value ladened, self-reflexivity was introduced. In this account, researcher provides the readers with his/her own predispositions, biases, values and aspirations etc. (Battalan, 2019)

I, being a woman, have been exposed to sexual and psychological harassment since long. I have experienced it as much as any other Pakistani woman. This gender positioning of mine makes me a little more compassionate towards women and sometimes drives my questions. While conducting interviews, I shared my personal traumas with the victims which did affect my interviews. To limit this, I tried to rephrase questions and ask those questions again and again to

saturate the responses. While interviewing men, I have had a presupposed notion of men as the perpetrators of digital violence, most of the time. However, I tried to keep this out of my head. I took ample amount of time to ask questions again and again and imply the anthropological technique of probing. I tried to keep the research as neutral as possible.

This research is a result of months of effort and hard work. It was made sure that this research remains as much value and bias free as it can be.

3.8 Anthropological Ethics and Considerations

The only ground to carry out anthropological research is when participants agree to work with the researcher. This yearns for the use of informed consent. The term informed consent is not merely signing (or agreeing) a consent form, but researcher have to explain objectives of the research along with information like funding and undertaking agency, benefit and harm because of the research, why it is being undertaken and how the data will be disseminated and used . Therefore, informed consent includes not only an explanation of data collection methods but a detailed explanation of the research topics that will be examined with the data collected from a study subject "informed consent is ultimately viewed as a process that encourages greater openness and disclosure on the pan of researchers, empowers voluntary participants in social research, and engenders a more collaborative relationship between researchers and researched." (Biswas, 2015). Hence, it starts off with rapport building as an inherent ethical consideration for the research. It not only helps collect data but also builds rapport through which the researcher gets informed consent for the research. It is an ethical-legal aspect of the research. The most important disposition of this is privacy,. One's privacy must never be breached. Sometimes, due to sensitivity of the topic, the researcher has to keep the respondents

anonymous. However, another problem that comes up is that not all the respondents understand informed consent. The researcher has to explain it to them.

For this particular research, several ethical factors were taken into consideration to ensure that the research followed all ethical protocols and the privacy and trust of the respondent is not breached in any way. Informed consent was obtained verbally, each objective along with questions were elaborated. All the respondents agreed on the condition of privacy except for a few. The standard practice is to obtain a written consent; however, the nature of research did not allow it. Appendix A contains the consent form which was followed as a standard to ask for consent. Participants were ensured of their privacy and anonymity. They were not comfortable with recordings so no recordings were made. The participants real names are not used except for two trans gender activists who wanted their names to be mentioned. The other respondents' names were replaced by pseudonyms.

3.9 Locale: Cyber Space

The world of twenty first century is replete with technology. These technologies have created a new frontier, commonly known as “cyberspace.” The term “cyberspace” first appeared in Neuromancer, a science fiction novel, by William Gibson (1984) who referred to it as a consensual hallucination (Berson, 2008). It describes an intangible, nonmaterial location or dimension created by computer systems to which people gain access, allowing them to communicate with one another via e-mail or engage in research etc. The movement involved in this type of activity requires pressing keys on a keyboard, moving a mouse, or voice commands. Some computer programs consist of games that are designed to give the user an experience that resembles physical reality; in virtual reality, for instance, the user is presented with feedback affecting the sensory systems such that occurrences in cyberspace feel real. (Chisholm, 2006).

This research determines cyber space as text messages, phone calls, emails, and social media apps(Instagram, Twitter, Facebook, snapchat, VChat, Signal, Telegram, Skype, and Tiktok, etc). Any technological tool which can be used to inflict harm to victim is taken under the umbrella of Cyber space.

3.9.1 Organizations

Three major organizations were considered: Saffar shemale association, Islamabad, Gender Interactive Alliance, Karachi, and Digital Rights Foundation.

SAFFAR(Shemale Association For Fundamental Rights)is the organization to protect the Rights of She-Male(Eunch's) through skills for livelihood as to maintain their challenges and increased the capacity building. Our initiative included that to rehabilitative the disabled and vocational training for sustainable livelihood[19].

Gender Interactive Alliance (GIA) is an organization working for the equality and civil rights of transgender people in Pakistan. The mission says that Transgender persons do not have the same level of rights as other Pakistanis[20]. They are also routinely harassed, face discrimination, and in some cases are subjected to violence simply for being transgender. They aim is to raise awareness of the issues concerning transgender people in Pakistan and cultivate a supportive, empowering and non-judgmental environment for them. One of the main objectives of GIA is to advocate and facilitate employment for transgender Pakistanis. They include the whole spectrum of gender identities such as intersexual, transsexual, hijra, khwaja sira, butch, cross-dressers, and transvestites.

[19] https://vymaps.com/PK/Saffar-358558207581683/
[20] https://genderinteractivealliance.wordpress.com/

The third most important organization is Digital Rights Foundation(DFR). DRF envisions a place where all people, and especially women, are able to exercise their right of expression without being threatened. According to DRF, free internet with access to information and impeccable privacy policies can encourage such a healthy and productive environment that would eventually help not only women, but the world at large.[21] It focuses on protection of women rights in digital spaces and help in strengthening and protecting women rights advocates. DRF seeks to establish a safe space for women. It also deals with work place harassment. In addition, DFG intends to propose valuable solutions to the government to address the issues of harassment.

3.9.2 Applications Interface

The observational data mainly came from Instagram, YouTube and Tic-tok. The comments and content of these three social media applications was thoroughly observed and analyzed to complete the field work for this research.

YouTube is a US bases online video sharing and social media platform, which is owned by Google. It was launched in 2005, by Steve Chen, Chad Hurley, and Jawed Karim. After Google, It is the second most visited website. YouTube has more than one billion monthly users, who collectively watch more than one billion hours of videos each day[22].

Instagram is an American social network for photo and video sharing , founded by Kevin Systrom and Mike Krieger. The app allows users to upload media files that can be edited with filters and organized with hashtags and geotagging. Messages can be shared publicly or with pre-

[21] https://digitalrightsfoundation.pk/about/
[22] https://en.wikipedia.org/wiki/YouTube

approved subscribers. Users can view content of other users by tags and location, and view trending content. Users can like photos and follow other users to add their content to their personal feed. Instagram is a simple social network of other people's photos. One can like or comment on the photos, and see what's new. It's easy and doesn't take much time or effort. This is one of the reasons it has become so popular so quickly.[23]

Tik-tok is a China based service for creating and viewing short videos, owned by the Beijing company " ByteDance "[24].It was launched in 2018, the international version is the leading video platform for short videos in China and is becoming increasingly popular in other countries, becoming one of the fastest growing and downloaded applications. It provides the users with free space to put their videos out on the internet for others to see. It is increasingly popular all over the world.

[23] https://ru.wikipedia.org/wiki/Instagram
[24] https://ru.wikipedia.org/wiki/TikTok

4. Data Analysis and Discussion

This Chapter emanates from the data collected during field work and is based on the analysis of the collected data. . In this chapter, data is presented and analyzed in numerous themes. This research thesis puts to use two techniques: content analysis and thematic analysis. It makes use of the data acquired through participant observation and in-depth conversational interviews. The major Analytical framework of methodology is netnography, which was used in this research by virtue of its nature.

This chapter divides into three main themes by virtue of genders and subsequent sub-themes.

4.1 Cyber Crimes against Trans -Genders

Crimes against trans genders are not new. They have always been one of the most vulnerable group prone to physical violence. Most of the time, they are denied the right of recognition at birth and are left to lurch in streets where gurus take them in. They do not get education opportunities and subsequently are left out of the job market. They have to compulsively choose sex work, dance and beggary. This research, however, focused on digital abuse and violence. Now is the time of social media and almost every other person in Pakistan uses social media. Trans people also use these applications a lot. This research revealed that now most of the trans people doing sex work book their appointments through social media. The increased use of social media has ushered into increased threats related to social media. It includes threat, abuse and stalking by 'Beela' groups. The trans activists and respondents first explained to me about the different terminologies that they use for themselves: intersex, khusra, khuwajasira and moorat. These people are the unprotected and vulnerable group of the population, who were erstwhile harassed only physically. Now, with the excessive use of technology everywhere, they are

stalked and chased through internet. Attacks on them are planned via cyber space. These major perpetrators of abuse and violence are beelas.

4.1.1 Crime syndicates against trans people are now creeping in cyber space -Beela violence

Beelas are a group of violent hunting men. It is a term used by the khwajasira community(Trans-Gender) for those who perpetrate violence against them for rejecting their coercive sexual behavior. Beelas are "an organised syndicate of criminals who plan, stalk and attack khwajasiras, trans-feminine people and young boys," according to Dr Moiz, a trans activist and a teacher in Habib University , Karachi. During my conversational interviews with khuwajasira community, my respondent Nadeem Kashish said, that beelas are the bad people;

'Beelay humari zuban mei buray ya badmash ko kehty hein'

In our language, Beela are the bad people or the bullies

Beelas are used to keeping moorats as sex-slaves. Now that most of the trans-genders use internet, beelas threaten them to stay with them or else they would make their explicit videos viral. The physical violence and cyber violence against trans gender community is tightly interwoven. One primary reason of this is that now those khuwajasira who do sex work to earn a living use internet to do video calls and audio call sexual services. They send them pictures and explicit content to satisfy the customer's needs. However, most of the time, these people keep records of these images and videos to blackmail them afterwards. One of my respondent told me that she used to go to dance parties for money, which were mostly booked through facebook. Those parties used to end up in multiple attempts of rape and abuse. Those beelas would then record themselves raping them. Those videos are made viral on the internet.

