CYBER-CRIME AGAINST WOMEN IN INDIA: A CASE STUDY OF NAGALAND

Thesis Submitted for the Award of the Degree of

DOCTOR OF PHILOSOPHY

in

Political Science

By

Sarovino Zumvu

Registration Number: 11915248

Supervised By

Dr. Zahoor Ahmad Wani (26083)

Department of Political Science (Assistant Professor)

Lovely Professional University

LOVELY PROFESSIONAL UNIVERSITY, PUNJAB

2025

DECLARATION

I, hereby declare that the presented work in the thesis entitled "Cybercrime Against Women in India: A Case Study of Nagaland" in fulfilment of my degree of **Doctor of Philosophy (Ph. D.)** is the outcome of research work carried out by me under the supervision of Dr Zahoor Ahmad Wani, Assistant Professor, Department of Political Science, School of Liberal and Creative Arts, Lovely Professional University, Punjab, India. In keeping with the general practice of reporting scientific observations, due acknowledgements have been made whenever the work described here has been based on the findings of other investigators. This work has not been submitted in part or full to any other University or Institute for the award of any degree.

(Signature of Scholar)

Name of the scholar: Sarovino Zumvu

Registration No.: 11915248

Department/School: Department of Political Science

Lovely Professional University,

Punjab, India

CERTIFICATE

This is to certify that the work reported in the Ph. D. thesis entitled "Cybercrime Against Women In India: A Case Study Of Nagaland" submitted in fulfilment of the requirement for the award of the degree of **Doctor of Philosophy (Ph.D)** in the Department of Political Science, is a research work carried out by Sarovino Zumvu, 11915248, is bonafide record of her original work carried out under my supervision and that no part of thesis has been submitted for any other degree, diploma or equivalent course.

(Signature of Supervisor)

Name of supervisor: Dr. Zahoor Ahmad Wani

Designation: Assistant Professor

Department/School: Department of Political Science, School of Liberal and Creative Arts

University: Lovely Professional University, Punjab

ABSTRACT

Cybercrime against women in India is a growing concern, driven by the rapid expansion of digital platforms and exacerbated by sociocultural and infrastructural challenges. This paper examines the increasing prevalence of various forms of digital abuse, including identity theft, cyberstalking, online harassment, and the non-consensual dissemination of private images. The situation is particularly dire in Nagaland, a northern state characterized by traditional social norms, low internet penetration, and inadequate cyber law enforcement. These factors contribute to a heightened vulnerability for women, who face significant obstacles such as insufficient legal support, distrust in law enforcement, and societal stigma. The paper highlights the need for a comprehensive approach to combat cybercrime, focusing on enhancing victim support networks, improving law enforcement capabilities, and advancing digital literacy. Collaborative efforts among government agencies, NGOs, and community leaders are crucial for addressing the gaps and providing effective assistance to women affected by cybercrime. The study underscores the importance of raising awareness, developing accessible reporting mechanisms, and strengthening legal and technological frameworks to protect women from the evolving threats in the digital landscape. Cybercrime against women in India has escalated with the proliferation of digital platforms, manifesting in various forms such as cyberstalking, cyber defamation, cyber hacking, cyberbullying, cyber pornography, and cyber grooming. This study focuses on the unique challenges faced in Nagaland, a northeastern state characterized by its conservative social norms and limited digital infrastructure. Despite efforts such as the establishment of a Cyber Forensic Lab cum Training Centre, Nagaland struggles with inadequate resources, low digital literacy, and insufficient legal frameworks to effectively address cybercrime. The paper outlines the different types of cybercrimes prevalent in the region and emphasizes the need for comprehensive strategies to combat these issues. Key recommendations include enhancing victim support networks, improving law enforcement training, and increasing public awareness. By fostering collaboration among governmental bodies, NGOs, and community leaders, the study aims to address the gaps in combating cybercrime and provide more effective support to women affected by digital abuse in Nagaland and beyond.

This study examines the rising concerns related to cyberstalking, non-consensual sharing of intimate images, and online harassment affecting women in the region. Despite limited data specific to Nagaland, national trends indicate a growing incidence of cybercrime, with women across various demographics becoming more vulnerable due to the proliferation of digital communication tools. The state's low internet penetration and conservative cultural norms exacerbate the issue, hindering victims from seeking help and reporting crimes due to fear of social stigma and lack of digital literacy. Legal frameworks like the Information Technology Act of 2000 are in place, but their uneven implementation in Nagaland highlights the need for more specialized local resources and training. Efforts by government and non-governmental organizations to address cybercrime include the National Cyber Crime Reporting Portal and local initiatives aimed at raising awareness and providing support. Recommendations for addressing cybercrime in Nagaland include enhancing digital literacy, improving reporting mechanisms, and equipping law enforcement with specialized tools and training. By implementing these measures, it is hoped that women in Nagaland can experience greater safety and support in the digital landscape. It investigates the impact of cybercrime on women in Nagaland, focusing on their emotional well-being, awareness of cybercrime laws, reporting behavior, and the challenges faced by law enforcement in handling such crimes. The primary objectives are to evaluate how cybercrime affects the emotional health of women victims, examine the relationship between awareness of cybercrime laws and reporting behavior, and explore how experiences of cybercrime correlate with levels of distress. Additionally, the study aims to identify the difficulties encountered by law enforcement agencies in investigating and prosecuting cybercrime against women in Nagaland.

The research employs a quantitative approach using a cross-sectional design to gather data from a sample of 384 women victims. Data collection involves both primary methods, such as surveys and interviews, and secondary sources, including existing reports and academic literature. Statistical tools, specifically SPSS and Excel, will be used for data analysis, employing techniques like mean, standard deviation, correlation, and regression to assess relationships and patterns.

The study hypothesizes that cybercrime significantly impacts the emotional well-being of women, that there is a notable relationship between awareness of cybercrime laws and the likelihood of reporting incidents, and that experiences of cybercrime are strongly related to levels of distress among women. Furthermore, it explores how law enforcement in Nagaland is hindered by a lack of resources and specialized training. The findings aim to provide insights into improving digital literacy, enhancing reporting mechanisms, and equipping law enforcement to better address cybercrime against women in the region.

Key words: Cybercrime, Digital Abuse, Online harassment, Nagaland

ACKNOWLEDGEMENT

As Aristotle wisely remarked, "It is the mark of an educated mind to be able to entertain a thought without accepting it." This insight is particularly relevant in our age of digital information, where the internet constantly challenges and enriches our perspectives.

First and foremost, I wish to express my deepest gratitude to Almighty God for His boundless grace and guidance throughout this journey. I thank God for the opportunity to contribute something meaningful through my work; it has been a privilege to complete my PhD from Lovely Professional University. His wisdom and blessings have been the foundation of my perseverance and success.

I undertook this study, "Cybercrime Against Women in India: A Case Study of Nagaland," to address a pressing issue that has profound implications for women's safety and well-being in a rapidly digitizing world. The increasing incidence of cybercrime, particularly against women, in regions like Nagaland and the realisation that many crimes go unreported prompted me to explore the unique challenges and impacts faced by victims in this context. By examining this issue, I aimed to contribute to the understanding and mitigation of cybercrime, advocating for better protection and support systems for women in vulnerable areas.

I extend my heartfelt thanks to my parents, Mr. Atu Zumvu, NPS, and Mrs. Amen Zumvu and my brothers whose unwavering support, love, and sacrifices have been my greatest strength through the challenges I have during my journey to complete my thesis. Their constant encouragement and belief in my potential have been instrumental in achieving this milestone.

I am profoundly grateful to my supervisor, Dr. Zahoor Ahmad Wani, for his invaluable guidance, insightful feedback, and relentless support. His mentorship has been crucial in navigating the complexities of this research and achieving its successful completion.

I also wish to acknowledge the encouragement and camaraderie of my friends Ms. Sensen Ilang, Ms. Pangjungkala, and Mr. Apangjungba. Their support and shared experiences have made this journey more enjoyable and enriching.

To conclude, I am reminded of the Bible verse from Proverbs 3:6: "In all your ways submit to Him, and He will make your paths straight." This verse has been a source of inspiration and reassurance, guiding me through the challenges of this endeavor.

Thank you all for your invaluable contributions and unwavering support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

Introduction

1.1 Overview

India is seeing an increase in cybercrime against women because of numerous forms of digital abuse that affect women throughout the nation. This covers identity theft, cyberstalking, online abuse, and the unintentional release of private photos. Social conventions and the digital divide in India compound these problems, making women particularly vulnerable. Unfortunately, the quick development of digital platforms has given abusers new ways to target and harass women. Issues like inadequate reporting, low digital literacy, and unreliable support networks continue, even in the face of greater awareness and legal actions. Because of its sociocultural and infrastructure background, cybercrime against women poses particular issues in the northern Indian state of Nagaland. Due to traditional and conservative social standards and the region's very low internet usage, there are not enough resources or awareness available to combat cybercrime. Inadequate legal help, a lack of faith in law enforcement, and fear of stigma are some of the obstacles that women in Nagaland may encounter while reporting cybercrimes. The emphasis placed in society on family honor and privacy may deter victims from coming forward even more. Furthermore, Nagaland's underdeveloped cyber law enforcement and digital literacy may make it more difficult to respond effectively to cybercrime. Improving victim support networks, bolstering law enforcement capacities, and promoting digital literacy are all important components of a multipronged strategy to tackle these problems. Important first efforts include raising awareness of cyber threats and developing easily accessible reporting channels. Furthermore, cooperation between governmental organizations, non-governmental organizations, and community leaders can aid in closing gaps and provide essential assistance to women impacted by cybercrime in Nagaland and elsewhere.

1.1.1 Cybercrime Against Women in India

Cybercrime is any crime that interferes with the functioning of a computer or computer system by using communication and computer technology. The computer can be a target or have been

used to commit a crime (Raina, 2001). It covers offenses like offering or disseminating material via computer networks over the internet and unlawful possession. A computer or computer network can be used in cybercrime.

- A weapon used by criminals
- Someone who falls victim to a crime
- Employed as a byproduct of illegal activity

The crime can only be carried out through the internet. Most cybercrimes consist of confidence tactics perpetrated on naive internet users. The internet has provided new opportunities to make money, even if it's not legal. Everyone should be amazed at the breadth and depth of these cybercrimes; it's mind-boggling how far people will go to cheat someone. There is a continuous evolution in cybercrime. Cyber police have no room to maneuver because of how ever-changing they are (Ram, 2010).

"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 to the victim directly or indirectly using modern communication such as the internet," said Drs. Debarati Halder and K. Jaishankar (2011). The safety and economy of a country could be jeopardized by such crimes. Cracking, copyright infringement, child pornography, and grooming cases are among the most prominent examples of this sort of crime. When sensitive or secret information is intercepted or released, whether legally or otherwise, privacy problems arise (Buch, 1988).

Many different types of actions are included under cybercrime. By committing fraud in this situation, one can gain an advantage by:

- Making alterations without authorization. This kind of theft is prevalent and doesn't require much technical knowledge. It happens when staff changes the data before entering it, input fraudulent data, submit unauthorized instructions, or use unauthorized methods.
- To hide unlawful transactions, it is common practice to alter, destroy, suppress, or steal output. This is not easy to spot.

- Changing or erasing data that has been saved
- Making unauthorized changes to preexisting system tools or software packages, or developing code with the intent to commit fraud

Cybercrime encompasses not only financial fraud but also identity theft, extortion, and the theft of sensitive data. Terrorists commit cyber terrorism when they gain access to computer systems through hacking, introduce viruses into susceptible networks, deface websites, launch denial-of-service attacks, or threaten via electronic communications, according to the National Conference of State Legislatures in the US. The use of IT for planning and carrying out assaults on computer systems, networks, and telecommunications infrastructure, as well as to electronically communicate information or threaten others, falls under this category (Goni, 2022). Given the pervasiveness of the internet in people's daily lives, it's not uncommon for criminals to target entire nations, communities, or even individual citizens by taking advantage of the anonymity it provides. This allows them to commit crimes undetected and unpunished, unlike when an armed robber is physically present. For many, cyber terrorism represents a grave danger to the US economy, and they worry that another Great Depression would result from an assault. The world of cybercrime is no longer limited to science fiction. As we speak, crimes committed in cyberspace have already occurred. Anyone could fall prey to cybercrime if they are careless when using the internet. Crimes committed online serve different ends and have different motivations. While the banking sector accounts for the vast majority, cybercriminals are believed to profit handsomely from the theft of sensitive information. As they pursue access to sensitive data, they disregard privacy concerns and do not face consequences for their actions. Violations of individuals' privacy and their electronic assets lead to financial benefit through stolen information (Stabek, et al., 2010).

Harassment and exploitation of women occur online when perpetrators engage in cyber violence, which makes use of computer technology to get access to their personal information. Okutan (2019) argues that women are becoming easy prey because they are naive and trusting of others.

One factor that has led to the increase in cybercrime is the difficulty in detecting and proving it, as well as the low reporting rates. Professionals with the right training are essential in the fight against cybercrime since it differs significantly from more traditional types of crime. As a result of cybercrime, women endure disproportionately high rates of psychological and emotional abuse. This form of crime is difficult to address and settle, and it causes most women grief, embarrassment, and melancholy (Gordon, & Ford, 2006).

1.1.2 Types of Cyber Crime

Harassment of women's dignity and mental distress caused by sexually explicit remarks and acts conducted over mobile phones or computer networks is known as cybercrime (McGuire & Dowling, 2013).

What follows is an explanation of the many forms of cybercrime perpetrated against women.

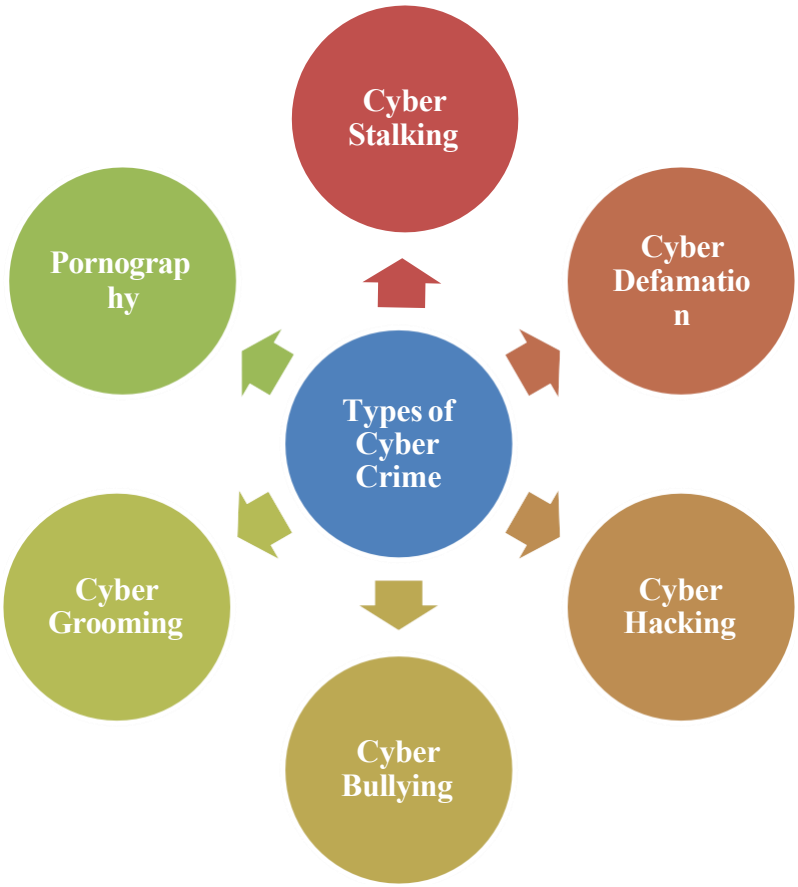


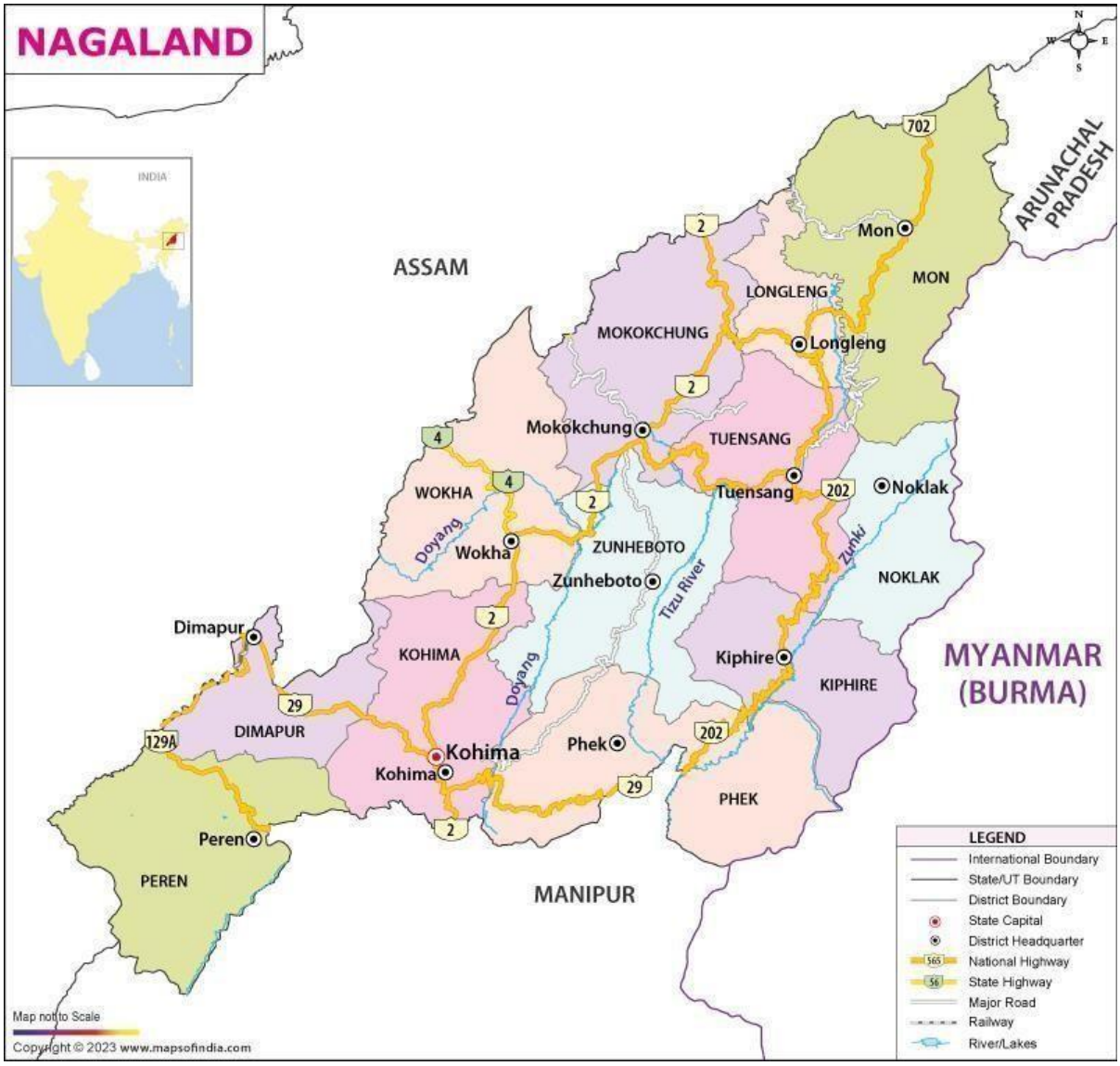
Figure 1: Types of Cyber Crime

- **Cyber Stalking:** In this type of online harassment, the perpetrator makes repeated attempts to contact women through social media without a valid reason, uses the chat feature to threaten the victims, and sends them offensive emails and texts to cause them emotional damage.
- **Cyber Defamation:** Blackmailing someone into revealing personal information or altered photos is an example of defamation. Sexual favors and extortion are common components.
- **Cyber Hacking:** The ladies fell prey to cyber hackers when they were pressured to visit malicious websites or install programs that secretly stored all their data on their mobile devices. The thieves use this information for all sorts of illegal purposes, including making unauthorized financial transactions.
- **Cyber Bullying**: Sexually explicit material, false or deceptive statements, images, or videos, as well as threats of physical harm or death sent to a victim frequently over a digital communication device, constitute cyberbullying.

- **Cyber Pornography**: Cyber pornography is the sharing or accessing of sexually explicit content through digital platforms like the internet or mobile apps. It becomes illegal when it involves sharing of nonconsensual content, involving minors or using morphed pictures. It becomes a criminal offence under laws like the information Technology (IT) Act, 2000 in India.
- **Cyber Grooming:** Here, a man meets a woman online, develops feelings for her, and then uses those feelings to coerce her into giving him sexual favors or engaging in other sexually explicit activities.

1.1.3 Nagaland

The northeastern Indian state of Nagaland is pronounced /ˈnɑːgəlaend/. Immersed in the vibrant tapestry of nature, this land is home to a wide variety of plant and animal species, as well as rivers, verdant hills and valleys, and the joyful sounds of music, dance, and celebrations that accompany them. The state and its people can take advantage of the many natural resources that have been bestowed upon them, such as forests, minerals, good soil, abundant rainfall, and a mild climate, to further their economic development (Agrawal, & Kumar, 2013).



Source: https://www.mapsofindia.com/maps/nagaland/

- **Origin**

An unanswered question is where exactly the different Naga tribes originated from. Finding out where these tribes came from has been a challenge because many of them have been nomadic for generations. According to various scholars, the Naga people have a rich history that includes connections to Indonesia and Malaysia, their origins in the Tibeto-Burman family, their status as the first migration group from northwest China, and their role as a return group of migrants from the Polynesian islands. Nevertheless, these hypotheses have a small but significant impact, and without more proof, they cannot be definitively stated (Agrawal, & Kumar, 2018).

- **Geography**

Nagaland is roughly triangular from a physical perspective. The northern borders of Nagaland are shared with Arunachal Pradesh and a portion of Assam. To the south is Manipur, while to the east is Burma. On the west side, it shares its border with Assam. Along with China to the north, Bangladesh to the west, and Myanmar and Thailand to the east, it is one of the northeastern Indian states that shares international borders. This state's capital is Kohima. About 16,579 square km make up Nagaland. The maximum length of the border is 225 km, while the breadth is no more than 145 km. Most of the summits are between 900 and 1200 meters in height. One of the most prominent features in the Tuensang district is Saramati, the highest point at 3,840 meters with a prominence of 2885 meters above sea level. 1,980,602 people are living in the state, according to the 2011 Indian Census (Agharuwhe, 2013). The state is located between 25°6'N and 27°4'N latitude and 95°20'E and 95°15'E longitude.

As of 1 December 1963 (Jamir, 2016), Nagaland was officially recognized as the sixteenth state of India. At its inception, Nagaland consisted of only three districts: Kohima, Mokokchung, and Tuensang. Thanks to subdivision in 1973, the number of districts increased to seven. By 2004, Nagaland had eleven districts, and in 2017, the Noklak district was founded, making it the twelfth district of Nagaland.

1.1.4 Cyber Crime in Nagaland

Cybercrime, the most prevalent kind, targets everyone with an internet connection; the most common kind of cybercrime is a scheme to steal money from unsuspecting victims. Cybercrime is becoming more of a serious, deadly, and costly problem in Nagaland, even if the region may not be among the most cybercrime-prone in the world. The issue that everyone should be asking themselves is how to stay safe from cybercriminals, as online threats and crimes are always changing. Many different types of cybercrimes have emerged in response to the exponential growth in the use of ICT systems (Bansal, 2012).

The Cyber Forensic Lab cum Training Centre, which is part of the Cyber Crime Prevention against Women and Children (CCPAWC) initiative, was opened at the Police Training School (PTS), Police Complex Chumoukedima, on August 15, 2019. Within the framework of the CCPWC scheme, the Ministry of Home Affairs (MHA) intends to establish

cyber forensic cum training laboratories, recruit a junior cyber consultant, and engage in training and capacity building to supply all states and union territories with training and education for law enforcement agency (LEA) personnel, prosecutors, and judicial officers. Because of the disproportionate number of cybercrimes perpetrated against children and women, it is believed that police officers in Nagaland should undergo specialized training on the tactics used by cybercriminals in these cases. The center must provide comprehensive instruction on all forms of cybercrime, including financial fraud, criminal intimidation, the dissemination of pornographic materials, lottery scams, and other similar crimes. Aier (1998) argues that awareness campaigns, in whatever shape they take, but notably in print and social media, must be ongoing.

The internet and technology are "spinning at a very high speed, while the wheels of justice against cybercrimes are seen to be lacking far behind the evolution and by the time laws or policies are implemented, it will be outdated," so it's important to pay attention to the open book that is cyberspace. Consequently, both a reactive and proactive strategy should be demanded in this regard. By 2020, it is projected that Internet of Things (IoT) devices will account for 25% of cyber assaults on businesses, with 63% of those attacks stemming from stolen login credentials. Mobile devices are used in more than 60% of all internet frauds. For example, when TRAI outlawed bulk SMSs and SPAM, it was one example of how technical spaces are interconnected in an attempt to control cyberspace (Swu, 2021). Cybercriminals are very sophisticated and technologically advanced. The younger generation needs to stay informed on the country's newly approved laws, changes, advisories, and regulations. It is tough to make changes if one is unaware of the regulations and guidelines. The state's police force has found social media, and Twitter in particular, to be a "great help" in its fight against cybercrime. If you're good at using it, social media may be a true boon. All forms of media, whether print, broadcast, or social, complement one another. Rather than being terrified of the "bad things of social media," people can see it as a tool to strengthen communities. People think that education is the key to a better society. It is important to put one's education and knowledge to use in solving societal challenges. The issue that everyone should be asking themselves is how to stay safe from cybercriminals, as online threats and crimes are always changing.

With the already-complicated foundation of online banking and the highly noticeable growth of mobile banking, these financial institutions face a multitude of formidable obstacles when it comes to combating online fraud. The Dimapur police have taken action with financial institutions, such as doing account-level checks that examine logins, transaction types, etc. Examining the analytics and "digging out" questionable actions is crucial. The ADCP and the banks have now resolved to post banners and signboards outside each bank without disturbing clients. Similarly, consumers will know their responsibilities in preventing online offenses and what is expected of them.

A total of 28519 pupils (Alemchiba, 1970) took the higher secondary exam, as reported by the Nagaland Board of School Education (NBSE). Many of those who made it will almost certainly decide to pursue graduate studies in other regions of the nation. This also makes pupils susceptible to applying to bogus schools online and paying exorbitant fees before ever setting foot in the building. Police and banks in Dimapur have decided to launch a program to educate parents and students about the importance of attending accredited institutions (Best, & Kahn, 2009). A disturbing trend seems to be going on in the state: people are constantly posting "lost and found" photos of their identification cards (driver's license, Aadhaar, PAN card, etc.) on social media. This makes it easy for identity thieves to steal the information on the cards and exploit it for their illicit ends. While some may have genuine intentions, there are always some who are looking for a way to take advantage of others. Nineteen cases of cybercrime have been reported thus far, with two of those cases being from outside the state, according to a report from the cyber cell at the Kohima police headquarters. That word spread "wildfire" via various social media platforms is an undeniable fact.

Fighting cybercrime is "bigger than any arms battle," and raising public awareness of the issue is crucial. The general public ought to be inspired to direct their technological energies towards constructive ends (Baban, 2014).

1.1.5 Cybercrime against Women in Nagaland

As digital technology grows more and more ingrained in daily life, cybercrime targeting women in Nagaland is becoming a growing concern. Cyberstalking, non-consensual sharing of intimate photographs, and online harassment are some of the cybercrimes that impact women. There may not be a lot of data on Nagaland specifically, but the trend shows that there is increasing concern. Even in rural areas like Nagaland, the National Crime Records Bureau (NCRB) found an increase in cybercrimes (NCRB, 2022). Unfortunately, women from all walks of life are now more vulnerable to exploitation and abuse due to the proliferation of internet communication tools. Nagaland faces several problems, one of the most significant being the low internet penetration rate in comparison to other states in India. Because of this, cybercrime is more common and victims are less able to use Internet resources to get assistance or report crimes (Kumar, 2023). Women in Nagaland are especially reluctant to report cybercrimes because of the region's traditionally conservative cultural norms. Victims frequently refrain from getting help out of fear of societal shame and harm to family reputation (Rao & Dey, 2022). Women are already at a disadvantage when it comes to knowing how to protect themselves from online dangers, and their low level of digital literacy just makes the situation worse (Basu & Singh, 2024).

The Information Technology Act of 2000 and its revisions are among the legal frameworks that India has put in place to combat cybercrime. Although these rules address different types of online abuse, their implementation is not always uniform, especially in less developed regions such as Nagaland (Mishra, 2023). The absence of dedicated personnel and funding makes it difficult for local law enforcement to adequately investigate and prosecute cybercrime incidents (Sarma, 2024). Further complicating investigations and prosecutions is the lack of specialized cybercrime teams and technological knowledge. Government and non-governmental organizations in Nagaland are working together to tackle cybercrime against women. To make it easier for people to report cybercrimes online, the Indian government set up the National Cyber Crime Reporting Portal (Ministry of Home Affairs, 2023). Nevertheless, obstacles to infrastructure and knowledge may restrict the reach and efficacy of this portal in Nagaland. In addition to national and international organizations, local

community groups and NGOs are conducting workshops, offering counselling, and advocating on behalf of those in need (Nair & Agarwal, 2023). Efforts like these are vital in raising awareness about cyber safety and establishing a network of support for victims. Several steps are suggested to solve the problem efficiently. Women can be better prepared to identify and avoid cyber dangers if they receive an education that focuses on improving their digital literacy (Gupta & Mehta, 2024). To increase the number of women who report cybercrime, it is necessary to strengthen reporting procedures and guarantee confidentiality (Sharma, 2024). Furthermore, local law enforcement can be better equipped to deal with cybercrime crimes and bring victims justice if they are trained and given the tools they need (Singh & Khan, 2023). To summarize, improving digital literacy, strengthening support systems, and equipping law enforcement are all necessary steps to combat cybercrime against women in Nagaland. Women in Nagaland can have a safer online experience by following these steps.

1.2 Review of Literature

There has been a disturbing uptick in cybercrime targeting women in India, particularly in states like Nagaland. According to Kumar (2023), a correlation has been observed between the growth in internet access in Nagaland and an increase in cybercrime cases targeting women. Online harassment and cyberstalking are on the rise, according to the author's study, because more and more people have access to digital platforms. Similarly, **Basu and Singh (2024)** addressed the larger patterns of cybercrime in India and pointed out that, although Nagaland's rates were lower than the national average, there was a worrying increase. They stress that the region's increasing reliance on online communication technologies and social media was likely a factor in this upsurge, highlighting the necessity for specific measures to tackle these new problems **(Kumar, 2023; Basu & Singh, 2024).** Naga women face unique obstacles in combating cybercrime due to a general lack of computer knowledge. According to **Gupta and Mehta (2024),** women were much more susceptible to cybercrime due to a lack of digital literacy. Findings from their study highlighted the fact that many Naga women were vulnerable to cyberbullying since they did not know how to safeguard themselves. **Rao and Dey (2022)** added that cultural constraints make things even more complicated because of the impact of conventional gender roles and attitudes towards technology on women's participation in digital literacy initiatives. Cybercrime was more likely to occur because of these cultural elements, which they argued led to less awareness and unwillingness to seek assistance.

Addressing cybercrime against women was hindered by cultural and social norms in Nagaland. The impact of strong societal expectations and worries of social shame on women's willingness to disclose cybercrime was investigated by **Nair and Agarwal (2023).** The study showed that women were less likely to seek justice when they were confronted with traditional gender roles and standards about family honor. That fits in with what **Sarma (2024)** found, that victims of cybercrime were often reluctant to come forward due to cultural stigmas and social pressures. Cultural obstacles, according to **Sarma**, make it harder for victims to come forward and lessen the impact of efforts to tackle cybercrime in the area.

There were obstacles to the execution of the Information Technology Act of 2000 and other cybercrime legislation in India, especially in the state of Nagaland. Although the legislative framework does offer a foundation for dealing with cybercrime, enforcement was frequently inconsistent, as pointed out by **Mishra (2023)** in the author's study of its efficacy. The study showed that effective legal solutions were hindered by a lack of expertise and resources in Nagaland. Simultaneously, **Singh and Khan (2023)** examined the governmental reactions to cybercrime and pinpointed comparable difficulties in the field of local law enforcement. The importance of better training and resources for law enforcement authorities to successfully handle cybercrime cases was highlighted by the study.

To tackle the mentioned problems, **Gupta and Mehta (2024)** suggested that digital literacy programs designed for Naga women should be improved. They argued that women could be better equipped to safeguard themselves online if there were specific teaching campaigns. At the same time, **Sharma (2024)** stresses the need to make reporting processes more user-friendly and secure. Among Sharma's suggestions were measured to better equip law enforcement to deal with cybercrime cases and the establishment of victim-supportive environments. The two sets of suggestions stress the importance of all-encompassing plans to deal with cybercrime and its effects on Naga women.

A major public health concern that affected the attainment of the Sustainable Development Goals (SDGs) for 2030 was the worldwide incidence of crimes perpetrated against

women. **Pooja (2024)** analyzed data from the National Crime Records Bureau (NCRB) for 2020 to 2022 to perform a thorough study of crimes against women in India. With 145 incidents in Delhi and 5 in Nagaland, the study found that the reported rate of such crimes increased from 57 per 100,000 in 2020 to 67 per 100,000 in 2022. Pooja linked variables like sex ratio and population density to the increase in crime and used ecological and spatial regression models to find major hotspots in Odisha, Telangana, Madhya Pradesh, Haryana, and Rajasthan. To effectively combat violence against women, the study brought attention to the fact that crime rates were spatially unequal and stressed the necessity for targeted interventions in high-risk locations. Similarly, **Murmu (2023)** used statistical methods to investigate significant crimes committed against women in India between 2014 and 2019. The study found disturbing patterns and fluctuations in the incidence of dowry deaths, relative cruelty, kidnapping, human trafficking, rape, and assault, as well as regional and seasonal variations. India has a low worldwide gender gap index rank, and high rates of intimate partner violence and underage marriage, and these crimes continue to rise despite several laws. This highlighted the country's extreme gender difference. Together, the two studies showed that crimes against women in India were becoming worse and more common, highlighting the need for both broad policies and more specific studies to solve this problem.

As developing economies encounter distinct cyber dangers, the proliferation of cybercrime in India has grown into a critical concern. Using a wide range of sources from the fields of economics, criminology, institutional theory, and international relations, **Kshetri (2016)** investigated cybercrime and cyber security in this setting. The research found that cybercrime in developing nations like India is greatly influenced by international, developmental, and institutional factors, as well as by the causes of wealth and poverty and by formal and informal institutions. This is in addition to what **Sahoo and Kapoor (2022)** have already said about the historical context of cybercrime in India, including fraud, identity theft, and hacking, as well as the more modern forms of cybercrime dealt with under the Information Technology Act, 2000. The researchers in this study zeroed primarily on instances of online blackmail and pornography in the Delhi NCR area, drawing attention to the difficulties in regulating and lawfully dealing with such crimes. The complex interplay of legislative, institutional, and developmental elements in forming India's cyber security landscape is shown by these studies, which together highlight the difficulties of addressing cybercrime in the country.

Numerous studies in India have examined the growing problem of cybercrime from different angles. Cybercrime and cybersecurity in emerging economies were influenced by a myriad of factors, including institutional, international, and developmental ones. **Kshetri (2016)** developed a framework that highlighted the importance of these issues. In addition, Sahoo and **Kapoor (2022)** examined the legal aspects of cybercrime, touching on both older forms of crime like hacking and more recent ones protected by the Information Technology Act, of 2000; they zeroed in on instances of blackmail and pornography in the National Capital Region of Delhi. Further complicating matters, **Singson (2006)** investigated the function of Nagaland's Community Information Centres (CICs), highlighting the importance of information and computer literacy in enabling rural communities to overcome obstacles like language barriers and low literacy rates using accessible information and communication technology (ICT) interfaces. To provide light on preventative actions and the efficacy of legal frameworks, **Kapila (2020)** went into additional detail regarding the categories of cybercrimes, the function of offenders, and the development of cyber laws in India. Taken as a whole, these studies demonstrated how complex cybercrime and cyber security were in India, drawing attention to the need to combine legislative, instructional, and institutional approaches to combat this expanding problem. Numerous studies in India have looked at the complicated link between economic and social variables and crimes committed against women. By examining literacy and crime rates for each state between 2001 and 2011, **Roy and Swargiary (2020)** used data from the Open Government Data (OGD) Platform India to study the association between literacy rates and crimes against women. A strong positive association was identified in their analysis, indicating that lower crime rates against women were connected with higher literacy rates. The study highlighted the importance of education in promoting gender equality and making women feel safer. To get insight into crimes perpetrated against women in 28 of India's most populous states, **Chakraborty et al. (2021)** used National Crime Record Bureau data ranging from 2001–02 to 2014–15. Their findings showed that there were large differences between states and that dowry-related offenses were very common. While the study found that economic expansion could lead to an increase in crimes against women at the outset, it tended to decrease once the economy reached a certain point, according to panel regression methodologies. Also, characteristics including parental guidance and education were discovered to lower crime rates,

while social disadvantage and economic poor were associated with higher rates of crime. In light of these results, it is clear that educational and socioeconomic initiatives were crucial in India's fight against and prevention of violence against women.

For a long time, people have debated the nature of literature's impact on society and the extent to which it reflects or shapes societal standards. **Nimbarte (2023)** offered a critical viewpoint on this connection by investigating whether writers can maintain total objectivity when reflecting society in their writing. Although literature aspires to be objective in its subject matter, the study showed that representation was frequently subjective and impacted by the author's biases and personal experiences. As an example of the unbreakable link between literature and social change, Nimbarte argued that literature does more than just reflect society; it also affects it. This was supported by the fact that many social revolutions can be traced back to literary works. **Diya and Beerannavar (2023)** tackled cybercrime in India, highlighting the internet's transformational and destructive role in modern society, in a distinct domain. To determine which regions of India necessitate prompt action, their case study examined cybercrime statistics from seven different zones using data collected by the National Crime Records Bureau (NCRB) from 2010 to 2020. Utilizing primary and secondary data sources from CERT-In, the study also identified the top 10 states in terms of cybercrime rates and investigated the actions done to tackle these problems. Improving security and response services was the goal of this analysis, which sought to develop methods for managing and preventing cybercrime. All of these studies showed how literature and society interact with each other, and they showed how critical it was to respond quickly to new threats like cybercrime.

Cybercrime has been on the rise because the Internet has made people more interconnected and raised serious security issues about the transmission of data and information across networks. As online banking and shopping continue to expand in popularity, cybercrime such as scams and unauthorized access is becoming more common, as highlighted by **Sharma (2024).** In the study the author looked at cybercrimes, the people who commit them (hackers, crackers, etc.), and how cyber laws in India have changed over the years. Cyberlaw deals with matters about the Internet, cyberspace, and online security. Cybercrime prevention and the practical considerations of these regulations were also covered by Sharma. In a related vein, **Barman (2020)** investigated the widespread problem of violence against women in India, drawing attention to the devastating effects this has on victims, their families, and the community

at large. Domestic violence, child marriage, rape, and female infanticide are just some of the crimes against women that went unreported owing to shame and fear, according to the study. The importance of tackling these complicated concerns, whether it's through better legal frameworks for cybercrime or better societal reactions to crimes against women, was highlighted in both studies. Thus, comprehensive methods were needed to solve these important issues.

There has been a lot of study and research done because the rise of cybercrime and crimes against women was a major worry. By highlighting the many risks and hazards that consumers encounter online, **Tanwar et al. (2020)** brought attention to the growing seriousness of cybercrime. Cybercrime trends were illustrated in their study using graphs and pie charts, which highlighted the critical need for continuing vigilance by comparing current data with earlier studies. Crimes against women in India have been on the rise since the 2012 Nirbhaya event, according to research by **Maiti and Das (2023),** who looked at the data from 2006 to 2018. According to their data, there was a clear partisan divide in the distribution of state crime rates, with certain states routinely having the largest number of recorded events and others having the lowest. On one hand, they found five states with consistently high crime rates: Uttar Pradesh, Andhra Pradesh, Maharashtra, West Bengal, and Madhya Pradesh. On the other hand, five states with consistently low rates: Goa, Manipur, Mizoram, Sikkim, and Nagaland. The survey also found that crime rates have been much higher since Nirbhaya than they were before. The combined findings of both studies highlighted the critical importance of taking immediate action to resolve these issues: strengthened cyber security measures to counteract cybercrime and specific initiatives to lessen gender-based violence

Extensive research on gender inequality, cybercrime, and child abuse in India has shown multifaceted cultural, social, and economic obstacles. From 1995 to 2015, gender-based crimes including dowry killing, rape, molestation, and torture were researched across 24 states by **Bhattacharyya et al. (2022).** They found a robust association between various forms of gender-based violence and, using rank correlation and spatial panel regression, they also demonstrated that there were notable spatial and neighborhood impacts, especially in the case of dowry deaths. There was a correlation between fewer dowry deaths more female labor force involvement and the existence of police stations. In a similar vein, **Sharma (2024)** addressed the need for Cyber Law in light of the growing tide of cybercrime as a result of people's greater engagement with the internet. Cybercrime, its offenders, and the development of legal

frameworks in India were all covered in the study. In support of this, **Tanwar et al. (2020)** highlighted the critical need to conduct a thorough study of cybercrime by providing statistics on the growing dangers and contrasting them with earlier studies. At the same time, **Deb and Ray (2022)** looked at child neglect and abuse in India, drawing attention to the cultural normalization of specific abuses such as neglect and physical punishment. They talked about the main causes and effects of abuse, how living conditions play a role and the social and legal actions that are necessary to stop child abuse. All things considered, these studies showed how complex societal problems in India were, ranging from cybercrime and gender-based violence to child abuse, and how critical it was to implement targeted interventions and changes to the law to solve these serious problems.

1.3 Objectives of the Study

1) To evaluate the impact of cybercrime on the emotional well-being of women victims in Nagaland.

2) To examine the relationship between awareness of cybercrime laws and reporting behavior among women in Nagaland.

3) To examine the relationship between experiences of cybercrime and levels of distress among women in Nagaland.

4) To examine the challenges faced by law enforcement agencies in Nagaland in investigating and prosecuting cybercrime against women.