'Humari baat huui the kay sirf party hey, nach gana houga phir chaly janaa. Par unhon ny hamary kapry pharny shuru krdiye aur apni kanch ki bottlon ka istemal kiaa. Phir woh video net py dalny ki dhamki deny lagy. Woh din aur aj ka din mein lahore chor kar yahan islamabad agai. Ab mein yahan makeup artist ka kam krte hun'

We agreed for a dance party. We were to leave afterwards but they started tearing off our clothes and raped us with their glass bottles. They threatened us to upload those videos on the internet. After that day, I left Lahore and came here in Islamabad. Now I work here as a makeup artist.

Another major problem with that a respondent faced owing to the fact that he was working as a trans activist were murder, rape and abduction threats. A case related to trans community was being challenged in the Federal Shariah court, which is being lead by the trans activist. He exclaimed that he is being added in whatsapp groups on daily basis. In those groups they abuse him and threaten him.

'Mjhy roz kisi whatsapp group mein dal dety hein. Dhamkian dety hein ky tmhy apahaj krdein ky, tangein kat dein gy, jaan sy mar dein gy, uthwa lein gy. Srf is liye ky mein apny haq ki baat krta hun'

They add me in whatsapp groups on daily basis. They threaten me with mutilation, murder and abduction. It is only because I ask for my rights.

These crimes are mostly perpetrated by organised crime syndicates, which erstwhile operated strictly in physical world. With the exacerbated use of internet and rampant social media applications, now these syndicates are operating in a world existing by virtue of energy: cyber space.

4.1.2 Cyber Stalking Against Trans Community

It is established that most of the trans people now use and earn through social media applications. They arrange and deal for their dance functions and sex work online. Some of them also have made their profiles public, which makes it easier for the stalker to chase them and keep a track on them. Recently, in the month of September, an organized beela syndicate ganged up and attacked the birthday party of Sehzadi Rai, hurting numerous Khuwjasira community members, including Dr Muhmmad Moiz and Firdous Gaeawala. Apparently, these attacks were being planned via phone and internet for days before the event. Dr Moiz indicated that the information was leaked by a moorat from the community.

Fig# 2

In thr above attached media, Dr Moiz is showing how a memeber of that Beela group tried to interact with him in the wake of their protests against beelas infront of Karachi press club. Afterwards, Dr Moiz and Firdous Gaewala used their social media to highligh the problems they were faceing related to the Beela crisis. They highlighted the fact that were being traced through social media time and again.

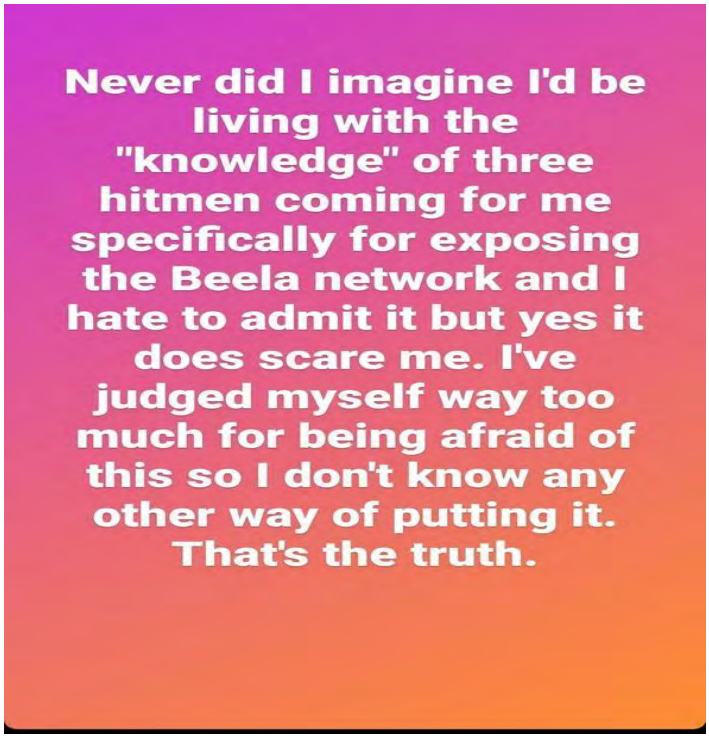


Fig #3

4.1.3 Threats Through the Use of Internet

Threatening to kill someone or abuse someone is very common. With the advent of the age of internet, the unbridled use cyber space has put human society at risk of unforeseen crimes. In Pakistan, the trans-community, particularly transgender people, live in poverty and can be seen begging and dancing at traffic lights and wedding receptions. The socio-economic divide in Pakistan makes it more difficult for them to fight for their rights. Families typically simply

ignore transgender individuals, and many of Pakistan's estimated 500,000 transgender people end up as beggars or sex workers. In the last few years, more than 100 people have been murdered in Sindh alone. Tran's people have lived on the outskirts of the subcontinent for centuries. For a long time, people have made dangerous and potentially lewd jokes about transgender people. The transgender and transsexual community in Pakistan faces institutional racism mostly because of their trans identity and gender orientation, but also on a social and political level, arising in their economic status remaining below the poverty line. According to Bindiya Raana, only a handful of trans people are educated and now their rights. All others are oblivious of their rights and are compulsively made to resort to sex work and dances. Now that they are turning towards social media for the booking of their functions or simply raising their voice against the atrocities that they have to face, they are being bullied in cyber space. A member of GIA told me that when she went to pick her friend's dead body up, who was killed in an acid attack by a beela, she started receiving threats.

Mujhy phone any lagy. Gaalian dety thy aur kehty thy tera bgi yaahi hal karein gy, tu bhi esy he taezab sy jaly ge.

They started calling me. They would threaten me with the same fate. They would tell me that you will also be burned with acid.

Incidents like these happen quite often and trans people are left at the mercy of these crime syndicates. This situation is worsening with the increased role of social media. The perpetrators of crime now stalk and trace their victims to abuse them psychologically and physically. Trans people are seen begging for their lives on social media and most of the time, very little help is done to protect them.

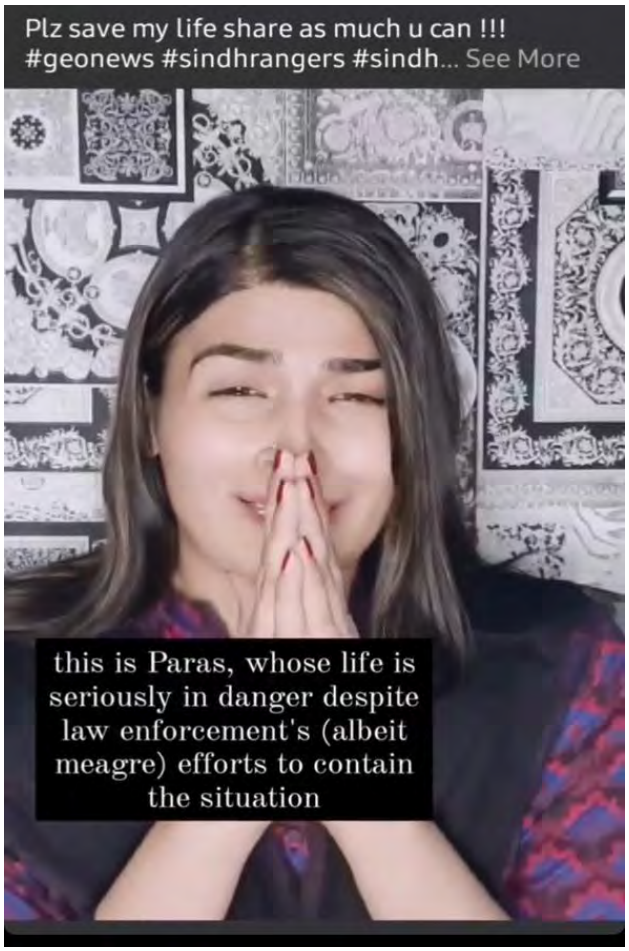


Fig #4

The above attached picture shows a trans gender Paras begging for her life on social media and yearning for help. She had been threatened and digitally abused via pictures and videos. Afterwards, beela groups traced her house where she lived in and tried to get a hold of her. The situation was later contained with the help of GIA and other trans activists.

4.1.4 Verbal Abuse Against Trans Community

Verbal abuse or calling someone out on social media has become a norm. Trans people are called out on streets and in markets. They are looked down as low-lives by numerous people. It is primarily because the work they do and how their professional identities shape up. They face abuse and bad mouthing everywhere. Cyber space is no exception.

Fig #5

Fig #6

The above attached screenshots are from beelas who are verbally abusing and threatening trans-genders. The picture on the left is a person who is calling out a trans as a lowlife sex worker, who needs his money to eat. He threatening to rape and kill her, if he catches her. On the right side, the man is saying similar things. According to him theses trans sex workers are a plaque that has ruined generations of men. He is calling out a trans-sex worker who is in hiding. He tried to trace her whereabouts by contacting other members of his gang.

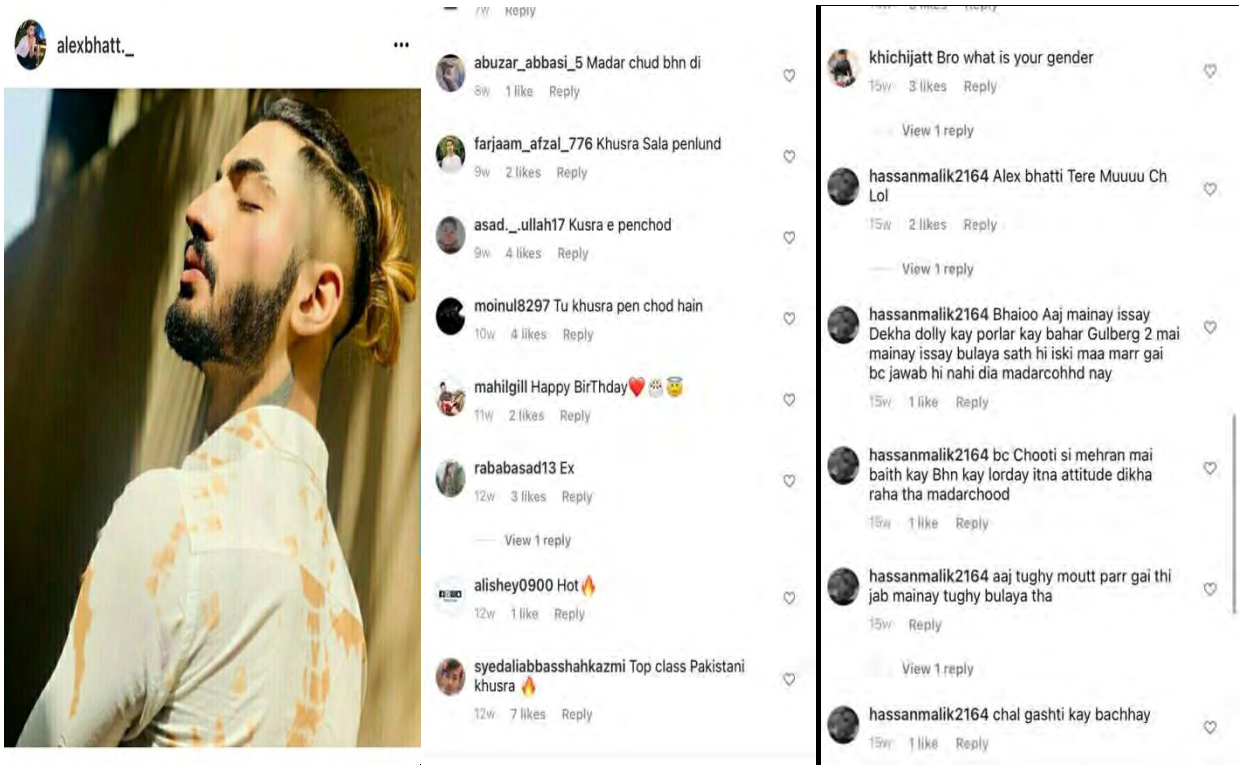


Fig #7 Fig # 8 Fig # 9

The above attached photos show an instagram trans model. He uploaded his picture and people started abusing him under that picture. People are calling him 'khusri'. Certain other abusive remarks are being commented under the photo. A person is calling him names and abusing Alex's family because he did not greet him while the person was stalking him outside his work place.

4.2 Cyber Crime against Women

Crimes in the cyber world affect everyone, without the bounds of time and space. However, mostly women are seen suffering at the hands of violence not only in the real world but also in a world that is build upon waves of energy: cyber world. This includes all kinds of offences from verbal abuse, name calling to revenge pornography. The field work done for this research and the

conversational interviews outlines a few themes which incorporate most of the types of cyber crimes perpetrated against women. These themes include verbal violence, cyber stalking, threats and revenge pornography. Verbal violence includes calling names, branding or stereotyping someone, writing mean comments or sending abusive direct messages. Stalking involves tracing someone's social media activity to know what are they doing or using their social media to get a hold of their life. Similarly, threatening to doctor images and sending private information to family and friends, identity theft and revenge pornography is very common.

Recently, a university student from Karachi was faced with online hate and abuse because of her views on feminism. She fell victim to cyber-harassment owing to the fact that she spoke about women rights openly.

"I never thought my opinions would trigger Pakistani men to the extent that they would start harassing me"

While giving interview to a local newspaper she put forward her reservations and called out the misogyny in society. People could not tolerate some opinions and ideas related to a universally organised movement striving to liberate women. Men in her comments section started calling her out, abusing her and threatening to rape her.

"Many men started sending me lewd and abusive messages on my Facebook and some of them even copied my pictures from my profile, threatening to doctor them just because they did not agree with my views on women's rights."

Likewise most women, she backed off and did not report the crimes to FIA's cyber crime wing . According to her, she yielded because of family pressure. She made all her accounts private and changed the privacy settings to limit access to random people.

Violence against women in Pakistan is as true as the existence of Pakistan itself. However, the notion of Honor attached with female bodies and subsequent shame slurs keep women from reporting such crimes. Kamal Bhasin, an imminent Indian feminist, once openly called out the hypocrisy of the society and questioned the concept of honor:

"My Honor is not in my Vagina"

This notion of honor and respect attached with female bodies drive Pakistani culture. It is imperative from day to day exchange of goods to ceremonial exchange of women and honour killings. The same notion crept into cyber space. People try to hide cyber crime and abuse because of the shame and stigma attached to it.

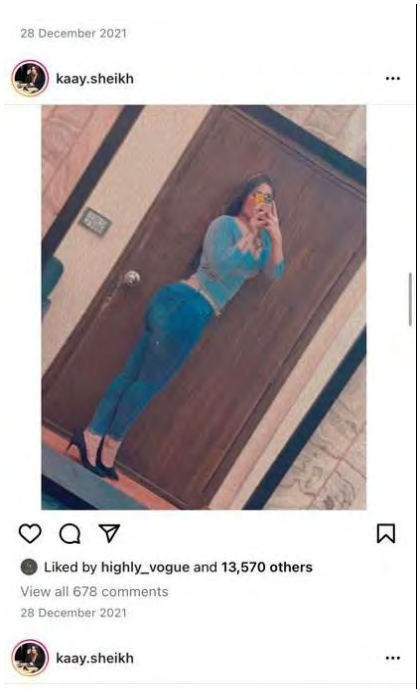
4.2.1 Verbal Abuse against women in Cyber Spaces

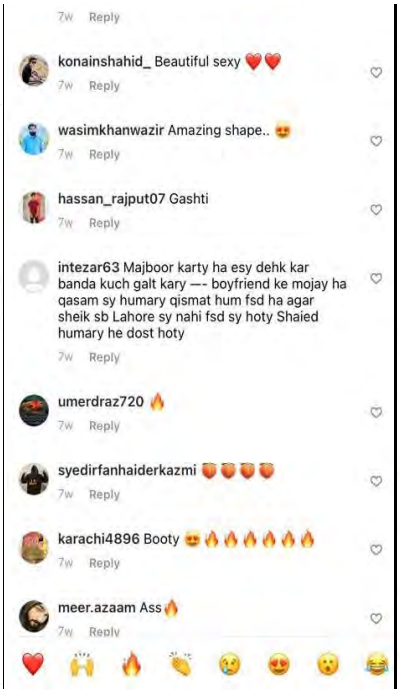
On a daily basis, numerous women face verbal abuse on their pictures, in their direct messages and the videos they post. Numerous others face abusive language and mean comments from their ex-intimate partners(boyfriends) A respondent told me that she broke up with her boyfriend of two years because of some reason. Now he makes fake accounts to call me a slut and a man pleaser. I have blocked him from my phone but he finds a way to contact me on my instagram.

"We were university fellows. We did MSC together and when I asked him to talk to his parents he started stalling me. I left him because I cannot deal with uncertainty. Now he calls me from unknown numbers and makes fake accounts to call me a whore who sleeps around and uses men for sexual pleasures. He sent the screenshots of our private conversations to my friends in university.

Women face such and other verbal abuses on daily basis. During my field, work I came across numerous such comments which were being made under photos of women. Random people

would ask them that how much money they charge for a night, making explicit comments about their body parts. They explicitly comment as to how they would like to have sexual relations with them and how attractive their bodies look.