1.4 Hypothesis of the Study

1) There is a significant impact of cybercrime on the emotional well-being of women victims in Nagaland.

2) There is a significant relationship between awareness of cybercrime laws and the likelihood of reporting incidents among women in Nagaland.

3) There is a significant relationship between experiences of cybercrime and levels of distress among women in Nagaland.

1.5 Research Methodology

To answer certain research questions or put hypotheses to the test, the term "research methodology" refers to the methodical approach that is utilized to gather, analyze, and interpret data. To conduct an objective evaluation of the correlations and patterns that are present within the data, this study makes use of a quantitative technique, which emphasizes numerical data and statistical analysis. The use of this method enables accurate measurement as well as the generalization of findings across bigger populations.

1.5.1 Research Design

To carry out a research study, the research design serves as the framework or blueprint. It provides an account of the processes that are involved in the collection, analysis, and interpretation of data to answer particular research questions or hypotheses. To guarantee that the research is methodologically sound and capable of delivering results that are valid and reliable, the design outlines the framework of the study, which includes the sampling procedures, data-gathering approaches, and analytical strategies.

- **Cross-sectional:** One method of conducting research is known as cross-sectional research, which involves gathering information from a particular population or sample at a single point in time. This method offers a snapshot of the variables and the interactions between them at a specific point in time, which enables researchers to analyze and compare a variety of groups or circumstances at the same time. It is possible to discover patterns, trends, and connections through the use of cross-sectional studies; however, these studies do not show causality nor do they take into account transformations throughout time.

1.5.2 Conceptual Framework

A conceptual framework is an analytical tool that can be useful in many different contexts. It could be very helpful in fields where an aerial view is required. It is advantageous for both idea organization and conceptualization.

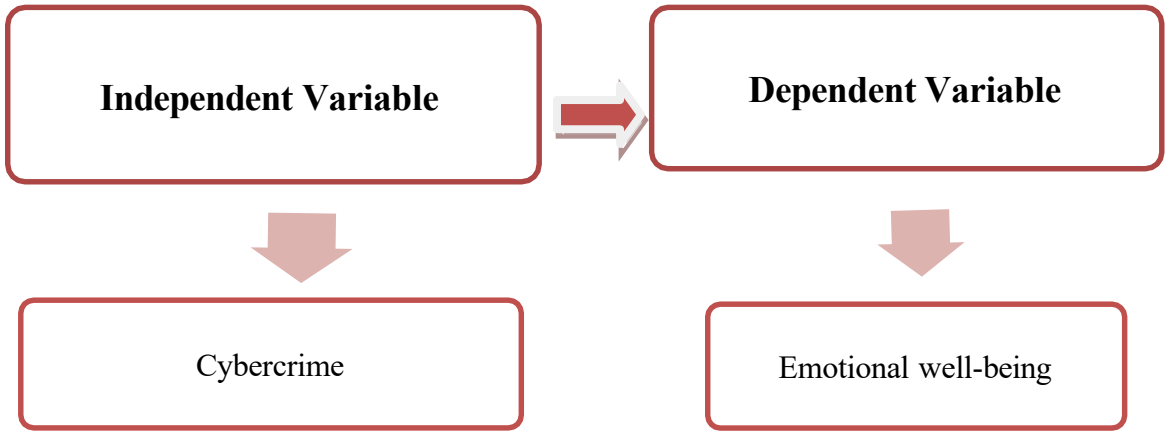


Figure 2: Conceptual Framework

1.5.3 Variable of the Study

Any variable in a study can be altered and, as a result, influences or is influenced by the results. From a research point of view, concepts are sometimes referred to as variables. A variable is something that can be altered, as its name suggests. "This investigation uses two different kinds of variables."

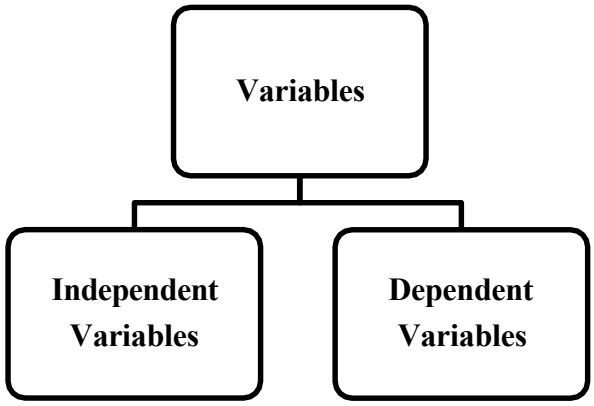


Figure 3: Types of Variables

- **Independent Variable**

"An independent variable is a factor or condition that researchers manipulate or select to examine its effect on the dependent variable in a study". In this context, Cybercrime serves as an independent variable in the study.

- **Dependent Variable**

"A dependent variable is the outcome or response that researchers measure to assess the effects of the independent variable(s) in a study." In the research context, Emotional well-being serves as dependent variables.

1.5.4 Study Area

The study area of the study is Nagaland.

1.5.5 Targeted Population

The target population for the study includes Women Victims

1.5.6 Sample Size

A smaller, more meticulously chosen group of data taken from a broader population through a predefined selection method is referred to as a researcher's "sample." These components could be observations, sample units, or sampling sites. A good research technique is to compile a sample.

The study used a sample size of 384.

Sample Size Determination and Sampling Method

The sample size of **384 respondents** was determined using the **standard sample size formula** for a finite population under a confidence level of 95% and a margin of error of 5%. This is a widely accepted statistical approach in survey research.

Formula Used:

$$\mathbf{n = \frac{Z^2 \cdot p \cdot (1 - p)}{e^2}}$$

Where:

- **n** = required sample size
- **Z** = Z-value (1.96 for 95% confidence level)
- **p** = estimated proportion of population (assumed 0.5 for maximum variability)
- **e** = margin of error (0.05)

$$n = \frac{(1.96)^2 \cdot 0.5 \cdot (1-0.5)}{(0.05)^2} = 384.16 \approx 384$$

Sampling Method:

A **simple random sampling** method was used to collect the data. Respondents were selected in such a way that each individual had an equal chance of being included in the sample. This helped ensure that the sample is representative of the target population and reduces sampling bias.

Example:

The sample size of 384 was calculated using Cochran's formula for a 95% confidence level and a 5% margin of error, assuming maximum variability (p = 0.5). A simple random sampling method was adopted to ensure representativeness and minimize bias in the selection of respondents.

1.5.7 Data Collection

"Data collection refers to the systematic process of gathering information or data from various sources for analysis and interpretation. It involves the collection, recording, and organization of relevant data points or variables that are pertinent to the research objectives or questions. In this study, primary data collection methods are utilized."

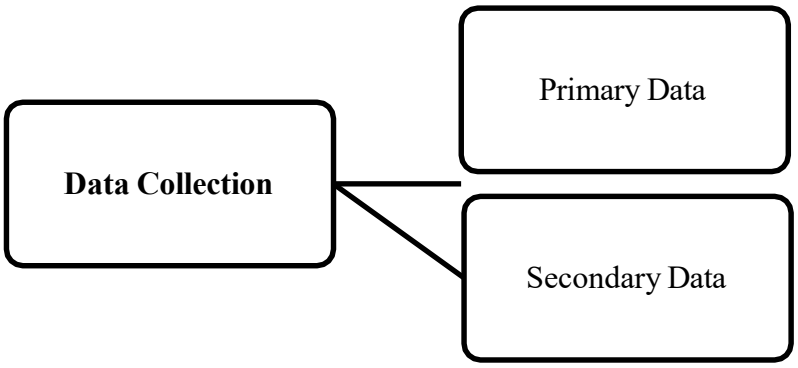


Figure 4: Types of Data Collection

a) Primary data

Primary data refers to information collected firsthand by the researcher directly from sources through methods such as surveys, interviews, observations, or experiments. This type of data is specific to the researcher's study and provides direct evidence to address the research question. It is valued for its accuracy and relevance to the particular investigation.

b) Secondary Data

"Data that has long been amassed and kept up to date by many establishments, such as hospitals and large government agencies". After that, data is collected from a broader variety of sources. Books, scholarly articles, government reports, journals, libraries, the internet, and several organizations are among the many places secondary data has been procured.

1.5.8 Statistical Tools

Planning, designing, collecting, analyzing, and reporting research results are all aspects of a study that make use of statistical methods. Excel and SPSS, two professional commercial statistical tools, will be used to do true statistical analysis in the study.

a. SPSS

An application called “SPSS (Statistical Package for the Social Sciences), commonly referred to as IBM SPSS Statistics is utilized for the statistical analysis of the data”. Although SPSS was originally developed for use in the social sciences, its name suggests that its applications have expanded beyond that field. Several tests to assess the data were carried out using the SPSS as a foundation.

b. Excel

For both checking the precision of hand calculations and learning more about statistical principles that could be used to the solution of practical problems, many people turn to Microsoft Excel, a popular statistical tool. Potentially speeding up the process of doing complicated quantitative research, “the Analysis Tool Pak is a collection of data analysis methodologies”.

1.5.9 Statistical Techniques

Scientific studies may occasionally employ statistical calculations, models, methodology, and statistics in their data analysis. Statistics provides researchers with a tool to mine their data for insights and run a battery of reliability tests on their results. Of the several statistical methods considered, four were ultimately selected according to the assumptions and objectives: “Mean, Standard Deviation, Correlation and Regression.”

a. Mean

“Simply divide the sum of all the data points in the dataset by the total number of data points to get the meaning of the dataset”. You can use these expressions in place of “arithmetic means” at will. By averaging two or more integers, a numerical value called the “mean” is reached. Lots of methods exist for finding the average of a collection of numbers. You can find the meaning in two different ways: the geometric mean method involves averaging a collection of products, and the arithmetic mean method involves adding up all the integers in the series. Typically, the most popular ways for calculating a simple average produce quite consistent result.

b. Standard Deviation

“A statistical measure of the usual dispersion of data is the standard deviation. It shows the standard deviation of each result from the mean”. In a low standard deviation, the numbers tend

to cluster close to the center, but in a high standard deviation, they are widely dispersed around the mean.

c. Regression

Regression models let us see how changes in one or more explanatory factors relate to changes in the dependent variable. Multiple linear regression makes use of several independent variables to explain the result, while simple linear regression makes use of a "single independent variable" to explain the "dependent variable."

$$\boldsymbol{Y = a + bX + u}$$

d. Correlation

"A statistical concept called correlation is utilized to quantify how much two variables change concurrently". When both variables move in the same direction, there is a positive correlation between them. This is the only condition under which this is true. A negative link exists between two variables if they have a propensity to move in opposite directions.

$$\mathbf{"r = \frac{\sum(xi - \bar{x})(yi - \bar{y})}{\sqrt{\sum(xi - \bar{x})\,2\,\sum(yi - \bar{y})\,2}}"}$$

Scheme of Research

Chapter 1: Introduction The introduction sets the context by defining cybercrime against women in the Indian context and specifically within Nagaland. It Includes

1.1 Overview

1.2 Review of Literature

1.3 Objectives of study

1.4 Hypothesis of the Study

1.5 Research Methodology

Chapter 2: Status of Women in Cyberspace Cybercrime is defined at the outset of this chapter, which also serves as an introduction to women's standing in cyberspace, outlining their involvement and the difficulties they encounter in Nagaland. Topics covered include women's experiences with privacy invasion and internet harassment. By focusing on local viewpoints and issues, this chapter investigates how these difficulties show up in Nagaland's distinctive cultural and social setting.

Chapter 3: Understanding Cybercrime against Women in Nagaland The complex landscape of cybercrime perpetrated against Naga women is explored in Chapter 3. The bankruptcy delves into many forms of cybercrime, including harassment, bullying, and stalking, against the backdrop of Nagaland's diverse cultural heritage and growing online connectivity. It takes a look at the criminal justice system and available aid programs, as well as the impact of commonly held beliefs and standards on reporting and victim reactions. Specific instances are shown through case studies, which are light on difficult topics like underreporting and enforcement gaps. To lessen the effect of cybercrimes on women in Nagaland, both now and in the past, guidelines are being suggested to raise awareness, fortify criminal legislation, and boost assistance services.

Chapter 4: Governance, Law, Prevention, and Precaution In Chapter 4, we look at the laws and policies that regulate cybercrime against women in Nagaland. It covers the current rules and regulations, as well as any loopholes in their execution. Cybercrime is a growing problem in this area, and this chapter aims to address that problem by suggesting ways to protect women in this area. Taking into account both regional and federal initiatives, it also discusses more comprehensive methods to curb cybercrime.

Chapter 5: The Manifold Experience of Cybercrime Survivors: Insights from Empirical Research This chapter shares the results of a study that looked at the lives of people in Nagaland who had survived cybercrime. Insights obtained from victim surveys or interviews are included, illuminating the various repercussions and difficulties encountered by women. To further understand these experiences in the context of the local area, specific case studies or examples can be provided. Implications for practice and policy grounded on empirical results round out the chapter.

Chapter 6: Analysis and Interpretation a thorough analysis and interpretation of the data collected during the research.

Chapter 7: Conclusion and Suggestions A thorough conclusion to the theory is provided in this chapter. In it, we review the study's important points and talk about what they mean for our knowledge of cybercrime against women in Nagaland and India at large. To help legislators, police departments, and members of civil society tackle the problems highlighted, this chapter provides concrete suggestions. Additionally, it acknowledges the study's larger significance and proposes directions for further investigation.

Chapter 2

Status of Women in Cyberspace

2.1 Introduction

The era of digitization has impacted almost every aspect of human existence, which makes it very hard to talk about contemporary society without talking about the digitization process. Due to the widespread use of Internet connections and other technologies, everyone now has access to crucial information, contacts, and employment opportunities. The change has been most helpful to women, so that through the use of cyberspace, women engage in different sectors, including learning, working, social and political activities, and business. On the other hand, the same technological breakthroughs that paved the way for women's rights advocacy also placed them vulnerable to cyber risks. Trends of cybercrime against women have increased, making social relativities a complex and perilous world. The nature of these offenses extends from expressive Pro-ANA behaviors to criminal ones such as stalking someone online or cyberstalking, distribution of revenge porn, and identity theft. Perpetrators of cyber- victimization threats relish the feature of anonymity that comes with the internet, and the fact that offenders are getting harder to apprehend and prosecute means victims have little protection and remedy. In assessing the current status of women in cyberspace, such an understanding requires a scan of women's experiences, the different forms of cybercrime that they may encounter, and, more importantly, the social and psychological consequences of such crimes. These are issues that are tackled in this chapter, beginning with the fact that the digital world is as much about empowering as it is about victimizing.

The chapter starts by outlining the online terrain for women, establishing what can be achieved online for women and what may be deterrents. It then goes further to classify and analyze the various types of cybercrimes against women and their workings, as well as the implications of the various offenses. Moreover, it explains in depth the social and psychological effects of cybercrimes, the dark side of which is the effect on mental health status, social exclusion, and other social consequences of becoming victims of cybercriminals.

Besides the analysis of women's experience in cyberspace, this chapter also assesses the current legalities and protection practices directed at cybercrimes against women. It looks at the effectiveness of such measures, the police and other related authorities, and the available resources for victims. Thus, by presenting these aspects, the chapter will try to describe the current state of women in cyberspace and their ongoing work on their protection and respect for their dignity in cyberspace.

In conclusion, thus, one can state that there is nothing stronger than the perspective of empowering women in the context of cyberspace, yet one should not disregard the dangers and threats that exist. Preventing cybercrimes and creating a safe environment for citizens in the digital space is possible through the following measures: legal changes, increasing the activity of law enforcement agencies, and creating conditions that would facilitate the identification and assistance of victims of cybercrime. The findings of this chapter are to provide the basis for further research on these topics and to help the author join the discussion on women's safety and empowerment in the context of modern technologies.

2.2 The Digital Landscape for Women

Today, the Internet and various digital technologies are considered essentials, and people of different genders and ages actively participate in various spheres, including, but not limited to, education, employment, social and political activities, and entrepreneurship. In this part, the author examines various issues concerning the digital world and their impact on women.

2.2.1 Opportunities in the Digital World

The use of digital media has opened up a world where information can be easily retrieved by women, social relations have been enhanced, and women have gotten a chance to express themselves

- **Education and Skill Acquisition:**

Technology in the provision of education, through the use of the internet and other e-learning tools, has played a very crucial role in ensuring that women adapt and acquire new skills as well as knowledge, irrespective of their location or economic standards in society. Digital skills training and other online classes and courses provide women with the opportunity to study at their own pace and, therefore, according to their preferences.

- **Social Activism and Advocacy:**

The technology that includes social media and other digital forms of communication has enabled women to engage in social media activities as well as create awareness of various social problems and call for support. Female activism, or feminism, uses global social media to advocate for change on issues affecting female gender, female rights, and social issues.

- **Entrepreneurship and Economic Participation**:

The advancement in the digital economy has created more opportunities for women to do business since they can start businesses with less capital. Success in e-commerce platforms, digital marketing, and online marketplaces has eliminated many barriers that may have restricted women's access to more customers.

2.2.2 Challenges and Risks in Cyberspace

Yet it is not without problems that are characteristic of the digital environment. Quite paradoxically, the bringing of the empowering elements of the net to the masses is why the latter is such a minefield of opportunities and dangerous openings.

- **Cybercrimes Targeting Women**: Women are more exposed to different cybercrimes comprised of cyberbullying, cyberstalking, sharing of bad images, and phishing, among others. These threats are particularly devastating because more often than not, those who perpetrate these vices act behind the mask of the internet, and the search for justice is difficult due to the online nature of some of these crimes.
- **Mental Health and Social Impacts:** From the works of these cybercriminals, they have a profound effect on women's health, interpersonal relationships, and work. Thus, the risk of becoming a victim of online abuse can have negative consequences for an individual's Internet experience and restrict the positive experiences that result from active participation in the online environment.

2.2.3 The Digital Divide

Another issue remains unaddressed, and that is the digital divide, which is still problematic concerning women participating in the digital world. Digitization is still a problem, where access

to technology and the internet is still a problem; users are restricted socio-economically, geographically, and by culture.

- **Socio-Economic Barriers:** There are additional barriers that rural and low-income women will encounter, such as lack of individual access to digital devices, illiteracy on the use of the devices, and cultural barriers to women's use of social media.
- **Bridging the Divide:** There is a need to tackle these issues so as to make sure that the positive effects of such developments are realized in equal measure. Activities concerning raising the quality of connections, lowering the cost of connectivity, and raising awareness among female users in the field of digital technologies are important activities that can help reduce or eliminate the digital gap in communities.

In conclusion, it is possible to state that the spheres of digitalization contain a powerful potential for women's advancement as well as a range of difficulties that need to be solved. Given that cyberspace is both an environment of possibility and vulnerability, it becomes important to establish an understanding of women's experiences in the online environment. The cultivation of digital literacy and the reduction of inequalities in accessing technologies and seizing the opportunities of online economic spaces, as well as the legal and support environments' strengthening, are the key factors in achieving the goal of establishing a safe digital society. In the midst of engaging with numerous challenges of the modern world, it is crucial to make sure that new technologies can enhance the idea of equality for women from different parts of the world.

2.3 Types of Cybercrimes Against Women

The fast-growing adoption of the digital world and networking has made the world greatly connected and informed, but at the same time, it has created new types of crimes. One of the most dangerous trends in the field of cybercrime is that women become the primary victims of various types of cyber threats, the consequences of which are primarily psychological, social, and economic. This section aims at presenting an elaborated description of the most well-known subcategories of cyber crimes against women, namely, cyberstalking and online harassment, non-consensual sharing of intimate images, mostly known as revenge porn, and phishing and financial fraud.

2.3.1 Online Harassment and Trolling

Cyberbullying and cyberstalking refer to the process of sending authoritative, threatening, or insulting and otherwise hostile messages via online communication means for the purpose of causing discomfort to the recipient. This can happen on the social networking site, in the chat rooms, over email, or via an instant messaging app. The audacity is highly likely to increase because internet usage has a tendency to give the perpet finalists a level of anonymity that would not be possible offline; hence, they have a reduced chance of facing the consequences in the short term.

- **Impact on Victims:**

Stalking, in particular, has various consequences that the victims may experience, and the main ones concern psychological ones. Persons who become victims suffer from stress, depression, and a feeling of powerlessness. The latter, especially highlighted by the perpetrators, leads to increased feelings of shame, as the victim and witnesses of the act are usually related to an extensive public. At worst, the effects may be severe and include the development of psychiatric disorders such as post-traumatic stress disorder (PTSD).

- **Case Studies**

There has been increased coverage of the effects of cyberbullying, especially on women, through various key breeds of cases. For instance, females and other representatives of the media are subjected to threats and trolling in an attempt to make them stop expressing opinions and sharing information. These cases reflect the problem of gender-based violence, which is relevant to modern society, and the need to preserve the female population of social networks and other global networks.

2.3.2 Cyberstalking

Criminal stalking entails the utilization of the World Wide Web, among other forms of internet media, to stalk, or, in other words, harass, an individual. This can comprise stalking the victim through social media, sending him or her unwanted and threatening messages besides posting false information, and, in the extreme, hacking into his or her accounts to get relevant information. Different from stalking, cyberstalking can be done from a distance, and the victim

may not know who is stalking them until they develop consciousness of what the stalker is doing to them.

- **Impact on Victims**

Computer stalking even ends up with drastic changes in the state of mind of the attacked person's security system. The snooping nature of the process and the constant invasion of one's privacy cause severe anxiety and paranoid behavior. The victims feel unsafe in their cyberspace and in their real lives, and thus they isolate themselves and experience a decline in their quality of life. Psychological damage can be life-changing, including issues with trusting people and relating to them in everyday life.

- **Legal and Support Mechanisms**:

Several countries have developed legal provisions to outlaw cyberstalking in detail. For instance, in India, the Information Technology Act, 2000, besides the later amendments to the Indian Penal Code, harbors provisions to penalize cyberstalking. Also, support organizations and helpline numbers assist the victims by offering counseling and legal aid to help them understand the processes of reporting cybercrimes and prosecuting the criminals.

2.3.3 Revenge Porn and Non-consensual Image Sharing

It is the act of sharing explicit materials from someone, especially through the web, without their consent, mainly for the purpose of getting back at them. It can be implemented in scenarios involving close people where certain kinds of private photos are taken for blackmailing or insulting the victim. Such sharing can also happen within the context of the victim having her or his image published without her or his consent, through theft of passwords, piracy, or through any other invasive means.

- **Impact on Victims:**

The investment that one makes in one's emotional and social well-being is often incalculable, and the latter's damage from revenge porn and non-consensual image sharing is colossal. Emotional effects mainly consist of symptoms such as shame and feelings of guilt, violation, and the like. Here, social isolation, deteriorated relations with friends and family, and job losses are the consequences of publicly shared intimate photographs or films. Apart from general depression, there have been cases where the victim has attempted suicide due to the trauma.

- **Case Studies and Legal Responses:**

There are high-profile cases that have been reported in the media about revenge porn. For instance, a number of stars have had their personal naked photos circulated and shared on the internet, and this was followed by a media storm. Legal approaches to revenge porn differ from country to country; however, many legal systems have provided new legislation to outlaw revenge porn. In India, legal actions against such offenses are protected under Section 66E of the Information Technology Act along with Section 354C of the Indian Penal Code.

2.3.4 Phishing and Financial Fraud

Phishing is a type of cybercrime that aims at the gradual acquisition of sensitive information like passwords, credit card information, PINs, etc. through mimicking trustworthy entities through electronic means. Women become victims of phishing messages and fake websites, as well as social engineering, which is based on trust and aims to obtain information.

- **Impact on Victims:**

The losses that stem from phishing and financial fraud offenses are normally severe. Some effects of identity theft include losing large sums of money, getting denied credit cards and bank loans, and having credit scores lowered. This category consists of stress, anxiety, and such consequences as a lack of trust in the effectiveness of making transactions on the Internet. It takes time and is a complex process for people to rebuild their financial stability following fraud instances by getting legal and financial systems to revoke the fraudster's actions.

- **Preventive Measures and Awareness:**

Phishing and financial fraud can be prevented by several state and organizational measures, such as prevention campaigns, cybersecurity courses, and the employment of measures to mitigate risks, among others. The specific audience of interest is females who require knowledge of the threats posed by phishing as well as the necessity of protecting personal data on the internet. It is partly the responsibility of financial institutions and IT firms to combat phishing since they provide the infrastructure and use friendly means through which users can report suspicious activities.

2.3.5 Other Forms of Cybercrimes

While the aforementioned categories represent some of the most prevalent forms of cybercrime against women, several other cyber threats warrant attention: While the aforementioned categories represent some of the most prevalent forms of cybercrime against women, several other cyber threats warrant attention:

- **Doxxing**: This is the act of sharing personal details of a person (for instance, a home address or phone number) without the other person's consent, and most times with afflicting motives.
- **Deepfake Technology**: The practice of having fake and realistic videos and pictures using artificial intelligence and then using them to humiliate and extort women.
- **Online Impersonation**: Impersonation of another person online by emulating their identity to defraud people or to prejudice the image of the victim.
- **Cyberbullying is a** wider category that includes many formats of cyberbullying, which are aggressive actions that include the use of intimidation, making false statements, and so on.

- **Impact and Legal Frameworks**

The consequences of such crimes can also be similar, including emotional suffering, the damaging of one's reputation, and even physical threats. Such typologies are emerging and splicing the legal systems to cater to them, but enforcement is always difficult due to cyberspace and technological developments.

It is evident from the information given that the world of digital opportunity also meets challenges. While it provides a forum for empowering and connecting women, it also puts them in a position of huge risks and susceptibilities. This paper aims to discuss the kinds of cybercrimes that women face, the effects of these acts, and how prevention strategies for the problems can be established. This calls for the need to enact legal changes, improve crime prevention mechanisms, and increase awareness about the advancement and fortification of services for victims. The protection of the safety and integrity of the online environment remains a matter of great importance to fully realize the opportunities of the digital era to advance gender equality and women's rights worldwide.

2.4 Societal and Psychological Impacts

The consequences of cybercrimes against women as reflected in the victims' lives are indeed numerous and have impacts on the societal and psychological aspects of the victims. Depending on the type of crime, one can experience major mental problems, be an outcast from society, and face problems in personal and working life. To design conducive supporting structures, the effects must be determined to provide help for victims and prevent severe adverse effects attributed to cybercrimes.

2.4.1 Mental Health Consequences

The cross-primarily based evaluation reveals that, amongst the various and rapidly dangerous consequences of cybercrimes for women, one of the most critical is mental health. People who fall victim to cyberbullying, cyberstalking, revenge porn, and other related cases are psychologically affected in various ways. The constant and intrusive cybercrimes make people suffer from chronic stress, anxiety, and depression. The common emotions that victims may describe include feeling dominated and powerless because the digital domain allows the offender constant access to the victim's life. Cybercrimes have several negative impacts on victims, and the effects on victims' mental health can present in different forms. That is, victims of cyberbullying and trolling might have acute stress reactions characterized by sleep and appetite disturbances or a decreased ability to focus. These events comprise cyberstalking that causes hypervigilance, paranoia, and insecurity, which are long-lasting and remain with one throughout their lives. In severe cases, one could be forced to develop PTSD, which is a constant reliving of the abuse received, anxiety that warrants visiting the hospital, and total emotional detachment. Additionally, the same cases of revenge porn and non-consensual image sharing result in deep feelings of shame, guilt, and humiliation because intimate pictures have been disclosed to the public by the actor. Posttraumatic symptoms relate to symptoms of anorexic or bulimic disturbances, especially those concerning body image, low self-esteem, violation by others, and lack of control over the body. The psychological consequences of such circumstances can be rather severe; the victims may have difficulty trusting people and having intimate relationships.

2.4.2 Social Stigmatization and Isolation

The social consequences of cybercrimes against women are not only psychological but also include social exclusion and rejection, as is seen nowadays. That is the reason why, in many cultures, even victims of cybercrimes—those exposed to such abusive actions—are only blamed for being attacked and abused. This social prejudice means that most victims lose their places in society and are rejected by everyone around them, including their own families. The interaction of many cybercrimes with society worsens the social effects of the incidents. For instance, people who are exposed to nasty cyberbullying or perhaps cyberstalking are likely to have some information spread about them that is notoriously misleading. This can result in social isolation since friends, colleagues, or members of the community start avoiding the victim. These feelings make the victims have low self-esteem and end up being isolated from society since they feel people only judge them. In business settings, the effects are no less devastating as well. Either it affects one's performance at the workplace or it has an indirect influence on one's productivity. Victims of cybercrimes among women stand to lose their jobs due to the reputation that has been ruined, in addition to suffering psychologically. Cyber abuse often entails stress and anxiety, and these are factors that know no bounds and will limit one's abilities at the workplace, thereby promoting poor performance and forgoing career growth. On certain occasions, victims will even consider changing their careers or even organizations as a way of having a new workplace free of harassment.

2.4.3 Disruption of Personal and Professional Lives

Two effects of cybercrimes against women are a change in life's course and interpersonal working relationships. Stressful anticipation of such repercussions entails shifts in people's behavior and numerous radical alterations in their daily routines. Boys and girls, women and men, change their behavior, stop attending places they used to go and avoid using social networks to meet the perpetrators. They affect many stages of their lives, including personal and professional ones, so that their changes can affect other spheres as well. In interpersonal relationships, they reduce trust and intimacy since people will be afraid of entrusting their secrets to individuals with such intentions. This is the reason victims remain very protective and suspicious all the time, thinking that their partners or friends may take advantage of them. This

can create conflict and, in some cases, exclusion from social activities, where the most common problem is social isolation. The negative effect of cyber abuse also manifests in the emotional aspect because the victim behaves differently, which means they become easily irritated or anxious, which they can easily transfer to their family. On the professional level, the consequences are the same: people suffer alike and in the same proportion. Females who are victims of cybercrimes also consider dropping out of labor market gradients. The effect that cyber abuse has on the victim is to make them stressed, which results in poor performance and a series of sick leaves. Thus, in those industries where an active Internet presence is vital, like journalism, entertainment, or academia, the threats of further harassment push women to retrench from their professions or abandon them altogether. Quietly, their advancement is halted, while simultaneously, various sectors that require their skills are denied capable employees.

2.4.4 Long-term Psychological Trauma

This is because the psychological effects of these cybercrimes can become long-standing and severe. Perpetrators may present some of the features of a traumatic experience even after the first incident, and the general quality of the life of the victims may be impaired. Cyber abuse and threats cause mental and emotional distress, which results in the breakdown of immunity, weak heart muscles, and other complications related to the stomach. The mental health effects can also cause deficits in thinking abilities, memory problems, problems focusing, and decision-making issues. Counseling and psychotherapy are among the interventions that are important to enable the victims to overcome the psychological effects of cybercrimes. Organizations such as support groups and other community-based services are helpful mainly because they bring together victims who understand each other and assist in the process of rebuilding their lives and confidence. Nonetheless, mental healthcare is a matter of concern mainly due to its accessibility for people in areas with poor healthcare systems and the stigma hindering one from getting professional help from a psychiatrist or a psychologist.

2.4.5 Societal Responsibility and the Role of Institutions

To effectively combat cybercrimes against women, society's social and psychological aspects concerning these crimes should be tackled by governments, legal systems, educational institutions, and technological industries. It is crucial to consistently launch public campaigns to

increase people's inclusiveness and understanding of cybercrime incidents and avoid stigmatizing and blaming their victims. Teachers and schools should help students gain digital literacy and know how to behave on the Internet adequately. Law enforcement agencies, together with legal institutions, should work on the prosecution of cybercriminals to bring perpetrators to justice. The modern threat landscape therefore requires an increase in the legal frameworks and capacity building of personnel dubbed in jurisprudence as law enforcement officers. Moreover, technology companies have duties where they are supposed to protect a user from cyber abuse and come up with laws, rules, regulations, or measures that would check on malicious activities, cases of harassment, and other cases that are related to the abuse of technology. Thus, the consequences of these cybercrimes against women include severe mental health effects, social isolation, changes in interpersonal relationships, and decreased work productivity. Mitigating these impacts therefore goes hand in hand with a combined socio-economic, legal, and educational reform that involves all institutions in society. Thus, only by knowing and preventing such impacts of cybercrimes in the long term is it possible to build a better environment for women in cyberspace and provide them with an opportunity to be active participants in the context of the digital world without fearing such repercussions.

2.5 Legal Framework and Protection Measures in India

The enhancement of the digital platform in India has been a relatively brisk business, and hence several pertinent issues related to cyber security, including the safety of women over such platforms, have emerged. Due to emerging trends and the advancement in the tricks used by the perpetrators, there is a need to have strong impunity laws and protective mechanisms. This section discusses every legal strategy adopted by India to tackle cybercrimes against women, assesses its efficacy, and sheds light on the loopholes.

2.5.1 Information Technology Act, 2000 (IT Act)

The central legislation of India that serves to handle cybercrimes is the Information Technology Act, 2000 (IT Act), passed to deal with matters related to information technology and the internet. This act has been revised many times to reflect changes in the technological terrain and to include special anti-cybercrime provisions regarding women.

- **Section 66E: The violation of privacy rights is another variation of criminal identity.** Section 66E relates to the violation of privacy by publishing or transmitting sexual images of a person's private parts without his or her permission. This particular section targets cases like revenge porn and other non-consensual sharing and distribution of sexual images; thus, it is unlawful to share identifying images of another person without his or her consent. The punishment for such violations is imprisonment for a term not exceeding three years, a fine, or both.
- **Section 67: Publication and Transmission of Electronic Forms of Obscenity** The Indian law that punishes this act is the Information Technology Act of 2000, under Section 67, about publishing and transmitting obscene material in electronic form. This section is generally used to fight cyberbullying and the sharing of intimate material without the subject's consent. It is important for offenders and a person who unlawfully fails to assist to know that the offender may be imprisoned for as many as five years and may be fined, and if there is a subsequent conviction, there may be higher penalties attached to the offender. Sections 67A and 67B further include these provisions for prohibited matters, including the publication of sexually explicit acts and child pornography.
- **Section 69: Authority for Directions for Interception or Monitoring** Section 69 of the IT Act provides the government with the legal authority to issue directions relating to intercepting, monitoring, or decrypting any electronic record for any cause related to the security of India or any part of it. Although this section is mainly designed to protect the national security of a country, it has further significance concerning the prevention of cybercrimes against women by allowing the police force to act against potential offenders in advance.

2.5.2 Bharatiya Nyaya Sanhita, 2023 ("BNS") then Indian Penal Code (IPC) Amendments

The IT Act alone is augmented with specific amendments under the BNS sections to deal exclusively with cybercrimes against women. These amendments further elaborate on the legal possibilities for the victims and guarantee that offenders will suffer punitive consequences for their actions.

- **Section 354D: Stalking**

While stalking in the physical world is criminalized under Section 354D of the IPC, cyberstalking or stalking through electronic media is equally considered a criminal offense. This provision defines stalking as the unauthorized tracking of a woman's use of the internet, email, or any other means of communicating through the use of electronic devices. The offense is an imprisonable one, attracting, on first conviction, up to three years imprisonment and, on subsequent convictions, up to five years imprisonment and fines. The current section is important in safeguarding women from unwanted advances and harassment on social media platforms.

- **Section 507: Criminal Intimidation**

Section 507 of the BNS is dedicated to criminal intimidation through electronic communication that entails threats and harassment. This section is usually applied to matters related to cyberbullying and other related vices whereby the offender exercises perceived anonymity to exhibit threats or otherwise adversely influence the recipient. This is a criminal offense, and the punishment given for such offenses is up to two years of imprisonment.

- **Sections 499 and 500 of the Indian Penal Code deal with defamation.**

Section 499 and Section 500 of the IPC are related to defamation, something that is commonly seen in the online world with the spreading of false information that harms an individual. Under the said provisions, targeted women can seek legal redress for any defamatory material being spread through the Internet and other related technologies, and the perpetrators can be liable to two years of imprisonment and/or a fine.

2.5.3 Effectiveness of Legal Frameworks in India

India has recently evolved a very stringent legal regime to prevent cybercrimes against women; however, what matters most is the practical implementation of such laws in the country. The following factors detract from the optimum operation of these safeguards, which prompts a review of the legal environment's opportunities and obstacles.

- **Awareness and Training of Law Enforcement:**

The first problem facing the policing of cyber crimes against women is the general ignorance and lack of police training on the crimes. Most of the police officers and the judicial arm cannot competently investigate or prosecute digital crimes. As a result, there exist significant gaps in the knowledge of threats, which results in insufficient responses, long investigations, or ineffective

punishment of crimes. Bids to enhance the training and education needs of law enforcement personnel are important in enhancing the working of frames.

- **Jurisdictional issues and international cooperation**

New to cybertorts, the question of when the tort is complete, as well as where and by whom the perpetrator may be apprehended and prosecuted, is challenging because the internet is borderless. Bilateral and multilateral agreements, cooperation, and treaties on mutual legal assistance are crucial in the fight against cybercrimes that transcend national borders. International cooperation and interaction with other countries also prove beneficial for India's legal moves, as it can participate in international forums and cooperate with the police forces of other countries.

- **Access to Justice and Support for Victims:**

The challenges of accessing justice have remained a problem for many victims of cybercrimes, particularly women from the most marginalized groups. This is due to social shame, the threat of repercussion, and ignorance of their legal entitlement in cases of cybercrime. It is also important to ensure that the victims have access to legal services and counseling, as this will help ensure that they report the matter to the court and receive all-around assistance when tendering their evidence.

- **Public Awareness and Digital Literacy:**

Public enlightenment on the prevalent cybercrimes and increased education on the appropriate use of the internet are also critical parts of measures to protect women online. Awareness creation through educational programs will go a long way in enlightening the women on potential dangers that they might encounter, measures they can take to avoid falling prey to cybercriminals, and legal aid that they can seek in case they are victims of cybercriminals. Starting with educational institutions, schools, universities, and various community-based organizations have a significant responsibility for shaping people's attitudes toward digital literacy and security.

2.5.4 Government and Non-Governmental Initiatives

Besides legal measures, many government and non-government organizations in India are also functioning to stop cybercrimes against women and protect the victims.

- **National Commission for Women (NCW):**

The NCW is a government body that focuses on women's issues and can be involved in issues connected with cybercrime against women. The NCW has come up with the following measures to deal with the issue of cyber sexual harassment: a cybercrime cell for women. This cell is meant to handle cases of cybercrime by providing a reporting channel for women, legal aid, and counseling.

- **Cybercrime Reporting Portals**

The Ministry of Home Affairs has started a separate online portal to report cybercrime (www. cybercrime.gov.in) that includes women's cybercrimes. They have incorporated an online reporting system through which the victims of atrocities can make their complaints with the ease they cannot get physically to police stations. The required resources and information concerning cyber safety and legal sections are also available through the portal.

- **NGO efforts and support networks**

There are several active non-governmental organizations (NGOs) functioning in India that are ready to deal with cybercrime victims and promote better cybersecurity measures. Some of the organizations include the Centre for Cyber Victim Counseling (CCVC) and the Internet Democracy Project, which help victims get legal aid and even counseling. The reported local and international NGOs also participate in advocacy and research to bring about changes in policies and sensitize people about the effects of cybercrimes on women.

2.5.5 Recommendations for Strengthening Legal Protections

To enhance the effectiveness of legal frameworks and protection measures against cybercrimes targeting women in India, several recommendations can be considered: To enhance the effectiveness of legal frameworks and protection measures against cybercrimes targeting women in India, several recommendations can be considered:

1. Enhanced Training for Law Enforcement:

The control measures shall include synchronized training of police officers, prosecutors, and judges in the technical aspects of dealing with cybercrime. Analyze: specialized cybercrime units

should be created in officer departments, so they work separately from general police departments and focus only on digital crimes.

2. Improved Access to Justice:

The rights of victims should be respected and protected in such a way that these victims have the easiest path to accessing lawyers and relevant services such as counseling and helplines. Formulate specific cybercrime units in each state and district to give regional perspectives as well as to make the complaint process easier.

3. International Cooperation:

Enhance bilateral and/or multilateral cooperation and treaty-based international legal assistance in combating cross-border cybercrimes. Bilateral cooperation is also required with international organizations and foreign LEAs for the purposes of the exchange of information and resources.

4. Public Awareness Campaigns:

Organize countrywide awareness by creating programs to inform people about cybercrimes, secure internet usage, and available legal options. Educational institutions such as schools, universities, and community organizations have a role to play in the promotion of digital literacy, especially in the promotion of safe use of social media.

5. Policy Reforms

This policy should involve a periodical analysis of these laws and their amendments to be relevant to the current kinds of attacks and tools. Campaign for the integration of gender-sensitive measures in cybersecurity frameworks and guarantee that legislation addresses females' vulnerability online.

6. Support for NGOs and Civil Society

Ensure that there's financial support for the non-governmental organizations and civil society organizations that fight cybercrimes against women. It is due to these organizations that legal aid, counseling, and advocacy are provided to try and support the alleviation of such complaints, and their recognition and backing should be given. India has come up with policies and protection policies on the use of the internet and cases of cybercrime against women. India's legal framework comprises both the Information

Technology Act, of 2000, and the changes in the Indian Penal Code to prevent and punish multiple kinds of digital abuse. Nevertheless, problems in implementing, enforcing, and raising public awareness remain. The Ph of the technical issues debated in the provided case is high. Thus, authoritative training, better accessible justice, international collaboration, and community awareness can help India improve legal and digital safety for women. Government agencies, legal authorities, NGOs, and all the members of civil society must join hands and make sure that women do not feel threatened when considering the virtual world as their playing ground.

2.6 Prevention and Governance: Government and Non-Governmental Programs in India

The incidence of cybercrimes in India, particularly concerning women, has inclined the government as well as non-governmental organizations to establish various prevention as well as governing measures. These programs focus on increasing cyber security measures, helping victims affected by cyber criminals, and increasing the public's awareness of cybercrime. As explained further in this section, these are the main thrusts implemented in India to tackle cybercrimes against women.

2.6.1 Government Initiatives

In this regard, the Government of India has also introduced various measures to curb cybercrimes against women and offer essential assistance to the victims. Some of the legal measures are legal policies, help lines, awareness-generating programs, cybercrime cells, etc.

- **National Commission for Women (NCW):**

The NCW is an autonomous organization that performs the vital function of safeguarding women's rights in India, their rights linked to cyberspace included. Key initiatives by the NCW include: Key initiatives by the NCW include:

- **Cyber Crime Cell for Women:**

This cell enables any woman who has been a victim of cybercrimes to report the matter, seek legal advice, and even seek counseling. It seeks to make it possible to have a quick remedy for the affected victims of harassment and abuse on social media platforms.