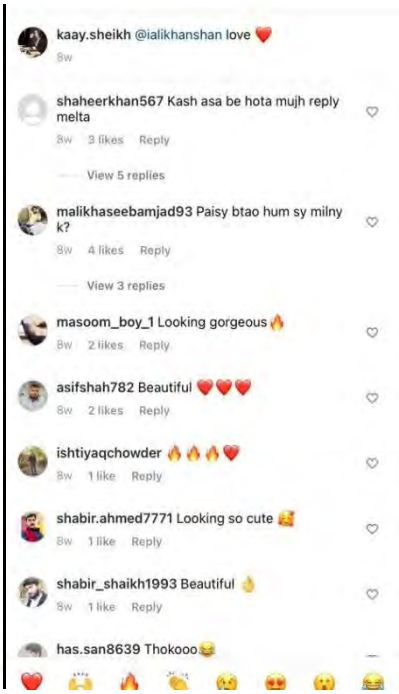


Fig # 10 Fig #11 Fig # 12

The images attached here are of an instagram model account. Her account is public and she frequently add her pictures. She runs a saloon and post images of her showing her body. In return, she gets mean comments as to what people would like to do to her body. As seen in the above attached screenshot, people are asking her rate. Inviting her to meet them for money. Some of them would fancy her body and would express their desire to sexual activities with her. In most of her posts, comments section is filled with verbal abuse or confessions of the desires they have.

4.2.2 Cyber Stalking Against Women

Stalking refers to behaviour of harassing or threatening the other person, often obsessively. Among numerous types of stalking, on is called Cyber Stalking. It is an extension of physical form of stalking; however, it transcends into the cyber world where identities are then compromised. In cyber stalking the internet, e-mail, chat rooms etc. are used to stalk another person. It includes harassment through e-mails. It is very similar to harassing through letters. For instance, former boy/girl friend sending mails constantly sometimes emotionally blackmailing and also threatening . This is a very common type of harassment via e-mails which also includes sending pornographic images and obscene messages. Similarly, making of false accusations or statements of fact (as in defamation), monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information that may be used to harass. (Dennis, 2019). Stalking is a continuous process, which includes a number of actions, each of which may be entirely legal in itself. Cyber stalking is the repeatedly harassing or threatening of an individual via the internet or other electronic means of communication. A cyber stalker is someone with amorous and/or sexual motives who constantly harasses someone else electronically: via the bulletin board, chats box, email, spam, fax, buzzer or voice-mail. Stalking generally involves the constant harassment or threatening of someone else: following a person, appearing at someone's house or workplace, making harassing phone calls, leaving written messages or objects, or vandalizing someone's property. Because the stalking activities are so diverse and have to be seen in their connection it is difficult to give a precise description of stalking.

While interviewing the respondents, I came across numerous such cases where the victims faces stalking. A respondent told me that her identity was compromised by her friend. Her friend made

a fake account in her name. The act is known as cat fishing. She used that account of instagram to talk to man. She posted her numerous pictures and made the account look like a real one. She used to talk to a man, acquired money from him. The money was exchanged with a promise of returning sexual favours. However, the catfish account shut down and told the man to contact the actual account. The victim did not know as to what was happening and started receiving anonymous messages on instagram asking for the promise to be fulfilled. The victim, Ayesha, had no idea as to what was going on. The man sent her screenshots of her earlier conversations. He knew where she lived and tried to reach her at her home. Her parents got aware of the situation and a complaint was made in the cyber crime department. The girl did not file a complaint against her friend and experienced serious psychological trauma.

'Mjhsy kehny laga bano mat, ab woh wada pura karo jo tumny mjhsy kia tha. Warna yeh sary screenshots tumhary ghar walon ko dikhaunga'

He told me not to pretend and fulfil the promise that I made to him. Or else he would show all the screenshots to my family.

This incident changed her life and put her in a psychologically different place. Other victims explained that getting pictures of penises is business as usual. Men send these pictures in direct messages asking to have audio call sex. Another victim told me about a Cyber stalking incident from her university, She graduated an year ago but she remembered how her privacy was breached. A man from her university started following her on social media. She hardly went to university because of her research work He would stalk her and call her via different mobile numbers. He made fake accounts to reach her. He would send her pictures of her while sitting in

different places in the university. She told me that the fear of being watched all the time made her scared.

'Aik din usny mjhy meri tasveer bheji mein library mein bethe the. Mein buhat dar gai aur mny usko block krdia. Agly din mjhy aik aur numbers sy call any lagi ky mjhy unblock krdou warna acha nahi houga. Mjhy itna khof araha tha ky mny man lia. Mjhy khny laga mein tumsy muhbat krta hun bas mjhy ghusa na dilaya karo'

One day he sent me a picture of me sitting in the library. I got so scared that I blocked him. The next day he called me from a new number and told me to unblock him or else it would not be good for me. I was so scared that I told him I will unblock him. He told me that he loved me so much and that I should not infuriate him.

Another victim told me about her experience with her ex boyfriend. They were in love for two years but somehow broke up. They boy had her private pictures and messages. He did not do anything for first two months; however, he started asking her to get back with him. To which she refused and blocked him. The boy then contacted the girl's friend through instagram to have her arrange a meeting for them without the girl knowing. She told her friend to block him immediately and called the boy to talk. She told her that her uncle works in the FIA and she would report him if he is persistent.

4.2.3 Threats of Abuse

Digital spaces are creeping with offenders having different intentions. Mostly women face threats of information leakage, rape and acid offences. Abuse is about entitlement and feeling in control. It is often triggered by unhealthy jealousy and envy. According to the UN, in the US, two out of every ten young women have been sexually harassed online and one in two say that

they were sent unwarranted explicit images. Threatening to abuse someone is really common. It includes acts messaging and email to threaten them to harm them. A respondent told me that her ex fiancé told her that he would ruin her face with acid. He felt rejected and inferior and consequently, he threatened to cause her physical harm. She started crying while telling me about her experience. She told me that she trusted the man but he threatened to ruin her life. She eventually told her father. The boy's family was from the biradari and the issue got resolved without the involvement of police.

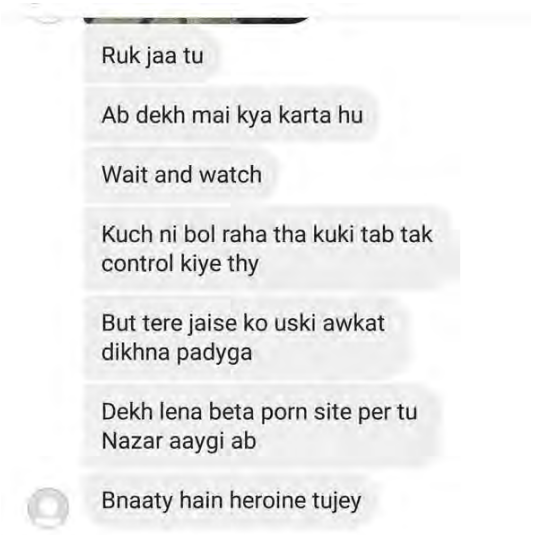


Fig # 13

The above attached image was shared with me from a victim. She started talking to a man online and became friends. Their friendship grew closer and the boy started asking the girl for her pictures. She did not know that the account was a catfish account and that the man was using someone else's copied pictures. She used to send him semi-nude pictures and videos. The girl came to know about him afterwards. She stopped sending him pictures but he would not take no for an answer. He started threatening to post her pictures on porn websites.

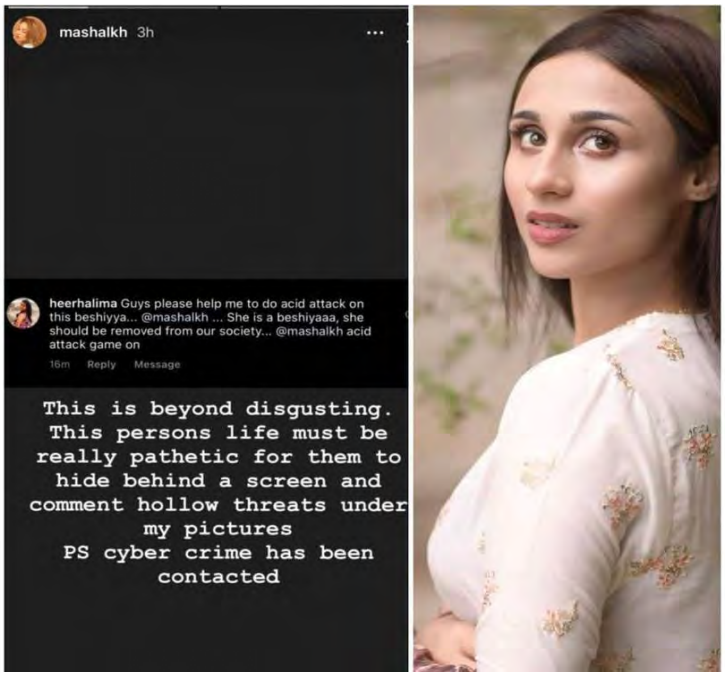


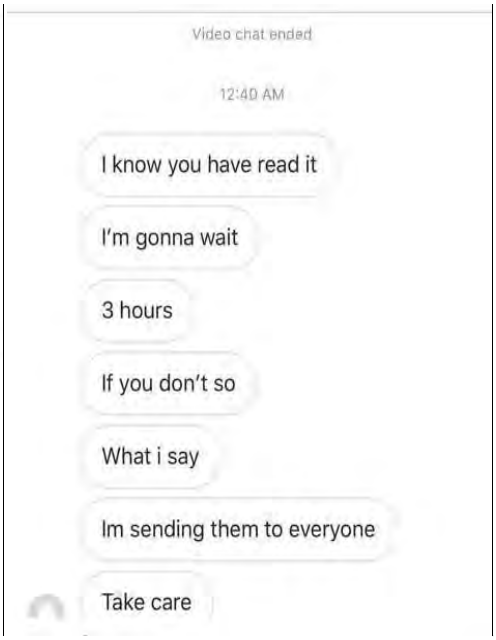
Fig # 14

The above attached image is from the account of an actress. Under one of her pictures, a fake account posted this comment. she highlighted it and called for cyber crime branch to help. The comment threatened her of acid attack and disfiguring her because apparently he/she deemed her 'behaya'(lewd). The comment added that acid attack game on for mashal khan. It clearly indicated that he/she was threatening to cause her harm.