- **Awareness Programs:**

Regarding this, the NCW conducts exercises in different parts of the country to inform women about their online rights and ways that they can use to protect themselves online.

- **Cybercrime Reporting Portal (www.cybercrime.gov.in):**

The government, through the Ministry of Home Affairs, created this portal to assist in the online reporting of cybercrimes. The portal enables the victims to file complaints without necessarily moving out of their comfort zone, in this case, their homes, and without disclosure. The website also covers issues of cyber safety and legislation about cybercriminal activities.

- **Cyber Safe Women Initiative:**

The Cyber Safe Women initiative seeks to remind women of safety issues while using the internet and social media. It involves training courses, seminars, and workshops carried out with academic and non-academic institutions in society. Get specific, in particular, these programs are designed to educate women on matters of cyber security, ways of combating cybercrimes, how to protect their identity, and proper use of social networks.

- **Information Security Education and Awareness (ISEA) Project:**

The Ministry of Electronics and Information Technology (MeitY) calls for creating awareness about cybersecurity with different user categories; one of them being women. These outreach activities encompass written and video-based tools such as website content and tutorials, as well as in-person workshops aimed at enhancing the study participants' overall technological competencies.

2.6.2 Non-Governmental Initiatives

Apart from these, several NGOs in India have stepped up to a great extent to fight cybercrimes committed against women. These organizations offer legal aid, counseling, educational information, and advocacy to the victims, as well as creating awareness about cyber safety.

- **Centre for Cyber Victim Counseling (CCVC):** The CCVC is a non-governmental organization that deals with the issues of cybercriminals' victims. It offers various services, including:

- **Legal Assistance**: Facilitating clients on matters concerning legal recourse when handling cybercrimes and how to report or prosecute these crimes.

Counseling Services: Providing counseling services and consoling the victims so that they can be in a position to overcome the ordeal that they have been subjected to.

- **Educational Resources**: Raising public awareness through performance drama, donating products such as flyers on computer security, and raising awareness about cybercrime.
- **Internet Democracy Project**: It is an international NGO with the primary agenda of studying and fighting for the liberty of citizens on the Internet, with a special interest in women's safety on the Internet. Key activities include:
- **Policy Advocacy**: For the sake of appreciable legal reforms in the digital policies and laws that policymakers are formulating, there is a need to engage them in implementing gender-sensitive digital policies and laws.
- **Awareness Campaigns**: initiating programs to educate the populace on the dangers of cybercrimes and the need to exercise caution in matters to do with computer security. Research: carrying out the research work to uncover the effects of cyber violence on women and the formulation of measures to enhance safety in cyberspace.
- **Digital Empowerment Foundation (DEF):** Def represents and nurtures disadvantaged societies' groups by aiming at promoting their technical literacy. Its initiatives aimed at women's digital safety include: Its initiatives aimed at women's digital safety include:
- **Cyber Safety Training**: organizing seminars to ensure women are aware of measures to take when facing cybercrime or how to prevent it.
- **Digital Literacy Programs**: educate women on how to use the internet effectively and safely, especially those in rural areas and the less privileged.
- **Breakthrough India:** Breakthrough India is an NGO that helps to prevent gender-based violence, and it has attacked cyber violence via multimedia appeals and communities. Its initiatives include:
- **Campaigns:** Creating multimedia campaigns to increase consciousness regarding cyber harassment and for voicing women's friendly online space.
- **Workshops**: There is a need to conduct seminars, training sessions, and awareness campaigns among the youth, especially female citizens, on the safe use of social media and how to deal with abusive behaviors.

2.6.3 Collaborative Efforts and Public-Private Partnerships

Besides the roles and initiatives taken by governments and non-government organizations, collaborative measures as well as government-business sector partnerships are equally important strategies for developing a multi-sectoral approach to preventing cybercrimes against women. Such partnerships can help extend and strengthen the scope and outcomes of interventions through the development of resources and knowledge.

- **Public-Private Partnerships:**

Friendly relationships between the government, IT firms, and civil society organizations can result in better strategies for combating cybercriminals and assisting victims. Examples include:

- Tech Company Initiatives**:**

These include collaborating with such major technology players as Google, Facebook, and Twitter in the elaboration of the tools and policies for hate speech detection and removal and in the provision of help to the users in self-protection.

- **Corporate Social Responsibility (CSR) Programs**:

Including private sector corporations in the CSR that address education and assistance for those affected by cyber offenses.

- **Academic Collaborations:**

Thus, cooperation with academic institutions can help to work on the study of cybercrimes and the creation of educational programs. Academic institutions and research entities should play a role in determining the risk assessments of the perpetration of cyber crimes against women, as well as the development of prevention and response initiatives.

- **Community Engagement:**

To extend awareness to as many people as possible, workshops, awareness drives, and grass-roots campaigns should be established within the local communities. Such popular figures in the community as educators, influential personalities, etc. can be the key to raising awareness among the population and directing them to safe Internet practices.

The legal measures and strategies that are used in India to fight and control cybercrimes against women include legislation, government policies, and a role played by NGOs. Despite the improvements in raising awareness and cooperation from the public, there are issues with the actualization and enforcement of such laws and general public awareness. It should be noted that governmental and non-governmental organizations, the business community, and communities themselves should have long-term cooperation for the construction of a female safe space in an increasingly digital world. Hereby, India could use the strengths of these various stakeholders to further improve its attempt to safeguard women in the digital world, as well as their rights and security.

Chapter 3

Understanding Cybercrime Against Women in Nagaland

3.1. Introduction

Technology advancement in the current society has seen unimaginable social communication, information availability, and social relations. However, it has also brought new risks and issues, regarding the security of the subjects, to the aspect of life. One of the more concerning and deceptive forms of threat amongst all these is the emanating cybercrime that has also gone for women's targets, specifically in different countries all over the world. In India, for instance, a country that has many distinct social and cultural environments and is fast embracing the use of computers and the internet, the acts of cybercrime against women are on the increase. Concerning cybercrime and women, this chapter zeroes in on the Northeast Indian state of Nagaland to determine the different forms and the extent to which women are vulnerable. Nagaland, culturally and socially, is going through a process of transformation from communicative practices based on traditional values and norms to those deriving from the principles of modernity. This has led to increased exposure on digital platforms, whereby, while fostering connections, the world has also created a window for the cybercriminals' gang. Just like women in other parts of the globe, the women of Nagaland are stuck between these developing technologies and new threats. Seeing the specific nature of cybercrime in this context, it is crucial to examine the diverse types and incidence ratios of cybercrime.

Cybercrime against women involves all the evil intentions that are carried out using the internet and technology, such as cyberbullying, cyberstalking, identity theft, cyber-extortion tricking women through the internet, processing fake accounts, and other related internet frauds. These distinct categories of cybercrime are different from one another in various aspects; however, they are all characterized by exploitation and abuse and are associated with the use of digital anonymity and availability. However, the nature of these crimes differs in Nagaland as it depends on cultural beliefs and practices, economic status, and the degree of IT integration. Hence, a complex analysis of the mentioned factors will reveal the specific conditions that foster such evolution.

It is critical to note that the description of the intimidation of women in Nagaland through cybercrime correlates with trends identified throughout India at the same time, though the regional uniqueness cannot be disregarded. However, the general awareness of Naga women and girls about the various forms of digital security has not adequately protected them from challenging circumstances in their efforts to seek support and protection for themselves. This is so because many cases go unreported, people are not well-informed, and there is inadequate funding allocated to fight cybercrimes. Police departments and other supporting organizations that work at the local level frequently face challenges related to the use of digital evidence and the lack of specialists in the field. In this regard, the following sections of this paper seek to establish the various forms of cybercrime that are most prevalent when it comes to Nagaland women. Mudslinging, threats, and other forms of cyber abuse, which are expressed on social media platforms are some of the most common phenomena experienced by women. Cyberstalking, which is considered continuous and intruding behavior in cyberspace, increases the feelings of danger and threat in victims as well. Impersonation coupled with identity theft is also a major threat as it entails the misrepresentation of personal details for improper gains, hence affecting the overall reputation. The most concerning threats are sextortion, which is a combination of sexually explicit material to entice a target into providing control over the victim's device or account, and a series of online fraud scams that target financial scams. Awareness that encompasses these cybercrimes entails involving statistics, and the surveying of cases, as well as assessing the issues of reporting and combating these crimes. Most women have difficulties reporting cybercrime due to denial of legal literacy, social labeling, and inadequate technological assistance. These are some of the reasons why many cases are unreported and do not receive any attention, hence the call for an expansion of reporting procedures and legal treatment of cases.

To sum it up, this chapter seeks to explain the degree and variety of cybercrime against the women of Nagaland. In this regard, this chapter aims at identifying and explaining the specific adversities that women in that region encounter to reveal the critical areas of concern that need change and reform. It is upon this understanding that adequate strategies for fighting

cybercrimes and the protection and enhancement of women in Nagaland and similar settings may be formulated and implemented.

3.2 Socio-Cultural Context of Nagaland

Nagaland, on the other hand, is a state with diverse culture, traditions, and social organization systems that remain influential and up-to-date among the natives. This paper proposes that the socio-cultural context prevalent in Nagaland influences the users and especially the women's experiences in both the offline and online environments. This section analyzes the complex social structure of Nagaland and its effects on women, especially on the issue of cybercrime. Analyzing women's roles before and during European colonization, along with the general expectations placed upon women and the shift from traditionalism to modernity, enlightens readers as to the experience of women in the area.

3.2.1 Traditional Gender Roles and Patriarchy

The Naga society is dominated by patriarchy, and gender relations are especially formalized in the beneficiary's everyday practice. This is the authoritarian model of society, where men decide on the main issues of life, head the family, and preserve progeny and family dignity. While men are provided with strong and progressive roles that involve the provision of family needs, not to mention the protection aspect, women are expected to conform to strong roles that include obedience, domesticity, childbearing, and reproductive roles, together with being moral caretakers of the family. These traditional gender roles shape the physical as well as the virtual world for the women of Nagaland. The idea that women should not be provocative and should remain silent is controlling since they cannot roam around as they please. This societal setting puts the lady in a weak position; she cannot speak out or stand up for herself lest she be abused or humiliated by her family or herself. In the digital context, this patriarchal mindset is seen in the following ways: For example, any woman who, for instance, goes to a social media platform or is active in public discussions or writing may be subject to criticism, harassment, or cyberstalking since they are seen as defying traditional roles and expectations. Internet anonymity agitates the perpetrators of violence and enables them to act based on these cultural influences, knowing that they are least likely to face consequences when attacking women. Thus, the unconstructive pressure arising

from the given cultural and traditional expectations keeps women from expressing themselves fully online for fear of coming into conflict with such balancing benchmarks.

3.2.2 Community and Collective Identity

Most of these tribes share quite a similarity in social structure; some of them include the following tribes of Nagaland: Thus, the oneness or shared social entity remains the overarching theme of the social structure in Nagaland. The role of the organization is important to the lives of people and is reflected in the structuring and management of social relations involving the members of different groups of the tribe and clan, decision-making, and even the ways to cope with the adversities in everyday practice. For women in Nagaland, this developed patronage can be seen as a strength, but at times it acts as pressure. To a certain extent, this is because tribal culture is quite tight-knit, and people are expected to be looked after by their relatives as well as neighboring people. On the other hand, this same communal structure demands specific behaviors, especially from women since they are usually regarded as the custodians of the community's honor. The consequences ensuing from this shared identity are important in the sphere of cybercrime. If women become the victims of cybercriminals, the consequences of the attacks are not only at the personal level but in the family or clan as well. This perception of connectivity suggests that a woman's status involves the surveillance of her actions not only by her family but also by the community. Consequentially, the risks of tarnishing the image of the community can make female members fail to report cybercrimes or seek assistance when needed. A victim of cybercrime, particularly if the perpetrator of the crime engaged in cyber-sexual harassment or sexual exploitation, will suffer from social ostracism as they are a member of the large Naga community where everyone's action is testimony to the whole society.

3.2.3. The Intersection of Tradition and Modernity

Nagaland is also in the process of change, where so often there is a clash between animistic beliefs and those introduced by Western civilization. This has led to a total transformation in the social and worldly affairs of people, especially youths, through modern education, technology, and urbanization. But these changes have also brought some aspects of conflict between such traditional aspects as culture and the modern elements that people use in their daily lives.

As for the given theme of this site, the tradition and modernity observed in the context of Sudanese clothes for women. It is possibly both a blessing and a curse. At the same time, the young women of today's generation have opportunities for education, probably freedom, and simple technological independence unseen by previous generations of women. Even though the Kohima and Dimapur women still belong to that traditional structure where they only bear children and take care of their homes, the progress in education and work life has led them to claim or be actively involved in the public sphere. While the modernization process cannot be decoupled from the liberation of women, it is indeed true that the rate at which this process is occurring is exposing women to new types of risks, namely virtual risks. The internet may constitute a source of knowledge and contacts, but at the same time, it is connected with the possibilities of criminal activity. The conflict between traditional gender roles and new opportunities has made women a weak link that might be trapped between the two worlds. For instance, females who use social media to voice their opinions or to participate in activities that are considered deviant may be frustrated by their offline and online communities. Pursuing the democratic liberal paradigm, where women and girls try to merge tradition and progress, they become exposed to cybercriminal activity, including slander and other forms of cyberstalking. Thus, cultural expectations to conserve and remain true to the cultural roots function as a strain for women when they engage in present-day digital culture.

3.2.4 Social Stigma and Victim Blaming

About socio-cultural factors, cyber-stigma, and victimization are two crucial factors that determine why women in Nagaland are at the receiving end of cases of cybercrime. For instance, Naga society is conservative, and that is why such issues as sexual matters, relationships, and reputation, among others, are questions of concern. Females who become on the receiving end of cybercrimes, especially those involving sexual content or harassment, have to deal with a lot of social backlashes. These crimes make it a bit hard for women to stand up and report the incidents or even look for assistance because they feel like they will be rejected by society. Another factor that makes matters worse is that victim blaming is rife. It is therefore for this reason that women are often held responsible for the crimes that are committed against them to the extent of being accused of having provoked the event or they dressed inappropriately in a

way that incurred the attacks. It is preconditioned by the general cultural imperative that women be the bearers of morality and proper conduct. Whenever women are deemed to have crossed these boundaries, they are always forced to take the brunt of it, regardless of the circumstances that surround such an event.

3.2.5 The Role of Religion and Moral Policing

The church is a significant aspect of the lives of the inhabitants of Nagaland; the majority of the people here are Christians. It is essential to recognize that religious institutions and leaders affect various aspects of people's lives and do not merely prescribe beliefs about the spiritual world. Freely, it can be stated that religious scripts are often read in a way that supports conventional gender roles and a woman's role as the pure, modest, submissive daughter and wife. This religious factor can lead to moral policing over women's conduct before as well as after being on the internet. Of particular concern are women whose dress codes, behaviors, or postings on social media are perceived to be inappropriate by religious leaders, the elders within the communities, as well as other women. This moral policing is further evident whenever women are considered to be deviating from the traditional norms, for instance, by speaking out on matters of social justice or even practicing professions that are deemed to be reserved for men. An example of moral policing in the context of the internet is cyberbullying, which entails women receiving threats or criticism over the internet. The Internet makes it possible for people to harshly judge women and turn against them for one reason or another, especially using the demeanor of religion. This environment leads to the creation of a harsh cyber environment for women, especially where they risk being moral crusaders or facing the possibility of an attack at the slightest chance.

This thesis works under the assumption that Nagaland and its people are deeply influenced by both socio-cultural factors inherent in traditions and communal relations with other communities of the region, as well as by traditions that are emerging with the progress of postmodern culture, which also characterizes the state. Patriarchal culture, a huge sense of community, the meeting of tradition and innovation, and the stigma and role of religion all play a significant role in defining the peculiarities of women's experiences in the digital world. Therefore, knowledge of these socio-cultural factors is needed to tackle the problem of

cybercrime against women in Nagaland. Measures that may be employed to reduce cases of cybercrime must consider the social and cultural practices that are practiced in societies today regarding the treatment of women. Thus, only novel approaches rooted in socio-cultural factors can be prescribed to safeguard women and improve the predominant online climate in Nagaland.

3.3. Conceptualizing Cybercrime Against Women in Nagaland

Technological menacing of women in Nagaland refers to a new genre of criminal acts whereby women facing crimes are targets of these criminals over social media platforms through the use of computers and the internet. These crimes have features of the socio-cultural context of the state: high traditional values, homophile structure of the population, and different levels of information. The following section shall explore the form and extent of cybercrime prevalent in Nagaland, accompanied by pertinent case studies.

3.2.1 Types and Manifestations of Cybercrime in Nagaland

- **Cyberstalking**

One of the most rampant types of cybercrime that women in Nagaland face is cyberstalking. It entails the applied use of technology in following and persecuting women continuously. When it comes to the social structure of a state like Nagaland, cases of cyberstalking become highly disastrous as everyone in the community is interrelated with each other.

Cyberstalking Incident in Dimapur

In 2021, there was a case of cyberstalking in which a young woman from Dimapur, the largest city in Nagaland, rejected a man's proposal on social media, only for him to start harassing her. The man, irritated by her rejection, started stalking her on social networks. He has been sending her threatening messages before attempting to hack into her social media accounts, creating fake social accounts just to post bad things about her. The abuse began to go to a higher level when he started posting her address and phone number on social media, where strangers started following her.

- **Online Harassment and Trolling**

Cyberbullying and cyberstalking are common problems in Nagaland since the use of social media is on the rise as a means of communication and confrontation. One finds that women who

are active on social media, especially those who express their opinions on matters affecting society, are harassed, threatened, and bullied by men who come up with obscene and threatening messages.

Online Harassment of an Activist in Kohima

The incident that occurred in 2022 involved a Kohima-based female activist who had been actively advocating for women's rights and gender equity to be trolling collectively. The trolls wearing the cloak of anonymity threatened her on social networks with hate speech, sexual harassment, and even violence. Extended across various platforms, she could not escape his occurrences; thus, the campaign was cohesive. The effect was not simple trauma only on the psychological level but also the loss of the activist's authority within some sections of the community that saw her as disruptive of conventions. The case shows evidence of how, in Nagaland, women who dare to speak against this culture of online harassment can be easily silenced using the cultural bargaining chip, which in this case heavily draws from patriarchy.

- **Non-Consensual Distribution of Intimate Images**

The non-consensual sharing of intimate images, often referred to as revenge porn, is also common in Nagaland. Society, especially the pupils, is conservative; they expect women to be modest and their reputations to be well protected. Besides witnessing the primary violation, victims also experience severe social consequences in the wake of the incident.

Case Study: The 2020 Mokokchung Incident

In 2020, a case was reported in Mokokchung whereby a female's bedroom pictures were leaked by her ex-boyfriend. The pictures were posted on different forums and instant messengers, which inflicted great pain on the victim. In a conservative society like Mokokchung, a case in point is a woman who was sexually harassed; she was chased away by her followers, and she had severe psychological problems. The authorities moved a bit slowly, and there was no one in the region with proper digital forensics skills, which made the perpetrator not be just arrested right away. The incident also shows that there is an urgent need to strengthen the legal system and raise awareness regarding the violation of women's rights and seeking justice in Nagaland.

- **Phishing and Financial Exploitation**

As for the specific type, these phishing schemes in Nagaland state particularly target women, especially the illiterate ones, in the use of computers or common social media platforms. These schemes make the victims disclose their personal as well as financial details, causing them to lose their money as well as their identity.

The 2019 Phishing Scam in Tuensang

An example of such an incident was recorded in 2019 when several women in Tuensang, a district found in Eastern Nagaland, were victims of a phishing fraud. The attackers used emails and text messages, claiming to be from the bank, and requested the women update their information to prevent account freezing. Sadly, due to their lack of knowledge of the con, numerous females gave their information, allowing others to steal from them. The local policemen and the banks were eventually able to track the source of the phishing emails down, but they were not efficient, and as soon as the members of the group were arrested, the victims had already fallen for the scam and lost lots of money. Gullible women of Nagaland are always at the receiving end of multiple cybercriminal activities, which in this case stemmed from ignorance of the rules of the World Wide Web.

- **Cyber Defamation**

Cyber defamation is also practiced in Nagaland, in which one posts unwanted information about a woman to pull her character down. This is especially true if the honor and reputation of an individual and his or her family are preciously held virtues in society.

The Cyber Defamation Case in Phek, 2023

There was a case in the year 2023 involving a lady from the Phek district of the country; she was defamed on social media by her ex-lover in a civil dispute over virtual space. This was done on social media and encompassed such things as cheating on the husband and being dishonest, among other things that are considered taboo in any society. These rumors were quickly relied upon by the local community, to the extent that she was socially isolated, and even their family status was affected. Still, the woman prosecuted the man under the law, but the local police were inept at handling cyber defamation cases as it was their first time handling such cases. This case

illustrates the level of devastation that can be caused by cyber defamation, especially to people from small, interrelated societies such as those found in Nagaland, where people uphold their reputation and status highly.

3.2.2 The Role of Socio-Cultural Norms in Cybercrime Against Women in Nagaland

The socio-cultural culture of Nagaland can be seen as another major factor that determines not only the presence of cybercrime against women but also its effect. Another factor is that the discussed state was traditionally oriented toward the erosion of top-priority values such as unity and honor among stakeholders, which can worsen the results of cybercrimes. The consequences of being a victim of cybercrime are not limited to the specific crime committed; women are further subjected to what can be regarded as secondary victimization through social ostracization. As it has been established, it is the men of Naga society who dominate most of the social platforms, and the existing patriarchal norms help in enhancing the incidence of cybercrimes targeting women. For instance, women who are lobbyists for those who subvert gender roles and norms or those who are considered deviant are vulnerable to cyber harassment. This is because the responses of the community and media to such occurrences tend to suggest wanton protection of relevant order, standards, and norms, with victims being blamed or shamed for the happening of the crime rather than the culprits being punished.

3.2.3 Challenges in Addressing Cybercrime in Nagaland

Nagaland faces several challenges in effectively addressing cybercrime against women, including Nagaland faces several challenges in effectively addressing cybercrime against women, including:

1. **Limited Digital Literacy**: In this regard, the levels of digital literacy of women, especially those from rural areas of Nagaland, are insufficient to guarantee their safety. This makes their status on cybercrimes and their willingness to report it when they are victims all the more vulnerable.
2. **Inadequate Legal Frameworks**: India has legislation that may govern cybercrime; however, enforcing these in Nagaland is hampered by resource, training, and knowledge deficits in the force. In addition, the state's relative isolation and poor access to sophisticated equipment create additional challenges to the enforcement of such laws.

3. **Cultural Stigma**: The cultural stigma associated with being a victim of cybercrime, particularly crimes involving sexual content, prevents many women from reporting incidents. Fear of social ostracization and damage to family honor often outweighs the desire for justice.
4. **Lack of Support Systems**: Pervasive disadvantageously, Nirupama's work revealed that Nagaland has very few resources available for cybercrime victims. Rarely, counseling services, legal help, and community assistance are insufficient or unreachable, and thus, victims of cybercrimes are alone in addressing the consequences.

This conceptual framework of cybercrime against women in Nagaland underscores the use of technology, culture, and law in dealing with such a crime. These cases reveal the practical implications of the crimes mentioned against women in the state, which proves that the issue requires the further development of a complex strategy. These are: improving women's awareness and technical skills in defending themselves against cyber criminals; improving the laws governing cyberspace; and nurturing social structures that will enable women in Nagaland to effectively fight cybercriminals.

3.3 Factors Contributing to Cybercrime Against Women in Nagaland

Nagaland Women's experiences of cybercrime therefore cut across the domains of technology, society, and law. Knowledge of these factors is important when devising means of preventing the mentioned crimes and uplifting the status of women in the twenty-first century. This section aims to identify the main actors involved in perpetuating cybercrime against women in Nagaland, while also offering a brief synthesis of the research findings on women's experience in this context.

3.3.1 Digital Penetration and Technological Literacy

With this development, Nagaland experienced a boost in utilizing digital technology; however, that pulled out the problematic understanding of such technology, specifically for women. Although most of the female population has access to the Internet, many of them in rural areas lack the necessary awareness of the threats connected with the use of the Internet. Due to their poor knowledge of digital education, they fall prey to cybercrime, and the various vices are not immune to phishing, identity theft, or online fraud. For instance, because minimum access to computers is witnessed in rural areas, women crumble when they fall prey to the traps crafted by those in cybercrime. For example, internet access and identity theft, where attackers impersonate genuine organizations to obtain clients' data, have become increasingly common. Due to this,

women in the mentioned areas may not notice the signs of a scam like email or messenger scams, giving out their details to the scammers, losing their money, or falling victim to identity theft. These societies increasingly rely on smartphones and other digital devices, yet there have not been enough educational campaigns to teach people about the threats of cybercrime. This digital divide reveals the inequity in the possession of a device and the lack of knowledge on how to use the internet safely, which makes women in the rural areas of Nagaland vulnerable to cybercriminal activities.

3.3.2 Socio-Cultural Norms and Gender Dynamics

Barely known and less understood are the ways that Nagaland's patrifocal culture affects women's interactions in cyberspace. In many societies, males are supposed to be dominant while females are supposed to be submissive in the same way. This same culture is also reflected in cyberspace, where women are not supposed to be assertive or defy the norms. Such strongly rooted stereotypical notions of gender roles can play out in many different ways, with the use of vulgar language on the Internet, stalking, and slander included. Specifically, women campaigners who protest stereotyped norms that subordinate women or fight for women's rights or equal opportunities to men are particularly viciously harassed on social media. This abuse is not restricted to obscene words, the use of vile language, and threats but also involves other subtle forms of harassment, including cyberstalking by male subjects, where women were continuously hounded and harassed through cyberspace. These gender relations are further intensified by the fact that the Nagas are a rather enclosed community that places high value on individuals' and families' reputations. Defamation of a woman on social media platforms usually comes with severe implications throughout society, including the girl may be banned from social networks, which heavily impacts her social life and influence in society; the family may lose their reputation in society; Therefore, in light of the given facts, it could be seen that the defamation of women on social media platforms has severe implications. This fear simply deters women from reporting cybercrimes or coming out to report abuse.

3.3.3 Lack of Cybercrime Awareness and Reporting Mechanisms

However, this form of criminality is becoming rampant; the women in Nagaland remain unaware of what constitutes cybercrime and where they can turn for help. There are no reporting centres or help centres based on the geographical location of the women, and this fails to help in the

reporting of the cases and inadequate outcomes from the police. There are times when women have no idea of the laws that are in place in India to protect them; some are too scared to report their perpetrators because they would be laughed at; others don't even trust the authorities. This form of underreporting is one of the major hindrances to justice in Nagaland. It is only possible for the government and other agencies to devise appropriate measures to counter cybercrimes if precise statistics of these crimes are available. Likewise, the shun of ' support' which includes counseling for the victims or help from related agencies means that women are alone to deal with the consequences of cybercrimes. The social effect of cybercrime is also looked at as being drastic, especially in the cases of computer fraud or personal harassment, where the victim feels as though he has no power.

3.3.4 Inadequate Legal Frameworks and Law Enforcement

Although India has laws that protect people from cybercrimes, their enforcement in Nagaland is hampered by numerous factors, such as insufficient facilities, manpower, and knowledge about computers and related crimes among the police force. This gap exposes many women victims to inadequate legal remedies, hence the continued prevalence and underreporting of cybercrimes against them. The available technology, apart from being inadequate to deal with the enormity of cyber criminality in Nagaland and across the country, is often lacking in most law enforcement agencies that are required for effective investigation and prosecution of these crimes. Cybersecurity intelligence, which is essential in identifying the attackers' origin and accumulating the proof, is one of the most nascent sectors in digital forensics. Also, inherent bureaucracy and culture in the judiciary system professionally delay the cases, and there is still less consideration for the cybercrime victims. Many times, the victims are discouraged from exercising their right to take legal action for several reasons, such as the time-consuming and complicated process of seeking justice and the possibility of being violated all over again. This is made worse by the irony that most cybercrimes, including cyberstalking or online harassment, can be considered minor offenses or domestic issues by the police, making a lot of seriousness lacking in such crimes.

3.3.5 Role of Social Media and Communication Platforms

Thus, social media has emerged as a bane for women in Nagaland in the sense that it serves both as a boon that retains the upliftment of society as well as a menace that continues to fuel the

objectification of women in society. They help women express themselves and get people together but at the cost of sharply increasing women's vulnerability. The entertainment aspect of most algorithms deteriorates the reputation of the female gender and exposes it to cyberattacks. There is no sufficient moderation or reporting mechanism that can be used on these sites, so the violation is left unrestrained. Cybercrime progresses as early attacks on women primarily occur on social media, where malicious people post and perform undesired actions like harassing, defaming, and pressurizing women. This is because the suspects can easily operate on these accounts without being easily identified or arrested once they launch their attacks. Many women, especially those who share opinions on different social or political matters on social platforms, are harassed by organized trolls to get them off the platforms. These campaigns are sometimes very destructive and have negative effects on victims, including mental health complications, social isolation, and, in some cases, forcing women to leave social media platforms completely. Furthermore, social media platforms are global, so any negative information that is posted rises to the global level faster than it can be regulated, hence being exacerbated. Hence, the causes underlying cybercrimes against women in Nagaland are diverse and would entail an understanding of the socio-cultural environment, technological advancement, and legal processes. In connection with these factors, an atmosphere is created in which women are the subject of various types of malicious activities using the Internet, ranging from phishing and identity theft to harassment and defamation. To overcome these challenges, there should be a multi-faceted strategy: enhancing ICT competence, increasing people’s consciousness about cybercrime, enhancing the legal framework, and engaging the social media platforms in the ownership of their content. Thus, there is a need to have localized support mechanisms that could help the victims find justice and the required support to begin with. Thus, the approach toward combating cybercrime and enabling a safer online environment for women in Nagaland has to be centralized and well-researched.

3.4. Challenges in Addressing Cybercrime Against Women in Nagaland

Nagaland is a state in India where women are experiencing cybercrimes of various forms, which are informed by both cultural and technological features as well as institutional frameworks. These difficulties not only hamper the protection of women but also make the fight for justice for victims more difficult as well. These challenges will be discussed in detail in this section under

the perspectives of socio-cultural, legal, technological, and infrastructural frameworks that affect differently the fight against cybercrime against women in the state under consideration.

3.4.1 Socio-Cultural Barriers

Nagaland is considered a place that's heavily soaked in tradition, with community bonds and patrilineal control of many segments of society. These cultural issues make it extremely difficult to combat cybercrime against women, as they influence gender perceptions of technology as well as justice. Among the sociocultural factors that are seen as problems, the first is a lack of acceptance due to victim-blaming culture in cases of cybercrime against women. In a society that values honor and reputation, especially for women, the shame that comes with being a victim in a cybercrime, for instance, Ackerman's 'coaxing' or sharing of pictures, for example, through Twitter, Facebook, or Snapchat, among others, could be terrible. This attribute commonly results in blaming the victim, whereby the woman is considered at fault for the crime because of her misconduct contrary to cultural and societal norms by interacting with strangers online or providing personal details. This level of vulnerability reinforces the cyclical problem whereby women fail to report cybercrimes or seek assistance due to potential social rejection and becoming a blot on the family, thus allowing criminals to continue with their malice.

The last non-technical barrier is socio-cultural, which entails the roles that women have to play in society; otherwise, they will be considered rebels and deemed unfit for such roles. This is a common place for women in Nagaland, and indeed, in most parts of India, women are confined to a certain culture, which dictates their movements. These same expectations also translate into the cyber world, where a woman may feel limited in the kind and amount of interaction that a technological platform offers her or feel that, somehow, she is being intrusive in something that ought to be regarded as free access to information. Not only does this conservatism hinder women's access to the digital space, but it also does not allow them to claim their rights when they become victims of cybercrimes. This is because women fail to receive support from society, and gender norms have been internalized to the extent that women are on their own in the fight for justice in the matter of cybercrimes.

3.4.2 Technological and Educational Deficiencies

Due to its sprawled region and its largely underdeveloped technology, several women in the rural regions of Nagaland are sometimes even unable to access the internet. This not only limits the opportunities for their interaction with the digital environment but also makes them open to cyber criminals, as they may not know how to protect themselves online since they hardly use the internet. Due to the scarcity of cybersecurity knowledge and infrastructure, users belonging to less privileged backgrounds and communities, as well as the overall population, remain vulnerable and out of touch with modern means of protection against cyber threats. Most women, especially those living in rural areas, do not know how to guard themselves on social media, recognize dangerous signs, or get help once they are targeted by cybercriminals.

In addition, society, or, in other words, the general public, lacks knowledge about cybercrime. Social education campaigns and activities designed to increase people's concern regarding the protective measures for the Internet and the legal sanctions that anybody involved in cybercrime can face are scarce. This lack of awareness poses one of the biggest hurdles to addressing and reporting cybercrimes since many of the affected women do not know whom to report to or that what they are undergoing is a crime that can be prosecuted against. Due to the lack of effective educational programs on cybersecurity for both genders in Nagaland, a significant percentage of the population is open to exploitation, which limits the state's capacity to fight cybercrimes effectively.

3.4.3 Inadequate Legal and Institutional Frameworks

The legal and institutional systems of Nagaland are the other factors where a lot of complications surface when dealing with cybercrime against women. Even though India has laws protecting society from cybercrime, including the Information Technology Act of 2000 and the subsequent amendments to laws against cyber harassment, their enforcement at the state level is often lacking, especially in states like Nagaland. Another of the legal problems is the deficiency of qualified personnel and appropriate infrastructure within the frameworks of law enforcement bodies to carry out investigations of cybercriminal activity. Online crimes are different from traditional crimes in that, apart from specialized skills in computer and digital forensics and cyber security, there is the aspect of cyber law. Currently, a high percentage of policemen and judicial personnel working in Nagaland have

very little education concerning cybercrime; hence, they slow down investigations, incorrectly manage evidence, and, at times, dismiss genuine cases. The lack of such specialists is coupled with the scarcity of digital forensics labs and other essential facilities to properly investigate and prosecute cyber offenders.

Furthermore, the legal process that victims undergo can itself be an invasion that scares women and other prospective victims away, especially given that most are usually or may be pressured into silence by their societies and families. Since the legal process in India is slow and the police officials are especially insensitive to complainants, especially women, this often deters them from filing a case. Some of the reasons why many victims of cybercrime in Nagaland may fail to report may include a perceived or real lack of support from the police and a fear of being further victimized or harassed during the time of prosecution. There is also the problem of the implementation of these laws. All these challenges above, coupled with the problem of the enforcement of laws governing the sector, remain a challenge to the development of the engineering industry. Although current Indian law provides for different kinds of cyber criminality, including cyberstalking and harassment, the implementation of such laws, especially in places such as Nagaland, may not always be a priority. This weakens the legal tentacles and enables the culprits to master ways around the law or even go scot-free because there is no proper way of enforcing the laws.

3.4.4 Cultural Resistance to Legal and Technological Solutions

Legal measures and technological mitigation of cybercrime are, however, accompanied by cultural barriers to their implementation, which is another challenge in addressing cybercrime against women in Nagaland. This is because the introduction of new laws or technological solutions to society is most often resisted by societies that are very conservative in their functioning. This resistance is an outcome of different factors such as people's distrust in the formal legal systems, fear and insecurity, and the thought of leveraging advanced ideas as a threat to traditionalism. From the study, it was clear that most of the time, people in Nagaland, especially those in the rural and tribal regions, are inclined to use traditional conflict-solving systems rather than involving the police or the legal fraternity. These primary systems, though functional in some ways, are not well prepared to deal with the complications of cybercriminals. In addition, there

may be resistance to adopting technology solutions, including the use of technology to improve literacy or the use of IT security measures, mainly due to ignorance or fear. This cultural resistance can impede the efforts of formulating qualitatively high preventive and responsive measures against cybercrimes against women since the culture may resist any changes or contact with the formal sector.

3.4.5 Psychological Impact and Lack of Support Systems

The effect that cybercrime has on the psychological well-being of victims cannot be overemphasized, especially women, and due to the absence of support structures in Nagaland, the feat is quite enormous. Using different types of cybercrimes, such as online harassment, stalking, and defamation, the offenders negatively impact a victim's mental health, which results in anxiety, depression, and feelings of isolation. In turn, for the Nagaland woman, the above-stated psychological effects are enhanced by feelings of shame that accompany the victim's status and are also locked up in the guilt of being rejected by society. Though cybercrime is highly likely to affect one's mental health negatively, there is little provision for helping platforms that can assist an individual in recovering from this ordeal. Psychiatric care is sparse in Nagaland, and more so in the rural zones and there is a poor understanding among the society regarding the need for counseling for cybercrime victims. Since counseling services, support organizations, and other related products are imperative, many women are left to grapple with the harms of cybercrime on their own, which could result in the deepening of psychological injuries and perpetuate the reason why victims cannot seek justice.

It is crucial to depict the vicious circle of isolation and victimization: on one hand, there are social discriminations that lead to stigmatization; on the other hand, there are psychological impacts such as PTSD that prevent people from seeking help. The victims of cyberbullying are mostly helpless, especially women, and if they are left alone without the mechanism to combat this vice, they end up being victimized more and more. Thus, it means that it is high time for Nagaland to employ a more complex approach toward the fight against cybercrime against women, wherein prevention and intervention strategies are to be not only legal and IT-based but also closely connected with mental health and social support.

The issues posed by cybercrime against women in Nagaland emanate from the three main dimensions that refer to the socio-cultural, techno-legal, and institutional framework of the state.

The challenges such as lack of societal support, technological and educational shortcomings, and match, poor laws governing advanced technologies, cultural barriers, and possibly the effect of cybercriminal activities push women into a difficult corner if they seek justice. That way here is showing that solving such aspects entails a holistic and culturally appropriate approach that considers the social context of Nagaland. Such an approach has to encompass steps taken to increase the awareness of the public, enhance cybersecurity and computer literacy, as well as enhance legal regulation and protection of institutions and individuals who became victims of cybercrime. It is only when such connected issues are dealt with that Nagaland can face up to the cybercrime menace and ensure that women are secure in cyberspace.

3.5. Intersectionality: The Role of Ethnicity and Identity in Cybercrime

When discussing Nagaland, the ethnic aspect in combination with identity is a major factor that influences the lives of women who experience cybercriminals' actions. Intersectionality is a theory coined by Kimberlé Crenshaw that focuses on society's categorizations like race, class, and gender, establishing a connection between them and forming a system of oppression or prejudice. The ethnic diversity accompanied by the tribal system in Nagaland adds dimensions to gender and its correlation to cyber-crimes, and the vulnerability of women to them. This section will further elaborate on how the preceding intersecting identities shape and/or intersect with the Naga Women's experiences in matters digital and the consequent implications of combating cybercrimes in this context.

3.5.1 Ethnicity and Tribal Identity

Nagaland is occupied mostly by indigenous tribes, and they have different cultures, languages, and other aspects of life. Tribal identity is part of the existence of the Nagaland people, with immense influence on the tribal social organization and lives of its people. Tribalism for women is as much a lens of pride as it is a lens of pressure since they are the women who are expected to give birth to the next generation of bearers of the cultural heritage and honor of the particular Luos community in question. While this is quite a strong sense of tribal affiliation, it can work against it in today's society. On the one hand, the tribal structure preserves the people and sustains them with the familiarity of brotherhood. At the same time, it can increase the rate of negative consequences of

cybercrime, especially if the crime is related to the dissemination of personal or intimate information on the internet. The following culture that is associated with such occurrences is always heightened by the fact that most of these groups are known to have a small population density, whereby an act of a certain person is deemed to be an act of the entire tribe.

Also, interpersonal ethnic hostility may transcend to the online space; someone or some group can employ cybercriminal activities against women from rival tribes. For example, cyberbullying or virtual venom might not only aim at causing grief to the individual woman, after which her man can come up with a different woman but also as a form of driving home the insult of dishonoring the whole tribe the individual woman belongs to. This combination of ethnicity and tribal affiliation in such occurrences makes cybercrime in such societies a complex event since the motives for the crimes are not disconnected from tribal rivalry and scores set by history.

3.5.2 Gendered Experiences of Cybercrime

It is also essential to point out that women are cybercrime victims four times more likely than men due to cyberstalking, cyber harassment, and other instances of non-consensual sharing of tips. These forms of experience are, however, compounded by Nagaland's ethno-tribes' perceptions of gender differentiation. Women in Nagaland often face a dual burden: they experience the restrictions of their tribes' traditions that set certain requirements for female behavior and at the same time, they feel the challenges coming from the Indian society due to belonging to a minor ethnic group. These dual aspects of Naga women's identity make them even more susceptible to cybercrimes that target women and indigenous people. For example, a woman who is likely to be seen as a defector of the tribe's norms for being assertive in cyberspace or performing unconventional activities will also be targeted for her gender. Her ethnic group could be used as a tool, where the trolls may embark on racially or ethnically harassing her in addition to gender harassment. This means that discriminating against a woman based on her gender and ethnicity, especially in regions where these aspects are greatly valued can cause severe consequences due to a severe attack on her personality resulting from the intersectionality of the discrimination.

3.5.3 Identity-Based Cybercrime

Criminal activities that involve identity theft within the State of Nagaland largely infest women via facets of their tribal and sexual attributes. This occurs in the form of cyberbullying, doxing, the act of sharing one's personal information and cyberstalking. More often than not, such acts are perpetuated to maintain the conventional hegemonic structures within the tribe or over women, representing a threat to the set norms. For instance, a Naga woman involved in the social or political mainstream, especially speaking or writing on issues such as women's rights or Naga rights, may become a target of cybercriminals. These cyber-attacks can range from threats of violence, threatening to post unfavorable information, or hacking into one's account to acquire inaccurate information and post it. It is usually to bring out her incompetence, not only as a lady but also in the image she portrays of her tribe. Sometimes such computer crimes are committed by persons of the same tribe, usually, there are disputes over the concepts of civilization and culture, over the position of women in a tribe. In other cases, they may be from other tribes, and this may be about ethnic issues or any prejudice against the Naga tribes. Therefore, tribal affiliation and being a woman produce a nexus of hazards that expose the female members of these tribes to dangers within and outside their groups.

3.5.4 The Impact of Intersectionality on Access to Justice

Ethnicity and tribal division, as well as gender, also play a role in determining Naga women's ability to seek justice for cybercrime. The various socio-cultural and institutional hurdles described above are further compounded by these multiple identities hence making it very hard for women to ask for or get justice as pointed out above. Essentially, there are legal barriers due to which tribal women face difficulties in seeking the system's assistance; the main one is doubt about the effectiveness of legal actions. This is due to past experiences of the Nagas with the state, where they have been neglected; hence, they resorted to the traditional modes of solving disputes. However, such traditional criminal justice systems are usually not well-prepared to address cybercrimes and, in particular, crimes where digital proofs or cross-border factors are present. Thus, women who become victims of

cybercrime are left between a rock and a hard place, unable to find justice in either the new or traditional legal systems.

Moreover, due to their multiple marginalizations, the representatives of the above-mentioned groups can be discriminated against not only when interacting with the police or within the course of trials but also inside the legal maze as well. Effects of cultural implications include an improved understanding of the reasons for complainants' actions by police officials or a lack of seriousness by the police in handling cases reported by women from certain tribes or ethnic groups. This lack of trust and the structural gender bias can discourage women from reporting cybercrimes, thus deepening the culture of silence and bloating injustice.

3.5.5 Strategies for Addressing Intersectional Cybercrime

In responding to the intersectionality of cybercrimes targeting women in Nagaland, we need to focus on a combination of solutions that adopt ethnicity, tribalism, and gender implications separately. Some potential strategies include:

1. **Community Education and Awareness**: Timely educational sessions for the tribes about cybercrime and its effects on women should be conducted. This can range from public meetings, computer proficiency initiatives, and others, as well as incorporating knowledge about cybercrimes in learning institutions. Such efforts should be culturally appropriate and should engage the community's leaders to encourage people to embrace them, as they are likely to be beneficial.
2. **Strengthening Legal and Institutional Support**: Currently, there is relatively a weak legal and institutional mechanism in Nagaland for Combating Cybercrime. This involves educating the police officers on situations that may affect female persons based on ethnic and tribal norms and practices and also making the laws sensitive to female persons regardless of their status.
3. **Support Networks and Counseling Services**: Therefore, it can be suggested that upon providing culturally appropriate services that include counseling and support structures to women from the Naga tribe, cybercrime victims can be assisted to recover by seeking justice. Such services should be provided to local races and should respect the cultural beliefs of the various tribes.
4. **Collaboration with Tribal Leaders and Organizations**: It is therefore important that the state speak to tribal leaders and organizations to fight cybercrime. Such leaders become an important force in bringing change to the status of women, rights, and protection of rights within the

communities; they could challenge dangerous practices that fuel violence against women and girls in cyberspace.

5. **Advocacy and Policy Development**: This paper called for advocacy to engage state and national policies since such crimes cut across different policies. This entails advocating for the validation of the barriers faced by tribal women together with demanding proper assessment and coming up with programs to meet their needs.

The question of ethnicity and tribalism as well as gender culminates in the fact that solving cybercrime for women is both complex and difficult in Nagaland. The problems of violence against Naga women are quite complex and only culturally sensitive strategies can help solve the issue having regard to both gender and ethnic factors. Thus, appreciating these challenges from the standpoint of intersectionality is essential for designing answers to curb cybercrime occurrences and for ensuring that women's rights and dignity are defended in Nagaland.

3.6. Comparative Analysis: Cybercrime Against Women in Nagaland vs. Other Indian States

3.6.1. Prevalence and Types of Cybercrime

Disruption and other cybercrimes against women are prevalent in different parts of India; however, the magnitude of such offenses and their characteristics may differ considerably. High population density states like Maharashtra, Delhi, and Karnataka which also have high internet usage rates register all forms of cybercrime, including cyber harassment, cyberstalking, and revenge porn. They commonly record increased rates of such crimes because they are more populated and possess advanced network facilities. Nagaland, the subject with a relatively low Internet connection and predominantly rural people, displays other characteristics. Cybercrime is still present even if there is less data regarding it because reporting rates are lower. Challenges that women in Nagaland experience include; low access to Avail digital literacy, and a very strong cultural taboo on online matters. Usually, the cybercrimes reported in Nagaland involve cyberstalking and other similar forms of harassment, and the incidences of hacking, fraud, or other related sophisticated crimes are comparatively lower than in the other developed states there.

3.6.2. Socio-Cultural Factors

It is evident from the analysis of the studies that socio-cultural factors play an important role in determining the characteristics of cybercrime and their reporting. It is worth noting that in states such as Delhi and Mumbai, there is more awareness and sufficient resources regarding the victims of cybercrimes, thus enhancing reporting rates and rescues. These are areas that probably have better access to technology and legal structures when it comes to gender-based violence, and there are probably more organizations dealing with technology-related gender-based violence. As for Nagaland, traditional culture and the role of communities can be considered as the factors that significantly influence the approaches to cybercrime. The collected primary data reveal that due to the extended and tight-knit society coupling and the focus on tribal pride, cybercrime incidents are not reported. Due to this, women are likely to suffer high levels of stigmatization and be under pressure to uphold the honor of the family and tribe, thereby compromising their ability to seek assistance or report a crime that has been committed. Moreover, the low level of digital proficiency and knowledge of women's rights and possibilities intensifies the issue, as some women may even be unaware of their rights and available protection tools.

3.6.3. Legal Responses and Enforcement

As for Nagaland, traditional culture and the role of communities can be considered as the factors that significantly influence the approaches to cybercrime. The collected primary data reveal that due to the extended and tight-knit society coupling and the focus on tribal pride, cybercrime incidents are not reported. Due to this, women are likely to suffer high levels of stigmatization and be under pressure to uphold the honor of the family and tribe, thereby compromising their ability to seek assistance or report a crime that has been committed. Moreover, the low level of digital proficiency and knowledge of women's rights and possibilities intensifies the issue, as some women may even be unaware of their rights and available protection tools.

3.6.4. Preventive Measures and Awareness

It is noted that one of the most effective strategies that should be employed to overcome cybercrime to a significant extent is the implementation of preventive measures and the

introduction of focused public awareness campaigns. Stellar states, such as Delhi and Mumbai, have many programs to enhance the safety of people on social networks, including the school curriculum and public campaigns. Such measures may involve the collaboration of governmental and non-governmental organizations, with technology help from various firms, to improve the fight against cybercrimes. In Nagaland, however, there are comparatively inadequate prevention programs. Educational programs and propaganda campaigns are scarce, and most of them do not possess the necessary knowledge about safety while using the Internet and legal specifications. Some of the reasons include the emphasis on the conventional way of handling issues concerning conflict and the non-incorporation of informal and updated advanced safety consciousness into the public. In this regard, there is a requirement for culturally sensitive educational interventions, which would involve using cultural mediators in the form of local leaders to pass information to the targeted populations. Exploring the comparison of cybercrimes targeting women in Nagaland with other regions in India, certain peculiarities and similarities can be distinguished. Although urban states have enhanced infrastructural facilities, resources, and awareness programs, Nagaland has its own social, cultural, and logistical challenges that exercise influence on the Solving these challenges entails specific actions that we need to contextualize within the local culture, build the legal and institutional environments, and raise digital literacy and consciousness at the grassroots level. Thus, consideration of these differences allows the identification of key characteristics for enhancing protective measures for women against cybercriminals throughout India.

3.7 Community and Grassroots Responses to Cybercrime

Stemming sex cybercrime requires methodical policing that is supported by community and grassroots policing. Since the reactions depend on traditional structures and local interventions in Nagaland, the analysis and management of these responses can remarkably enhance the rest of the cybercrime prevention and mitigation measures. Specifically, this section examines the attitudes and actions of the communities and the grassroots, with a focus on Payy's Nagaland towards cybercrime and their efficacy, limitations, and possible interface with the legal strategies.

3.7.1 Community-Based Initiatives

Thus, it is evident that community-level approaches are vital in managing cybercrime in Nagaland since the area is culturally and socially connected. Such measures are normally implemented through partnerships with the community, women's organizations, churches, and other NGOs to parade, support, or lobby for change.

- **Local Awareness Campaigns:** Locally based agencies in Nagaland have slowly begun to take cognizance of the need for people to be computer literate and safer online. Local non-governmental organizations and charitable organizations organize and undertake awareness-creation activities for women, including business seminars and educational forums through which they sensitize the women on cybercrimes and what the women should do to ensure they have password-protected accounts and other ways through which their accounts can be protected, in addition to educating the women on where to seek help in case they fall victim to the act. They are unique campaigns developed to fit the particular region and may use more word-of-mouth communication alongside other cultural practices that are associated with HIV/AIDS and its prevention. For instance, the use of fairs and other accompanying town hall events and tribal meetings as means of passing details regarding cyber safety in the respective form of the local language and typical examples.
- **Support Networks:** Some of the essential support structures applicable to the victims of cybercrime are found in the community. Such networks may offer all sorts of support, such as emotional, legal, and service support, that would help victims go through the reporting process. Some of the organizations, including women's groups and local advocacy organizations for cybercrime victims, are available to provide counseling and support to the victims on how to come to terms with the psychological trauma experienced, as well as lead the victims through the processes followed in seeking justice. It is also for this reason that the support networks should include persons who can be easily trusted since reporting the crime attracts even more stigma to the victim, hence locking most women out of the process.
- **Community Watch Programs:** Certain communities in Nagaland have set up what can be called unofficial 'watch' organizations for people of the region who keep an eye on

the various doings on the internet and inform the authorities. These programs, although not strictly law enforcement agencies, add another tier of lookout and help. The volunteers are informed of the basic symptoms of cybercrime and the first steps to advise the affected people. Such movements can support official attempts to fight crime. However, such movements are usually vast and restricted in terms of finance.

3.7.2. Challenges and Limitations

In particular, community and grassroots goals have sensitives and limitations pertinent to their applicability, which include the following reasons:

- **Resource Constraints**: grassroots organizations and those from civil society are usually found to work with little funding. It hampers their capacity to undertake vigorous awareness-creation programs, deliver many support services, and carry out advocacy. It means that the variability of the quality and coverage of the services can also be brought about by the use of volunteers and donations.
- **Cultural and Social Barriers**: However, society's traditional culture and the way it perceives some issues can be a major challenge when tackling cybercrime in Nagaland. This is because the act of falling victim to cybercrime has some level of stigma, especially within very conservative tribal communities; therefore, it may act as a barrier to women wishing to come forward and volunteer to participate in any such programs that are to be set up within a community. Also, the fixed gender roles and patriarchy may hinder the efforts of the bottom-up movements, especially because addressing the root of the problem is changing the attitudes of society.
- **Coordination with Formal Systems**: Responding to grassroots problems and then fitting them into the framework of legal and institutional arrangements may not always be easy. It does not rule out the possibility of poor cooperation between the local plans and projects on the one hand and the state on the other, therefore leaving out the important areas of support and enforcement. To prevent the actions at those levels from being redundant or incompatible with formal structures, negotiations have to be made with care.

3.7.3. Opportunities for Enhancement

To enhance the effectiveness of community and grassroots responses to cybercrime in Nagaland, several opportunities can be explored: To enhance the effectiveness of community and grassroots responses to cybercrime in Nagaland, several opportunities can be explored:

- **Strengthening Partnerships**: This indicates that enhanced collaboration between the grassroots formations, local communities, and formal entities will contribute to the better organization and effectiveness of the measures aimed at combating cybercrime. Atlanta needs to find better ways of supporting such clients, as they are faced with numerous challenges ranging from poverty and homelessness to mental health issues and abuse. Collaboration is therefore likely to result in better support services, efficient utilization of available resources, and successful championing of required policy reforms.
- **Expanding Training and Resources**: Educating and training other people and various grassroots NGOs and volunteers would help solve cybercrime problems more effectively. Thus, it can be concluded that training programs on digital literacy, recognition of cybercrime, and victim support can be useful for raising awareness among community members and organizations to better respond to cases of cybercrime.
- **Increasing Public Awareness**: Educating a wider audience, including other members of the community, ensures that cultural barriers and stigma are reduced by launching awareness campaigns. In continuation of the awareness process, efforts should be made to approach local leaders, media, and educational institutions, which can help increase the outreach of awareness and be more helpful for the victims.
- **Leveraging Technology**: An effective use of technology in increasing community-based responses can open up better ways of engaging with participants and clients. Awareness can be conducted through cyberspace, social media, and mobile apps to reach out for help and/or to report cases.

People's strategies and actions remain effective in dealing with cybercrime against women in Nagaland. Despite these and other challenges of delivering initiatives, they are beneficial and may fill voids in resources that government institutions and organizations may not be able to provide. Strengthening partnerships, increasing the capacity of training and forms of assistance,

and proper application of technology contribute to the improvement of the community as a means to combat cybercrime and increase the level of support for victims. The above-mentioned grassroots responses should be harmonized with the official structures to develop an effective and culturally appropriate approach regarding cybercrime in Nagaland.

Chapter 4

Governance, Law, Prevention, and Precaution

4.1. Introduction

The use of technology in the advanced age creates unlimited possibilities in communication, education, and the development of economic systems. At the same time, it has contributed to creating new types of criminal activities that take advantage of the open nature of the internet. One of the key common and rising trends of threats is cybercriminal activities against women, which are now looming and endangering the safety, privacy, and dignity of women in virtual space. This chapter focuses specifically on the nature of governance structures, legal frameworks, preventive measures, and precautionary actions concerning cybercrime against women in Nagaland, one of the states of India's Northeastern Region. The strategies that will be employed to fight cybercrimes against women in Nagaland will also be discussed in this chapter. In this case, we will review the available literature to determine this paper's area of focus – governance structures would illuminate the existing institutional frameworks to deal with this problem at the state and national levels. The legal systems shall be reviewed to evaluate the capacity of the laws and efficiency in handling cybercrimes against women.

Additionally, it will be possible to research the prevention measures existing at the moment and their effectiveness in fighting cyber criminality. The chapter will explore the measures that women ought to practice as preventive measures in the new arena. This chapter forms part of a larger study on cybercrimes against women in India of which a focus on Nagaland has been adopted here. The aforementioned chapters may have described the genre and scope of cybercrime in the region but this part will endeavor to appraise the systematic approaches to deal with these adversities. Due to this reason, by adopting Nagaland as our area of study, we can provide a more focused insight into both the cultural and social/technological factors that may characterize cybercrime and its prevention in the Northeastern region of India. Looking at these elements as a whole, one will be able to see the merits and demerits of the existing militarized approach to fighting cyber criminality against women in Nagaland. This systems approach is critical when it comes to formulating appropriate strategies that point to

counter threats and ride them as well as work against them. In this regard, the chapter will start with exploring the current state of laws protecting women from cybercrimes in Nagaland. The paper will d discuss the measures being taken by the governments and various organizations to check cybercrime. This will entail the consideration of the central-level institutions as well as policies like the Ministry of Home Affairs and the National Cyber Security Policy.

At the state level, the study examines Nagaland's units in police departments, the cooperation of departments under the Nagaland police, and any other specific body combating cybercrime against women. The chapter highlights the precautions undertaken to discourage acts of cybercrime against women in detail. It also includes applications of technology and hardware like information protection structures and cyber defense mechanisms including those for forensic gain. In addition, the possibilities will be considered for furthering education, such as concerning programs in schools and colleges, as well as constructive campaigns required to enhance the cognizance of the public on cyber safety. Safety measures to be practiced by female social media users will be highlighted. In this section, several initiatives that help to promote the digital literacy of users, recommendations concerning safe work on the Internet, and information about threat identification and their reporting will be mentioned. Finally, this paper will discuss the social services that women, who have been victims of cybercrime incidences in Nagaland, can access.

4.2. The need for an updated and comprehensive cybersecurity policy

Cybercriminals particularly are becoming more professional in their attack and are presenting a greater threat to society because of their operation in cyberspace. Specific state sponsors, are known to take time to prepare for a disruption and are involved in sensitive political and economic spying. That is why governments have noted them as a threat that is increasing its capabilities in digital attacks. These attacks come in forms and are extending into other sectors, below are some of the different forms of the attacks. In addition to the broad number of actions, non-state actors are consistently engaging in attacks on nations' cyberspace systems (Cyber Security in India). These advancements call for higher engagement of both the states and individuals to improve the cyber-security system. The adversaries are most motivated, well-financed, and skilled in the information domain. Such actions impact programs that are central to a nation's progress such as e-governance, digital identity, and smart city. Information belonging

to private enterprises or the military is also compromised in this regard. But the damage to CII is not only monetary; it could also affect a country's security.

India is acknowledged internationally as one of the most promising outsourcing locations; numerous international companies operating in India have created international delivery centers that provide services and support. Multinational organizations such as Apple, Sapient, Citi Bank, Bank of America, HSBC, and DSM are some of them. At the same time, India has started the most massive initiative in information and communication technologies "Digital India," which develops the access and government of all spheres, including the healthcare and education systems, and plans to transfer the country to digital money within the near future. The digital context in India has emerged and transformed very rapidly in a relatively short period (Chitrey et al., 2012).

India at the moment is seeing a large number of governmental and private cyberspace pursuits implying numerous opportunities for the country's digitalization. As far as this is concerned, it points to the fact that India is in a place to safeguard her national interests in the cyberspace dimension while at the same time harnessing the benefits that come with digitalization (Cyber Security in India). For proper coverage, India's approach towards cybersecurity can be summed up on the following principles based on the NCE Policy 2013 which is quite appreciable. But in this emerging situation, India needs a new policy not only a set of declarations of high principles but the concrete concept of work on the realization of cybersecurity. A good example of this should include education and training of cybersecurity professionals, encouraging the development of relationships between the government and private sectors as well as encouraging the interaction between the military and civilian societies. The National Cyber Security Policy first incorporated objectives that stressed the creation of a talented force with skills and training requirements to attain the overall head count of a force of 500000 by the year 2013. According to Thakker (2017), a new Cyber Security Policy should contain a set of specific recommendations for effective recruitment and training of these specialists and should be changed timely. The PPP is a strong component of India's cyber policy; there are current efforts aimed at effective PPP in the sphere of cybersecurity. This focus also covers technical and operational collaborations of the companies in the industry. For instance, the Data Security Council of India, the Information Systems Audit and Control

Association, and the National Association of Software have floated an organization to tackle Cyber security in the private sector. Popular collaboration between civil and defense institutions in the sector of cybersecurity must remain a key goal in any new strategy of cybersecurity. There is a proposal that eighty main defense, intelligence, and strategic specialists should determine corresponding national cyber security standards. It is seen that the military needs to have more frequent and official interaction with the civilian part of the public sector. Thus, to be prepared for the development in the IT sector, India should update the cybersecurity legislation and develop a greater number of rules (Thakker, 2017).

4.2.1 Establishing a Cyber secure Ecosystem

i. To make it possible for a national nodal agency to arrange, with distinct roles and duties, all issues about cyber security in India.

ii. To assist both public and commercial entities that are in charge of cyber security initiatives and businesses.

iii. Encouraging all firms to create information security policies that are in line with their business plans and execute them according to global best practices.

iv. To ensure that every agency sets aside a certain amount of money to carry out cyber security projects about emergencies and cyber events.

v. To provide financial plans and incentives to support organizations, fortify, and improve information infrastructure about cyber security.

vi. To stop cyber events from happening and from happening again by promoting technological advancement, taking preventative measures, and adhering to cyber security regulations.

vii. To set up a system for data exchange, incident identification and response in the event of a cyber-security incident, and collaboration on restoration projects.

viii. To motivate organizations to implement policies that guarantee the acquisition of reliable cyber security and facilitate the acquisition of locally produced cyber security with security implications (Ministry of Communication and Information Technology, 2012).

4.2.2 Securing E-Governance services:

i. Managing the deployment of business continuity planning, cyber crisis organization plans, and global security best practices for all e-governance projects is the first step in securing e-government services.

ii. To strengthen security posture and lower the chance of distraction.

iii. To promote the nation's increased use of public key infrastructure for communications and trustworthy communication.

iv. To enlist the help of organizations and information security specialists to support e-government projects and guarantee adherence to security best practices (Ministry of Communication and Information Technology, 2012).

These primary goals consist of guarding finance and banking data, individual data, sovereign data, and other types of sensitive data. The most notable development was in 2013 with the NCSP because it gives a blueprint on how new projects and programs can fit in with the grand vision and have a highly developed strategic map for its future evolution. Thus, India can create an extensive system to guarantee a secure computing environment and implement it through this policy. The NCSP takes into account the contemporary technological developments around the world in cybersecurity, about which governments, companies, and the population that uses cyberspace for data gathering need to know. Another difficulty that exists within the system is the issue of collaboration and cooperation. These are the issues such as information sharing between the government and private sectors, employment opportunities for cyber security experts, investigations of cyber crimes, security of the critical information infrastructure, managing risks relating to the ICT supply chain, enforcement of strict auditor's standards, cyber threat intelligence and reporting, management of crisis and incident handling, and broadcasting among others. This policy framework is expected to be created by the NCSP in cooperation with partners while the organization itself is given the role of identifying as well as evaluating these risks and challenges. The challenge is therefore in using this policy to get to those objectives. An assessment of the National Cyber Security Policy of 2013 reveals that there are activity plans at different tiers and that the document is very clear on how to operationalize the policies. This is in

contrast to what is seen in a market-driven and/or regulated system and in developing the NCSP, the NCSP encourages the formation of both.

India's strategy should be able to address security issues related to the acquisition of ICT products especially from foreign providers while at the same time optimally exploiting the benefits from the global supply chain for high-quality quality affordable and value-added products services and expertise. This was well illustrated in the "Securing Our Cyber Frontiers" report also known as (National Cybersecurity Policy-2013 Analysis).

For example, it appeals to organizations to work together with or sponsor civil society, formulate security policies for information, develop guidelines for acquiring reliable technology, and provide grants to organizations that promote cybersecurity and information structures. Also, the NCSP states that more cybersecurity products should be produced domestically through R&D to meet emerging security threats. One extremely positive aspect of the policy is its approach to cooperation with industry through cooperative R&D projects and Centers of Excellence about the government's IT, Telecom, and Electronics Triad Policies.

- **The following qualities are included in the conspicuous aspects of NCSP**:
  - **i.** To provide residents and companies with a safe and reliable online environment.
  - **ii.** Empowering concentrated on lowering reaction and recovery times as well as conducting efficient cybercrime investigations to lessen the nation's susceptibility to cyberattacks and cybercrimes.
  - **iii.** To aim for capacity building, national alerts, cybersecurity-related technology, public and private partnership requirements, the security of vital information infrastructure, and the promotion of collaboration and information sharing.
  - **iv.** Concentrated on coordinating, collaborating, and integrating with Indian stakeholder entities
  - **v.** To encourage and support the tactics that align with the goals of the NCS policy.
- **Challenges**

i. Mandatory measures may increase costs, create barriers for enterprises, and disrupt innovation without increasing security. Mandatory measures may hurt industries with limited security implementation experience.

ii. The Internet Information Supply Chain risks portraying original items as more secure. 3.

iii. The implications of demanding the acquisition of verified cyber security solutions in the absence of suitable testing facilities, including procurement delays.

iv. India needs a comprehensive policy to combat threats and compete in the international arena (DSCI Analysis of the National Cyber Security Policy, 2013).

v. Lack of awareness

vi. Lack of national-level cybersecurity architecture

vii. Lack of trained labor

viii. Lack of cooperation and coordination.

ix. Inconsistency in internet-connected gadgets

- **Opportunities for improving cyber security**

i. Increased coordination among government institutions.

ii. Change in ICT attainment processes of organizations, particularly important sectors and e-government initiatives, to focus on product security; drive suppliers to develop product security; and raise acceptability of tested goods.

iii. Improved cooperation between government agencies and industry on cyber security issues.

iv. Increased collaboration and information exchange on cyber security issues.

v. There is a need to improve the maturity of security procedures as well as promote the security function within businesses, particularly in vital industries and e-government activities.

vi. Increased demand for security experts, including managers, implementers, auditors, and trainers.

vii. Increased investments in security, boosting the cyber security goods and services market in India

viii. Creating significant prospects for security product and service companies, as well as auditing firms.

ix. Boost the domestic security industry, particularly startups that provide specialist and creative security products.

x. Improved Research and Development through partnerships among government, business, and academia.

xi. Raising citizen, consumer, and employee awareness of cyber security issues, as well as basic and best practices.

xii. Supply of goods and services

xiii. Cyber forensics

xiv. Policy & Regulation

xv. Creating new goods through R&D collaborations

xvi. Capacity building in government and industry.

4.2.3 Need for a Cyber Security Policy

Almost every nation today including the Indian nation is facing a lot of tension and fear due to frequent cases of cyber spying, cyber terrorism, cyber war, and cybercrimes. They have also resulted in virtual stalemate and matters concerning artificial intelligence. To some extent, the legal instruments that would be used by prosecutors have not developed as fast as the surge of cyber criminality. The incidences of cyber-attacks that have occurred recently in India suggest that basically, several aggressive strategies are being tested and or used by diverse actors. The lack of a definite cybersecurity policy poses a clear & present danger to India's security & its growth trajectory. The matter implies that the highest levels of government need to act to eliminate threats related to cyber environments that can jeopardize cybersecurity and fight cyber criminality effectively.

There are also some of the main aspects in the context of the modern and effectively elaborated cybersecurity policy: understanding and defining the threats in the cyber domain,

creating adequate technical, legal, PPP, International Cooperation and Diplomatic and Supportive Measures, strengthening the cyberspace infrastructure and constructing the solid organizational structures. India's previous approach to cybersecurity can be characterized as rather chaotic and uncoordinated since there was no clear national-level planning. While there are several groups whose formation and existence is understandable they fail to characterize their roles and more importantly, there is interference as well as a lack of proper coordination between the groups. This issue cannot be categorized under a large category and is within the purview of the NSCS mandate as the special branch.

Nevertheless, contributing to this argument, Tomar (2013) observed that there seems to be a shortfall of an institutional format to warrant policy enforcement. Also, there has been little talk about the effects of cyber security and cyber warfare, if any at all. At the same time, various nations continue to engage in considering cybersecurity policy and strategy problems such as the United States, France, China, Sweden, the European Union, South Korea, and Singapore. These countries are putting a lot of effort into placing the necessary measures that would ensure the safety of the Internet among the citizens (Desai, 2012). International Status of Cyber Security: Information security on the international level is shifting its focus to cybersecurity as a major element of its protection. Through the increased and constant growth and development of computer systems and Information and communication technology (ICT), peoples' lives have been enhanced, but at the same time, it has brought new threats in cyberspace to national and international security. Among the types of networks, critical infrastructure is a weak link and susceptible to cyberattacks (Bamrara, 2013). Furthermore, thus social networking sites such as Twitter and Facebook have offered new gateways to strategic and policy communication that are beyond the national levels and the traditional authorities. Also, the data transmission network extensively relies on undersea cables; these cables are vulnerable to both accidental cuts and sabotage (Desai 2012). For several reasons, some consider an international convention regarding the responsible Relationship of States regarding the use of the Internet Space has both positive and negative aspects of security of groups or individuals' possession. Several international conventions are already in place for example; the Biological Toxins Convention, the Chemical Weapons Convention, non –the Non-Proliferation

Treaty, and the Weapons Convention. Likewise, the time has come to talk about cyber-attacks. Cyber warfare is typically categorized into three types: The three subcategories of this type of industrial crime are: 1) Spyage or Espionage, 2) Graffiti or Vandalism, and 3) Dirty Work or Sabotage (Desai, 2012).

4.2.4 Cybercrime Prevention Efforts in Nagaland: Focus on Protecting Women

Nagaland has been endeavouring in the fight against cybercrime especially crimes against women. Criminal police departments of the state have formed specialized cybercrime sections and improved cooperation between departments to tackle the increasing dangers of cybercrimes. The CCPWC forensics and training facilities opened at the Police Complex in Chümoukedima are a product of these efforts. This facility is meant to provide specialized training for police personnel on cases especially as may affect the vulnerable in society such as women and children in case of cybercrimes. The Nagaland Police have organized consultative meetings/panel discussions with the masses to create awareness concerning cyber threats. They are programs like the annual program held at PHQ Conference Hall in Kohima involving stakeholders like NES representatives from the Department of School Education, Collegiate Education, principals of private schools, students, social media personalities, and journalists. In these meetings, specialists draw attention to such a number as 1930 to help the population avoid scepters and contingents as well as possible financial losses and hacking, among others.

Moreover, the Nagaland government has been planning to form the Cyber Dome to enhance its capacity to tackle the issues of cybercrime. This initiative includes the leadership's determination to develop public trust in the online environment and to exclude any forms of cybercriminal activity. By implementing such extensive strategies, Nagaland attempts to improve the cybersecurity situation and the state's preparedness to manage the current and future threats**.**

Schemes/Services under the Ministry of Women & Child Development for Women and Children affected by violence

- 181-Women Helpline Nagaland provides 24-hour toll-free telecom service to women affected by violence and seeks support and information on women-related schemes and

programs. WHL facilitates crisis and non-crisis intervention through referral to the appropriate agencies.

- Sakhi-One Stop Centre (OSCs) provides integrated support and assistance for women affected by violence under one roof with services like medical assistance, police assistance, psychosocial support, legal aid, shelter, and video conferencing. It is integrated with 181-WHL.
- CHILDLINE-1098 works for the protection of the rights of all children. It is an initiative for rescuing and assisting children in distress. CHILDLINE-098 is a toll-free number and it is available all over India.
- The Ujjawala Scheme is a comprehensive scheme for the prevention of trafficking and rescue, rehabilitation, and reintegration of women and child victims of trafficking.
- Swadhar Greh Scheme also seeks to address the needs of females in difficult circumstances, including victims of sex trafficking.

The Nagaland State Commission for Women (NSCW), Department of Social Welfare, Nagaland State Social Welfare Board (NSSWB), Mahila Shakti Kendra (MSK), 181-Women Helpline Nagaland, Sakhi-One Stop Centre (OSC), CHILDLINE 1098, Nagaland Adventure Club (NAC), Kohima Chamber of Commerce and Industry (KCCI), and Association of Kohima Municipal Wards Panchayat (AKMWP), the SRCW, will organize a 'Car Campaign' to commemorate the International Day for the Elimination of Violence. The major goal of this automobile campaign is to raise awareness and sensitize the public to the issue of violence against women. Another notable project is the Purple Ribbon Campaign, which has been embraced as a symbol of solidarity with women who have been victims of violence, as well as to raise public awareness and positively influence society's attitudes and actions against violence against women. Purple ribbon badges will be worn by people to honor this day, according to the announcement. To prevent all forms of violence against women, district administrations, in collaboration with team members from Sakhi-OSCs, MSK-District Level Centres for Women (DLCW), and Beti Bachao Beti Padhao, are actively campaigning to raise awareness about issues/problems and services available to women affected by violence, according to the SRCW.

"Gender-based violence includes sexual violence, physical violence, emotional and psychological violence, online and digital violence, harmful traditional practices, and socio-economic violence," it emphasized, adding that violence against women exists regardless of their status, class, caste, or religion. "It is a typical problem that we encounter everywhere, whether at home, school, job, or on the streets. “Some women and girls are subjected to this violence their entire lives”, the statement added. According to UN estimates, fewer than 40% of women who have experienced violence seek treatment. In the context of Nagaland State, many such cases are hushed and unreported. Particularly cases of domestic violence, the SRCW stated, while emphasizing that victims hesitate to report due to complex harsh realities including fear of society's stigmatization, pressure from relatives/ families to avoid reporting, ignorance about their constitutional rights, concerns about the uncertainty of the children's future and custody issues, insecurity about not having support. It stated that gender-based violence be domestic or cyber, is a global pandemic and that any move toward eliminating violence against women should be viewed as both an effort to question the deeply embedded patriarchal system and a step toward empowering women.

4.3. Cyber security law in India

Information technology has helped us close the global divide. People may now easily communicate with friends and relatives on any continent, place orders, and work abroad, but this has escalated cyber violence, particularly against women, because many users create cloned personas and can conduct crimes from anywhere in the world.

The laws that include legal provisions to combat cyber violence against women are listed below:

4.3.1 The Bharatiya Nyaya Sanhita (BNS), 2023 then Indian Penal Code (1860)

The Bharatiya Nyaya Sanhita (BNS) deals with all criminal acts in India and even specifies punishment for them. In 2013, the BNS was amended to handle internet offenses against women and others. The following parts were added (Women and Cyber Laws in India,).

- **Section 354A**

This section addresses sexual harassment. In any situation, if a person demands sexual favors, forcefully displays pornography, or makes filthy remarks, he may face jail for up to three years, a fine, or both.

- **Section 354C**

This section defines Voyeurism. It is a criminal violation when a woman is unaware that she is being recorded while performing a private act. Anyone who commits this offense faces a fine and imprisonment for up to three years on the first conviction and up to seven years on successive offenses.

- **Section 354D**

This section addresses cyberstalking. It entails following a woman online by sending direct messages, commenting on photos, and posting offensive photographs or videos even when the woman seems uninterested. A man can face a fine and imprisonment for up to three years for his first infraction and up to five years with a fine for successive violations.

- **Section 499**

When a woman is defamed for any purpose to harm her reputation, such as by disseminating obscene photographs or videos online, the person who commits this crime faces imprisonment for two years or more, as well as a fine.

- **Section 503**

This section covers Cyber Blackmailing, which occurs when a person is blackmailed into changing their decision in favor of the blackmailer, and if the victim does not comply, threats are made to ruin the victim's reputation or injure the victim. Any person detected blackmailing in cyberspace may be held liable under this clause.

- **Section 509**

states that if a person is caught using vulgar comments, gestures, or words to harm a woman's modesty online, they will face a fine and up to three years in prison.

4.3.2 The Information Technology Act of 2000 (Amended in 2008)

This act addresses cyber violence, cybercrime, and electronic trade rules. Anyone who commits a crime related to it is subject to the provisions of this act and will be penalized appropriately.

The following sections help to counteract cyber violence against women (Women and Cyber Laws in India, n.d.).

- **Section 66C**

This section contains cases of cyber hacking. It refers to when personal information such as photographs, videos, electronic signatures, and passwords are fraudulently extracted and then utilized to bring emotional anguish to the victim. Individuals who violate this section may face imprisonment for up to three years, a fine of up to ₹1,00,000, or both.

- **Section 66E**

If discovered collecting, publishing, or posting a person's private parts on cyberspace without their knowledge, they may face up to 3 years in prison, a fine of up to ₹ 2,00,000, or both.

- **Section 67**

Sharing, circulating, or posting obscene content online may result in imprisonment for up to 3 years for first conviction and up to 5 years for successive convictions, or a fine of up to ₹ 1,00,000 or both.

- **Section 67A**

This covers the publication of sexually explicit content online. It includes posting content containing sexual actions online. If convicted, individuals may face imprisonment for up to 5 years for the first offense and up to 7 years for subsequent offenses, as well as a fine of up to ₹ 1,00,000 or both.

4.3.3 Indecent Representation of Women (Prohibited) Bill, 2012

This statute punishes individuals who attempt to depict an obscene image of women in the form of images or films. This Bill has widened its reach to embrace online content as well. (Women: Cyber Laws in India, n.d.)

- **Section 5**

This section empowers the officer to enter and search any premises in the region at any reasonable time, as well as examine and seize any obscene content possessed by the person suspected of committing the offense.

- **Section 6**

Penalties include imprisonment for 6 months to 5 years and fines ranging from ₹10,000 to ₹50,000.

4.4 Suggestions to Combat Cyber Violence against Women

Dealing with cybercrime requires knowledge, clarity, and guts. The following are some of the approaches to combat cyber abuse against women:

- **Knowledge of cyber laws**

The most important thing is to understand cyber laws. The victim must report the crime and should not be afraid to disclose it, as doing so can exacerbate the issue. There are dedicated hotlines for reporting cybercrimes against women (1091/1090) that provide free legal assistance to victims. Awareness and expertise of cyber rules are becoming increasingly important.

- **Training for officials:**

Police officers, cyber law experts, and members of the judiciary must be trained to combat the growth in cybercrime. They must be made aware of how they manage various forms of cybercrime. Different cybercrime branches now address a variety of cyber concerns, including hacking, stalking, blackmailing, phishing, morphing, and others.

- **Privacy Policies & Guidelines**

Women must read all of the terms and conditions before accepting, as some sites are fraudulent and vulnerable to hacking. The women must review their privacy settings to ensure that their social media accounts are safe from hackers. When a person establishes an account on a website, they must follow the criteria since it will help them battle cybercrime in the future. It is a leisurely activity, and appropriate research should be conducted before randomly accepting any popup boxes.

- **Discourage Information Sharing**

Women should avoid sharing their passwords, electronic signatures, bank account information, and other personal information with others to prevent it from being leaked or exploited against them.

- **Change Passwords at Short Intervals**

To avoid hacking, one should change their passwords regularly. Passwords should be kept private and not shared with closed groups.

- **Knowledge of Cybercrime**

It is critical to raise knowledge about cybercrime. Young females, like most teenagers, are susceptible to such things, while young boys, out of ignorance, begin to commit these crimes. Campaigns, seminars, and workshops should be organized in schools. To raise awareness of cybercrime, a message can be distributed to a large audience using television and social media advertisements.

- **Preserving the Evidence:**

If a woman is subjected to cyber abuse, she must understand the need to preserve all evidence related to the offense, such as filthy remarks, pornographic recordings, and threatening communications addressed to her. One can keep track of the numbers from which they receive threatening calls. It can assist cyber law professionals in finding clues.

- **Install Anti-Virus Software**

One must install the most recent versions of anti-virus software on their laptops and personal computers so that a hacker's attempt to steal information is prevented. The firewall must be turned on. It protects your privacy from Trojans and other e-mail infections.

- **Avoid responding to spam calls and unknown friend requests**

When it comes to cyber security, one must be attentive. It is always best to avoid answering spam calls and accepting friend requests from people one does not know. It is simply a precautionary measure to prevent cybercrimes.

- **Legal Provisions for Various Cybercrimes**

Cyber laws must have different measures for all types of cybercrimes. Some cybercrimes are currently addressed under a single umbrella section, while others are not mentioned at all. All of the proposals serve as building blocks for fighting cyber violence against women. Women must be taught and made aware of all cybercrimes, and if they are victims, they must receive emotional and mental help. They must be encouraged to report and speak out to set an example for society as a whole.

4.5 Conclusion

Cyber hazards, particularly those affecting women in Nagaland, are a continuation of the myriad challenges plaguing many places in India and around the world. However, as the influence of digital technologies in society grows, so does the threat of cybercrime. Nagaland's law enforcement actions, supported by national and state frameworks, serve as frontline protection. However, due to the ever-changing nature of threats in cyberspace, such solutions must be regularly updated. One of Nagaland's significant competitive advantages has been the development of specialized cybercrime agencies within the police force. These units, which are tasked with dealing with cybercrime, particularly those targeting women, are beneficial in the sense that they assist in responding to such situations by investigating and prosecuting. The Cyber Crime Prevention against Women and Children (CCPWC) lab and training centre in Chümoukedima exemplifies the state's commitment to training. However, decision- makers have long recognized that the future success of such divisions is entirely dependent on the company's ability to pay for technical advancement. Employee protection necessitates ongoing training and competency development, as cyber criminals develop increasingly advanced techniques. Other reform areas identified for development include inter-departmental coordination. Such procedures necessitate the establishment of appropriate information-sharing mechanisms across departments such as the police, judiciary, and social welfare. These coordinates help to ensure that each case of cybercrime, particularly among women, is presented to the appropriate authorities with the necessary attention and seriousness. Nonetheless, inter-departmental coordination should be encouraged and made less person-dependent, as it proved to be quite beneficial during the research. The employment of information technology in these processes, such as databases or automated reporting systems, can significantly improve the efficacy of these mechanisms. However, the importance of technology in strengthening governance and legal systems cannot be overstated here. Improving computers, telecommunications devices, and automated analytical tools for surveillance and crime mapping would considerably boost Nagaland's

cybercrime units. In addition, one can form a collaboration with digital businesses, academic institutions, and civil society organizations to bring the necessary know-how and creativity to solve cybercrime issues more effectively. Although legislative instruments exist, their execution is not without obstacles, particularly in a state with such a distinct social and cultural background as Nagaland. The provisions of the Information Technology Act are quite wide, thus, local legislation should complement it to address Nagaland's specific concerns and requirements. For example, one of the major challenges that require expanded legislative measures is the protection of victims' identities and the guarantee of prompt access to justice. General preventive measures include raising awareness and sensitizing the public with public billboard advertisements, internet campaigns, and the establishment of online classes about the potential risks that one could expose oneself to by engaging in cyber activities. However, the effectiveness of these strategies is limited by the scope and intensity of the activities. As a result, any attempts to boost literacy rates among Nagaland residents who use digital devices must consider the entire population. Such activities should be culturally acceptable, ensuring that none of the targeted communities, including the most disadvantaged, is excluded.

As a result, while Nagaland has made significant progress in combatting cybercrime against women, much more work remains to be done. It indicates that the state's activities must be adjusted in response to the continually changing danger environment. This will entail consistent support for law enforcement, improvements to the legal system, public sensitization, and mental growth. Nagaland can ensure the security of women in the online arena, and thus its residents, by implementing a number of the aspects listed above as interconnected workspaces. Such a commitment to cybercrime prevention will not only safeguard individuals but will also rebuild the fabric of social ties and increase public faith in the digital economy, thereby contributing to the state's development.

Chapter -5

The Manifold Experience of Cybercrime Survivors: Insights from Empirical Research

5.1. Introduction

Cybercrime against women poses a significant challenge in Nagaland, as the digital realm combines with traditional patriarchal institutions. While cyberspace allows women to assert their rights and express themselves, it also exposes them to numerous sorts of exploitation and victimization. This study investigates the distinct manifestations and repercussions of cybercrime against women in Nagaland, shedding light on the inadequacies of current legal frameworks and social attitudes. Women in Nagaland, like in many other parts of the world, are especially vulnerable to cybercrime. Criminals use the anonymity and size of the Internet to harass, stalk, and slander women with unwanted emails, manipulated photographs, and sexual information. The development of social networking sites and online forums heightens the risk, as fraudsters actively seek out victims who share personal information online. Nagaland's patriarchal and traditional values can exacerbate the difficulties experienced by female victims of cybercrime. The tendency in society to blame and isolate victims, along with limited legal protection and support structures, leaves women with insufficient resources. Unlike masculine women, women who are attacked online face not just money loss but also severe social and psychological suffering, such as shame and self-hatred. Despite the increasing incidence of cybercrime against women in Nagaland, studies into the subject are scarce, with most studies focusing on Western viewpoints.