4.2.4 Revenge Pornography

Revenge pornography is very common and potentially very dangerous for the victim. The Black's law dictionary defines Pornography as "*Lewd and lascivious materials depicting erotic images, designed to arouse sexual desire*". In simple words, cyber pornography can be described as using the cyber space to create, display ,spread, import or publish pornographic or lewd content. It all started off with the advent of information technology and internet, that allowed easy access to everything. The accelerated use of cyber space and putting one's life on social media. Revenge pornography is a cyber crime which is often coupled with other offences such as

stalking, threat and verbal abuse. It is indicated that revenge porn most often occurs where the victim had an intimate relationship with the perpetrator. It can be physical or verbal via digital spaces. Most often, perpetrators use these images as a bait to trap the victim to give in. They receive sexual favours and sometimes money. Money is mostly involved when the victims are men. However, it is not entirely true. Women too had to pay hefty sums to the blackmailers.



Fig# 15 Fig #16

The above attached screenshots were shared during an interview, the girl told me that this boy bullied her into doing nude video calls and sending him pictures. He would not delete those pictures and ask for money and sexual favours. He threatened her to expose those pictures and he eventually did. He sent those pictures to her friends and family. She had to register a complaint with the FIA to get rid of him. Similarly, another victim told me about her friend, she was married and his husband would take her pictures for fun. However, she realised after sometime

that the husband was selling those pictures privately on a website. When she confronted the husband, he refused and eventually threatend to leave her He humiliated her and called her a whore.

4.2 Cyber Crime against Men

Men and women both face serious crimes in the online world. The nature of crimes against men differ slightly. They mostly face economic crimes and defamation. However, crimes against women are mostly sexual in nature, It does not mean that men do not face crimes of sexual nature. The field work done for this research and the conversational interviews outlines a few themes which incorporate most of the types of cyber crimes perpetrated against men. These themes include verbal violence, cyber stalking, threats to defame and destroy life and economic frauds. . Verbal violence includes calling names, branding or stereotyping someone, writing mean comments or sending abusive direct messages. Stalking involves tracing someone's social media activity to know what are they doing or using their social media to get a hold of their life. In addition, scamming with money is another common cyber crime that men face. I did not come across any women who faced this. This does not, in anyway, imply that women do not face these crimes. They do but relatively less than that of men

4.2.1 Cyber Stalking and Threats Against Men

Men are usually known to get into the fights which are physical in nature. The verbal abuse that men face online mostly come from their followers when they do not agree with them or after a scandal is unearthed. These instances ; however, are not very serious. Men face stalking coupled with verbal abuse. A respondent told me that started working in an organization, where he was not welcomed by his colleagues. He started receiving abusive messages related to him and his family. His email accounts got hacked and unknown devices started logging into his accounts

and his whatsapp account got compromised. Another respondent told me, that he used to be in causal relationship with a girl. The girl made it clear that she only wanted sexual relationship. However, after sometime, the girl started contacting his family. She stalked him and his family through social media accounts. She would ask his nephews and brothers about him and bully them in telling him what was going on in his life. Meanwhile, the man got married but the women would not stop chasing her. She had his pictures, she would send those pictures to him and threatened him to meet her or else she would publically shame him.

Another victim told me that, he could not marry the girl he loved because of family pressure. She did not stop chasing him. Later, she befriended his wife and started talking to her. He told me that he did not know about this. One day, his wife invited her friend at home and then he came to know about this. After she left, he called her to stop her from coming to his house. The victim exclaimed that his wife and his ex girlfriend are still in contact and he is living in fear.

4.2.2 Economic Frauds Perpetrated Through Cyber Spaces

Economic frauds perpetrated through the use of online world are very common. Two of my respondents fell victim to these crimes. One of them told me about the experience of him nd his friend. They contacted an agency who advertised on the internet for a job at the United Nations. He, in need of a job, contacted the agent. He told them that they are based in Sialkot and since the boys were form Islamabad, they needed to fill their forms online. They filled their forms provided by the agency. He then asked them to deposit 15 thousand each as fee for the submission of forms. They made the transactions but never heard back from the agency.

Another respondent told me that he received an email from a business account. Apparently, It was from a women from based in Brazil. She mentioned that she worked in an insurance

company and there was a person with the same sir name as my respondent. She was given the task to locate his family. A huge amount was to be paid but she needed to get some paper work done. She told him that she would keep only 5 percent and would transfer the millions of money to him. He thought that it was real because she shared all her information and company cards with him. The company actually existed. He agreed to help her. She told him that he needs to transfer 700 dollars first to get the paper work done. After that, he would be the sole owner of the old man's money. He arranged the money and transferred it to her account. Following the transfer, she cut off all the contacts and the money was never reimbursed.

4.2.3 A Specimen of Hacking- Case Study

One out of all other cases of cyber violence against men stood out. The victim was willing to provide me with details of the atrocity he was facing. He is a teacher at The Islamia University of Bahawalpur, Baghdad-ul-Jadeed, Campus. As soon as he joined , he and his father started receiving calls/messages labeled “spam”. The content of the calls and messages was the same (blockage of HBL Debit Cards) to both of them. The number of spam calls/messages increased to an extent that he became emotionally tortured and suffered from neuropathic pain. His first salary account (HBL Debit Card) was received by someone in his name. The person who received it and the person who delivered the card neither contacted him nor the concerned bank (Bahawalpur-Islamia U Old Campus Bahawalpur). Apart from other instances, a message was left on his phone by an unknown number with the above-mentioned content (blockage of ATM). The number was blocked through PTA. The first Debit Card was blocked for not following proper SOPs (Checking CNIC before delivery) and wrong delivery. The second salary account (HBL Debit Credit Card) was dispatched through (TCS) and delivered by a member of a different service provider (M&P). The second Debit Card was blocked on suspicion of information sharing. His primary email “z*****.b*****@gmail.com” was synchronized with the privileged email “z******.b*****@iub.edu.pk” on his personal device Huawei Mate 10 lite, Model RNE-L21, Build

Number RNE-l21 8.0.0355 (c18). While writing a draft for some unusual happenings and grievances to the worthy vice-chancellor on the Google docs of his primary email, he received a mail of the draft from his official account. He perceived that email as a threat not to report to higher-ups. Apart from that all his services i.e. photos, contacts, and research being conducted with other scholars had also been compromised. The person who trespassed his personal virtual space must have been held accountable for stealing his identity, unauthorized accessing of accounts, and stalking. The victim made several attempts to change his passwords but he could not do that. At last, it turned out that the recovery email and number provided were of a person that he did not even know. On November 10, 2021, a new password of the same account was provided by the IT helpdesk but it is still vulnerable as it is not on standard encryption despite request. The victim emailed and informed the I.T helpdesk that he will not take responsibility for any activity done from his accounts. Besides that, his access to connectivity and basic services for the privileged accounts were also denied. His device DESKTOP-T47D8LH was also purposely infected with ransomware. The device contains all of his intellectual property, scanned copies of his identity card, driving license, educational testimonials, personnel, and family folders. A folder that he specifically dedicated to his father was missing that emotionally drains impacted the victim. Location of an unknown device in his primary email "z******.b*****@gmail.com" also proved that his privacy has been repeatedly breached. The victim's previous Twitter account with the user name @Z******11 has been restricted temporarily and followers and following are turned down to zero. In addition, two sim cards in the victim's name have also been shown on his credit and his whatsapp account also got hacked. In the victim's words:

'FIA must Investigate into the matter as a mentally challenged hacker has held me hostage in the virtual world, breached the privacy of those who are in contact with me, and has caused a significant amount of paranoia and distress among others. Not only is my career at stake[but also] I lost confidence in using technology. I believe that working with the fear of identity and

privacy being compromised is the worst possible ordeal for any respectable citizen. I herby, categorically highlight that I have no history of the rivalry of any kind in past or present'

5. Social and Psychological Impacts on the Victims of Cyber Crime

The research aimed at understanding the individual experience of cyber crime and how it impacted the victims. It provides an emic perspective of the issue at hand.

5.1. Social Impacts of Cyber Violence

5.1.1 Social Isolation

The impact of identity theft on a victim at an emotional level can lead the person becoming distressed and be left feeling violated, betrayed, vulnerable, angry and powerless. It made the victims relatively anti-social. Most of the times people keep on asking the victims about the details of the trauma they faced, which makes it difficult to overcome the experience of violence. In case of women, families try and get women married as soon as possible. Trans people are already a marginalised community; however within their own community they are mostly accepted and understood. On the other hand, men are sympathised with. If the perpetrator is a woman, she is labelled as a sex worker, a vile woman and a 'whore'.