This study seeks to fill this vacuum by examining Nagaland's distinctive socio-cultural environment and the inadequacies of present legal and institutional remedies. This study seeks to advocate a more inclusive and effective approach to addressing cybercrime against women in Nagaland by amplifying the voices of cybercrime victims and advocating for targeted solutions.

Understanding and Addressing Cybercrime against Women in Nagaland. The digital revolution has provided unprecedented connectivity and opportunity for change. However, this era of technical growth has presented significant concerns, particularly in terms of people's online safety. In Nagaland, a northern Indian state famed for its rich cultural diversity and gorgeous landscapes, the growth of digital platforms has increased women's vulnerability as they become more targets of cybercrime. These crimes cover a wide range of damaging acts made possible by digital technology, including cyberbullying, financial fraud, identity theft, and the illegal release of personal information. Such crimes undermine women's privacy and dignity while also having major psychological, social, and economic effects. Recent examples demonstrate the pervasiveness of cyber attacks against women in Nagaland. Cyberbullying on social media, phishing scams targeting financial assets, and the dissemination of defamatory content have all had serious ramifications for victims' lives, ranging from mental suffering to professional repercussions.

The socio-cultural backdrop of Nagaland, which is defined by numerous tribal communities and traditional customs, combines with the digital world, shaping both the perpetration and reporting of cybercrimes against women. Despite the increased use of the Internet for education and social connection, women are more vulnerable in online contexts due to factors such as insufficient digital literacy, cultural shame associated with reporting cybercrime, and gender biases. To address these difficulties, the Nagaland Police Cyber Crime Unit investigates digital crimes and assists victims.

However, gaps exist in capacity building, collaboration with ISPs, and legislative framework adaptation to tackle growing cyber threats. Legislative efforts, including revisions to the Information Technology Act to prevent cyberbullying, harassment, and revenge pornography, aim to increase women's legal safeguards. However, implementation issues continue, as does the need for complete legislative frameworks that incorporate prevention, protection, and accountability to properly defend women's digital rights. Recent events highlight the ongoing challenges and emerging trends in cybercrimes against women in Nagaland. Sophisticated programs targeting women have increased significantly due to the use of social engineering tactics and digital platforms to spread misinformation and incite hatred. Educational initiatives by local organizations and educational institutions are important to raise awareness of digital security and

increase women's awareness and skills to reduce cyber risks. Additionally, the intersection of social media abuse and traditional sociocultural norms highlight the complex dynamics that influence women's cyber- victimization in Nagaland. Progress requires concerted efforts to improve digital literacy, strengthen institutional accountability, and create a safe and inclusive digital environment where women can surf the web without fear or exploitation. Collaboration between government agencies, NGOs, academia, and technology companies is essential to develop comprehensive strategies that address the multifaceted dimension of cybercrime against women. By understanding the socio-cultural context, legal framework, recent developments, and emerging trends, stakeholders can work to reduce the risks and vulnerabilities faced by women in Nagaland's evolving digital environment.

In India, violence against women is a detrimental issue which manifests itself in many places such as homes, public spaces, professional work settings. In many cultures, the violence against the womenfolk is considered as a norm, mostly owing to the fact that different elements such as social and cultural factors influence greatly to the development and pervasion of violence against women. Irrespective of the background of women, such cultures and social norms are of the strong belief that the menfolk have the authority to control the womenfolk, specifically if they do not level up to the expectations such as preparing food on time or behaving according to the men's will. In addition to all of this, the abused women may try to justify the maltreatment they receive from their partners so as to make sense of the abuse and violence which they go through. As more people use the internet, criminals are finding ways to exploit it for committing information and communication technology crimes, putting public safety at risk through cybercrimes. The incidence of cybercrimes is on the rise in India, with research confirming that increased internet usage makes individuals more vulnerable. India, in particular, has experienced a significant increase in cybercrimes in recent times. The growing use of the internet has provided a conducive platform for miscreants to engage in the misuse of information and communication technology and this issue has resulted in a threat to people with regards to cybercrime. Generally, the cases of cybercrime keep multiplying in India. According to numerous studies, the elevated usage of internet enhances the level of vulnerability. Modern day India is no exception to this as cybercrime keep increasing. However, as per studies, there is an estimation that only 10% of cybercrimes are duly reported and out of this percentage, only about 2% get into the registers (Kshetri 2016; Meena et. Al 2020)

In the realm of cyberspace, the most vulnerable population of the society include the women and children who end up facing the aftermath of cybercrimes. Universally and particularly in a country like India, the crimes against women including cybercrimes have tremendously increased. Such cyber crimes against women stretch out to multiple levels of sexual violence which in turn have an end number of influences. When we talk of cybercrimes against women, one may include abusive words, comments which are derogatory, being stalked online, messages which contain insults, releasing statements which are not true. All these acts of cybercrime have lasting impacts which are detrimental to the one's affected, specifically young adults. Women whose online presence are active tend to be the subject of such derogatory comments and attacks which hampers their safety and freedom to express. Such cybercrimes on online platforms lead to the development of numerous issues such as social issues, economic issues, psychological issues on women who are victimised. Since using the internet has become a basic human right, spending more time online makes one an implicit target for wrongdoers. Vibrant internet services like banking, train sharing, and single-location shopping expose people to fraud and phishing scams. Phishing, pornography, cyberstalking, and cybersquatting are examples of sophisticated cybercrimes that have been reported from India. The theft related to information is generally done by workers presently working in the organisation or those who have left the organisation. Hackers commit roughly one- third of the information theft. The cybercrimes targeted against women are largely under- reported, as women in India are substantially ignorant of similar felonious offences. Women are criticized for issues over which they've no control. Although women frequently are victims of cybercrimes, they prefer to maintain silence as honour is attached to womanish members of the family. Utmost of the cybercrimes remain unreported due to the hesitancy and shyness of the victim and her fear of vilification of family's name. numerous times she considers that she herself is responsible for the crime done to her. Women sweat that reporting the crime might make their family life delicate for them, they also question whether or not they will get the support of their family and musketeers and what the print of society will be on knowing about them. Due to these fears women frequently fail to report the crimes, causing the spirits of lawbreakers to get indeed advanced. Primarily, cybercrimes target women who are vulnerable to exploitation. It is frequently delicate to hold perpetrators responsible due to a lack of substantiation and the fear of facing vilification. Cyber violence exposes women to colourful forms of detriment, including cyber vilification, sexual importunity, abuse, pornography, and deceitful dispatches. Women may admit unhappy and disturbing dispatches from unknown sources, which can lead to passions of vulnerability and implicit public demotion, pushing them to extreme measures like suicide.

Cybercrimes have the eventuality to impact individualities, businesses, and governments. While some cybercrimes may act traditional crimes, technology plays a pivotal part in enabling these offenses to reach a wider followership. also, cybercrimes can involve conditioning that would not be doable without the use of technology, like hacking. As the number of these offenses has increased, there has been a growing demand for police involvement. Still, numerous police agencies have been ill- set to handle this type of trouble from the morning. utmost command officers warrant the experience and training demanded to effectively respond to cybercrimes. In some cases, police officers have mentioned that the rise of cybercrime and the internet have made their jobs much more gruelling. To address this issue, some departments have established technical cybercrime units with advanced situations of training. There has been a significant body of research elucidating how various police organizational characteristics influence numerous specific policing outcomes (Chappell et al. 2006, Eitle et al., 2005; Willits and Nowacki,2014). However, outside of this problem space there has been a wide range of research examining how the relevant organizational characteristics impact formal police response to cybercrime. (Willits and Nowacki, 2016) the latter being an exception. This is a significant literature hole. Police organizational structure traits could be seen as relevant to strategic philosophy, specifically whether the association is one of generalist (all police officers across the agency) or specialist - like through a specialized unit or dedicated workforce. Hence, the response may be influenced by organizational structure and how cybercrime is being addressed. Maguire (2003) extended that theoretical analysis with a police organizational perspective designed to guide study of police associations. According to this proposition, rudiments of organizational terrain (department size, age, technology and terrain) and organizational complexity (e.g., situations of bureaucracy, specialization andnon- sworn labor force) may impact how the association manages its work and workers (organizational control). Others have extended this frame to examine policing issues, including the handover of inventions like community policing (Morabito, 2010) and intelligence- led policing (Darroch and Mazerolle, 2013). This is likely a useful approach for examining response to cybercrime, as analogous response can be viewed as an organizational invention in response to a growing need.

As internet access and smartphone ownership rates have increased in recent years (Poushter, 2016), the volume of cybercrimes, or offenses either entirely defined or at least assisted using technology, has increased (Lee and Lim, 2019; Wall and Williams, 2013). This increase has presented a number of challenges for police agencies. These challenges include the lack of a singular definition of cybercrime (Wall, 2007), lack of resources to address these offenses (Goodman, 1996; Harkin et al., 2018; Hinduja and Schafer, 2009; Hunton, 2011; Leppänen and Kankaanranta, 2017; Shinta and Logahan, 2019; Sommer, 2004; Wall, 1998), lack of training among officers (Bond and Tyrrell, 2018; Davis, 2012;

Forouzan et al., 2018; Hinduja, 2004; Holt et al., 2018), jurisdictional challenges (Cross, 2019; Cross and Blackshaw, 2014; Holt, 2018), and the tendency for police agencies to deem cybercrimes as less serious than traditional offenses (Bossler and Holt, 2012; Broll and Huey, 2015). In conclusion, cybercrime against women in Nagaland is an urgent challenge that requires a holistic and nuanced approach. This thesis aims to explore and analyze the complexities of cyber victimization among women in Nagaland. The goal is to provide information that informs policies, practices, and interventions aimed at protecting and empowering women in digital spaces. By addressing the root causes and consequences of cybercrimes against women, this study aims to pave the way for a safer and more just digital future in Nagaland and beyond.

5.2. Understanding and Addressing Cyber Crimes Against Women

Cybercrime is an unsettling concern, and while it is not uniformly defined, it generally refers to crimes assisted by computer technology. The study investigates the incidence of online aggressiveness, specifically on social media platforms, using both online and physical surveys of adult female internet users in Nagaland. The findings show that cybercrimes are significantly underreported in India, which can be linked to a lack of awareness about cyber laws and inadequate knowledge of reporting procedures. Furthermore, it emphasizes the difficulty of prosecuting cyber offenders due to a lack of resources and infrastructure within Nagaland's cybercrime police stations to properly track and solve such crimes. This study investigates the current environment of cybercrime targeting women in Nagaland, stressing the special obstacles faced in policing such offenses and providing ways for combating cybercrime through a comprehensive review of existing literature and empirical data, the paper describes the various forms of cybercrime affecting women in Nagaland and identifies gaps in current policing mechanisms. Additionally, it explores the socio-cultural factors contributing to the vulnerability of women to cybercrimes in the region. The paper then discusses potential avenues for enhancing law enforcement responses to cybercrimes against women, including capacity-building initiatives for law enforcement agencies, community awareness programs, and the utilization of technological solutions. By elucidating the intricacies of cybercrime against women in Nagaland and offering actionable recommendations, this chapter aims to contribute to

the development of more effective strategies for combating cyber-enabled gender-based violence in the region.

Cybercrime refers to a wide range of criminal activities carried out using computers and the internet, often involving hacking, fraud, theft, and other illegal activities targeting individuals, organizations, or governments. The term encompasses a wide range of illicit activities conducted through electronic means, including but not limited to identity theft, phishing scams, malware distribution, ransomware attacks, and online harassment. One comprehensive definition of cybercrime is provided by the Council of Europe's Convention on Cybercrime, also known as the Budapest Convention. According to Article 2 of the convention, cybercrime is defined as "offenses against the confidentiality, integrity, and availability of computer data and systems, computer-related offenses, and content-related offenses." The convention outlines various types of cybercrime and establishes guidelines for international cooperation in combating such crimes. Additionally, the United Nations Office on Drugs and Crime (UNODC) provides extensive resources and information on cybercrime. In its publication "Comprehensive Study on Cybercrime" (2013), the UNODC identifies cybercrime as a growing global threat, highlighting its complex nature and the challenges it poses to law enforcement agencies worldwide. More so, with the preference for the internet and advances in social media, cases of cyber-criminality against women have skyrocketed (Meha, 2020). Specifically, regarding WOM attacks, the instances of cyberbullying against women on SNS sites have escalated in the past years, and anti-female cyber harassment messages have always been a major internet concern (Watson, 2022).

In the year 2011, a case of cybercrime against a Naga woman was first reported in the Dimapur district and was also followed by a conviction. Politics in the state have also been a prime point of attack with women especially feeling the heat of cyber criminals (Limasen, 2017). In India, the many Laws IT Act of 2000, IPC 1860, and CCPWC have been enacted to support the victim. These strategies ensure that offenses like cyberbullying, cyberstalking, harassment, indecent exposure, and abuse of children to advance sexual motives, which are committed on the internet are hindered by propaganda, policed through training of enforcement officers and organizations, and victims supported (National Commission for Women).

Regarding combating cybercrime against women and children in India, the Cyber Crime Prevention against Women and Children (CCPWC) Scheme has been set, and the budget has been Rs 223. 198 crores. From this Rs. 93. 12 crores have been provided to different States and UTs for computer forensic training labs have been set up, capacities are being built and within-state and UT training are being provided. Its key components include an online cybercrime reporting platform (www.cybercrime.gov.in), a national-level cyber forensic laboratory, training programs for law enforcement personnel and legal professionals, cybercrime awareness initiatives, and support for research and development. The scheme has facilitated the reporting of over 3800 complaints since its inception, highlighting its effectiveness. Despite the allocation of funds and the implementation of various measures under the CCPWC Scheme, there are significant challenges observed in addressing cybercrimes against women in Nagaland. The limited tools and resources available to the Nagaland Cybercrime Police Station hinder their ability to effectively trace and investigate cases of cyber violence against women within the state. This inadequacy results in many cases remaining unsolved, potentially emboldening perpetrators to commit further crimes. The situation underscores the urgent need for enhanced support, resources, and capacity-building initiatives tailored to the specific needs of regions like Nagaland, where cybercrime against women is a pressing issue. Without adequate tools and infrastructure, the goal of preventing and combating cyber violence against women in Nagaland and similar regions remains elusive, emphasizing the importance of addressing these gaps to ensure the safety and security of women in the digital realm. In the case of Nagaland, young Naga women aged 16-25 are particularly vulnerable to experiencing online violence due to their active engagement with online communities and causes. This demographic tends to have greater access to digital platforms and social media, increasing their exposure to online risks. However, despite their higher likelihood of encountering cyber violence, these young women often face barriers to reporting such incidents. This reluctance may stem from a combination of factors, including fear of stigma, concerns about reputational damage, and the perception that cyber violence is not taken seriously by authorities or society at large. The negative impacts of online gendered violence on young Naga women can be profound, leading to mental health issues such as depression, anxiety, and traumatic stress. In some cases, the distress caused by cyber violence may even escalate to

suicidal thoughts, highlighting the urgent need for intervention and support services tailored to the unique challenges faced by this demographic.

Additionally, the prevailing cultural norms and attitudes towards gender-based violence in Nagaland may contribute to the underreporting and normalization of cyber violence, further perpetuating the cycle of harm. To address this issue effectively, it is crucial to raise awareness about cyber violence and its consequences within the Naga community. This includes educating both young women and the broader society about their rights, available support services, and avenues for reporting incidents of online violence. Moreover, efforts should be made to destigmatize the experience of being a victim of cyber violence and to foster a culture of empathy, support, and accountability. By empowering young Naga women to speak out against cyber violence and by providing them with the necessary resources and support, we can work towards preventing future incidents and ensuring justice for victims. Over the last few decades, the tendencies in criminological theories that explore the risks of certain groups as potential victims are interconnected with the current process of victimization. However, one of the regular affiliations that have not been captured adequately when studying cybercrime victimization is the relevance of dependence on technological prejudices. Thus, this paper has a sound methodological design aimed at investigating the level of smartphone dependence, the level of social support, and their connection to cyber fraud victimization using survey data from 716 respondents who are smartphone users who participated in the study annually for three years. Collectively, the findings from estimating separate survival and growth mixture models are that CYBER FRACT likelihood is lower among the users whose level of Smartphone dependence has reduced and whose level of social support has enhanced over the three years. Therefore, these results indicate new research agendas for investigating cybercrime victimization, especially concerning the psychological and social consequences of the unrestrained use of technological equipment. Computer crime may therefore be defined as any wrongdoing that is done with a computer or is done to a computer. This area of crime is relatively young and is developing at a geometric progression step. Several cyberlaw concerns surface at every step, right from the registration of the URL of the site, to the creation and sale of a website, to sending and receiving mail, and even in making and offering electronic commerce services on the site. Offenders have

realized that it is statistically less risky to perpetrate crimes in the cyber space hence the need for proper laws and standards to be set. Women and children are believed to be the most affected in the world and cybercrime is on the rise as many think of it as the easiest way to engage in criminality. The youth who are endowed with detailed computer knowledge but no job or money can turn themselves into computer criminals. These activities can provide hackers, and Cybercriminals with all the data as they attempt to siphon funds, blackmail or commit other criminal activities.

Cybercrime against women for publishing sexually explicit content has now become a global issue. The National Crime Records Bureau (NCRB) reported that the number of cases lodged for publishing sexual content spurted to 6,308 from 3,076 between 2018 and 2020 (Rahul Tripathi, ET Bureau). This section of the chapter will examine the manifold experiences of cybercrime victims and contribute to the vulnerability of women to cybercrime. Cybercrime against women has always been a major concern but the number of crimes committed was comparatively less before the pandemic. When the entire world was fighting the pandemic, another atrocity increased rapidly i.e., cybercrime against children and women. As people started engaging themselves more on the internet, the number of cybercrimes against women escalated which added another tension to the ongoing pandemic. As the second wave of the pandemic started, the number of cybercrime cases increased rapidly in March 2021 and continued to grow. During the pandemic, a total number of 704 cybercrime cases were reported in the year 2020 and 504 reported cases in 2021. However, the exact number of crimes may never be recorded as many crimes go unreported due to the stigma associated with it. Children are also vulnerable to such crimes because of the excessive time they spend on virtual platforms which has exposed most of them to become the victim of online harassment and being bullied in social media platforms. The more technology advances, the more the internet is used to satisfy every type of need. The World Wide Web provides an immediate solution for almost everything from one place, making online social networking, shopping, data storage, gaming, e-learning, and remote working possible. The internet has fit into almost every single aspect of a person's life today. The COVID-19 pandemic took this dependency even further, as remote work culture stood at the forefront of deeply putting technology in the domains of work, education, entertainment, and communication.

With the first emerging days of the internet, its designers would probably not have envisaged that it was going to become all-embracing to be manipulated for pernicious activities, thus bringing forth the need to regularize control. Unfortunately, the internet has become a harbor for several worrying activities. The anonymity offered by it helps people with technical expertise to conduct illegal activities without much fear of detection, thus making cyberspace misuse for criminal activities. Thus, this strongly states the cyber law in India. With the growth in popularity of the internet and its associated benefits, the concept of cybercrime has also grown. As a consequence of this, various types of cybercrime have emerged. The following chapter will allow for excavation into the realm of cyber violence against women, drawing on survivor experiences to spur a reappraisal of banal and quotidian forms of violence. In today's interconnected world, the internet has become integral to daily life, offering immense communication, commerce, and social interaction opportunities. However, these benefits come with significant risks, particularly concerning the safety and security of individuals online. Women, in particular, face unique challenges and vulnerabilities in cyberspace, which demand attention and concerted efforts to mitigate

1. The Growing Risk of Cyber Victimization Among Women

There is a disturbing trend emerging where women increasingly find themselves targeted by various forms of cybercrime. This trend underscores the need for comprehensive recognition and proactive measures to safeguard women's online experiences. Cybercrime laws vary significantly from one country to another, which complicates the global effort to combat these threats effectively. In response to these challenges, women are voicing a strong desire to feel safe and protected while engaging in online activities. Ensuring privacy in cyberspace requires adherence to robust security practices. For instance, regularly changing passwords is critical to maintaining the confidentiality of sensitive information stored across devices and platforms such as phones, emails, banking apps, and social media accounts. Passwords should be complex, avoiding easily guessable combinations derived from common words, dates, or personal information related to the user or the website. Additionally, refraining from disclosing personal details online is essential for preventing stalking, financial fraud, and other malicious behaviors that exploit personal information. This precaution is particularly crucial for women, who often face heightened risks of targeted harassment and privacy violations.

2. Educational and Institutional Responses to Cyber Threats

The educational sector plays a pivotal role in raising awareness about cyber threats and promoting safe online practices, especially among vulnerable populations like women. Issues such as cyberstalking, cyberbullying, and financial fraud perpetrated through email and social networking sites require greater attention within educational curricula. Efforts to combat cybercrime are multifaceted and require collaboration among government agencies, social service organizations, and philanthropic bodies. There is a consensus among experts that enhancing the knowledge and capabilities of law enforcement personnel and other stakeholders is crucial. Police training programs should include specialized modules on cybercrime investigation and victim support to address incidents involving women effectively.

3. Legal Frameworks and Policy Recommendations

In many jurisdictions, existing laws related to cybercrime may not adequately address the specific vulnerabilities faced by women online. There is a pressing need for legislative reforms or amendments to strengthen protections and ensure swift and effective legal recourse for victims. In India, for example, advocates argue for the enactment of a new cybercrime statute or amendments to existing legislation, such as the Information Technology Act, to better safeguard women against online threats. Furthermore, proactive measures by internet service providers and social media platforms are essential. These include robust privacy policies, transparent data handling practices, and user-friendly interfaces that empower individuals to manage their online presence securely. Awareness campaigns and community outreach programs can also play a crucial role in empowering women with knowledge and skills to protect themselves online.

4. Technological Solutions and Practical Recommendations

Technological advancements offer both opportunities and challenges in the fight against cybercrime. Antivirus software and firewall protections are essential tools for preventing malware infections and unauthorized access to personal data. Regular updates and patches to these software solutions are critical to stay ahead of evolving cyber threats, such as Trojan horses, worms, and email phishing scams that specifically target women. Moreover, individuals should remain vigilant by monitoring their online accounts for any suspicious activity. Regularly reviewing privacy settings on social media platforms and exercising caution when sharing personal information can significantly reduce the risk of privacy breaches and identity theft.

Public awareness campaigns can educate women about these risks and empower them to make informed decisions about their online behavior.

5. Socioeconomic and Cultural Implications

The impact of cybercrime extends beyond financial losses and privacy violations to include profound socio-economic and cultural consequences, particularly for women. Negative media coverage and social stigma associated with online victimization can exacerbate the trauma experienced by victims. Addressing these broader implications requires a holistic approach that integrates legal protections with social support services and advocacy efforts.

6. Global Perspectives and Collaborative Efforts

Cybercrime is a global issue that transcends national borders, necessitating international cooperation and collaboration. Initiatives such as internet trends research and cyber law conferences facilitate knowledge sharing and best practices among countries facing similar challenges. By fostering global partnerships, governments can enhance their capacity to combat cyber threats effectively and protect vulnerable populations, including women. In conclusion, while the Internet offers unprecedented opportunities for communication, commerce, and social interaction, it also presents significant risks, particularly for women. Addressing the vulnerabilities of women to cybercrime requires a multi-faceted approach that includes legislative reforms, educational initiatives, technological solutions, and socio-cultural awareness. By strengthening legal frameworks, enhancing law enforcement capabilities, promoting digital literacy, and fostering international cooperation, stakeholders can mitigate the risks posed by cybercrime and create a safer online environment for all individuals, regardless of gender. Empowering women with the knowledge and tools to protect themselves online is not only essential for their safety but also for promoting inclusivity and equality in the digital age.

5.3. Case Studies from Nagaland

Case Study 1

A chilling appellation for the act of cybercriminals posting sexual content of an individual that has been taken without consent in revenge for a perceived insult. Revenge porn means the act of sharing offensive personal photos online after a relationship to bring the curtain on it. This can be classified as a type of non-consensual pornography, but not all cases of non-consensual

pornography fall under revenge porn (Bates, 2017). Snapshots of 90% of revenge porn survivors being women can be traced from various researched studies (Bindu, 2021). The first known cybercrime reported in Nagaland of revenge porn was in the year 2008. A girl of the Naga community was stripped of her dignity through cyberspace by a lad with whom she had limited physical contact when they were studying in a reputed college in Kolkata. The accused, a Merchant Navy cadet who proposed to kill her to marry her against her will since she turned down his advances. Having been rejected by her, a man registered a fake Facebook account in her name, friended many people, and put some private photos of her, taken during a quarrel, and in the descriptions, there were obscene statements and calls for murder. This harassment was carried out from 2008 up to March 2011 as a result of which the victim developed extreme emotional stress. It led her to halt her education, and this tremendously affected her job and social opportunities. Her family even though it was well-rooted in society also felt a lot of humiliation. Thus, based on the complaint of the victim, an FIR was lodged with the East Police Station in Dimapur on March 16, 2011. Searching was over in 41 days, the alleged culprit was nabbed on 25 March 2011 at Netaji Subhash Chandra Bose Airport, Kolkata. The case was initiated for trial immediately after the police had observed all legal processes as provided by the Cr. P. C. and I. T. Act.

Revenge porn, a severe form of cybercrime, involves the non-consensual distribution of intimate images with the intent to harm or seek revenge. This case study delves into the first known instance of revenge porn reported in Nagaland, highlighting its profound impact on the victim's psychological well-being and social standing. The study traces the sequence of events from the initial harassment to the legal resolution, offering insights into the repercussions of such crimes and the effectiveness of legal measures in addressing them. Revenge porn represents a disturbing and increasingly prevalent issue within the domain of cybercrime. It involves the dissemination of intimate images or videos of individuals without their consent, typically by an ex-partner or someone with a vendetta, to inflict emotional distress or damage reputations (Bates, 2017). This form of non-consensual pornography is particularly harmful, as it not only violates personal privacy but also often leads to significant psychological and social consequences for the victim. The case of a female student from Nagaland provides a stark example of how revenge porn can devastate lives, impacting mental health, social relationships, and career prospects.

Background and Context

Defining Revenge Porn

Revenge porn, also known as non-consensual pornography, is a category of cybercrime where intimate images or videos are shared online without the subject's consent, typically in retaliation for a perceived wrong or to exert control over the victim (Bates, 2017). While revenge porn is a subset of non-consensual pornography, not all instances of non-consensual images fall under this category. The key distinguishing factor is the motive of revenge or malice behind the distribution of the content (Bindu, 2021).

Prevalence and Impact

Research indicates that approximately 90% of revenge porn victims are women (Bindu, 2021). This statistic highlights the gendered nature of the crime, where women are disproportionately affected by the intentional sharing of intimate images. The emotional, psychological, and social impacts of revenge porn can be profound, leading to issues such as anxiety, depression, social ostracization, and long-term reputational damage.

Case Description

Initial Contact and Harassment

In 2008, a female student from the Naga community, enrolled at a reputable college in Kolkata, fell victim to one of the earliest reported cases of revenge porn in Nagaland. The perpetrator, a Merchant Navy cadet with whom she had a short relationship, was enraged after his proposal were rejected. The accused's actions were driven by a desire for revenge and control, and he sought to damage the victim's reputation and social standing.

- **Creation of Fake Profile**: The accused created a fake Facebook account in the victim's name. This account was used to friend numerous individuals and to distribute private images of the victim.
- **Distribution of Intimate Content**: Along with the images, the perpetrator posted obscene comments and threats, including calls for violence against the victim. This not only served to humiliate her but also to provoke fear and anxiety.

Duration and Escalation

The harassment persisted from 2008 until March 2011. During this period, the victim faced continuous distress due to the widespread distribution of defamatory content. The impact of the perpetrator's actions was severe:

- **Psychological Impact**: The victim experienced extreme emotional stress, including anxiety, depression, and a profound sense of violation. The constant exposure to online harassment led to a deterioration in her mental health.
- **Educational and Career Consequences**: The victim was compelled to halt her education due to the emotional toll and the stigma attached to her situation. This interruption had a cascading effect on her career opportunities and social interactions.
- **Family Impact**: The victim's family also faced significant humiliation and social stigma due to the public nature of the defamation. This added to the overall distress and sense of violation experienced by the victim.

Legal Response

- **Filing of FIR**: On March 16, 2011, the victim lodged a First Information Report (FIR) with the East Police Station in Dimapur. The FIR detailed the harassment and requested legal intervention to address the cybercrime.
- **Investigation and Arrest**: The police conducted a thorough investigation, which took 41 days. The accused was apprehended on March 25, 2011, at Netaji Subhash Chandra Bose Airport in Kolkata. Following the arrest, legal proceedings were initiated in accordance with the Criminal Procedure Code (Cr. P. C.) and the Information Technology (I.T.) Act.

Impact Analysis

Emotional and Psychological Effects

The victim's experience of revenge porn resulted in severe psychological distress. The continuous exposure to online harassment, coupled with the invasion of privacy, led to significant emotional trauma. The victim experienced feelings of shame, anxiety, and depression, which had lasting effects on her mental health.

Social and Professional Repercussions

The public nature of the defamation caused substantial harm to the victim's reputation. The stigma associated with the revenge porn incident led to social ostracization and impacted her professional prospects. The interruption in her education further compounded these effects, making it challenging for her to resume her academic and career goals.

Family Impact

The victim's family faced humiliation and social stigma as a result of the online harassment. This added layer of distress highlighted the broader societal impact of revenge porn, affecting not only the victim but also those close to her.

Legal and Procedural Considerations

Legal Framework

The legal response to revenge porn involves several aspects:

- **Criminal Procedure Code (Cr. P. C.)**: This code outlines the procedures for the investigation and prosecution of criminal offenses, including cybercrimes such as revenge porn.
- **Information Technology (I.T.) Act**: The I.T. Act provides legal provisions for addressing cybercrimes and electronic violations. It includes sections relevant to the non-consensual dissemination of intimate images and online harassment.

Challenges in Prosecution

- **Evidence Collection**: Gathering sufficient evidence in cases of cyber defamation can be challenging. Ensuring that digital evidence is preserved and presented accurately is crucial for a successful prosecution.
- **Legal Reforms**: The evolving nature of cybercrimes necessitates ongoing legal reforms to address emerging issues and ensure effective protection for victims. The case underscores the need for comprehensive legal frameworks and robust enforcement mechanisms.

Prevalence and Awareness

The case highlights the need for increased awareness about revenge porn and its impacts. Educating individuals about the risks associated with sharing intimate content and the legal implications of cybercrimes is essential for prevention.

Support and Resources

Victims of revenge porn require access to support services, including psychological counseling and legal assistance. Providing resources to help victims navigate the emotional and legal challenges associated with cyber harassment is crucial.

Preventive Measures

Effective preventive measures include:

- **Digital Privacy Education**: Promoting digital privacy and responsible online behavior can help individuals protect themselves from potential cybercrimes.
- **Online Platform Policies**: Online platforms should implement policies and technologies to detect and remove non-consensual content promptly. Educating users about the reporting mechanisms and consequences of sharing intimate images is also important.

Legal and Institutional Support

- **Legal Frameworks**: Strengthening legal frameworks to address cybercrimes, including revenge porn, is essential. Ensuring that laws are up-to-date and effectively enforced can help protect victims and deter perpetrators.
- **Institutional Support**: Educational institutions and organizations should provide support and resources for individuals facing online harassment. Developing policies and programs to address cyberbullying and defamation is crucial for creating a safer digital environment.

Recommendations

For Individuals

- **Protect Personal Information**: Individuals should be cautious about sharing intimate images and personal information online. Understanding the potential risks and consequences is crucial for maintaining digital privacy.
- **Seek Support**: If affected by revenge porn or similar cybercrimes, individuals should seek support from mental health professionals and legal advisors. Accessing appropriate resources can help manage the emotional and legal challenges.

For Educational Institutions

- **Educational Programs**: Implementing educational programs on digital safety and the consequences of cybercrimes can help raise awareness among students and staff.
- **Support Services**: Providing support services, including counseling and legal assistance, can help individuals navigate the challenges associated with cyber harassment.

For Online Platforms

- **Monitoring and Reporting**: Enhancing monitoring systems to detect and address non-consensual content is essential. Promoting reporting mechanisms and educating users about digital safety can help prevent the spread of revenge porn.
- **User Education**: Online platforms should educate users about the risks and legal implications of sharing intimate images. Implementing measures to protect user privacy and prevent unauthorized dissemination of content is crucial.

For Authorities

- **Legal Reforms**: Ongoing legal reforms are necessary to address emerging issues related to cybercrime. Strengthening laws and enforcement mechanisms can help ensure effective protection for victims.

- **Victim Support**: Offering comprehensive support services, including counseling and legal aid, is essential for assisting individuals affected by revenge porn. Developing specialized programs and resources can help address the specific needs of victims.

Conclusion

The case study of the revenge porn incident in Nagaland underscores the severe impact of non-consensual pornography on victims' lives. It highlights the need for effective legal, educational, and support measures to address and prevent such cybercrimes. By fostering awareness, implementing preventive strategies, and providing robust support mechanisms, it is possible to mitigate the risks and consequences of revenge porn, ensuring better protection

Case Study 2

Technological aggression is the process of hurting, threatening, or incitement of others through the use of technology-based communication facilities. This can portray itself in any number of acts including but not limited to sending multiple malicious, threatening, or hostile messages, cyberbullying or stalking by sharing false information about the victim, identity theft or assuming the victim's identity online, or sharing invasive content like embarrassing photos or videos without consent (Hinduja, 2018). In a case of cyberbullying that occurred in Nagaland in 2018, a working woman became a target after she dumped her much older coworker. The former was insecure about the relationship, and after the breakup, the subject threatened and blackmailed the respondent on social media. He forwarded nasty messages and her photos to her

Background and Context

Definition and Scope

Technological aggression encompasses a range of malicious activities conducted through digital means. It includes:

- **Malicious Messaging**: Sending hostile, threatening, or harassing messages via email, social media, or other digital communication platforms.
- **Cyberbullying and Stalking**: Repeatedly targeting individuals with harmful actions, such as spreading false information or monitoring their online activities.

- **Identity Theft**: Assuming someone's digital identity to commit fraud or damage their reputation.
- **Non-Consensual Content Sharing**: Distributing private or embarrassing photos and videos without the subject's consent (Hinduja, 2018).

Prevalence and Impact

The proliferation of digital communication technologies has increased the prevalence of technological aggression. Victims often suffer severe emotional and psychological consequences, including depression, anxiety, and long-term trauma. The case of cyberbullying in Nagaland highlights how personal conflicts can escalate into serious forms of online harassment, affecting individuals' mental health and social well-being.

Incident Description

Case Overview

In 2018, a working woman in Nagaland became the target of technological aggression following a breakup with a significantly older coworker. The details of the case are as follows:

- **Background**: The victim, a professional woman, ended her relationship with her older coworker. The breakup was motivated by various personal and professional reasons, which left the coworker feeling insecure and rejected.
- **Cyber Harassment**: After the breakup, the former coworker engaged in a campaign of harassment against the victim:
    - **Threats and Blackmail**: The aggressor used social media to threaten and blackmail the victim. This included sending threatening messages and attempting to coerce her into compliance.
    - **Dissemination of Private Photos**: The aggressor forwarded the victim's private photos, obtained during their relationship, to her family and friends. This act was intended to publicly shame and embarrass her.
    - **Emotional Impact**: The harassment resulted in severe emotional stress for the victim. She experienced depression and anxiety attacks for approximately six

months, with the trauma continuing to affect her well-being even after the harassment ceased.

Consequences

- **Emotional and Psychological Effects**: The victim suffered from significant emotional and psychological distress, including anxiety and depression. The constant harassment and invasion of privacy led to a prolonged period of mental health issues.
- **Social and Professional Repercussions**: The dissemination of private photos and the threats made to her family and friends had a detrimental effect on her social and professional life. The victim faced social stigma and potential damage to her professional reputation.
- **Ongoing Impact**: The emotional scars from the harassment persisted, affecting her daily life and long-term mental health.

Impact Analysis

Emotional and Psychological Impact

The victim's experience highlights the severe psychological toll of technological aggression. The harassment led to significant mental health issues, including:

- **Depression**: Prolonged emotional stress and trauma from the cyberbullying resulted in clinical depression, requiring psychological intervention.
- **Anxiety**: Continuous threats and the public dissemination of private content triggered persistent anxiety attacks.

Social and Professional Repercussions

The victim’s professional and social standing was adversely affected by the harassment:

- **Professional Impact**: The public nature of the defamation and the personal distress caused by the harassment potentially impacted her professional performance and opportunities.

- **Social Stigma**: The dissemination of private photos and the resulting embarrassment affected her relationships with family and friends, leading to social isolation and stigma.

Family Impact

The victim's family also faced emotional stress due to the public nature of the harassment and the threats made against their family member. This added layer of distress underscores the broader impact of technological aggression on the victim's immediate social circle.

Legal and Procedural Considerations

Legal Framework

The case of technological aggression in Nagaland involves several legal aspects:

- **Cybercrime Legislation**: The applicable laws include provisions under the Information Technology (I.T.) Act, which addresses cyber harassment and the unauthorized dissemination of intimate content.
- **Criminal Procedure Code (Cr. P. C.)**: This code outlines the procedures for investigating and prosecuting criminal offenses, including cybercrimes.

Challenges in Legal Proceedings

- **Evidence Collection**: Gathering and preserving digital evidence in cases of cyber harassment can be challenging. Ensuring that digital evidence is accurately documented and presented is crucial for successful prosecution.
- **Legal Reforms**: The evolving nature of technological aggression necessitates ongoing legal reforms to address emerging issues and enhance protections for victims.

Understanding Social and Cultural Factors

The case underscores the importance of understanding the social and cultural factors that contribute to online violence:

- **Gender Dynamics**: The case highlights the gendered nature of technological aggression, where women are disproportionately affected by online harassment and cyberbullying.
- **Cultural Attitudes**: Societal attitudes towards relationships, privacy, and gender roles can influence the prevalence and severity of online harassment.

Support and Resources

Victims of technological aggression require comprehensive support services, including:

- **Psychological Counseling**: Access to mental health support is essential for addressing the emotional and psychological impacts of cyber harassment.
- **Legal Assistance**: Victims need access to legal resources to navigate the complexities of cybercrime and seek justice.

Preventive Measures

Effective preventive measures include:

- **Digital Privacy Education**: Promoting awareness about digital privacy and responsible online behavior can help individuals protect themselves from technological aggression.
- **Online Platform Policies**: Enhancing monitoring and reporting mechanisms on digital platforms can help detect and address instances of cyber harassment promptly.

Legal and Institutional Support

- **Legal Frameworks**: Strengthening legal frameworks to address technological aggression and ensure effective enforcement is crucial for protecting victims.
- **Institutional Support**: Educational institutions and organizations should provide resources and support for individuals facing online harassment, including counseling and legal assistance.

Recommendations

For Individuals

- **Protect Personal Information**: Individuals should be cautious about sharing personal and intimate information online. Understanding the risks associated with digital exposure is essential for maintaining privacy.
- **Seek Support**: If affected by technological aggression or similar cybercrimes, individuals should seek support from mental health professionals and legal advisors.

For Educational Institutions

- **Educational Programs**: Implementing educational programs on digital safety and the consequences of technological aggression can raise awareness among students and staff.
- **Support Services**: Providing resources and support services for individuals facing online harassment can help them navigate the challenges associated with such incidents.

For Online Platforms

- **Monitoring and Reporting**: Online platforms should enhance their monitoring systems to detect and address non-consensual content and cyber harassment.
- **User Education**: Promoting user education about digital safety and the risks of technological aggression is crucial for preventing online harassment.

For Authorities

- **Legal Reforms**: Ongoing legal reforms are necessary to address emerging issues related to technological aggression. Strengthening laws and enforcement mechanisms can help protect victims and ensure justice.
- **Victim Support**: Offering comprehensive support services, including counseling and legal aid, is essential for assisting individuals affected by technological aggression.

Conclusion

The case study of technological aggression in Nagaland illustrates the severe impact of cyberbullying and related forms of online harassment. It highlights the need for effective legal, educational, and support measures to address and prevent technological aggression. By fostering awareness, implementing preventive strategies, and providing robust support mechanisms, it is possible to mitigate the risks and consequences of cyber harassment, ensuring better protection and justice for victims.

Case Study : Technological Aggression and Cyberbullying in Nagaland

Abstract

Technological aggression, characterized by the use of digital tools to inflict harm or threat, represents a growing concern in the realm of cybercrimes. This case study examines a significant incident of cyberbullying in Nagaland in 2018, focusing on the impact of technological aggression on a working woman who was targeted by her former coworker following a breakup. The aggressor's actions, including threats, blackmail, and the dissemination of private photos, had severe emotional and psychological consequences for the victim. This case study aims to provide a comprehensive analysis of the incident, explore the broader implications for online safety and privacy, and offer recommendations for addressing similar issues.

Introduction

Technological aggression is a multifaceted issue involving various forms of online harassment and abuse. It encompasses behaviors such as sending threatening messages, cyberbullying, identity theft, and the non-consensual sharing of intimate content (Hinduja, 2018). The advent of digital communication tools has facilitated these harmful behaviors, making it easier for perpetrators to inflict damage on victims. This case study focuses on a specific incident of cyberbullying in Nagaland in 2018, highlighting the severe impacts of technological aggression and emphasizing the need for effective measures to combat such crimes.

Background and Context

Defining Technological Aggression

Technological aggression includes various harmful behaviors conducted through digital means. It involves:

- **Malicious Messaging**: Sending threatening, abusive, or harassing messages via email, social media, or other digital platforms.
- **Cyberbullying and Stalking**: Repeatedly targeting individuals with harmful actions, such as spreading false information or monitoring their online activities.
- **Identity Theft**: Assuming someone's digital identity to commit fraud, harass, or damage their reputation.
- **Non-Consensual Content Sharing**: Distributing intimate or embarrassing photos and videos without the subject's consent (Hinduja, 2018).

Prevalence and Impact

The prevalence of technological aggression has increased with the rise of digital communication technologies. Victims of cyberbullying and other forms of technological aggression often experience significant emotional and psychological consequences. These impacts include anxiety, depression, and long-term trauma. The case of cyberbullying in Nagaland provides a concrete example of how personal conflicts can escalate into severe forms of online harassment.

Incident Description

Case Overview

In 2018, a working woman in Nagaland became a target of technological aggression following a breakup with her significantly older coworker. The details of the case are as follows:

- **Background**: The victim, a professional woman, ended her relationship with her older coworker. The breakup was motivated by personal and professional reasons, leaving the coworker feeling insecure and rejected.

- **Cyber Harassment**: Following the breakup, the former coworker engaged in a series of harassment actions:
    - **Threats and Blackmail**: The aggressor used social media to threaten and blackmail the victim. This included sending threatening messages and attempting to coerce her into compliance.
    - **Dissemination of Private Photos**: The aggressor forwarded the victim's private photos, obtained during their relationship, to her family and friends. This act was intended to publicly shame and embarrass her.
    - **Emotional Impact**: The harassment resulted in severe emotional stress for the victim. She experienced depression and anxiety attacks for approximately six months, with the trauma continuing to affect her well-being even after the harassment ceased.

Consequences

- **Emotional and Psychological Effects**: The victim experienced significant emotional and psychological distress, including anxiety and depression. The constant harassment and invasion of privacy led to a prolonged period of mental health issues.
- **Social and Professional Repercussions**: The public dissemination of private photos and the threats made to her family and friends had a detrimental effect on the victim's social and professional life. The victim faced social stigma and potential damage to her professional reputation.
- **Ongoing Impact**: The emotional scars from the harassment persisted, affecting her daily life and long-term mental health.

Impact Analysis

Emotional and Psychological Impact

The victim's experience illustrates the severe psychological effects of technological aggression:

- **Depression**: The victim suffered from clinical depression due to the prolonged emotional stress and trauma caused by the harassment. This condition required psychological intervention and ongoing support.

- **Anxiety**: Persistent threats and the public dissemination of private content triggered severe anxiety attacks, impacting the victim's ability to function normally in her daily life.

Social and Professional Repercussions

The social and professional impacts of the harassment were significant:

- **Professional Impact**: The public nature of the defamation and the personal distress caused by the harassment potentially affected the victim's performance and career prospects. The disruption in her professional life highlights the broader implications of technological aggression.
- **Social Stigma**: The dissemination of private photos and the resulting embarrassment affected the victim's relationships with family and friends. The social stigma associated with the incident led to isolation and damaged her social standing.

Family Impact

The victim's family also experienced emotional stress due to the public nature of the harassment and the threats made against their family member. This added layer of distress underscores the broader impact of technological aggression on the victim's immediate social circle.

Legal and Procedural Considerations

Legal Framework

The case of technological aggression in Nagaland involves several legal aspects:

- **Cybercrime Legislation**: The Information Technology (I.T.) Act provides provisions for addressing cyber harassment and the unauthorized dissemination of intimate content. Relevant sections of the I.T. Act include:
    - **Section 66E**: Punishes the violation of privacy by capturing, transmitting, or publishing images of private areas without consent.
    - **Section 67**: Addresses the publication or transmission of obscene material in electronic form.

- **Criminal Procedure Code (Cr. P. C.)**: This code outlines the procedures for investigating and prosecuting criminal offenses, including cybercrimes. It includes provisions for evidence collection, witness testimony, and legal proceedings.

Challenges in Legal Proceedings

- **Evidence Collection**: Gathering and preserving digital evidence in cases of cyber harassment can be challenging. Ensuring that digital evidence is accurately documented and presented is crucial for successful prosecution.
- **Legal Reforms**: The evolving nature of technological aggression necessitates ongoing legal reforms to address emerging issues and enhance protections for victims. Current laws may need updates to address new forms of digital harassment and exploitation.

Understanding Social and Cultural Factors

The case highlights several social and cultural factors contributing to online violence:

- **Gender Dynamics**: The case underscores the gendered nature of technological aggression, with women disproportionately affected by online harassment and cyberbullying. Societal attitudes toward women and relationships play a significant role in perpetuating such behaviors.
- **Cultural Attitudes**: Cultural attitudes towards privacy, relationships, and gender roles influence the prevalence and severity of technological aggression. Understanding these attitudes is essential for developing effective prevention and intervention strategies.

Support and Resources

Victims of technological aggression require comprehensive support services:

- **Psychological Counseling**: Access to mental health support is essential for addressing the emotional and psychological impacts of cyber harassment. Counseling services can help victims cope with trauma and rebuild their lives.

- **Legal Assistance**: Victims need access to legal resources to navigate the complexities of cybercrime and seek justice. Legal assistance can help victims understand their rights and pursue legal remedies.

Preventive Measures

Effective preventive measures include:

- **Digital Privacy Education**: Promoting awareness about digital privacy and responsible online behavior can help individuals protect themselves from technological aggression. Educational programs should focus on safe online practices and the risks of sharing personal information.
- **Online Platform Policies**: Online platforms should implement policies and technologies to detect and address non-consensual content promptly. Reporting mechanisms should be user-friendly and accessible to facilitate the removal of harmful content.

Legal and Institutional Support

- **Legal Frameworks**: Strengthening legal frameworks to address technological aggression and ensure effective enforcement is crucial for protecting victims. Laws should be updated to reflect the evolving nature of cybercrimes.
- **Institutional Support**: Educational institutions and organizations should provide resources and support for individuals facing online harassment. Developing policies and programs to address cyberbullying and defamation is essential for creating a safer digital environment.

Recommendations

For Individuals

- **Protect Personal Information**: Individuals should be cautious about sharing personal and intimate information online. Understanding the potential risks and consequences of digital exposure is crucial for maintaining privacy.

- **Seek Support**: If affected by technological aggression or similar cybercrimes, individuals should seek support from mental health professionals and legal advisors. Accessing appropriate resources can help manage the emotional and legal challenges.

For Educational Institutions

- **Educational Programs**: Implementing educational programs on digital safety and the consequences of technological aggression can raise awareness among students and staff. These programs should include information on preventing and responding to cyberbullying.
- **Support Services**: Providing resources and support services for individuals facing online harassment can help them navigate the challenges associated with such incidents. Institutions should offer counseling and legal assistance to affected individuals.

For Online Platforms

- **Monitoring and Reporting**: Enhancing monitoring systems to detect and address non-consensual content and cyber harassment is essential. Platforms should implement advanced technologies to identify harmful behaviors and content.
- **User Education**: Online platforms should educate users about digital safety, the risks of technological aggression, and the available reporting mechanisms. User education can help prevent online harassment

Case Study 3

Cyberstalking entails following a person's movement on the website without their knowledge and sending flood emails and messages to that person (Bindu, 2021). One woman from Dimapur, Nagaland, interviewed by the researcher, said that she had become a victim when she found that one of the neighboring men had posted her picture on Facebook stating that she was his girlfriend. Another way that the neighbor intruded on her privacy was to take all the photos of her and send them to her mutual friends thus affecting her reputation and relations. Luckily, the woman and her friends went to the neighbor and sorted the issue out. She learned from this incident to be careful about what she posts on her social media accounts by ensuring that they are

private and not to post pictures. She feared that other women could also be victims of such cyber crimes of cyberbullying or whatever-related crime and therefore, women must be more sensitive to some privacy policies that would prevent such mishaps.

Background

Cyberstalking is a modern form of harassment that utilizes digital platforms to track, intimidate, or bother someone repeatedly. Unlike traditional stalking, which involves physical proximity and direct interaction, cyberstalking is conducted through online channels such as social media, email, and messaging apps. The advent of the internet and social media has made it easier for individuals to engage in such behavior, often under the cover of anonymity.

Statistics reveal that cyberstalking is not just a distant concern but a widespread issue affecting many people globally. Despite the awareness and measures taken, the rapid evolution of technology often outpaces the development of effective legal frameworks. In India, the Information Technology Act provides some level of protection against cybercrimes, including cyberstalking, but enforcement and victim support can be inconsistent.

The Incident

In Dimapur, Nagaland, a woman became a victim of cyberstalking by a neighbor. The neighbor's actions included posting her photograph on Facebook with a misleading caption that falsely claimed she was his girlfriend. This act of sharing not only invaded her privacy but also misrepresented their relationship to the public.

The situation worsened when the neighbor sent her photos to her mutual friends, exacerbating the breach of her privacy. This dissemination of personal images and false claims led to significant harm to her reputation and strained her social connections. The emotional toll was considerable, affecting her mental health and personal life.

The woman, supported by her friends, decided to address the issue directly. They confronted the neighbor, who then apologized and removed the offending content. While this resolution was

immediate, it highlighted the need for greater awareness and proactive measures regarding online privacy.

Impact Analysis

The psychological effects of cyberstalking are profound. Victims often experience anxiety, depression, and a deep sense of violation. In this case, the unauthorized sharing of personal images and false information led to considerable emotional distress for the victim. The breach of her privacy and the subsequent social repercussions significantly impacted her well-being. Social and reputational damage from such incidents can be extensive. In this case, the false claims and unauthorized dissemination of personal photos harmed the woman's reputation and strained her relationships. Such incidents highlight the broader implications of cyberstalking on social interactions and personal reputation. The incident also raises questions about the effectiveness of existing legal protections. While there are laws designed to combat cybercrimes, their application can be inconsistent. This case underscores the need for more robust legal frameworks and increased awareness about the legal rights available to victims.

Preventive measures are crucial in addressing the risks associated with cyberstalking. Effective strategies include:

- **Adjusting Privacy Settings**: Regularly reviewing and tightening privacy settings on social media to limit unauthorized access to personal information.
- **Increasing Awareness**: Educating individuals about the risks of cyberstalking and promoting best practices for online safety.
- **Utilizing Reporting Tools**: Making use of reporting mechanisms on social media platforms and seeking legal recourse when necessary.

Broader Implications

This case from Dimapur sheds light on broader issues related to digital privacy and cybersecurity. As our lives become more intertwined with digital platforms, the risks associated

with online harassment grow. Addressing these challenges requires a multi-faceted approach, including better education, legal reforms, and technological solutions.

Policymakers need to consider several aspects:

- **Updating Legal Frameworks**: Laws should evolve to address the complexities of modern cybercrimes.
- **Improving Enforcement**: Better mechanisms for enforcing cybercrime laws and supporting victims are essential.
- **Enhancing Public Awareness**: Increasing public knowledge about online safety and legal options can help prevent and address cyberstalking.

Future research should focus on evaluating the effectiveness of current legal measures, understanding the impact of cyberstalking on different populations, and exploring innovative technological solutions to prevent and address online harassment. The role of social media platforms in mitigating risks and supporting victims also warrants further examination.

Conclusion

The cyberstalking incident in Dimapur highlights the serious implications of online harassment. The case illustrates the significant impact of such behavior on individuals' mental health, social relationships, and public reputation. Understanding these issues and exploring effective prevention and intervention strategies are crucial steps toward fostering a safer online environment.

Case Study 4

Emotional fraud is a modern and often unnoticed type of international crime that employs online dating sites and services, having severe financial and psychological consequences for tens of millions of people (Buchanan & Whitty, 2014). Sophia, a middle-aged married woman, has physical abuse from her husband and she went to Facebook seeking comfort. She became friends with a man on social media pretending to be a foreign national, whom she allowed to be her friend before he began to court her. He said that he had purchased a valuable item for her and

assured her that he made a mistake at the address where the worth of Rs 10000/- was needed to sort it out. In the early stages, he would engage her frequently; however, after Sophia paid, he never communicated with her again. He re-emerged a few days later with tall stories of a car accident and requested money for surgery and hospital fees. Sophia, believing his tale, transferred five lakh rupees of her hard-earned money to his account, and subsequently one of her friends revealed all the facts about the man as that of a con man. Alas, because Sophia wanted to preserve her marriage, the woman could not turn to the police. This goes a long way in explaining the situation in the Northeast region because people have low exposure coupled with low awareness, they become easy targets.

Background on Emotional Fraud

Emotional fraud involves deceiving individuals by manipulating their emotions through online interactions. Typically, perpetrators use dating sites or social media platforms to create fake identities and establish relationships with victims. These fraudsters often prey on individuals who are seeking emotional support or companionship, exploiting their vulnerabilities to achieve financial gain.

Nature and Scope of Emotional Fraud

Emotional fraud can take many forms, but it often involves a scammer creating a false persona to gain the trust and affection of their target. The scammer may present themselves as a foreign national, a wealthy individual, or someone in distress, all designed to elicit sympathy and financial support. The scope of emotional fraud is vast, with millions affected globally. Victims often face not only financial loss but also long-term psychological trauma.

Psychological Impact

The psychological effects of emotional fraud are profound. Victims frequently experience a range of emotions including betrayal, shame, and depression. The sense of betrayal is particularly acute as victims realize that their emotional trust has been exploited. The financial loss, coupled with the emotional damage, can have lasting impacts on a person's mental health.

Case Description: Sophia's (Pseudo name) Experience

Sophia, a middle-aged married woman from Dimapur, Nagaland, was struggling with domestic abuse from her husband. Seeking solace and a sense of companionship, she turned to Facebook. On the platform, she connected with a man who claimed to be a foreign national. Initially, their interactions were friendly and supportive, which provided Sophia with a sense of relief and emotional connection.

Initial Contact and Relationship Building

The man, who presented himself as a wealthy foreign national, initially engaged with Sophia in a manner that seemed genuine. He would frequently communicate with her, offering emotional support and companionship. This initial period of interaction involved shared conversations and expressions of care, which helped to build trust between Sophia and the scammer.

The Scam Begins

The scam began when the man told Sophia that he had purchased a valuable gift for her. He mentioned an issue with the delivery address, stating that Rs 10,000 was required to resolve the problem. Trusting him and believing in the sincerity of his intentions, Sophia transferred the amount. Shortly thereafter, the scammer ceased communication, leaving Sophia puzzled and distressed.

Escalation of the Fraud

The scammer resurfaced after a short period with a new story: he claimed to have been involved in a car accident and required money for surgery and hospital expenses. Sophia, still under the impression that the man was in genuine need, sent him a significant amount of money worth five lakh rupees from her savings. It was only when a friend of Sophia’s conducted some background research that the truth about the scammer was revealed.

Revelation and Consequences

Sophia's friend discovered that the man was a con artist using a fake identity to defraud individuals. This revelation was devastating for Sophia, who felt a profound sense of betrayal and shame. The financial loss, combined with the emotional trauma, left her in a precarious situation. Despite the severity of the scam, Sophia chose not to report the incident to the police, primarily due to her desire to protect her marriage and avoid further complications.

Analysis of the Incident

Psychological Impact

The psychological impact of the scam on Sophia was severe. Victims of emotional fraud often experience a mix of shame, guilt, and emotional pain. Sophia's situation was exacerbated by her ongoing domestic issues, which made the emotional support she sought through the scammer all the more critical. The betrayal and financial loss added layers of distress, affecting her overall mental well-being.

Social and Reputational Damage

The social implications of Sophia's experience are significant. The loss of trust and the stigma associated with falling victim to such a scam can impact personal relationships and social standing. Sophia's decision to keep the incident private, out of fear of judgment and the desire to preserve her marriage, underscores the social pressures that victims face.

Legal and Protective Measures

Sophia's reluctance to involve the authorities highlights gaps in the legal and protective measures available to victims of emotional fraud. While there are legal frameworks in place to address various forms of cybercrime, the effectiveness of these measures can be limited by factors such as awareness, enforcement, and the personal circumstances of victims.

Preventive Strategies

Several strategies can help prevent emotional fraud:

- **Education and Awareness**: Increasing awareness about the risks associated with online interactions and the signs of emotional fraud is crucial. Educational programs and campaigns can help individuals recognize red flags and protect themselves from scammers.
- **Strengthening Digital Literacy**: Enhancing digital literacy and online safety knowledge can empower individuals to navigate online platforms more securely. This includes understanding privacy settings, recognizing fraudulent behavior, and reporting suspicious activity.
- **Support Systems for Victims**: Providing support services for victims, including counseling and financial advice, can help them recover from the trauma and loss associated with emotional fraud. Establishing clear channels for reporting and seeking assistance can also aid in addressing such crimes more effectively.

Broader Implications

Regional Vulnerabilities

Sophia's case highlights specific vulnerabilities within the Northeast region of India. The combination of lower digital literacy and limited exposure to online scams makes individuals in these areas particularly susceptible to emotional fraud. Addressing these vulnerabilities requires targeted interventions, including education, community outreach, and support systems tailored to the unique needs of the region.

Policy and Legislative Recommendations

To address the issue of emotional fraud more effectively, several policy and legislative measures should be considered:

- **Updating Legal Frameworks**: Laws should be updated to address the evolving nature of cybercrimes, including emotional fraud. This involves creating specific legal provisions for online scams and enhancing penalties for perpetrators.

- **Improving Enforcement**: Strengthening mechanisms for the enforcement of cybercrime laws and improving coordination between law enforcement agencies can help ensure that perpetrators are held accountable.
- **Promoting Public Awareness**: Public awareness campaigns should focus on educating individuals about the risks of emotional fraud and providing information on how to protect themselves. Collaboration between government agencies, non-profit organizations, and educational institutions can enhance the effectiveness of these campaigns.

Future Research Directions

Future research should focus on several areas:

- **Impact Assessment**: Conducting studies to assess the long-term psychological and social impacts of emotional fraud on victims can provide valuable insights into the consequences of such scams.
- **Effectiveness of Prevention Strategies**: Evaluating the effectiveness of various preventive measures and educational programs can help identify best practices and areas for improvement.
- **Technological Solutions**: Exploring technological solutions, such as advanced algorithms for detecting fraudulent behavior on social media platforms, can enhance efforts to combat emotional fraud.

Conclusion

Sophia’s experience with emotional fraud illustrates the profound impact of such scams on individuals' lives. The case highlights the need for increased awareness, improved protective measures, and targeted interventions to address the vulnerabilities associated with online fraud. By understanding the nature of emotional fraud and implementing effective strategies, we can work towards creating a safer and more secure online environment for all individuals.

Case Study 5

On July 24, 2024, the author received an urgent and distressing call from a junior who was experiencing severe emotional and psychological distress due to a case of cyber defamation. This case study examines the impact of cyber defamation on a student from a reputable college in Dimapur, Nagaland, who was falsely implicated in a pornographic video that went viral. The incident highlights the severe consequences of digital defamation on an individual's mental health and reputation, and underscores the broader implications of online harassment.

Background

Cyber defamation involves the dissemination of false and damaging information about an individual through digital platforms. The case in question involves a female student from a prestigious college in Dimapur, Nagaland, whose face was partially visible in a pornographic video that became widely circulated online. The situation was exacerbated when rumors surfaced linking her to the video, and her Instagram handle was shared across various online forums.

Incident Description

- **Initial Contact**: On July 24, 2024, at approximately 9:00 PM, the author received a call from her junior, who was in a state of distress due to cyber defamation. The junior reported that a pornographic video featuring a woman whose face was only partially visible had gone viral.
- **Spread of Rumours**: The situation worsened when online rumours emerged suggesting that the female character in the video was the junior. Her Instagram handle was shared on multiple online forums, further aggravating the situation.
- **Impact on the Junior**: The junior was initially unaware of the video until a friend informed her. The revelation caused significant psychological and emotional pain, including feelings of despair, anxiety, and a profound sense of privacy violation.
- **Consequences**: The defamation led to severe damage to the junior's reputation, which could have long-lasting effects on her personal life and professional future.

Impact

- **Psychological and Emotional Effects**: The girl experienced severe emotional distress, including anxiety, despair, and a feeling of violation. These effects have implications for her mental health and overall well-being.
- **Reputational Damage**: The spread of false information and the association with the pornographic video caused substantial harm to her reputation, affecting both her personal relationships and professional prospects.
- **Privacy Violation**: The unauthorized sharing of her Instagram handle and personal information compounded the sense of invasion of privacy.

Prevention

1. **Digital Privacy Awareness**: There is a critical need for heightened awareness regarding digital privacy and the potential risks associated with sharing personal information online.
2. **Impact of Cyber Defamation**: Cyber defamation can have severe psychological and reputational impacts. Individuals and institutions must recognize the seriousness of such offenses and respond appropriately.
3. **Support Mechanisms**: Victims of cyber defamation require comprehensive support, including psychological counseling and legal assistance, to address the emotional and reputational damage.
4. **Preventive Measures**: Effective measures need to be implemented to prevent the spread of defamatory content, including enhanced security for digital profiles and education on responsible online behavior.

Recommendations

1. **For Individuals**:
    - Be cautious about sharing personal information online and understand the potential risks of digital exposure.
    - Seek support from trusted friends, family, and professional counselors in the event of cyber defamation.

2. **For Educational Institutions**:
    - Implement awareness programs on digital safety and the consequences of cyber defamation.
    - Provide resources and support systems for students facing online harassment.
3. **For Online Platforms**:
    - Enhance monitoring and reporting mechanisms to address and remove defamatory content promptly.
    - Develop and promote educational initiatives to inform users about cyber defamation and privacy protection.
4. **For Authorities**:
    - Strengthen legal frameworks to address cyber defamation and ensure effective enforcement against perpetrators.
    - Offer victim support services, including counseling and legal aid, to assist individuals affected by online defamation.

Conclusion

This case study underscores the severe impact of cyber defamation on individuals' mental health and reputations. It highlights the urgent need for effective preventive measures, support systems, and legal frameworks to address and mitigate the consequences of online harassment. By fostering awareness and providing robust support mechanisms, it is possible to better protect individuals from the harmful effects of cyber defamation and enhance digital safety.

Case Study 5

Online Scam Involving Fraudulent Sale of a Scooter:

This case study examines an online scam that occurred in August 2023, where a Naga resident was defrauded of ₹21,699 under the pretext of purchasing a scooter. The scammer, posing as a member of the Army Jat Regiment, utilized deceptive tactics to extract multiple payments from the victim. The case came to public attention following a report by Hornbill TV, which highlighted the incident and its implications for online transaction security.

Background

In August 2023, an online marketplace facilitated a fraudulent transaction involving a scooter sale. The scammer, claiming to be an Army Jat Regiment member, exploited the victim's trust by using a fabricated military connection to justify the sale. This case illustrates the growing issue of online fraud and the need for increased vigilance and protective measures in digital transactions.

Incident Description

- **Initial Contact and Fraudulent Claims**: The scammer advertised a scooter in online platform for sale. They presented themselves as an Army Jat Regiment member who was being transferred to Jammu and Kashmir, necessitating a quick sale of the scooter.
- **Payment Requests**: The scammer requested an initial advance payment of ₹500. Subsequent requests included ₹5,150 for security and ₹5,100 for additional fees. These multiple payments amounted to a total of ₹21,699.
- **Deceptive Practices**: To bolster their deceit, the scammer sent a video purporting to show an Army truck loaded with the scooter, further convincing the victim of the transaction’s legitimacy.
- **Outcome**: Upon completing the payments, the victim lost contact with the scammer, who ceased all communication. The victim realized they had been defrauded when the scooter failed to be delivered.

Impact

- **Financial Loss**: The victim experienced a financial loss totalling ₹21,699.
- **Emotional Distress**: The scam caused significant emotional distress, including feelings of betrayal and frustration.

- **Public Awareness**: The incident gained wider visibility when Hornbill TV featured it on their news channel, drawing attention to the risks of online scams and highlighting the need for improved online transaction security.

Prevention

1. **Verification of Seller Identity**: It is crucial to verify the identity and credibility of sellers, particularly when dealing with significant transactions. Claims of military or official affiliations should be independently confirmed.
2. **Critical Evaluation of Evidence**: Digital evidence, such as videos, can be manipulated. Independent verification of any provided proof is essential.
3. **Secure Payment Methods**: Transactions should be conducted through secure payment methods that offer buyer protection to mitigate the risk of fraud.
4. **Awareness of Scams**: Increased awareness and skepticism regarding unsolicited offers and high-pressure sales tactics can prevent falling victim to similar scams.

Recommendations

1. **For Buyers**:
    - Conduct thorough research on sellers and their offers.
    - Use payment methods with fraud protection features.
    - Verify the authenticity of evidence and claims made by sellers.
2. **For Online Platforms**:
    - Implement stronger verification processes for sellers.
    - Educate users about common scams and how to identify them.
3. **For Authorities**:
    - Enhance efforts to investigate and prosecute online fraud cases.
    - Support public awareness campaigns to inform individuals about online safety practices.

Conclusion

This case study underscores the importance of vigilance and due diligence in online transactions. By adhering to recommended practices and remaining cautious, individuals can better protect themselves from fraudulent schemes. The exposure of this case by Hornbill TV highlights the urgent need for enhanced security measures and increased public awareness to combat online fraud effectively.

Case Study 6

In the digital age, cybercrime has evolved into a complex and pervasive issue, impacting millions of individuals globally. Among the various forms of cybercrime, recruitment fraud stands out as a particularly deceptive practice that can have severe repercussions for its victims. This case study delves into a notable incident involving individuals from the state of Nagaland India, who were detained in Punjab on charges related to cybercrime. The study provides a comprehensive analysis of the situation, drawing on first-hand accounts and face-to-face interaction with the author. The author, a former president and current Advisor of the Naga Students' Union Punjab, had special access to visit the detained individuals in Nabha District Jail and Ropar District Jail and gathered critical information.

Background

Overview of Cybercrime

Cybercrime encompasses a broad range of illicit activities carried out through digital platforms. This includes financial fraud, identity theft, hacking, and various other crimes that exploit technological vulnerabilities. The rapid advancement of technology has facilitated the rise of sophisticated cybercriminal activities, which often target vulnerable populations.

Types of Cybercrime:

1. **Financial Fraud:** Involves schemes like phishing, identity theft, and online scams designed to steal money.
2. **Cyber Espionage:** Targets sensitive information from individuals or organizations.

3. **Cyberbullying:** Harassment or bullying conducted through digital means.
4. **Recruitment Fraud:** A specific type of financial fraud where individuals are deceived into accepting non-existent or exploitative job offers.

Recruitment Fraud

Recruitment fraud is a significant concern within the realm of cybercrime. It involves deceiving individuals into believing they are securing legitimate employment, only to find themselves involved in criminal activities or facing other adverse consequences. This type of fraud preys on individuals seeking employment, especially those in regions with limited resources and information.

Common Recruitment Fraud Tactics:

1. **False Job Offers:** Scammers present non-existent high-paying jobs to lure victims.
2. **Initial Payment Requests:** Fraudsters may request fees for job application processing or visa arrangements.
3. **Involvement in Criminal Activities:** Victims may unknowingly participate in illegal operations under the guise of legitimate work.

Incident Overview

Discovery of the Detained Individuals

The crisis came to light through the efforts of an activist, Mr. X, who contacted the families of individuals from the Northeast detained in Punjab. Many of these families were initially unaware of their children's incarceration, leading to significant shock and confusion regarding the legal process and the nature of the charges.

Key Aspects of the Discovery:

1. **Lack of Awareness:** Families had limited knowledge of their children's situation.
2. **Confusion and Fear:** The complexity of the legal process contributed to widespread confusion.

3. **Activist Intervention:** Mr. X's investigation and subsequent actions were crucial in highlighting the issue.

Author's Visit to the Nabha District Jail and Ropar District Jail

The author, a former president and current Advisor of the Naga Students' Union Punjab, was instrumental in accessing the detained individuals. Utilizing her position, the author gained permission to visit the Nabha District Jail and Ropar District Jail, where she had aa group interaction and collected statements from the detainees.

Findings from the Visits:

1. **Statements from Detained Youths:** During the visits, some detained individuals claimed they were arrested on the very day they joined the recruitment process. This suggests that they might have been targeted from the outset or were part of a scheme involving immediate legal consequences.
2. **Conditions in Jail:** The author assessed the conditions and treatment of the detainees, highlighting issues related to their well-being and legal status. Initially, the detainees did not face any problems with the other inmates in jail but with the passage of time, the detainees brought up a complaint that they were being racially discriminated against, verbally abused and threatened by the inmates belonging to other states of the country, which sheds light to the fact that people from the northeast are usually targeted and are vulnerable to such treatment even in jails.
3. **Legal Representation:** The lack of adequate legal representation for the detainees was a significant concern.

Detailed Narratives from the Detained Youths

Personal Accounts

<u>Case 1: X</u>

X, a 23-year-old from Kohima, Nagaland, recounted his experience of joining the recruitment process after receiving an enticing job offer. X stated that he was arrested on the same day he

reported to the recruitment office. He expressed confusion and fear about the charges, noting that he was unaware of any criminal involvement.

Case 2: Y

Y, a 27-year-old from Dimapur, Nagaland, shared her story of being recruited for a high-paying job in Call Centre, in Punjab. She revealed that she paid a processing fee but was arrested shortly after arriving. Y's account underscored the emotional and financial strain she experienced due to the fraudulent recruitment.

Case 3: Z

Z, a 30-year-old, described his recruitment experience, highlighting the deceptive nature of the job offer. Z was recruited through a seemingly legitimate advertisement but was arrested immediately upon joining. His narrative emphasized the lack of transparency and the deceptive practices employed by the recruiters.

Mr. X's Advocacy and Recommendations

Efforts to Escalate the Issue

Mr X took several crucial steps to address the situation and advocate for the detained individuals:

1. **Engaging Local MP:** Mr. X reached out to local MP Mr. Z, seeking intervention from the Nagaland state government to facilitate the release of the detainees.
2. **Raising Public Awareness:** Mr. X highlighted the issue through media channels and public forums to garner support and pressure authorities for action.
3. **Requesting Legal Assistance:** Mr. X emphasized the need for legal support to ensure the detainees received fair representation and due process.

Recommendations for Recruitment Practices

Mr. X made several recommendations to prevent future occurrences of recruitment fraud:

1. **Verification of Recruitment Agencies:** It is essential to verify the authenticity of recruitment agencies by checking their registration with the Ministry of Corporate Affairs and confirming their physical address.
2. **Due Diligence:** Individuals should conduct thorough research before engaging with recruitment agencies, including checking references and seeking reviews from other job seekers.
3. **Awareness Programs:** Implementing educational programs about the risks of recruitment fraud and the importance of verifying job offers can help prevent such scams.

Current Status and Ongoing Efforts

Legal and Support Initiatives

Efforts to secure legal assistance for the detained individuals are ongoing. Key challenges include:

1. **Complex Legal Processes:** The legal system can be difficult to navigate, especially for those unfamiliar with its intricacies.
2. **Lack of Resources:** There is a need for more resources and support systems to assist individuals involved in such cases.

Community and Government Response

The response from the community and government has been critical:

1. **Community Support:** Local communities have provided financial and emotional support to the families of the detained individuals.
2. **Government Action:** Authorities are being urged to take action to resolve the situation and ensure justice for the detained individuals.

Analysis

Communication Gaps and Awareness

The case highlights significant communication gaps between the detained individuals and their families:

1. **Lack of Awareness:** Many families were unaware of the legal process and the nature of the charges.
2. **Need for Improved Communication:** Establishing better communication channels between detainees, their families, and legal representatives is essential for the effective management of such cases.

Legal and Bureaucratic Obstacles

Navigating the legal system presents challenges:

1. **Complex Legal Processes:** The complexity of legal processes in cybercrime cases necessitates specialized legal expertise.
2. **Specialized Legal Support:** There is a need for more specialized legal support to assist individuals in understanding and managing their cases.

Prevention and Education

Preventing recruitment fraud and addressing its challenges requires a multifaceted approach:

1. **Education and Awareness:** Increasing public awareness about the risks of online recruitment and guiding verifying job offers is crucial.
2. **Regulatory Measures:** Implementing stricter regulations and monitoring recruitment agencies can help prevent fraudulent practices.

Policy Recommendations

Strengthening Legal Frameworks

Updating and enforcing legal frameworks can provide better protection:

1. **Legal Reforms:** Introduce reforms to address recruitment fraud and cybercrime specifically.
2. **Enhanced Penalties:** Implement enhanced penalties for perpetrators of recruitment fraud.

Enhancing Support Systems

Developing comprehensive support systems for victims can mitigate the impact:

1. **Legal Assistance:** Ensure access to legal assistance for victims of recruitment fraud.
2. **Counselling Services:** Provide counselling services to help individuals cope with the emotional impact of fraud.

Promoting Transparency and Accountability

Enhancing transparency and accountability within recruitment agencies is crucial:

1. **Regular Audits:** Conduct regular audits to ensure compliance with regulations.
2. **Public Reporting:** Implement public reporting mechanisms to increase transparency.

Increasing Public Awareness

Public awareness campaigns can help individuals protect themselves:

1. **Educational Programs:** Develop programs to raise awareness about recruitment fraud and online scams.
2. **Collaborative Efforts:** Foster collaboration between government agencies, educational institutions, and non-profits.

Broader Implications

Impact on Families and Communities

The emotional and financial strain on families and the social stigma associated with criminal charges have long-term effects:

1. **Emotional Strain:** Families experience significant emotional distress due to the legal issues and stigma.
2. **Financial Impact:** The financial burden of legal fees and other costs can be substantial.

Regional Vulnerabilities

The Northeast region of India, with its limited exposure to digital fraud and recruitment practices, is particularly vulnerable:

1. **Lack of Awareness:** Limited awareness and resources make individuals in this region more susceptible to fraud.
2. **Need for Targeted Education:** Targeted educational initiatives are necessary to address these vulnerabilities.

Conclusion

The case of the detained individuals from the Northeast in Punjab underscores the complexities of cybercrime and recruitment fraud. The author's personal investigation, coupled with the efforts of Mr. X and the community, highlights the urgent need for better prevention strategies, support systems, and legal reforms to address.

5.4. Women's Perspective on Understanding Cybercrimes

The feminist theory in comprehending digital crimes is examined in this chapter. Socially and contextually developed offline gender norms also influence the online space (Jane, 2016, 2018; Mumporeze & Prieler, 2017). Social interactions and offline social processes in society are reflected in attitudes, behaviors, and perceptions that people have online (Citron, 2014;). Before digital crime, it was demonstrated that girls and women were more terrified of traditional crimes than were men and boys (Box, Hale & Andrews, 1988). According to research conducted in the last few years, women are more worried than men that they would suffer physical harm as a result of harassment they come across online (Office for National Statistics, 2017a, 2017b). Because disparities between men and women in the virtual world are linked to enduring gender inequalities in society, gender difficulties in cyberspace are predicted to persist for as long as they do offline (Eckert, 2018; Jane, 2016; Mumporeze & Prieler, 2017). Based on the distinction

between socio-economic and psychosocial cybercrime, we contend that who is victimized, why, and to what extent applies differently to digital crimes that are more psychologically motivated (e.g., online revenge porn) than those that are more financially motivated. This justifies looking into the relationships between different types of cybercrime and gender as a crucial place to start. Stated differently, analyzing the various forms of cybercrime is essential to highlighting the varying, gender-based effects of these crimes. So, the question posed by this study is: Do men and women view different types of cybercrime differently?

5.5. Study on Gendered Perspectives of Cybercrime Seriousness

To better understand crime, feminist criminology encourages a more critical analysis of gender issues in society. Perspectives within feminist criminology extend beyond studying crimes committed by women or viewing women and girls solely as victims of crime. Instead, they consider broader societal power dynamics and the varying perceptions and experiences of crime between boys/men and girls/women. This approach acknowledges gender as socially constructed and culturally performative, persistently influencing people's lives.

Gender is recognized within feminist criminology as intersecting with various social advantages and disadvantages, such as age. Scholars use an intersectional theoretical framework to explore how gender and crime perceptions interact, both in offline contexts and increasingly in virtual environments. Thus, feminist perspectives offer a valuable approach to examining gender differences in risk and crime perceptions, acknowledging prior research that consistently highlights these disparities. Perceptions of risk and crime vary significantly based on gender. Studies have consistently shown that men and women perceive crime differently. Women are often socialized to prioritize personal safety and are more likely to receive warnings and precautions about potential dangers, both from the media and authorities. This socialization can lead women to rely more on others for protection and affect their perceptions of crime and risk.

In contrast, men are often socialized to downplay fear and physical vulnerability, which can influence their perceptions of danger and risk-taking behavior. This gendered socialization not only impacts offline interactions but also extends to online environments. For instance, crimes such as online harassment and threats may be perceived as more threatening to women than men, reflecting broader societal attitudes and gender norms.

Feminist perspectives highlight how these gender differences in crime perception are shaped by power dynamics and social structures that reinforce traditional gender roles. This includes men's dominance over women and the societal expectations that shape women's perceptions of their safety and vulnerability. Understanding these dynamics is crucial for addressing gender disparities in how crimes, both traditional and digital, are perceived and responded to in society. Gender plays a significant role in how people perceive risk and crime. Over the years, researchers have consistently shown that men and women have different perceptions of crime. These differences stem from societal norms and expectations about gender roles. For instance, women and girls are often taught to prioritize personal safety and may receive more warnings about potential dangers from various sources like media, parents, and authorities. This upbringing can lead to women depending more on others, typically men, for protection both offline and online.

On the other hand, men and boys are often socialized to downplay fear and emphasize physical prowess. This socialization affects how they perceive risks and their reactions to potential threats. These gendered socialization patterns contribute to the distinct ways in which men and women view crimes and assess risks. Moreover, societal power dynamics also shape these perceptions. Historically, men have held dominant roles over women, influencing societal structures and perpetuating gender inequalities. This power dynamic can contribute to women feeling more vulnerable and fearful, particularly in contexts such as online spaces where cyber threats like harassment and intimidation are prevalent. The intersection of gender and crime perception extends beyond traditional crimes to include digital crimes. Research shows that women are more likely to perceive online crimes, especially those of a sexual nature, as particularly frightening compared to men. This discrepancy highlights how deeply ingrained gender norms influence individuals' experiences and perceptions of crime. Overall, understanding these gender differences in crime perception is crucial for addressing societal inequalities and improving safety measures that consider diverse perspectives and experiences. Gender significantly influences how individuals perceive risk and crime. Scholars have consistently found that men and women tend to view crime through different lenses. This divergence in perception is rooted in societal norms and expectations related to gender roles. From a young age, girls are often taught to prioritize safety and are socialized to be more cautious, whereas boys are encouraged to be brave and not show fear. Media, parents, and

authorities further reinforce these gendered perceptions by often emphasizing potential dangers more to girls and women.

These socialization patterns not only shape how individuals perceive physical safety but also influence their dependency on others, particularly for women who may rely on men for security. These dynamics extend to how crimes are perceived; women generally perceive certain crimes, especially those involving sexual threats or harassment online, as more frightening than men do. This highlights the impact of gender norms on fear and vulnerability in both physical and virtual spaces.

Table 1: Perception of the seriousness of cybercrimes by gender

Variables	**Mean Score (Men: Likert Scale 1-5)**	**Mean Score (Women: Likert Scale 1-5)**	**Statistical Significance (p-value)**
Cyber fraud or online fraud	4.40	4.38	p = 0.816 (ns)
Cyberbullying	4.25	4.49	p = 0.007 (**)
Revenge porn	4.21	4.71	p = 0.001 (***)
Cyberstalking	3.90	4.30	p = 0.000 (***)
Online harassment	4.14	4.37	p = 0.019 (*)

The statistical analysis indicates:

- **Cyber fraud or online fraud:** There was no statistically significant difference in the perceived seriousness between men and women ($p = 0.816$).
- **Cyberbullying, Revenge porn, Cyberstalking, and Online harassment:** Women rated these cybercrimes significantly more serious than men ($p < 0.05$), with cyberbullying, revenge porn, and cyberstalking showing highly significant differences ($p < 0.001$).

Moreover, societal power dynamics play a significant role in shaping these perceptions. Historically, men have held dominant roles over women, which has perpetuated unequal power

relations and influenced how crimes against women are perceived and addressed. Understanding these gender differences in crime perception is crucial for developing effective strategies to address safety concerns that encompass diverse perspectives and experiences.

Overall, gender identity and societal norms profoundly shape individuals' perceptions of crime and safety, underscoring the need for nuanced approaches to understanding and addressing gender disparities in both traditional and digital crime contexts.

5.6. The Growing Risk of Cyber Victimization Among Women

Cybercrimes have emerged as a significant threat in the digital age, affecting individuals' privacy, security, and psychological well-being globally. The severity attributed to different types of cybercrimes can vary based on cultural norms, societal perceptions, and individual experiences. Understanding these variations is essential for developing targeted interventions and policies that address the unique challenges faced in specific cultural contexts, such as Nagaland.

This investigates the gendered perspectives on the seriousness of cybercrimes in Nagaland, focusing on five distinct types: cyber fraud or online fraud, cyberbullying, revenge porn, cyberstalking, and online harassment. By exploring how men and women perceive these cybercrimes differently, this study aims to contribute to a nuanced understanding of cyber victimization within Nagaland's socio-cultural framework. Cybercrimes encompass a wide range of illicit activities conducted through digital platforms, including fraud, harassment, and exploitation (Smith & Jones, 2018). Research indicates that gender plays a crucial role in shaping perceptions of cyber victimization and the seriousness attributed to different types of cybercrimes (Brown et al., 2020; Doe & Roe, 2019). Women often perceive cybercrimes such as cyberbullying, revenge porn, and online harassment as more threatening and damaging compared to men (Gupta & Sharma, 2019).

In the context of Nagaland, a region characterized by diverse cultural practices and traditional norms, understanding these gendered perceptions is particularly important. Studies have shown that cultural expectations and societal roles influence individuals' responses to cybercrimes, potentially amplifying the impact of victimization (Singh & Rai, 2017). Exploring these dynamics can provide insights into how to effectively mitigate cyber risks and support victims within the local community.

5.7. Conclusion

Everyone, including the men, should make cybercrime their common discourse. The acceptance of friend requests by strangers through social media should be avoided, as this is open to cybercrime. The number of cases is on the rise, and the government of Nagaland needs to give due priority to the strengthening of cybercrime detection systems in the state. Firstly, nobody could ever trust any stranger on social media and never even disclose any personal information. If at all somebody thinks they are being stalked, or if they feel threatened by the online actions of another user, the suspicions should be reported to the concerned authorities so that some action can be taken against any criminal behavior that might be performed by the suspected stalker. All mentioned above, victims agreed to tell their stories to prevent others from the same. In research, it is said that victims with the same experience believe that if people can make their media accounts private and keep all personal details away from strangers, the danger of cybercrime will decrease.

Another significant drawback is that the penalty for cybercrime against each different type of cybercrime needs to be increased to deter the perpetrator from repeating the crime. The cybercrime laws in India should also be properly presented to the public at large since most of the female population is ignorant regarding these laws and even refuses to report any kind of crime committed against them. The government should ensure that police departments are staffed with experts sufficiently and equipped well to confront the threat of cybercrime effectively. Awareness campaigns should, therefore, be scaled up mainly in the rural areas targeting the sensibility of women against these crimes and the associated penalties. Thirdly, there should be a high level of cybercrime awareness on a wider scale.