5.1.2 Stereotyping and Victim Blaming

Victimization can lead victims to feelings of outrage, anxiety, a preference for security over liberty, and little interest of adopting new technology due to loss of confidence in cyber. The victim can go into stages of grief, suffer from anger or rage. In some cases, victims may even blame themselves and develop a sense of shame; sextortion is a good example of this given how it initially starts. In this research, it was observed that it is one of the most prevalent social responses regarding abuse.

Victims of Cyber abuse, predominantly women, are labelled and stereotyped as a result of cyber violence. They are asked demeaning questions and blamed as the problem creators. The victims

exclaimed that they were asked inappropriate questions and were labelled as if they made the perpetrator do it. Why would they allow someone to infringe their privacy or they were promiscuous themselves to allow men to have access to them. Eventually, they stopped meeting those people and were always socially awkward. They are usually labelled as people with no honour and less social dignity. In case of women, their experiences are mostly kept secret to avoid problems in seeking good marriage proposals. In case of men, affluence plays a significant role. They are not bullied post trauma as much as women are. Trans people, however, are not even considered as part of the mainstream community. Nonetheless, most people from trans community support the victims by providing them help and emotional support.

5.1.3 Lack of Trust

The victims of digital crimes struggle with trusting people online and in real world. They feel devastated and violated. They tend to look at other people with doubt. They are unable to form new relationships and friendships. Women victims are too often scared to trust people around them. They develop paranoia and become delusional . One of the victims exclaimed that my experience has made me cautious to the point of delusion. Even the slightest doubt makes me shiver. Others told me that they feared that they were being watched and followed by someone. As victims, in most cases, do not know their perpetrators, so they look at all strangers with doubt. Trans people mentioned that most of them stopped participating in those activities which threatened them. Most of them eluded cities and vanished from social media. One of the trans activist faced so much threats online that she stopped going out of her house. She started to develop neuropathic pain.

5.1.4 Learned Helplessness

Victims of cyber violence might accept a situation that they cannot comprehend, even if it makes them uncomfortable. When people face abuse they consider themselves as helpless. This helplessness is a product of learned behaviour where the victims consider themselves as the cause of the atrocity. Women are usually culturally conditioned to tolerate intense behaviours. Similarly, in cyber space where the perpetrator is anonymous they tend to think that it was meant to happen. In cases where perpetrators were romantic partners or ex-friends, women blamed themselves. They learned that they were helpless and cannot do anything to stop this because they are weak and it was bound to happen.

5.1.5 Problems in Relationships and Family

A cyber stalking victim expressed that his married life was being affected because he was continuously being harassed and stalked by her erstwhile romantic interest, who left him and then came back to harass him. She tried contacting his family and his wife by cat fishing them. She told his wife that he had physical relationships with her and they also have a child. It made the victim's life miserable; however, it got cleared later and she took money to spare him. According the victim, those were the worst five months of his life. Similarly, numerous female victims showed concerns about their romantic relationships and the fear that they had in them.

5.2 Psychological Impacts of Cyber Violence

5.2.1 Depression and Anxiety

The victims of Cyber bullying and harassment face numerous psychological issue including depression, anxiety and social awkwardness. They suffer from mental exhaustion which sometimes translates into physical ailments; for instance, a victim of cyber bullying developed

neurological disorder because of severe depression he faced. Similarly, a victim who was being stalked online was always anxious that she had palpitations and her insomnia worsened. Trans victims also expressed that they felt frustrated, violate and depressed because of continuous threat that loomed.

5.2.2 Suicidal Tendencies

A number of Harassment and bullying victims were at the verge of killing themselves. Bindiya Rana, the head of a trans activist organisation told that when trans people are bullied to the point of frustration they try to end their lives. A victim of identity theft and stalking exclaimed that she tried killing herself but she survived. Numerous people face depression, anxiety and panic attacks because of this; however, a few of them give in and attempt suicide. One of the trans victims told about her friend who killed herself in because of beela violence.

5.2.3 Self Harm

Self Harm included picking on one's skin, cutting the skin, pulling one's own hair, binge eating, burning one's self with lighters and cigarettes. Cuts, scratches, bruises, bite marks or other wounds are normally observed in people who do self harm. Similarly, Excessive rubbing of an area to damage the skin is another kind. Among the victims a few did self harm which included all these activities.

5.2.4 Drug Addiction

Drug addiction such as ice/meth, alcohol, marijuana, LSD, opium and cocaine are the most used drugs. The victims from Karachi's trans community mentioned the problem of substance abuse to overcome depression and anxiety. Two of my female victims, four men and almost all of the trans victims had a history of substance abuse. A few of them were still struggling with drug

addiction and substance abuse. Gender Interactive alliance caters for these cases and provide help and support to all such trans community members.

5.2.5 Paranoia and PTSD

Victims of cyber violence often causes paranoia and anxiety disorders, worrying about everything, making up scenarios in head and drawing conclusion. They start developing negative self image and low self esteem . They may get triggered by different events, insomnia, or indulgence in drugs. They create situations with threatening interpretations. This kind of anxiety leads to the anticipation of danger and negative beliefs. These fears morph into delusion which eventually turns to conviction. This leads to persistent paranoia and fears. The victims told that they felt they were being watched or their accounts were being hacked. One of my male victims told that all of his online activity was monitored and he always felt unsafe while using his phone and credit cards. Similarly, these victims suffer from Post traumatic stress disorder(PTSD) because their trauma leads to a sense of current perceived threat. The painful memories lead to appraisals of numerous intrinsic and extrinsic threats. These traumas keep coming back and haunt them like a spectre. Trans people who suffer beela violence in person and online, their bodies were violated. The thoughts of the abuse keep coming back and it cannot be completely shed. Resultantly, they are always distracted and psychologically disturbed.

5.3 Recommendations to Curb Cyber Crimes

Cyber violence is a menace that must be nipped in the bud because prevention is always better than cure. Apart from legal measures and inaction of cyber crime laws, one must always be cautious and vigilant while using the cyber space. A few victims recommended some measure to be safe:

1- One should spend Lesser time on the internet

2- In case a problems arises, one should seek help from their closed ones and in extreme cases legal help must be sought.

3- On should limit sharing pictures and personal details on the internet.

4- Connections and relationships in real life must be made and one should avoid making friends with strangers on the internet.

5- One should always keep screenshots of conversations as evidence.

One should always be vigilant and avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs. Cyber stalking can be avoided by not disclosing any information pertaining to one self. This is as good as disclosing your identity to strangers in public place. One should never send one's credit card number to any site that is not secured, to guard against frauds.

6. Conclusion

The discourse on violence in Pakistan has been focused on physical violence. It has rarely been studied in the realms of digital spaces that too through the perspective of the victims of cyber violence. The advent of digital age has struck twenty first century like a lightning bolt. It has eased mundane human life and has connected the whole world. Having said that, the cyber space that goes beyond time and space has brought a witches' brew of problems. Cyber violence or cyber crime is the progeny of age of cyber space. It affects men, women and trans genders of all age. They face creepy criminals lurking around in digital spaces. It is very easy to mask one's identity in cyber world and it helps the perpetrators of cyber violence. Cyber criminals hide under the cloak of hidden identities and inflict offence in the form of verbal abuse, stalking, threats, revenge pornography and cyber economic theft etc.

The findings conclude that trans-genders face a major issue which is different than that of men and women. They face organised crime syndicates known as beelas. Erstwhile they operated in the form of gangs hunting down trans community. Now, these organised crime syndicates track and trace trans genders through social media. They hunt them down, upload their personal videos and threaten them. They try to keep them as sex slaves, ask them for intimate videos and pictures. The same groups are the perpetrators of online abuse against trans genders.

The most common victims of cyber violence are women. They face numerous offences at the hands of cloaked perpetrators. They face verbal abuse, unsolicited private pictures, stalking, identity theft, blackmailing and revenge porn. The perpetrators are usually ex intimate partners, friends or someone they have known from their work place. On the other hand, men face similar

crimes but one major crime that they face is economic theft. None of the female respondents in the sample had faced economic crime online.

From the findings, it can also be concluded that these crimes have taken a toll on the social life of the victims. The psychological baggage still haunts them like a spectre. A few of them even tried to take their lives. In addition, anxiety, depression and self harm became their common problems. A few of them tried therapy but most of the victims did not. In some cases the victims blamed themselves and the people around them also blamed them. The concept of honour in case of women was a dominant factor. It kept numerous women from seeking legal help. The research also concluded that these crimes took these victims to social isolation and stigmatization. At the end, a few of the victims gave recommendations which were coupled with researcher's own perspective.

Bibliography

Al-Nasrawi, S. (2021). *Combating Cyber Violence Against Women An Overview of the Legislative and Policy Reforms in the Arab Region.* Emerald Insight. doi:ISBN: 978-1-83982-849-2

Arora, Y., & Sharma, B. (2018, December). The Dark Side of Cyber Pornography. *Pen Acclaims , 4*. doi:ISSN 2581-5504

Bada, M. (2022). The Social and Psychological Impact of Cyber-Attacks . *Benson & McAlaney (2019/20) Emerging Cyber Threats and Cognitive Vulnerabilities, Academic Press* .