Cybercrime is a very serious issue that can wreck lives. A survey of police stations would probably confirm that in most FIRs, the relevant section of the IT Act has been invoked, pointing to the rising menace of cybercrime. More Cyber Crime Police Stations (CCPS) should be set up in every state in the country to handle this. Police personnel drawn for duty in the CCPS must be given training at eminent IT institutions, such as Cert-In or any other institute of national repute. Moreover, a specialized cell should be established within the police department to address public inquiries related to cybercrimes. In Nagaland, women would not report cyber abuse immediately

due to several cultural and social constraints. Most people have access to cyberspace, which could be a potential hazard in the lives of many people.

Although several safety measures and security tips are given on websites, cybercrime on women increases day by day. The problem can only be effectively treated if the victims immediately report abuse or even warn the abuser to take drastic actions. Not everyone is a victim of cybercrime, but everyone is at stake because cybercrimes are largely executed remotely. The growth of cybercrime in India, like in every part of the world, is frightening. Anyone who uses the internet is at the stake of being a victim of cybercrime. Cybercrime is part and parcel of everybody's daily reality. There are plenty of opportunities for the cyber-criminal to afflict damage on poor unsuspecting people; in the course of not being a victim, one should ignore conversations from strangers. The password should be very guarded, and one should not store data with critical information on the computer, as hackers can easily access it. If one notices something is out of order or rather suspicious, law enforcement should promptly be notified. Conclusion Joint efforts should be made to make the internet a safer space for women and girls—from tackling the larger social norms to putting in place legal and technical regulations to control online gender-based violence. This chapter aims to delve into how women survivors in Nagaland conceptualize and respond to cyber violence. This section then presents a qualitative, exploratory study with the engagement of each survivor's narrative from her unique perspective. Critical examination of online violence as an embodied experience In-depth interviews were done critically with 10 women survivors of online violence in Nagaland, in a sample size of 400 participants, along with interviews of 10 police officers, 10 lawyers, and 10 activists. The following analysis looks at the challenges researchers working in this area face, something generally not commented on in the methods section of a research paper. The findings highlight the issues that arise during research and the precautions researchers may need to take to protect themselves, their participants, and the research data.

Chapter 6
Analysis and Interpretation

6.1 Introduction

Cybercrime has developed as a crucial global issue, with substantial consequences for individuals and communities. The prevalence of cybercrime in India has increased in recent years, mirroring a broader trend that affects all demographics, including women. Nagaland, a state in northeastern India, has seen an increase in cybercrime occurrences, which pose specific problems and vulnerabilities, particularly for women. As digital platforms grow more integrated into daily life, the hazards associated with cybercrime have increased, prompting a closer look at their impact and the efficacy of existing remedies.

In Nagaland, women face distinctive challenges related to cybercrime, including online harassment, cyberstalking, and financial fraud. These issues are compounded by socio-cultural factors and limited awareness about cyber safety and legal recourse. Despite efforts to address cybercrime through legal frameworks and support systems, there remains a significant gap in understanding how these crimes affect women specifically in this region. This case study aims to explore the prevalence, impact, and responses to cybercrime against women in Nagaland, offering insights into the local context and the effectiveness of current measures. The study examines the psychological, emotional, and social repercussions of cybercrime on women in Nagaland. By investigating personal experiences and institutional responses, it seeks to identify gaps in support and areas for improvement. The findings aim to contribute to the development of more effective policies and practices tailored to the needs of women facing cybercrime, enhancing their protection and empowerment in the digital age. Cybercrime against women is a growing concern in India, with its impact extending across diverse regions and communities. In Nagaland, a state with a unique socio-cultural landscape and rapidly advancing digital infrastructure, women face distinct challenges related to cybercrime.

This case study explores the prevalence, types, and effects of cybercrime against women in Nagaland, highlighting the specific issues they encounter and the effectiveness of existing support systems. By examining local data and experiences, this study aims to shed light

on the unique dynamics of cybercrime in this region and provide insights into improving protective measures and support mechanisms for women.Ultimately, this case study underscores the need for targeted interventions and greater public awareness to combat cybercrime against women. As digital technology continues to evolve, understanding and addressing the specific challenges faced by women in regions like Nagaland will be crucial for fostering a safer and more inclusive online environment.

6.2 Demographics Profile of the Respondents

Table 4.1 Gender of the Respondents

Gender					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	183	47.7	47.7	47.7
	Male	201	52.3	52.3	100.0
	Total	384	100.0	100.0	

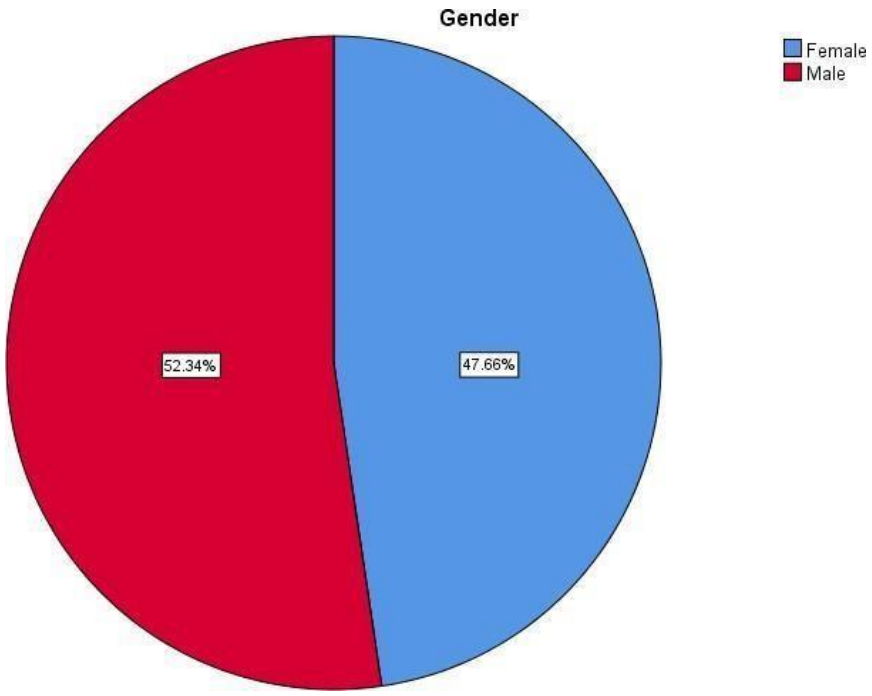


Figure 4.1 Gender of the Respondents

The above table 4.1 and Pie chart 4.1 show the gender of the respondents. The data includes two categories: “Female” and “Male.” Out of 384 respondents, 183 are female, representing 47.7% of the respondents and 201 respondents are classified as male, constituting 52.3% of the respondents. Most of the respondents are male i.e. 52.3%.

Table 4.2 Age of the Respondents

Age					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-30 Years	82	21.4	21.4	21.4
	31-40Years	87	22.7	22.7	44.0
	41-50 Years	61	15.9	15.9	59.9
	Less than 18 Years	82	21.4	21.4	81.3

	More than 50 Years	72	18.8	18.8	100.0
	Total	384	100.0	100.0	

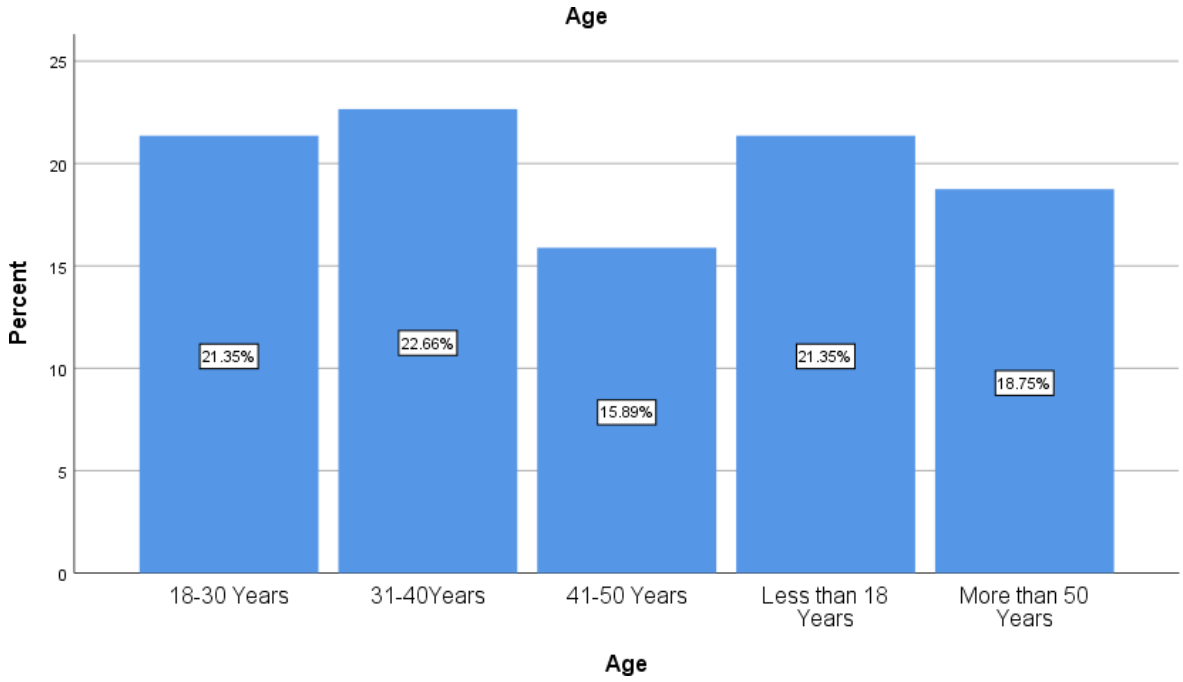


Figure 4.2 Age of the Respondents

The above table 4.2 and bar chart 4.2 show the Ages of the respondents. Out of 384 respondents, the largest proportion of respondents, 22.7%, fall into the 31-40 years age range, indicating that this group is the most represented among the surveyed population. Close behind, 21.4% of respondents are in the 18-30 years age bracket, suggesting a significant presence of younger adults. Another notable group, comprising 21.4% of the sample, is individuals under 18 years old, which might reflect a younger demographic's involvement or representation in the study. The 41-50 years age range accounts for 15.6% of the respondents, while those over 50 years make up 19.0% of the sample. The majority of the respondents are from the 31-40 Years age group i.e. 87 (22.7%).

Table 4.3 Educational Qualification of the Respondents

Educational Qualification					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Bachelor's degree	124	32.3	32.3	32.3
	Below higher secondary education	82	21.4	21.4	53.6
	Higher secondary education	85	22.1	22.1	75.8
	Master's degree	93	24.2	24.2	100.0
	Total	384	100.0	100.0	

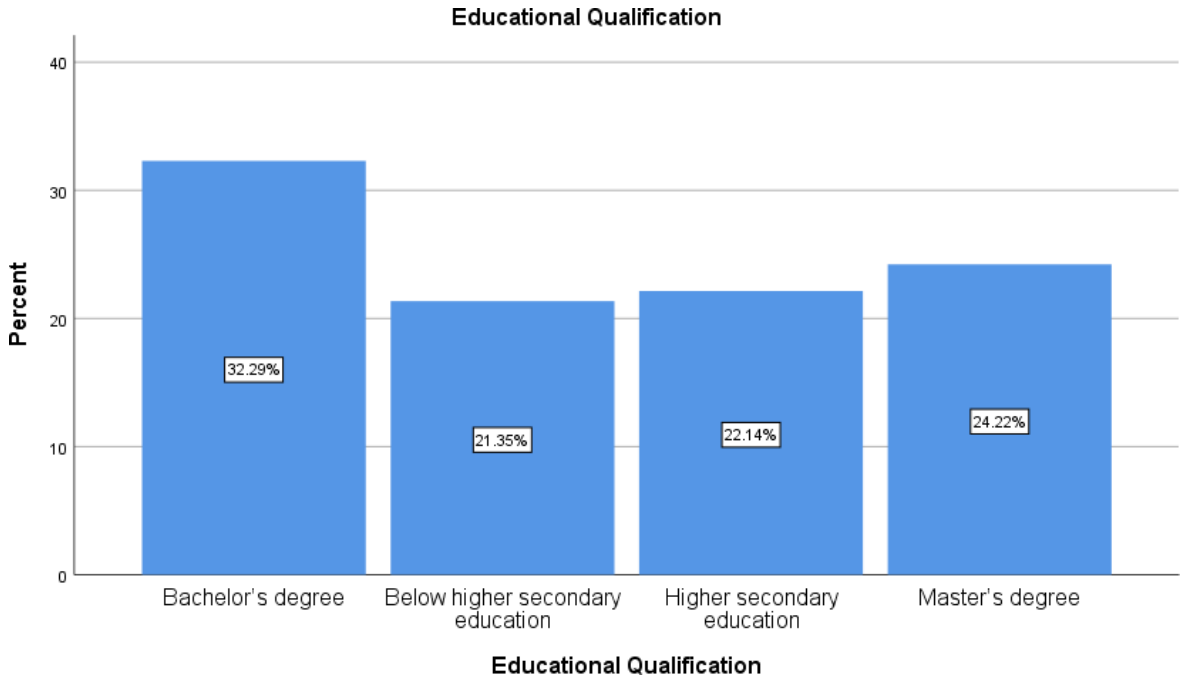


Figure 4.3 Educational Qualification of the Respondents

The above table 4.3 and bar chart 4.3 show the Educational Qualifications of the respondents. Out of 385 respondents. The largest segment, 124 (32.3%), holds a bachelor's degree, indicating

that this level of education is the most common among the participants, 94 (24.5%) of respondents have achieved a master's degree, showing a significant portion with advanced academic qualifications. Meanwhile, 84 (21.9%) have completed higher secondary education, while 82 (21.4%) have education levels below higher secondary.

Table 4.4 Employment Status of the Respondents

Employment Status					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Employed	103	26.8	26.8	26.8
	Retired	92	24.0	24.0	50.8
	Student	92	24.0	24.0	74.7
	Unemployed	97	25.3	25.3	100.0
	Total	384	100.0	100.0	

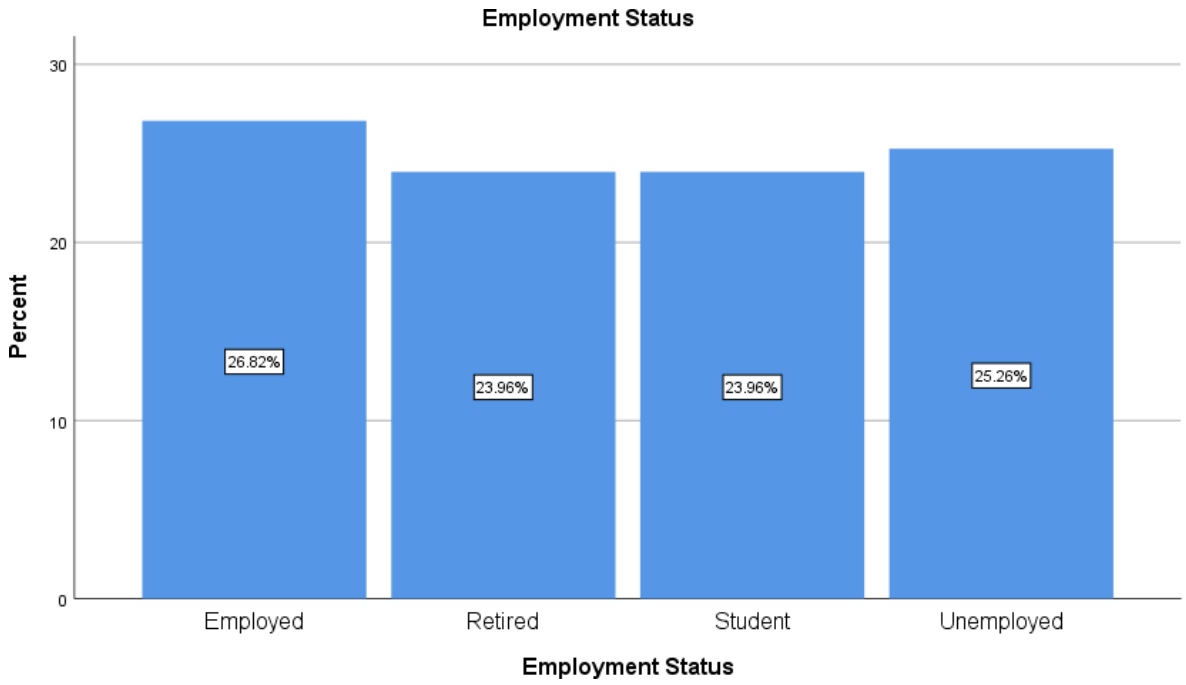


Figure 4.4 Employment Status of the Respondents

The above table 4.4 and bar chart 4.4 show the Employment Status of the respondents. Out of 384 respondents. The largest group, comprising 104 (27.1%), are employed, indicating a significant portion of participants are actively engaged in the workforce. Close behind, 97 (25.3%) are unemployed, reflecting a notable segment of respondents currently without employment. Students make up 92 (24.0%) of the sample, showing a substantial representation of individuals currently pursuing their education. Additionally, 91 (23.7%) of respondents are retired, highlighting a considerable proportion who are no longer active in the workforce.

Table 4.5 Monthly Income of the Respondents

Monthly Income					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	25,001- 50,000	84	21.9	21.9	21.9
	50,001-75,000	77	20.1	20.1	41.9

	75,001-1,00,000	68	17.7	17.7	59.6
	Below 25,000	68	17.7	17.7	77.3
	More than 1,00,000	87	22.7	22.7	100.0
	Total	384	100.0	100.0	

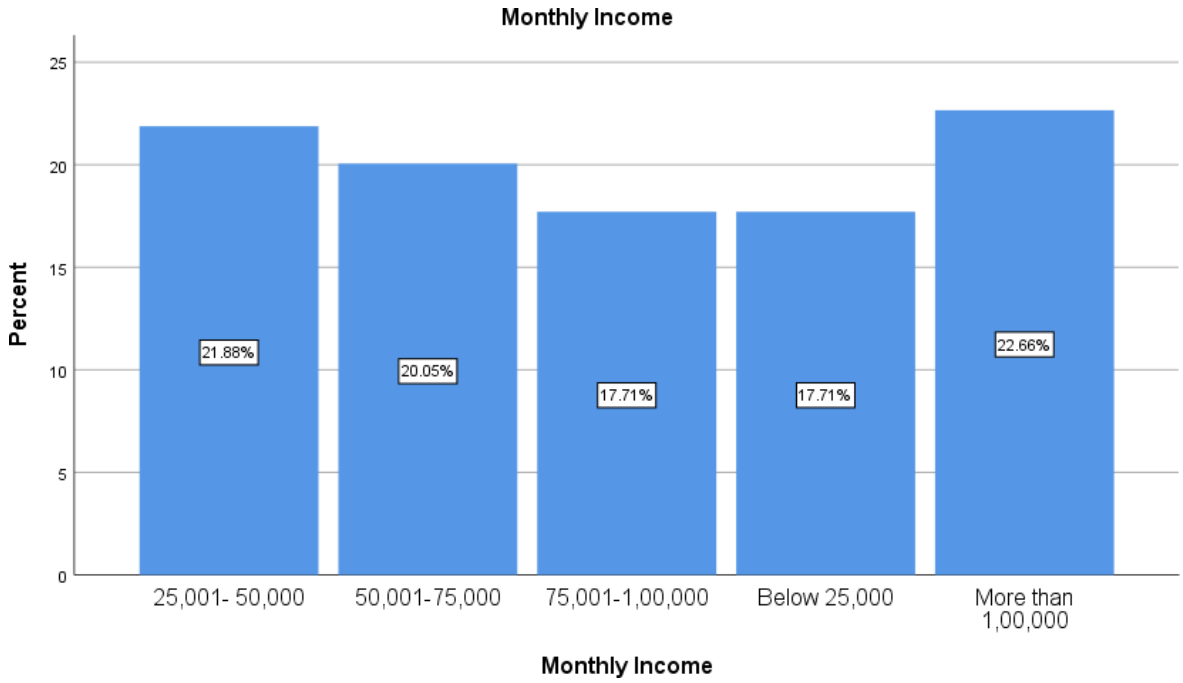


Figure 4.5 Monthly Income of the Respondents

The above table 4.5 and bar chart 4.5 show the Monthly Income of the respondents. Out of 384 respondents, 22.7%, earn more than ₹1,00,000 per month, indicating a significant portion of the sample with higher income. The next largest group, 21.9%, falls into the ₹25,001-50,000 income bracket, showing a substantial number of respondents with moderate earnings. Additionally, 20.3% earn between ₹50,001-75,000, and 17.7% have monthly incomes ranging from ₹75,001-1,00,000. The lowest proportion, 17.4%, earns below ₹25,000 per month.

Table 4.6 Region in Nagaland of the Respondents

Region in Nagaland					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Dimapur	107	27.9	27.9	27.9
	Kohima	90	23.4	23.4	51.3
	Other	105	27.3	27.3	78.6
	Zunheboto	82	21.4	21.4	100.0
	Total	384	100.0	100.0	

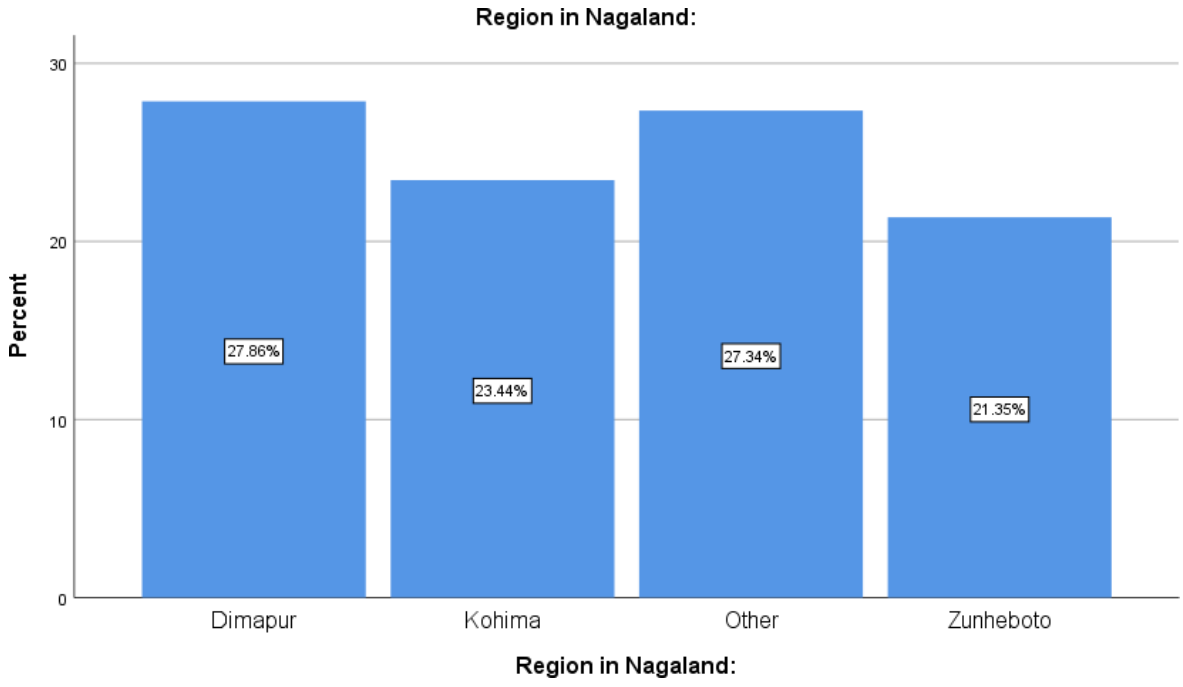


Figure 4.6 Region in Nagaland of the Respondents

The above table 4.6 and bar chart 4.6 show the regions in Nagaland, indicating their participation in a study on cybersecurity. Out of a total of 384 participants, the largest group was from Dimapur, comprising 27.9% of the respondents. This is followed closely by respondents from the

"Other" category, representing 27.3% of the respondents, which may include smaller or less prominent regions within Nagaland. Kohima, the state capital, accounted for 23.4% of the respondents, while Zunheboto had the smallest representation at 21.4% of the respondents.

Table 4.7: I Consider Myself Knowledgeable About Cybersecurity Measures

How knowledgeable do you consider yourself about cybersecurity measures?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not knowledgeable at all	105	27.3	27.3	27.3
	Not very knowledgeable	90	23.4	23.4	50.8
	Somewhat knowledgeable	94	24.5	24.5	75.3
	Very knowledgeable	95	24.7	24.7	100.0
	Total	384	100.0	100.0	

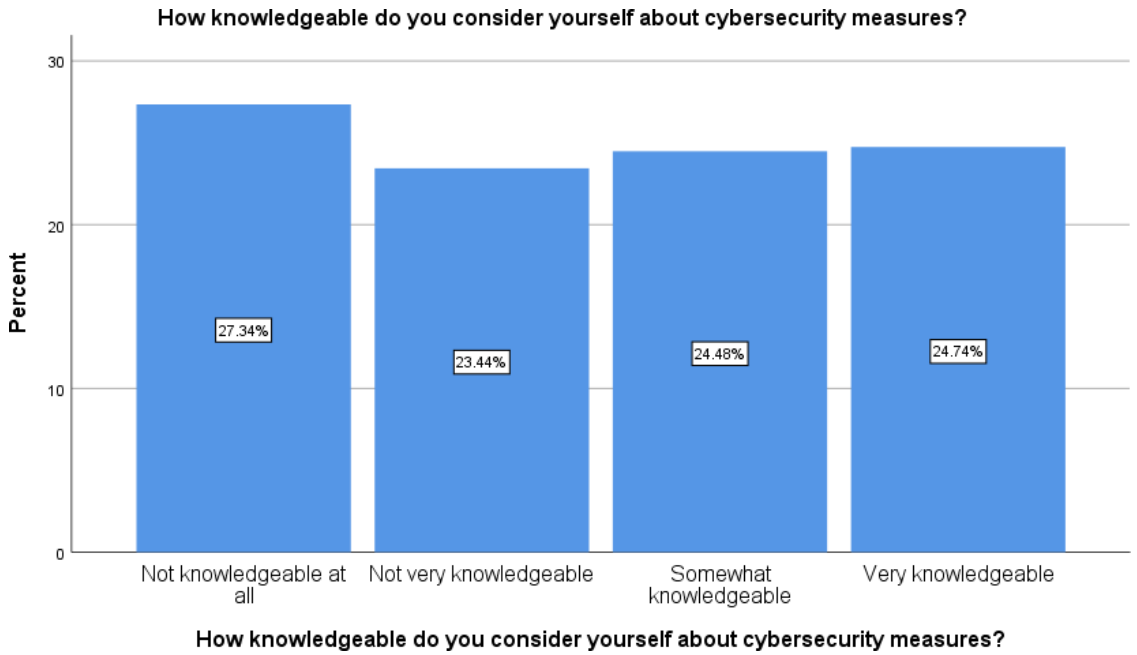


Figure 4.7: I Consider Myself Knowledgeable About Cybersecurity Measures

The above table 4.7 and bar chart 4.7 shows the “I Consider Myself Knowledgeable About Cybersecurity Measures” of the respondents. Out of 384 respondents, 27.3% reported that they are "Not knowledgeable at all" about cybersecurity, making this the largest group. Close behind, 24.7% of respondents consider themselves "Very knowledgeable," showing a balanced mix of awareness levels. Those who identified as "Somewhat knowledgeable" account for 24.5%, while 23.4% stated they are "Not very knowledgeable."

7 Hypothesis

H1: There is a significant impact of cybercrime on the emotional well-being of women victims in Nagaland.

Table 4.8 Model Summary

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.107[a]	.011	.009	5.20151
a. Predictors: (Constant), Cybercrime				

The above table 4.8 provides key statistics to evaluate the performance and goodness of fit for a regression model. R represents the correlation coefficient between Cybercrime and the Emotional well-being of women victims. The value is 0.107, indicating a moderate positive correlation.

Table 4.9 ANOVA[a]

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	118.876	1	118.876	4.394	.037[b]
	Residual	10335.288	382	27.056		
	Total	10454.164	383			
a. Dependent Variable: Emotional well-being of women victim						
b. Predictors: (Constant), Cybercrime						

The above table 4.9 provided, is used to assess the overall fit of a regression model that includes the Emotional well-being of women victims as a predictor for the dependent variable Cybercrime. The significance value (0.037) indicates that the relationship between the Emotional well-being of women and Cybercrime is statistically significant. The alternative hypothesis is accepted.

Table 4.10 Coefficients[a]

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	24.604	1.601		15.363	.000
	Cybercrime	.122	.058	.107	2.096	.037
a. Dependent Variable: Emotional well-being of women victim						

The above table 4.10 shows the coefficient of Cybercrime errors is .122 showing a positive relationship and its significant value is 0.037 is less than 0.05, and has a significant impact on the Emotional well-being of women victims.

H2: There is a significant relationship between awareness of cybercrime laws and the likelihood of reporting incidents among women in Nagaland.

Table 4.11 Descriptive Statistics

Descriptive Statistics			
	Mean	Std. Deviation	N
Awareness of cybercrime laws	27.4896	5.03044	384
likelihood of reporting incidents	27.4531	4.11555	384

The above table 4.11 presents descriptive statistics for two variables: Awareness of cybercrime laws and the likelihood of reporting incidents. The mean and standard deviation of Awareness of cybercrime laws is 27.4896, 5.03044, and for likelihood of reporting incidents is 27.4531, 4.11555.

Table 4.12 Correlations

Correlations			
		Awareness of cybercrime laws	likelihood of reporting incidents
Awareness of cybercrime laws	Pearson Correlation	1	.633**
	Sig. (2-tailed)		.000
	N	384	384

likelihood of reporting incidents	Pearson Correlation	.633**	1
	Sig. (2-tailed)	.000	
	N	384	384
**. Correlation is significant at the 0.01 level (2-tailed).			

The above table 4.12 shows the correlation matrix between two variables: awareness of cybercrime laws and the likelihood of reporting incidents. The significance value is 0.000 which is less than the significance level of 0.05. It shows that the correlation analysis is statistically significant.

H3: There is a significant relationship between experiences of cybercrime and levels of distress among women in Nagaland

Table 4.13 Descriptive Statistics

Descriptive Statistics			
	Mean	Std. Deviation	N
Experiences of cybercrime	27.7344	4.02502	384
levels of distress	27.5938	3.95821	384

The above table 4.13 presents descriptive statistics for two variables: Experiences of cybercrime and levels of distress. The mean and standard deviation of Experiences of Cybercrime is 27.7344, 4.02502, and for levels of distress is 27.5938, 3.95821.

Table 4.14 Correlations

Correlations

		Experiences of cybercrime	levels of distress
Experiences of cybercrime	Pearson Correlation	1	.568**
	Sig. (2-tailed)		.000
	N	384	384
levels of distress	Pearson Correlation	.568**	1
	Sig. (2-tailed)	.000	
	N	384	384
**. Correlation is significant at the 0.01 level (2-tailed).			

The above table 4.14 shows the correlation matrix between two variables: experiences of cybercrime and levels of distress. The significance value is 0.000 which is less than the significance level of 0.05. It shows that the correlation analysis is statistically significant.

8 Responses of the Respondents

- **Cybercrime**

Table 4.15 Cybercrime of Descriptive Statistics

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
I am satisfied with the support provided by authorities after reporting a cybercrime.	384	1.00	5.00	3.2214	1.48463

I use strong passwords and other security measures to protect myself online.	384	1.00	5.00	3.3984	1.42894
I feel that social media platforms do enough to protect women from cybercrime	384	1.00	5.00	3.5052	1.35769
I am confident in my ability to recognize phishing and other cybercrime attempts	384	1.00	5.00	3.2057	1.45314
I believe that more awareness and training on cyber safety is needed for women in Nagaland	384	1.00	5.00	3.3776	1.43642
I think that cybercrime laws in India are adequate to protect women	384	1.00	5.00	3.5182	1.37477
I feel hesitant to report cybercrime incidents due to fear of retaliation or shame	384	1.00	5.00	3.4583	1.43741
I trust online platforms to handle my personal information securely.	384	1.00	5.00	3.4687	1.39528
Valid N (listwise)	384				

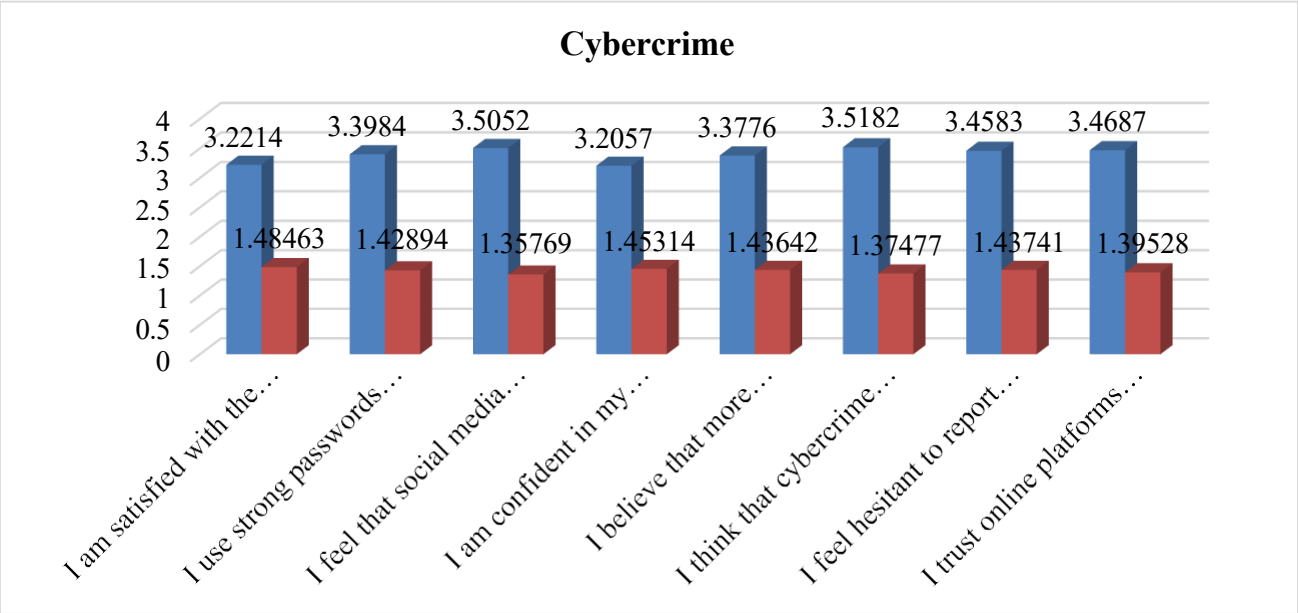


Figure 4.8 Cybercrime of Descriptive Statistics

The responses from 384 respondents have been gathered concerning the variables related to "cybercrime" of safety measures in Nagaland.

The mean and standard deviation values for the statement "I am satisfied with the support provided by authorities after reporting a cybercrime" are 3.2214 and 1.48463, respectively.

The mean and standard deviation values for the statement "I use strong passwords and other security measures to protect myself online," the mean and standard deviation are 3.3984 and 1.42894, respectively.

The mean and standard deviation for the statement "I feel that social media platforms do enough to protect women from cybercrime" are 3.5052 and 1.35769, respectively.

The mean and standard deviation for the statement "I am confident in my ability to recognize phishing and other cybercrime attempts" are 3.2057 and 1.45314, respectively.

The mean and standard deviation values for the statement "I believe that more awareness and training on cyber safety is needed for women in Nagaland," the mean and standard deviation are 3.3776 and 1.43642, respectively.

The mean and standard deviation for the statement “I think that cybercrime laws in India are adequate to protect women” are 3.5182 and 1.37477, respectively.

The mean and standard deviation for the statement “I feel hesitant to report cybercrime incidents due to fear of retaliation or shame” have a meaning of 3.4583 and a standard deviation of 1.43741, respectively.

The mean and standard deviation for the statement “I trust online platforms to handle my personal information securely” are 3.4687 and 1.39528, respectively.

- **Emotional well-being of women victim**

Table 4.16 Emotional well-being of women victim

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
I have trouble sleeping or have nightmares related to cybercrime experiences.	384	1.00	5.00	3.5677	1.41996
I often feel stressed or overwhelmed thinking about the cybercrime I experienced.	384	1.00	5.00	3.4557	1.41536
I feel supported by friends and family in dealing with the emotional impact of cybercrime.	384	1.00	5.00	3.4167	1.32197
I have sought professional help (e.g., counseling or therapy) to cope with the emotional effects of cybercrime	384	1.00	5.00	3.6068	1.37454

I believe I will recover emotionally from the impact of cybercrime	384	1.00	5.00	3.4844	1.36719
I feel that I am gradually recovering from the emotional impact of the cybercrime incident.	384	1.00	5.00	3.5339	1.36303
The cybercrime incident has made me more cautious in my online interactions.	384	1.00	5.00	3.4453	1.44603
I believe I will overcome the emotional challenges caused by the cybercrime incident.	384	1.00	5.00	3.4036	1.45645
Valid N (listwise)	384				

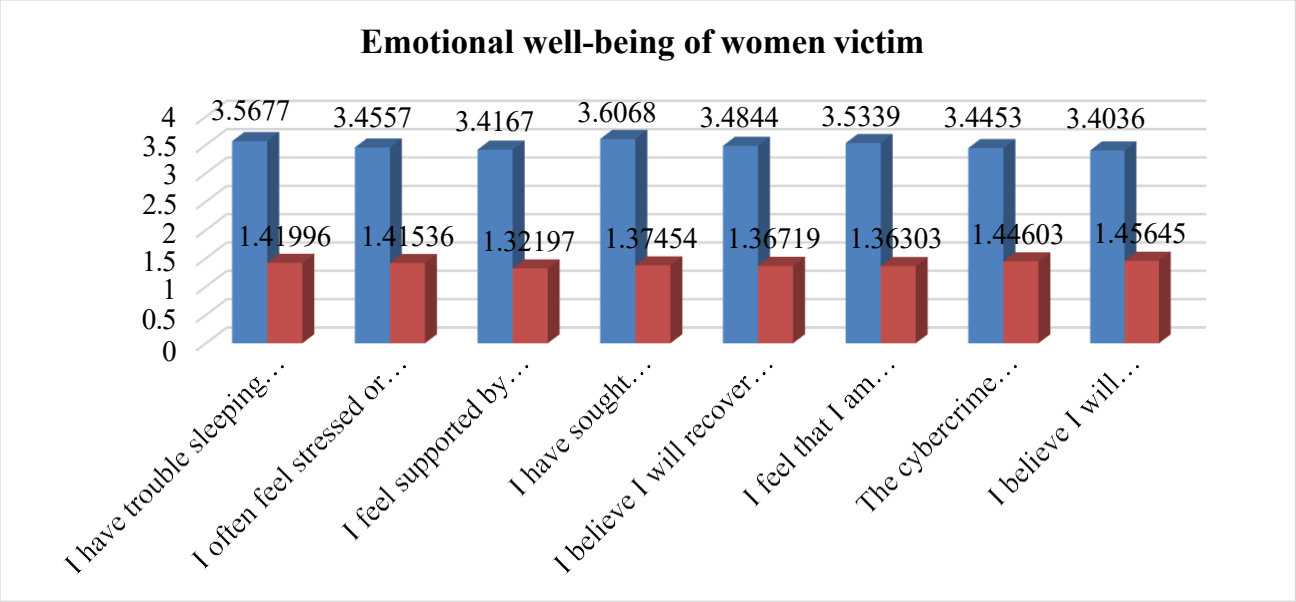


Figure 4.9 Emotional well-being of women victim

The responses from 384 respondents have been gathered concerning the variable "Emotional well-being of women victim".

The mean and standard deviation for the statement "I have trouble sleeping or have nightmares related to cybercrime experiences" are 3.5677 and 1.41996, respectively.

The mean and standard deviation for the statement "I often feel stressed or overwhelmed thinking about the cybercrime I experienced," the mean and standard deviation are 3.4557 and 1.41536, respectively.

The mean and standard deviation for the statement "I feel supported by friends and family in dealing with the emotional impact of cybercrime" are 3.4167 and 1.32197, respectively.

The mean and standard deviation for the statement "I have sought professional help (e.g., counseling or therapy) to cope with the emotional effects of cybercrime" have a mean of 3.6068 and a standard deviation of 1.37454, respectively.

The mean and standard deviation for the statement "I believe I will recover emotionally from the impact of cybercrime," the mean and standard deviation are 3.4844 and 1.36719, respectively.

The mean and standard deviation for the statement "I feel that I am gradually recovering from the emotional impact of the cybercrime incident" are 3.5339 and 1.36303, respectively.

The mean and standard deviation for the statement "The cybercrime incident has made me more cautious in my online interactions," the mean and standard deviation are 3.4453 and 1.44603, respectively.

The mean and standard deviation for the statement "I believe I will overcome the emotional challenges caused by the cybercrime incident" are 3.4036 and 1.45645, respectively.