Balakrishnan, V. (2015). Cyberbullying among young adults in Malaysia: The roles of gender, age and internet frequency. *Copmuters in human behavior*, 149-157. doi:http://dx.doi.org/10.1016/j.chb.2015.01.021

Battalan, G. (2019, September 30). Anthropology and Research Methodology. doi:https://doi.org/10.1093/acrefore/9780190264093.013.354

Bernard, H. (2006). *Research Methods In Anthropology* (fourth ed.). United States of America : AltaMira press.

Berson, I. R. (2008, september 25). Grooming Cybervictims:The Psychosocial Effects of Online Exploitation for Youth. *Taylor and Francis*, 5-18. doi:https://doi.org/10.1300/J202v02n01_02

Biswas, S. (2015, June). Ethics in Anthropological Research: Responsibilities to the Participants. *Human Biology Review* (4), 250-263. doi:ISSN 2277 4424

Braun, V., & Clarke, V. (2012). *APA handbook of research methods:Thematic Analysis* (Vol. 2). Research Gate. Retrieved from https://www.researchgate.net/publication/269930410_Thematic_analysis

Brezina, T. (2017). General Strain Theory. *Oxford Research Encyclopedia*. doi:https://doi.org/10.1093/acrefore/9780190264079.013.249

Burton, P., & Mutongwiz, T. (2009, December). Inescapable violence: Cyber bullying and electronic violence against young people in South Africa. *Centre for Justice and Crime Prevention*(CJCP no 8).

Chaubey, R. K. (2012). Cyber Crime and its Classification. In R. K. Chaubey, *An Introduction to Cyber Crime and Cyber Law* (pp. 24-37).

Chisholm, J. F. (2006, December 5). Cyberspace Violence against Girls and Adolescent Females. *The New York Academy of Science*, 74-87. doi:https://doi.org/10.1196/annals.1385.022

Cho, Y., DioGuardi, S., Nickell, T., & Lee, W. (2021). Indirect cyber violence and general strain theory: Findings from the 2018 Korean youth survey. *Children and Youth Services Review*. doi:https://doi.org/10.1016/j.childyouth.2020.105840

(2015). *Combatting Online Violence Against Women & Girls:A Worldwide Wake-up Call.* United Nations Educational, Scientific and Cultural Organization. UNESCO. Retrieved August 2021, from https://en.unesco.org/sites/default/files/highlightdocumentenglish.pdf

(2019). *Cyber violence against women and girls.* Europena Institute for Gender Equality.

Dashora, K. (2011). Cyber Crime in the Society: Problems and preventions. *Journal of Alternative Perspectives in the Social Sciences, 3*(1), 240-259.

Dennis, M. A. (2019, September 19). *Cybercrime*. Retrieved from Encyclopedia Britannica : https://www.britannica.com/topic/cybercrime/Identity-theft-and-invasion-of-privacy

Digital Rights Foundation. (2020, July).

Dominy, M. D. (2018, September). Reflexivity. *Research Gate*, 1-3. doi:http://sci-hub.tw/10.1002/9781118924396.wbiea1976

Dorokhova, E., vale, H., Laçí, V., & Mahmutovic, A. M. (2021). *Selected Case Studies and a Cybersecurity Governance approach.* Switzerland: Geneva Centre for Security Sector Governance (DCAF).

(2018). *ELIMINATING ONLINE VIOLENCE AGAINST WOMEN AND ENGENDERING DIGITAL EQUALITY.* The Due Diligence Project. The Office of the High Commissioner for Human Rights. Retrieved from https://www.ohchr.org/Documents/Issues/Women/WRGS/GenderDigital/DueDiligenceProject.pdf

Emerson, R. M. (2012). *ethnographic field notes.* USA: university of chicago press.

Fedorko, B. (2016). *For the Record:Documenting violence against trans people Experiences from Armenia, Georgia, Germany, Moldova, Russia, and Ukraine.* Transgender Europe.

Goldsmith, A., & Brewer, R. (2014, June 10). Digital drift and the criminal interaction order. *Sage Journals, 19*(1), 112-130. doi:https://doi.org/10.1177%2F1362480614538645

Gossman, P. (2020, October 22). Online Harassment of Women in Pakistan. *Human rights watch*. Retrieved from https://www.hrw.org/news/2020/10/22/online-harassment-women-pakistan

Grabosky, P. N. (2001, June 1). Virtual Criminality: Old Wine in New Bottles? *Sage Journal, 10*(2), 243-249. doi:https://doi.org/10.1177%2Fa017405

Herjavc, R. (2021, August 26). *Cyber CEO: The History Of Cybercrime, From 1834 To Present*. Retrieved from Herjavec Group: https://www.herjavecgroup.com/history-of-cybercrime/

Holt, T. J. (2021). *Crime online: correlates, causes, and context* (4th ed.). , Carolina: Durham, North Carolina Carolina Academic Press . doi:9781531020477

Huang, C., Hu, B., Jiang, G., & Yang, R. (2016). Modeling of agent-based complex network under cyber violence. *Physica A*. doi:http://dx.doi.org/10.1016/j.physa.2016.03.066

Impe, A.-M. (2019). *Reporting Against Violence agaist Women and Girls.* United Nations Educational, Scientific and Cultural organization. Retrieved from https://reliefweb.int/sites/reliefweb.int/files/resources/Reporting%20on%20violence%20against%20women%20and%20girls_%20a%20handbook%20for%20journalists%20-%20UNESCO%20Digital%20Library.pdf

Jahankhani, H., Nemrat, A. A., & Far, A. H. (2014, November). Cyber Crime Classification and Characteristics . *Research Gate*, 169-163. doi:10.1016/B978-0-12-800743-3.00012-8

Jamal, S. (2020, July 1). Cyber harassment on the rise in Pakistan. *World Asia*. Retrieved from https://gulfnews.com/world/asia/pakistan/cyber-harassment-on-the-rise-in-pakistan-report-says-1.7235458

King, R. (2017). DigitalL Domestic Violence: Are Victims of Intimate Partner Cyber Harrasment Sufficiently Protected by New Zealand's Current Legislation? *Victoria University of Wellington Law Review, 29*(29-40).

Klimczuk, A. (2015). *The SAGE Encyclopedia of Economics and Society.* (F. F. Wherry, Ed.) Los Angeles: Sage Publications . Retrieved from https://www.researchgate.net/deref/http%3A%2F%2Fdoi.org%2F10.4135%2F9781452206905.n128

Kottak, C. P. (2015). *Cultural Anthropology* (16th.ed ed.). United States of America: McGraw-Hill Education.

Kozinets, R. V. (2014). *Netnography Redefined.* Sage Publications. Retrieved from ISBN 978-1-4462-8574-9

(2015). *Measuring Pakistani Women's Experience of Online Violence.* Lahore: Hamara Internet, Digital Rights Foundation.

Meriam Webster. (n.d.). Retrieved from Meriam Webster : https://www.merriam-webster.com/dictionary/cybercrime

Mohsin, M. (2016, April 16). The Cyber Harassment of Women in Pakistan. *The Diplomat*. Retrieved from https://thediplomat.com/2016/04/the-cyber-harassment-of-pakistans-women

National Response Center for Cyber Crime. (n.d.). Retrieved from Federal Investigation Agency.

(2017). *Online Harassment Report.* Pew Research Center.

(2017). *Online Violence Against Women In Pakistan Submission to UNSR on violence against women.* Digital Rights Foundation.

Peterson, J., & Densley, J. (2017). Cyber Violence: What do we know and where do we go from here? *Aggression and violent Behavior*. doi:http://dx.doi.org/10.1016/j.avb.2017.01.012

Peterson, J., & Densley, J. (2017). Cyber Violence: What Do We Know and Where Do We Go From Here?. Aggression and Violent Behavior. *Research gate , 34*, 193-200. doi:http://sci-hub.tw/10.1016/j.avb.2017.01.012

Powell, A., Scott, A. J., & Henery, N. (2018, July 30). Digital harassment and abuse: Experiences of sexuality and gender minority adults. *Sage Journals*. doi:https://doi.org/10.1177%2F1477370818788006

(2018). *Providing a gender lens in the digital age: APC Submission to the Office of the High Commissioner for Human Rights' Working Group on Business and Human Rights.* Association for Progressive Communications (APC).

Šepec, M. (2019). Revenge Pornography or Non-Consensual Dissemination of Sexually Explicit Material as a Sexual Offence or as a Privacy Violation Offence. *Law Journal of University of Maribor, 13*(2). doi:10.5281/zenodo.3707562

Thotakura, S. (2014, March). Crime: A conceptual Understanding. *Indian Journal of Applied Research , 4*(3). doi:DOI: 10.15373/2249555X/MAR2014/58

Todd, M. (2017, May). Virtual Violence: Cyberspace, misogyny and online abuse. *Research gate*.

Turan, N., Polat, O., Karapirli, M., Uysal, C., & Turan, S. G. (2011). The new violence type of the era: cyber bulllying among university students. *Neurology, psychiatry and Brain Research*, 21-26. doi:http://dx.doi.org/10.1016/j.npbr.2011.02.005

United Nations office on drugs and Crime. (n.d.). Retrieved from https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

Usman, M. (n.d.). Cyber Crime: Pakistani Perspective. *1*(3).

West, J. (2014). *Cyber-Violence Against Women.* University of British Columbia, .

Annexure

Annexure A

Informed Consent Form For the Respondents

Annexure A

Informed Consent Form for Respondents

Assalam o Alikum/Hello

My name is Sadaf Qayyum. I am an Mphil student from the department of Anthropology at Quaid e Azam University, Islamabad. This research is being conducted in the pursuit of completion of my Mphil Degree. The topic of this research is, ' Digital criminality: A Netnographic perspective on cyber crimes in Pakistan.' The aim of this research id to understand the experiences of victims of cyber violence emanating from cyber crime and the socio-psychological impacts on the victims and their subsequent coping mechanisms. It also explore the nature of cyber violence and possible motives of the perpetrators behind such crimes. This research also seeks to incorporate the victim's perspective on digital abuse and their coping mechanisms.

I am conducting an interview with you in order to complete this work. I assure you that all information gathered from you, including your identity, will be used for education purposes only and will be kept strictly confidential.

Your corporation is highly appreciated and significant. Thank you.

Signature of Researcher

I_____, hereby agree that I have read and understood the provided information and have had the opportunity to ask questions. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving a reason and without cost. I am participating in this research on my own discretion.

Signature of the respondent

Annexure B

Interview Guide for the Purpose of in-depth Conversational Interviews

(Female Respondents)

Annexure B

Interview Guide For Female Respondents

Topic: Digital criminality: A Netnographic perspective on cyber crimes in Pakistan

Interviewer: Sadaf Qayyum

---

1. Demographic profile of respondent

Basic information of the respondent:

-Name:

-Age:

-Gender:

-Qualification:

-Occupation:

-Socio-Economic Status:

-Education :

-Marital Status:

-Residence :

2. Cyber Space

2.1 What do you know about Cyber space?

2.2 How do you perceive the concept of Cyber Space?

2.3 What is the usage of Cyber Space for you?

2.4 Do you use social media?

2.5 How many social media apps do you use?

2.6 Which one of the social media application is your favorite?

3. Cyber Violence/Offence/Abuse

3.1 What do you know about Cyber or digital violence?

3.2 Do you know about types of cyber violence?

3.3 Have you ever been digitally abused?

3.4 Do you know someone who has been digitally abused or had faced cyber crimes?

3.5 What kind of Abuse did you face?

3.6 Did you know the offender?

3.7 Would you please explain the nature of relationship with the offender?

3.8 What did the offender do to cause you harm?

3.9 Did you report the crime perpetrated to harm you?

4**. Psychological Impacts**

4.1 How did you feel when you were experiencing this abuse?

4.2 Would you please explain the feelings that you had at that moment?

4.3 Did you try to hurt yourself?

4.4 How did you expect the people around you to behave?

4.4 How did your family behave?

4.5 How did your friends and peers behaved?

4.6 Did you feel anxious?

4.7 How was your sleeping pattern during the phase?

4.8 Did your eating habits or habits in general got affected, if yes how?

4.9 Were you ever diagnosed with depression?

4.10 Did you seek medical help?

5. Social Impacts

5.1 How did it impact your relationship with your peers?

5.2 How did it affect your interaction with people?

5.3 How often did you interact with strangers after that?

5.4 Did you feel ashamed?

5.5 Did you share your experience with your community?

5.6 How did the people around you behave?

5.7 Were your peers forthcoming and supportive?

5.8 Did you feel unsafe after your experience?

6. Coping Mechanism

6.1 What is the first thing that you did after experiencing cyber violence?

6.2 Did you seek legal help?

6.3 What did you do to ward off this online abuse?

6.4 how did you stop this abuse from entering into your real life out of cyber world?

Annexure C

Interview Guide for the Purpose of in-depth Conversational Interviews

(Trans-Gender Respondents)

Annexure C

Interview Guide For Trans-Gender Respondents

Topic: Digital criminality: A Netnographic perspective on cyber crimes in Pakistan

Interviewer: Sadaf Qayyum

---

1. Demographic profile of respondent

Basic information of the respondent:

-Name:

-Age:

-Gender pronoun preference:

-Qualification:

-Occupation:

-Socio-Economic Status:

-Education :

-Residence :

2. Cyber Space

2.1 What do you know about Cyber space?

2.2 How do you perceive the concept of Cyber Space?

2.3 What is the usage of Cyber Space for you?

2.4 Do you use social media?

2.5 How many social media apps do you use?

2.6 Which one of the social media application is your favorite?

3. Cyber Violence/Offence/Abuse

3.1 What do you know about Cyber or digital violence?

3.2 Do you know about types of cyber violence?

3.3 Have you ever been digitally abused?

3.4 Do you know someone who has been digitally abused or had faced cyber crimes?

3.5 What kind of Abuse did you face?

3.6 Did you know the offender?

3.7 Would you please explain the nature of relationship with the offender?

3.8 What did the offender do to cause you harm?

3.9 Did you report the crime perpetrated to harm you?

4. Beela Violence through Beela syndicates

4.1 Who are beelas?

4.2 How do they find people such as yourself?

4.3 How do they operate?

4.4 Do they harass you online?

4.5 Did they ever try to abuse you online?

4.6 Would you please elaborate the mechanics of beela syndicates and your experience with it?

5. **Psychological Impacts**

5.1 How did you feel when you were experiencing this abuse?

5.2 Would you please explain the feelings that you had at that moment?

5.3 Did you try to hurt yourself?

5.4 How did you expect the people around you to behave?

5.4 How did your family behave?

5.5 How did your friends and peers behaved?

5.6 Did you feel anxious?

5.7 How was your sleeping pattern during the phase?

5.8 Did your eating habits or habits in general got affected, if yes how?

5.9 Were you ever diagnosed with depression?

5.10 Did you seek medical help?

6. Social Impacts

6.1 How did it impact your relationship with your peers?

6.2 How did it affect your interaction with people?

6.3 How often did you interact with strangers after that?

6.4 Did you feel ashamed?

6.5 Did you share your experience with your community?

6.6 How did the people around you behave?

6.7 Were your peers forthcoming and supportive?

6.8 Did you feel unsafe after your experience?

7. Coping Mechanism

7.1 What is the first thing that you did after experiencing cyber violence?

7.2 Did you seek legal help?

7.3 What did you do to ward off this online abuse?

7.4 how did you stop this abuse from entering into your real life out of cyber world?

8. Let them speak/ suggest

Would you suggest any measures legal or social to avoid such incidents from happening?

Annexure D

Interview Guide for the Purpose of in-depth Conversational Interviews

(Male Respondents)

Annexure D

Interview Guide For Male Respondents

Topic: Digital criminality: A Netnographic perspective on cyber crimes in Pakistan

Interviewer: Sadaf Qayyum

---

1. Demographic profile of respondent

Basic information of the respondent:

-Name:

-Age:

-Gender:

-Qualification:

-Occupation:

-Socio-Economic Status:

-Education :

-Marital Status:

-Residence :

2. Cyber Space

2.1 What do you know about Cyber space?

2.2 How do you perceive the concept of Cyber Space?

2.3 What is the usage of Cyber Space for you?

2.4 Do you use social media?

2.5 How many social media apps do you use?

2.6 Which one of the social media application is your favorite?

3. Cyber Violence/Offence/Abuse

3.1 What do you know about Cyber or digital violence?

3.2 Do you know about types of cyber violence?

3.3 Have you ever been digitally abused?

3.4 Do you know someone who has been digitally abused or had faced cyber crimes?

3.5 What kind of Abuse did you face?

3.6 Did you know the offender?

3.7 Would you please explain the nature of relationship with the offender?

3.8 What did the offender do to cause you harm?

3.9 Did you report the crime perpetrated to harm you?

4. Money Theft

4.1 Have you ever faced money crime?

4.2 How did you get in contact with the perpetrator?

4.3 How much money did you give them?

4.4 Do you know anyone with similar experiences?

5. Psychological Impacts

5.1 How did you feel when you were experiencing this abuse?

5.2 Would you please explain the feelings that you had at that moment?

5.3 Did you try to hurt yourself?

5.4 How did you expect the people around you to behave?

5.4 How did your family behave?

5.5 How did your friends and peers behaved?

5.6 Did you feel anxious?

5.7 How was your sleeping pattern during the phase?

5.8 Did your eating habits or habits in general got affected, if yes how?

5.9 Were you ever diagnosed with depression?

5.10 Did you seek medical help?

6. Social Impacts

6.1 How did it impact your relationship with your peers?

6.2 How did it affect your interaction with people?

6.3 How often did you interact with strangers after that?

6.4 Did you feel ashamed?

6.5 Did you share your experience with your community?

6.6 How did the people around you behave?

6.7 Were your peers forthcoming and supportive?

6.8 Did you feel unsafe after your experience?

7. Coping Mechanism

7.1 What is the first thing that you did after experiencing cyber violence?

7.2 Did you seek legal help?

7.3 What did you do to ward off this online abuse?

7.4 how did you stop this abuse from entering into your real life out of cyber world?

8. Let them speak/ suggest

Would you suggest any measures legal or social to avoid such incidents from happening?