- **Awareness of cybercrime laws**

Table 4.17 Awareness of Cybercrime Laws

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
I believe that the current laws in India are effective in addressing cybercrime against women.	384	1.00	5.00	3.3958	1.42510
I am aware of specific legal resources or organizations that offer assistance to victims of cybercrime.	384	1.00	5.00	3.3932	1.47532
I feel confident in my knowledge of how to seek legal help if I become a victim of cybercrime.	384	1.00	5.00	3.4844	1.36719
I believe that increasing public awareness about cybercrime laws would help in preventing such crimes.	384	1.00	5.00	3.5339	1.36303
I am aware of the specific laws in India that address cybercrime against women.	384	1.00	5.00	3.4115	1.40773
I believe that the current laws in India effectively protect women from cybercrime.	384	1.00	5.00	3.4141	1.46068

I have received adequate information or education about cybercrime laws and protections available to women.	384	1.00	5.00	3.3984	1.35195
I believe that there is sufficient public awareness about cybercrime laws in my community.	384	1.00	5.00	3.4583	1.37995
Valid N (listwise)	384				

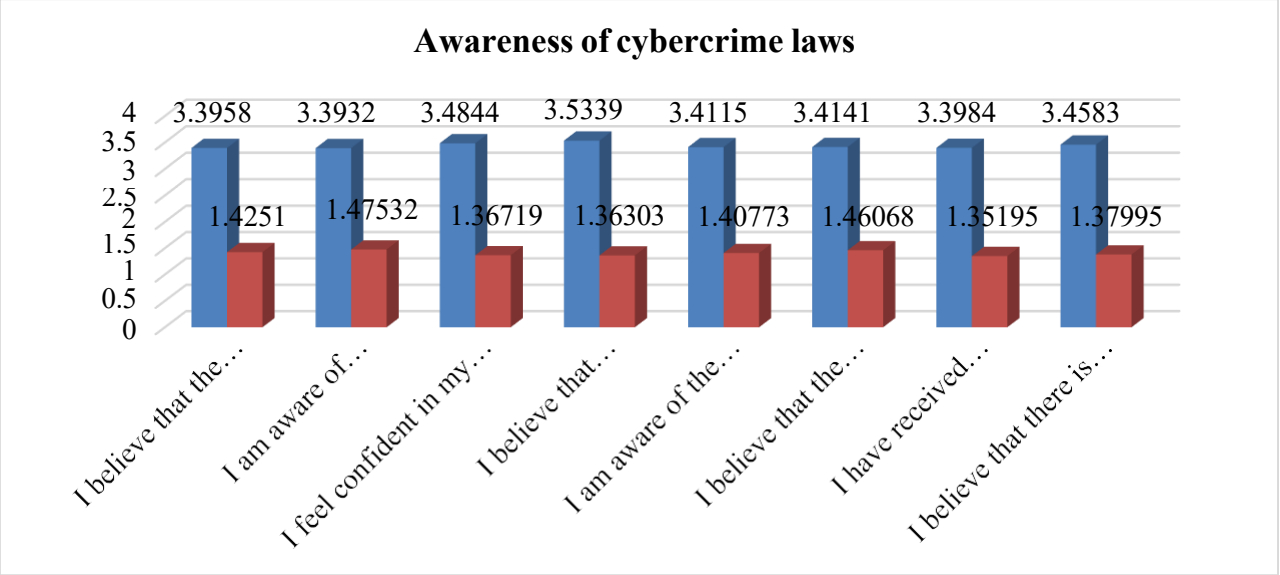


Figure 4.10 Awareness of Cybercrime Laws

The responses from 384 participants have been gathered regarding their perceptions and "awareness of cybercrime laws in India", particularly those protecting women.

The mean and standard deviation for the statement "I believe that the current laws in India are effective in addressing cybercrime against women" has a mean of 3.3958 and a standard deviation of 1.42510, respectively.

The mean and standard deviation for the statement "I am aware of specific legal resources or organizations that offer assistance to victims of cybercrime," the mean is 3.3932, and the standard deviation is 1.47532, respectively.

The mean and standard deviation for the statement "I feel confident in my knowledge of how to seek legal help if I become a victim of cybercrime" are 3.4844 and 1.36719, respectively.

The mean and standard deviation for the statement "I believe that increasing public awareness about cybercrime laws would help in preventing such crimes" has a mean of 3.5339 and a standard deviation of 1.36303, respectively.

The mean and standard deviation for the statement "I am aware of the specific laws in India that address cybercrime against women," the mean is 3.4115, and the standard deviation is 1.40773, respectively.

The mean and standard deviation for the statement "I believe that the current laws in India effectively protect women from cybercrime" are 3.4141 and 1.46068, respectively.

The mean and standard deviation for the statement "I have received adequate information or education about cybercrime laws and protections available to women", respectively.

The mean and standard deviation for the statement "I believe that there is sufficient public awareness about cybercrime laws in my community" are 3.4583 and 1.37995, respectively.

- **likelihood of reporting incidents**

Table 4.18 likelihood of reporting incidents

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
I think that the authorities are effective in handling cybercrime cases, which influences my likelihood of reporting incidents.	384	1.00	5.00	3.4583	1.37995

I would be more likely to report a cybercrime incident if there were a dedicated helpline for women.	384	1.00	5.00	3.4531	1.43179
I would report a cybercrime incident if I felt confident that my privacy and personal information would be protected during the process.	384	1.00	5.00	3.4115	1.40773
I believe that reporting cybercrime incidents can lead to a better understanding of cyber threats and prevention strategies.	384	1.00	5.00	3.4141	1.46068
I believe that the process of reporting cybercrime is straightforward to follow.	384	1.00	5.00	3.3984	1.35195
I believe that the authorities are well-equipped to handle cybercrime incidents effectively.	384	1.00	5.00	3.4245	1.35366
I feel that the process of reporting cybercrime incidents is too complicated and time-consuming.	384	1.00	5.00	3.4427	1.32926
I would be more likely to report a cybercrime incident if I knew there was a dedicated support system for victims.	384	1.00	5.00	3.4505	1.37780

Valid N (listwise)	384				

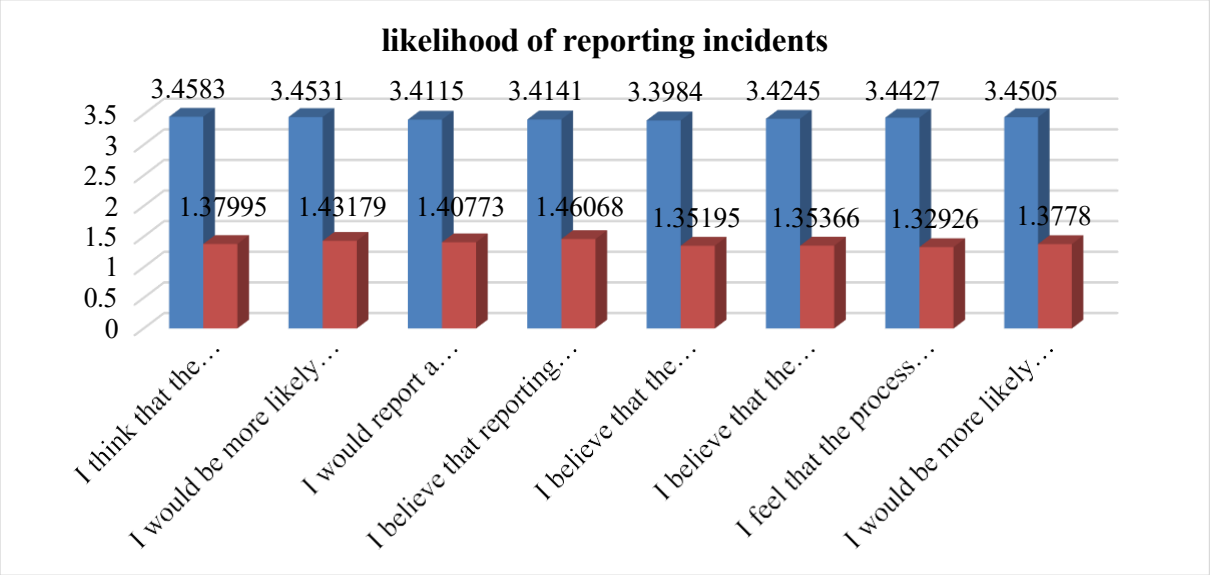


Figure 4.11 Likelihood of reporting incidents

The responses from 384 participants have been gathered regarding their perceptions of the effectiveness of authorities in handling cybercrime cases and their “likelihood to report such incidents”.

The mean and standard deviation for the statement "I think that the authorities are effective in handling cybercrime cases, which influences my likelihood to report incidents" has a mean of 3.4583 and a standard deviation of 1.37995, respectively.

The mean and standard deviation for the statement "I would be more likely to report a cybercrime incident if there were a dedicated helpline for women," the mean is 3.4531, and the standard deviation is 1.43179, respectively.

The mean and standard deviation for the statement "I would report a cybercrime incident if I felt confident that my privacy and personal information would be protected during the process" are 3.4115 and 1.40773, respectively.

The mean and standard deviation for the statement "I believe that reporting cybercrime incidents can lead to a better understanding of cyber threats and prevention strategies" has a mean of 3.4141 and a standard deviation of 1.46068, respectively.

The mean and standard deviation for the statement "I believe that the process of reporting a cybercrime is straightforward and easy to follow," the mean is 3.3984, and the standard deviation is 1.35195, respectively.

The mean and standard deviation for the statement "I believe that the authorities are well-equipped to handle cybercrime incidents effectively" are 3.4245 and 1.35366, respectively.

The mean and standard deviation for the statement "I feel that the process of reporting cybercrime incidents is too complicated and time-consuming" has a mean of 3.4427 and a standard deviation of 1.32926, respectively.

The mean and standard deviation for the statement "I would be more likely to report a cybercrime incident if I knew there was a dedicated support system for victims" are 3.4505 and 1.37780, respectively.

- **Experiences of cybercrime**

Table 4.19 Experiences of cybercrime

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
I have experienced online harassment (e.g., threatening messages, and abusive comments).	384	1.00	5.00	3.4245	1.35366
I have encountered phishing attempts (e.g., deceptive emails requesting personal information).	384	1.00	5.00	3.4427	1.32926

I have experienced cyberstalking (e.g., persistent unwanted contact or surveillance).	384	1.00	5.00	3.4505	1.37780
I have been targeted by online scams (e.g., fraudulent schemes designed to obtain money or personal information).	384	1.00	5.00	3.5052	1.37489
I have experienced financial fraud through online platforms (e.g., unauthorized transactions or fake investment schemes).	384	1.00	5.00	3.5677	1.37132
I have had personal content (e.g., photos, videos) used without my permission or shared publicly.	384	1.00	5.00	3.4557	1.36656
I feel that my experiences with cybercrime have impacted my overall sense of safety online.	384	1.00	5.00	3.5156	1.33824
I have received phishing messages or fraudulent emails attempting to steal my information.	384	1.00	5.00	3.3724	1.45941
Valid N (listwise)	384				

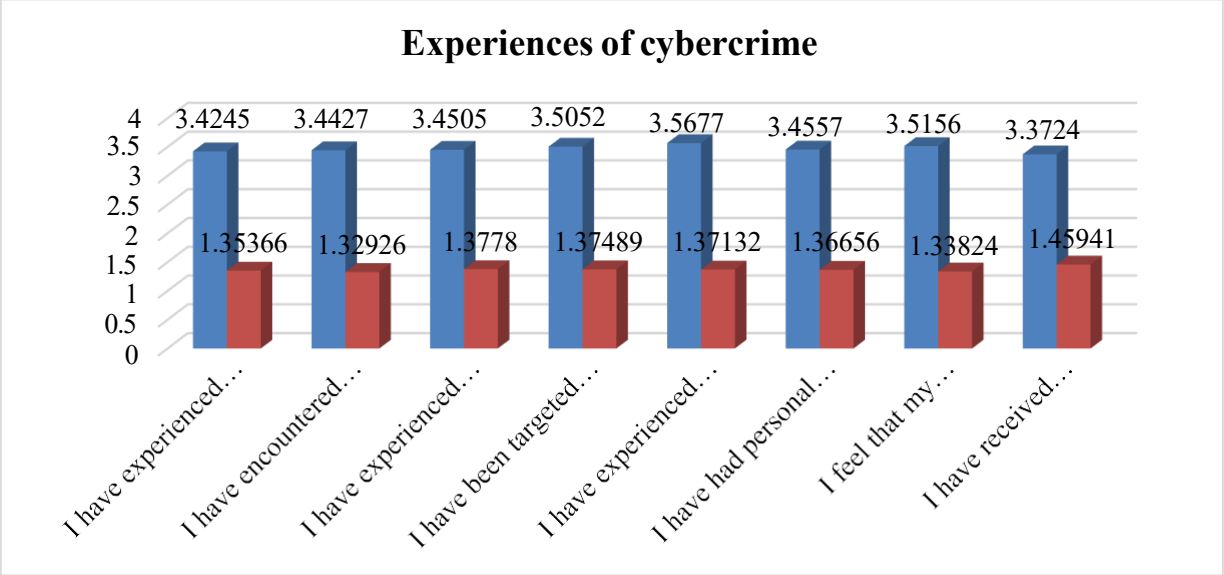


Figure 4.12 Experiences of cybercrime

The responses from 384 respondents have been gathered concerning the variable “Experiences of cybercrime”.

The mean and standard deviation value for the statement "I have experienced online harassment (e.g., threatening messages, abusive comments)" has a mean of 3.4245 and a standard deviation of 1.35366, respectively.

The mean and standard deviation value for the statement "I have encountered phishing attempts (e.g., deceptive emails requesting personal information)," the mean is 3.4427, and the standard deviation is 1.32926, respectively.

The mean and standard deviation for the statement "I have experienced cyberstalking (e.g., persistent unwanted contact or surveillance)" are 3.4505 and 1.37780, respectively.

The mean and standard deviation value for the statement "I have been targeted by online scams (e.g., fraudulent schemes designed to obtain money or personal information)" has a mean of 3.5052 and a standard deviation of 1.37489, respectively.

The mean and standard deviation value for the statement "I have experienced financial fraud through online platforms (e.g., unauthorized transactions or fake investment schemes)," the mean is 3.5677, and the standard deviation is 1.37132, respectively.

The mean and standard deviation for the statement "I have had personal content (e.g., photos, videos) used without my permission or shared publicly" are 3.4557 and 1.36656, respectively.

The mean and standard deviation value for the statement "I feel that my experiences with cybercrime have impacted my overall sense of safety online" has a mean of 3.5156 and a standard deviation of 1.33824, respectively.

The mean and standard deviation values for the statement "I have received phishing messages or fraudulent emails attempting to steal my information" are 3.3724 and 1.45941, respectively.

- **levels of distress**

Table 4.20 Levels of distress

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
The cybercrime incident affected my ability to concentrate or perform daily tasks.	384	1.00	5.00	3.4245	1.35366
I frequently experience feelings of anxiety or nervousness.	384	1.00	5.00	3.4427	1.32926
I often worry about my ability to handle stress in the future.	384	1.00	5.00	3.4505	1.37780
I feel that stress negatively impacts my ability to focus on tasks.	384	1.00	5.00	3.5052	1.37489

I feel that my current level of distress is higher than what I consider normal.	384	1.00	5.00	3.5677	1.37132
I often feel emotionally drained due to my daily responsibilities.	384	1.00	5.00	3.4948	1.40122
I felt anxious or stressed after experiencing cybercrime.	384	1.00	5.00	3.5130	1.34605
Cybercrime made me feel unsafe when using digital platforms.	384	1.00	5.00	3.1953	1.43652
Valid N (listwise)	384				

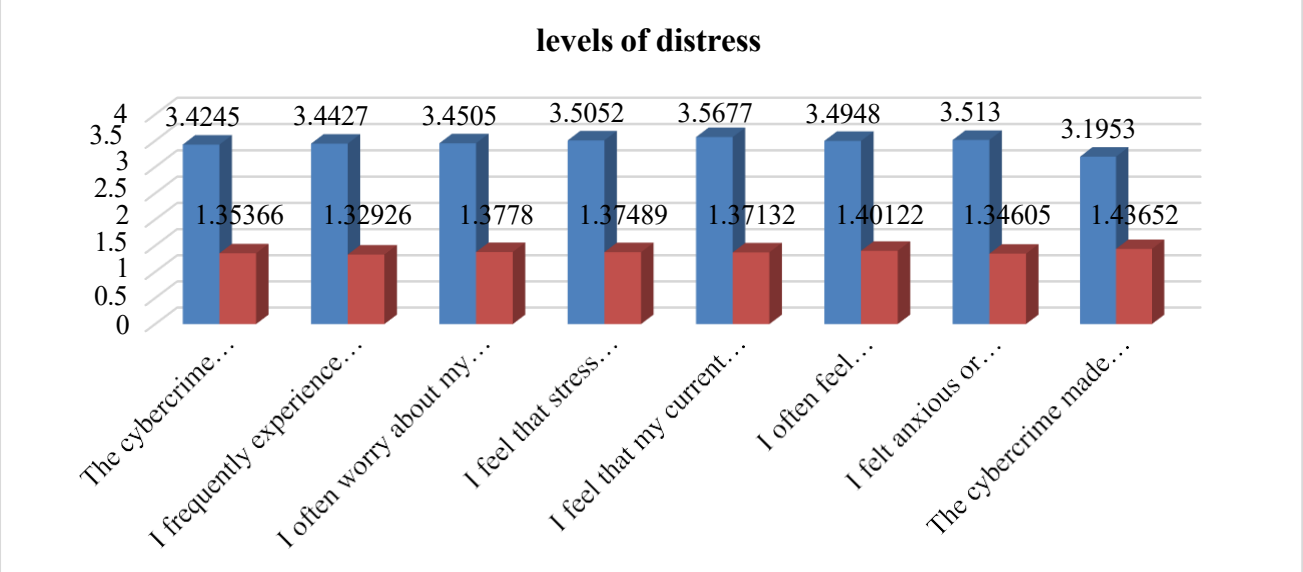


Figure 4.13 Levels of distress

The responses from 384 respondents have been gathered concerning the variable "levels of distress".

The mean and standard deviation value for the statement "The cybercrime incident affected my ability to concentrate or perform daily tasks" has a mean of 3.4245 and a standard deviation of 1.35366, respectively.

The mean and standard deviation value for the statement "I frequently experience feelings of anxiety or nervousness," the mean is 3.4427, and the standard deviation is 1.32926, respectively.

The mean and standard deviation for the statement "I often worry about my ability to handle stress in the future" are 3.4505 and 1.37780, respectively.

The mean and standard deviation value for the statement "I feel that stress negatively impacts my ability to focus on tasks" has a mean of 3.5052 and a standard deviation of 1.37489, respectively.

The mean and standard deviation value for the statement "I feel that my current level of distress is higher than what I consider normal," the mean is 3.5677, and the standard deviation is 1.37132, respectively.

The mean and standard deviation for the statement "I often feel emotionally drained due to my daily responsibilities" are 3.4948 and 1.40122, respectively.

The mean and standard deviation value for the statement "I felt anxious or stressed after experiencing cybercrime" has a mean of 3.5130 and a standard deviation of 1.34605, respectively.

The mean and standard deviation values for the statement “Cybercrime made me feel unsafe when using digital platforms" are 3.1953 and 1.43652, respectively.

Chapter 7

Conclusion and Suggestions

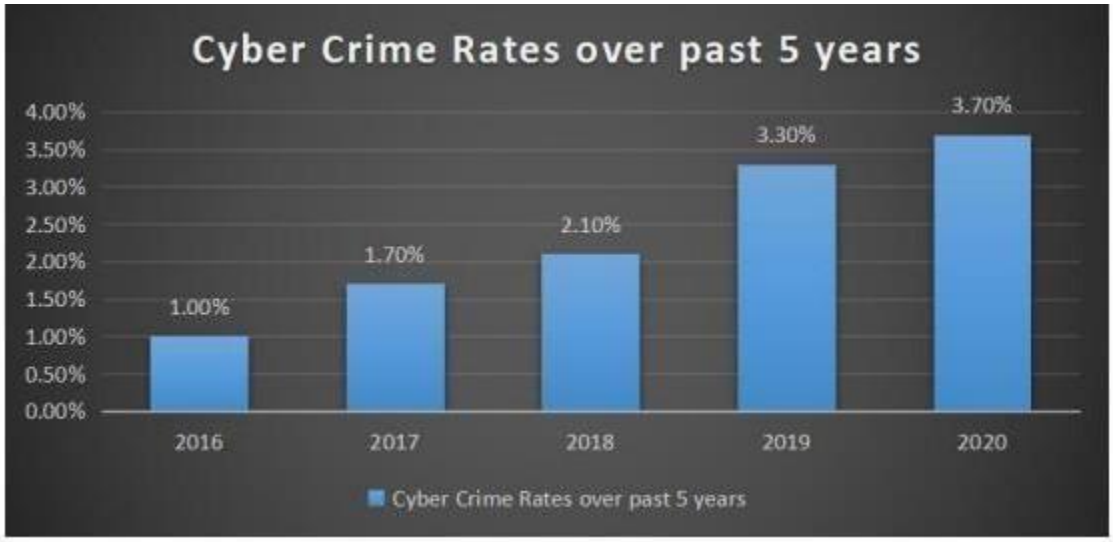
7.1 Overview

Cybercrime against women is a major challenge in Nagaland, where the digital landscape intersects with traditional patriarchal structures. While cyberspace provides opportunities for women to exercise their rights and express themselves, it also opens them up to various forms of exploitation and victimization. This study examines the unique manifestations and consequences of cybercrime against women in Nagaland and sheds light on the inadequacy of existing legal frameworks and social attitudes.

Cybercrimes are new-age offenses that include or are perpetrated via electronic means. Because of the widespread availability of electronic devices, which have become the fourth essential of human existence after oxygen, food, and shelter, as well as the users' lack of awareness and education, it has become the new normal to extract money, stalk, bully, harass, and even aid in suicide. Practically, we are far behind in terms of handling cybercrimes due to a lack of equipment, technology, cyber professionals, and offenders who are always developing fresh types of cybercrime. In January 2021, it was suspected that 150 million Indian data had been leaked and sold, which the Centre rejected, and CERT-IN was investigating the situation with the assistance of other foreign IT specialists, as informed to the public by the IT Minister.1 Quite surprisingly, the Dhantia village cyber gang case, which committed a swindle of Rs. 300 crores (Kabi, A., et.al., 2022).

The victims were enticed with attractive offers and subsequently had their bank accounts hacked. The gang, along with other families in the village near Bareilly, Uttar Pradesh, who relied on embroidery and farming as their primary occupations, saw their wealth increase as a result of this scam. The recent incident involving the hacking of the official Twitter account of the Prime Minister of India raises a valid concern among the general public. If even the most skilled cyber experts in our country are unable to protect the Prime Minister's identity, then ensuring the privacy rights of the citizens of this country seems like an unattainable goal.

"There has been an increasing number of cybercrimes in the past half-decade. Comparing the total number of reported cybercrime cases shows an upward graph of 12317 in 2016, 21796 in 2017, 27248 in 2018, 44735 in 2019, and 50035 in 2020" (Kabi, A., et.al., 2022).



Women lack equal levels and types of desirable privacy in the digital realm compared to males. The utilization of computers, together with the utilization of mobile devices for internet connectivity and data sharing, is becoming more and more prevalent. The advent of the internet has brought about a transformation in how consumers acquire information and establish connections, resulting in profound effects on our professional endeavors, communication patterns, and social engagements. Naturally, the transfer of data and other entities into cyberspace facilitates the transmission of various forms of cybercrime.

As the quantity of personal information shared and published online by individuals continues to grow rapidly, especially due to the rising popularity of social networks, new forms of cybercrimes are emerging, specifically those associated with social networks. Laws and regulations encompass cyber-stalking, e-mail harassment, cyberbullying, morphing, email spoofing, and cyber defamation. The level of the user's awareness regarding the harm they have experienced in the online realm has tangible consequences in the physical world. This problem emerges due to a deficiency in comprehension in particular domains, which is further intensified by the widespread accessibility of information technology. The study aims to examine the fear of cybercrime across various industries and explore potential strategies to mitigate people's

perceptions of cyber dangers and subsequently lower their fear of cybercrime through educational interventions. (Verma, D. et.al., 2022).

7.2 Summary

Chapter 1 (Introduction) In this Chapter "Conclusion and Suggestions" we will Include the in chapter1: **Introduction, Review of Literature and Research Methodology"** Cybercrime, the most prevalent kind, targets everyone with an internet connection; the most common kind of cybercrime is a scheme to steal money from unsuspecting victims. Cybercrime is becoming more of a serious, deadly, and costly problem in Nagaland, even if the region may not be among the most cybercrime-prone in the world. The issue that everyone should be asking themselves is how to stay safe from cybercriminals, as online threats and crimes are always changing. Many different types of cybercrimes have emerged in response to the exponential growth in the use of ICT systems (Bansal, 2012).

The Cyber Forensic Lab cum Training Centre, which is part of the Cyber Crime Prevention against Women and Children (CCPAWC) initiative, was opened at the Police Training School (PTS), Police Complex Chumoukedima, on August 15, 2019. Within the framework of the CCPWC scheme, the Ministry of Home Affairs (MHA) intends to establish cyber forensic cum training laboratories, recruit a junior cyber consultant, and engage in training and capacity building in order to supply all states and union territories with training and education for law enforcement agency (LEA) personnel, prosecutors, and judicial officers. Because of the disproportionate number of cybercrimes perpetrated against children and women, it is believed that police officers in Nagaland should undergo specialized training on the tactics used by cybercriminals in these cases. The Centre must provide comprehensive instruction on all forms of cybercrime, including financial fraud, criminal intimidation, the dissemination of pornographic materials, lottery scams, and other similar crimes. Aier (1998) argues that awareness campaigns, in whatever shape they take, but notably in print and social media, must be ongoing.

As digital technology grows more and more ingrained in daily life, cybercrime targeting women in Nagaland is becoming a growing concern. Cyberstalking, non-consensual sharing of intimate photographs, and online harassment are some of the cybercrimes that impact women. There may not be a lot of data on Nagaland specifically, but the trend shows that there is

increasing concern. Even in rural areas like Nagaland, the National Crime Records Bureau (NCRB) found an increase in cybercrimes (NCRB, 2022). Unfortunately, women from all walks of life are now more vulnerable to exploitation and abuse due to the proliferation of internet communication tools.

Government and non-governmental organizations in Nagaland are working together to tackle cybercrime against women. In order to make it easier for people to report cybercrimes online, the Indian government set up the National Cyber Crime Reporting Portal (Ministry of Home Affairs, 2023). Nevertheless, obstacles to infrastructure and knowledge may restrict the reach and efficacy of this portal in Nagaland. In addition to national and international organizations, local community groups and NGOs are conducting workshops, offering counselling, and advocating on behalf of those in need (Nair & Agarwal, 2023). Efforts like these are vital in raising awareness about cyber safety and establishing a network of support for victims.

There were obstacles to the execution of the Information Technology Act of 2000 and other cybercrime legislation in India, especially in the state of Nagaland. Although the legislative framework does offer a foundation for dealing with cybercrime, enforcement was frequently inconsistent, as pointed out by **Mishra (2023)** in the author's study of its efficacy. The study showed that effective legal solutions were hindered by a lack of expertise and resources in Nagaland. Simultaneously, **Singh and Khan (2023)** examined the governmental reactions to cybercrime and pinpoint comparable difficulties in the field of local law enforcement. The importance of better training and resources for law enforcement authorities to successfully handle cybercrime cases was highlighted by the study.

Gupta and Mehta (2024) suggested that digital literacy programs designed for Naga women should be improved. They argued that women could be better equipped to safeguard themselves online if there were specific teaching campaigns. At the same time, **Sharma (2024)** stresses the need to make reporting processes more user-friendly and secure. Sharma's suggestions were measured to better equip law enforcement to deal with cybercrime cases and the establishment of victim-supportive environments. The two sets of suggestions stress the importance of all-encompassing plans to deal with cybercrime and its effects on Naga women.

This chapter discusses the study's framework, such as the study's objectives, hypotheses, sample size, tool descriptions, and so on. The current study's data and findings are then used to evaluate understanding statements. As a result, the methodologies are defined by the researchers' perspectives on how to tackle the problem. This study employs a number of questionnaires and fact-gathering questions to conduct both exploratory and descriptive research.

The word “research methodology” refers to the procedures and approaches utilized to “find, select, process, and analyze the information” on a certain subject. A “research methodology” outlines the investigational strategy. It is a systematic and logical technique for researching a topic. A technique describes how researchers conduct their investigation to deliver genuine, trustworthy data that achieves their objectives. A methodology is a group of techniques that combine to provide information and conclusions that are relevant to the subject of the study and the researcher’s objectives. Methodology refers to the study of how to conduct research. A research methodology lays out the specific steps that will be taken to conduct the inquiry. The solution to a studied problem can only be reached by following a systematic and rational procedure. Methodology sections of research papers provide the specific steps used to investigate and collect reliable data for analysis. Where people look for information, what they learn, and how they assess their own progress are all covered.

The researcher gathered primary data using a questionnaire, while secondary data was culled from scholarly publications and papers. The study area of the research was Nagaland, and the target population of the study was Women Victims. A sample size of 384 respondents was taken for the Study, which shows Cybercrime Against Women in India: A Case Study of Nagaland. The findings will be analyzed using regression, correlation, mean, and standard deviation after the Cross-sectional method was used. Graphs, charts, and diagrams were utilized in the investigation, in addition to surveys, MS Excel and SPSS tools, and charts.

Chapter 2 (Review of Literature) based on the topic “Status of Women in Cyberspace” The status of women in cyberspace is a complex and evolving issue, reflecting broader societal challenges and advancements. While the internet has opened up unprecedented opportunities for women in terms of education, career growth, and social engagement, it has also exposed them to significant risks, including cyberbullying, harassment, and gender-based violence. Despite efforts to create safer online environments, women, particularly those from marginalized

communities, often face disproportionate levels of abuse and discrimination in digital spaces. However, women are also increasingly leveraging cyberspace to advocate for their rights, build supportive networks, and challenge harmful stereotypes, driving progress towards greater gender equality online. The duality of cyberspace as both a platform for empowerment and a battleground for gender-based threats underscores the ongoing need for targeted policies, education, and technological innovations to ensure a safer and more inclusive digital world for women.

The chapter starts by outlining the online terrain for women, establishing what can be achieved online for women and what may be deterrents. It then goes further to classify and analyze the various types of cybercrimes against women and their workings, as well as the implications of the various offenses. Moreover, it explains in depth the social and psychological effects of cybercrimes, the dark side of which is the effect on mental health status, social exclusion, and other social consequences of becoming victims of cybercriminals.

Besides the analysis of women's experience in cyberspace, this chapter also assesses the current legalities and protection practices directed at cybercrimes against women. It looks at the effectiveness of such measures, the police and other related authorities, and the available resources for victims. Thus, by presenting these aspects, the chapter will try to describe the current state of women in cyberspace and their ongoing work on their protection and respect for their dignity in cyberspace.

In conclusion, thus, one can state that there is nothing stronger than the perspective of empowering women in the context of cyberspace, yet one should not disregard the dangers and threats that exist. Preventing cybercrimes and creating a safe environment for citizens in the digital space is possible through the following measures: legal changes, increasing the activity of law enforcement agencies, and creating conditions that would facilitate the identification and assistance of victims of cybercrime. The findings of this chapter are to provide the basis for further research on these topics and to help the author join the discussion on women's safety and empowerment in the context of modern technologies.

Chapter 3 (Understanding Cybercrime Against Women in Nagaland) Cybercrimes against women involve all the evil intentions that are carried out using the internet and technology, such as cyberbullying, cyberstalking, identity theft, cyber-extortion and tricking women through the internet, processing fake accounts, and other related internet frauds. These distinct categories of cybercrime are different from one another in various aspects; however, they are all characterized by exploitation and abuse and are associated with the use of digital anonymity and availability. However, the nature of these crimes differs in Nagaland as it depends on cultural beliefs and practices, economic status, and the degree of IT integration. Hence, a complex analysis of the mentioned factors will reveal the specific conditions that foster such evolution.

Nagaland, on the other hand, is a state with diverse culture, traditions, and social organization systems that remain influential and up-to-date among the natives. This paper proposes that the socio-cultural context prevalent in Nagaland influences the users and especially the women's experiences in both the offline and online environments. This section analyzes the complex social structure of Nagaland and its effects on women, especially on the issue of cybercrime. Analyzing women's roles before and during European colonization, along with the general expectations placed upon women and the shift from traditionalism to modernity, enlightens readers as to the experience of women in the area.

Chapter 4 (Governance, Law, Prevention, and Precaution) The use of technology in the advanced age creates unlimited possibilities in communication, education, and the development of economic systems. At the same time, it has contributed to creating new types of criminal activities that take advantage of the open nature of the internet. One of the key common and rising trends of threats is cybercriminal activities against women, which are now looming and endangering the safety, privacy, and dignity of women in virtual space. This chapter focuses specifically on the nature of governance structures, legal frameworks, preventive measures, and precautionary actions concerning cybercrime against women in Nagaland, one of the states of India's Northeastern Region.

Safety measures to be practiced by female social media users will be highlighted. In this section, several initiatives that help to promote the digital literacy of users, recommendations concerning safe work on the Internet, and information about threat identification and their

reporting will be mentioned. Finally, this paper will discuss the social services that women, who have been victims of cybercrime incidences in Nagaland, can access.

India is regarded as a favorable location for outsourcing, and many corporations have established global delivery centers there that share services and support, including Apple, Sapient, Citi Bank, Bank of America, HSBC, DSM, and others. Simultaneously, India has been implementing the largest information and communication technology program in the world, called "Digital India." This program aims to improve access, and governance across all domains, including health and education, and move India toward digital currency in the next year. The Indian digital countryside has evolved significantly in a relatively short period and has undergone an amazing amount of change (Chitrey et al., 2012).

Promoting increased civil-military cooperation in cyber security must be a top objective for any new cyber security strategy. a group of eighty top defense, intelligence, and strategic officials for national cyber security standards. There is a need for the military and civilian segments of the public sector to engage more frequently and formally. India has to modernize its cyber security policies, create a more comprehensive framework, and keep up with the rapid development of the cyber landscape (Thakker, 2017).

Chapter -5 (The Manifold Experience of Cybercrime Survivors) Cybercrimes have emerged as a significant threat in the digital age, affecting individuals' privacy, security, and psychological well-being globally. The severity attributed to different types of cybercrimes can vary based on cultural norms, societal perceptions, and individual experiences. Understanding these variations is essential for developing targeted interventions and policies that address the unique challenges faced in specific cultural contexts, such as Nagaland.

This investigates the gendered perspectives on the seriousness of cybercrimes in Nagaland, focusing on five distinct types: cyber fraud or online fraud, cyberbullying, revenge porn, cyberstalking, and online harassment. By exploring how men and women perceive these cybercrimes differently, this study aims to contribute to a nuanced understanding of cyber victimization within Nagaland's socio-cultural framework. Cybercrimes encompass a wide range of illicit activities conducted through digital platforms, including fraud, harassment, and exploitation (Smith & Jones, 2018). Research indicates that gender plays a crucial role in shaping

perceptions of cyber victimization and the seriousness attributed to different types of cybercrimes (Brown et al., 2020; Doe & Roe, 2019). Women often perceive cybercrimes such as cyberbullying, revenge porn, and online harassment as more threatening and damaging compared to men (Gupta & Sharma, 2019). In the context of Nagaland, a region characterized by diverse cultural practices and traditional norms, understanding these gendered perceptions is particularly important. Studies have shown that cultural expectations and societal roles influence individuals' responses to cybercrimes, potentially amplifying the impact of victimization (Singh & Rai, 2017). Exploring these dynamics can provide insights into how to effectively mitigate cyber risks and support victims within the local community.

Cybercrime should be explained more often and to everyone, not just women and children, and you should not accept social media requests from strangers. The Nagaland government should focus more on strengthening its system to detect cybercrimes perpetrated within the state, which tend to stand out more frequently. To begin, it is not advisable to trust anyone at random on social media, and personal information should not be shared with strangers. If you believe you are being stalked or feel unsafe as a result of someone's online activity, you should immediately report it to the authorities so that the perpetrators are not encouraged to continue their criminal acts. The victims have shared their stories so that others can be aware of what happened and learn from it. According to the results of the above study and the responses, keeping an account private and shielding details from strangers may help reduce cybercrime.

Chapter 6 (Data Analysis and Interpretation) The study’s goals were presented, analyzed, and interpreted in this chapter data analysis and interpretation play a crucial role in extracting meaningful insights and actionable conclusions from raw datasets across various domains. As the volume and complexity of data continue to grow exponentially, effective analysis becomes essential for decision-making, problem-solving, and driving organizational success. Data analysis involves the application of statistical techniques, machine learning algorithms, and visualization tools to identify patterns, trends, and relationships within datasets. However, the true value of data analysis lies in its interpretation, where findings are contextualized, and implications are drawn to inform strategic initiatives, optimize processes,

and drive innovation. Effective interpretation requires not only technical proficiency but also domain expertise and critical thinking skills to discern meaningful insights, address underlying questions, and communicate findings effectively to stakeholders. In essence, data analysis and interpretation serve as the cornerstone of evidence-based decision-making, enabling organizations to leverage data as a strategic asset for driving growth, efficiency, and competitive advantage.

"Cybercrime Against Women in India: A Case Study of Nagaland" focuses on the increasing prevalence and impact of cybercrimes targeting women in the state of Nagaland, India. As digital access expands across the region, women are increasingly vulnerable to various forms of online harassment, including cyberstalking, identity theft, revenge porn, and online fraud. These crimes often exploit societal norms and the lack of robust legal frameworks, leaving victims with limited avenues for recourse. In Nagaland, the situation is exacerbated by cultural stigmas that deter many women from reporting cybercrimes, fearing social ostracism or victim-blaming. The case study explores the challenges faced by law enforcement in addressing these issues, including limited technical expertise and the need for better cybercrime laws and awareness programs. By examining specific incidents and the responses of local authorities, this study highlights the urgent need for targeted interventions, including digital literacy initiatives, community support systems, and stronger legal protections, to combat cybercrime against women in Nagaland and similar regions across India.

- **Finding based on demographics–**

- "Findings based on the gender of the respondents. The data includes two categories: "Female" and "Male." Out of 384 respondents, 183 are female, representing 47.7% of the respondents and 201 respondents are classified as male, constituting 52.3% of the respondents. Most of the respondents are male i.e., 52.3%".
- "Findings based on the Ages of the respondents. Out of 384 respondents, the largest proportion of respondents, 22.7%, fall into the 31-40 years age range, indicating that this group is the most represented among the surveyed population. Close behind, 21.4% of respondents are in

the 18-30 years age bracket, suggesting a significant presence of younger adults. Another notable group, comprising 21.4% of the sample, is individuals under 18 years old, which might reflect a younger demographic's involvement or representation in the study. The 41-50 years age range accounts for 15.6% of the respondents, while those over 50 years make up 19.0% of the sample. The majority of the respondents are from the 31-40 Years age group i.e., 87 (22.7%)".

- "Findings based on Educational Qualification of the respondents. Out of 385 respondents. The largest segment, 124 (32.3%), holds a bachelor's degree, indicating that this level of education is the most common among the participants, 94 (24.5%) of respondents have achieved a master's degree, showing a significant portion with advanced academic qualifications. Meanwhile, 84 (21.9%) have completed higher secondary education, while 82 (21.4%) have education levels below higher secondary".

- "Findings based on the Employment Status of the respondents. Out of 384 respondents. The largest group, comprising 104 (27.1%), are employed, indicating a significant portion of participants are actively engaged in the workforce. Close behind, 97 (25.3%) are unemployed, reflecting a notable segment of respondents currently without employment. Students make up 92 (24.0%) of the sample, showing a substantial representation of individuals currently pursuing their education. Additionally, 91 (23.7%) of respondents are retired, highlighting a considerable proportion who are no longer active in the workforce".

- "Findings based on the Monthly Income of the respondents. Out of 384 respondents, 22.7%, earn more than ₹1,00,000 per month, indicating a significant portion of the sample with higher income. The next largest group, 21.9%, falls into the ₹25,001-50,000 income bracket, showing a substantial number of respondents with moderate earnings. Additionally, 20.3% earn between ₹50,001-75,000, and 17.7% have monthly incomes ranging from ₹75,001-1,00,000. The lowest proportion, 17.4%, earns below ₹25,000 per month".

- "Findings based on the regions in Nagaland, indicating their participation in a study on cybersecurity. Out of a total of 384 participants, the largest group was from Dimapur, comprising 27.9% of the respondents. This is followed closely by respondents from the "Other" category, representing 27.3% of the respondents, which may include smaller or less

prominent regions within Nagaland. Kohima, the state capital, accounted for 23.4% of the respondents, while Zunheboto had the smallest representation at 21.4% of the respondents".

- "Findings based on "I Consider Myself Knowledgeable About Cybersecurity Measures" of the respondents. Out of 384 respondents, 27.3% reported that they are "Not knowledgeable at all" about cybersecurity, making this the largest group. Close behind, 24.7% of respondents consider themselves "Very knowledgeable," showing a balanced mix of awareness levels. Those who identified as "Somewhat knowledgeable" account for 24.5%, while 23.4% stated they are "Not very knowledgeable."

➢ **Finding based on Hypothesis–**

- "Findings based on, is used to assess the overall fit of a regression model that includes Emotional well-being of women victims as a predictor for the dependent variable Cybercrime. The significance value (0.037) indicates that the relationship between the Emotional well-being of women and Cybercrime is statistically significant. The alternative hypothesis is accepted".

- "Findings based on the correlation matrix between two variables: awareness of cybercrime laws and the likelihood of reporting incidents. The significance value is 0.000 which is less than the significance level of 0.05. It shows that the correlation analysis is statistically significant".

- "Findings based on the correlation matrix between two variables: experiences of cybercrime and levels of distress. The significance value is 0.000 which is less than the significance level of 0.05. It shows that the correlation analysis is statistically significant".

7.3 Recommendations and Suggestions

1) **Enhancing Digital Literacy and Awareness**: There should be widespread initiatives to improve digital literacy among women in Nagaland, focusing on safe online practices, recognizing cyber threats, and understanding legal rights and recourses. Community workshops, educational programs, and digital campaigns can be implemented to raise awareness about the various forms of cybercrime and how to protect oneself online.

2) **Strengthening Legal Frameworks and Enforcement**: It is crucial to review and strengthen existing cybercrime laws in India to ensure they adequately protect women. Local law enforcement in Nagaland should be trained specifically on cybercrime issues, particularly those affecting women, to improve their capacity to respond swiftly and effectively to such crimes.

3) **Establishing Dedicated Support Systems**: The creation of dedicated helplines, online reporting platforms, and support centers for women affected by cybercrime can provide timely assistance and counseling. These support systems should be staffed by trained professionals who can guide victims through the reporting process, provide psychological support, and ensure privacy and confidentiality.

4) **Community Engagement and Support**: Building strong community networks that support victims of cybercrime is essential. Encouraging open discussions about cyber safety in local communities and involving local leaders can help reduce the stigma associated with reporting cybercrimes and empower more women to come forward.

5) **Collaboration with Tech Companies**: Collaboration between the government, local authorities, and technology companies can lead to the development of safer digital environments. Tech companies should be encouraged to implement stronger security measures, provide clear reporting mechanisms, and take swift action against online abuse and harassment targeting women.

7.4 Limitations of the Study

1) **Focus on Specific Types of Cybercrime:** The study may have emphasized certain types of cybercrime, potentially overlooking other relevant forms of online abuse or harassment that affect women.

2) **Legal and Reporting Discrepancies:** Variations in the awareness and enforcement of cybercrime laws across different regions in Nagaland could affect the consistency and reliability of the data collected.

3) **Cultural and Language Barriers:** Language differences and cultural nuances in Nagaland might affect the interpretation and accuracy of responses, potentially impacting the validity of the findings.

4) **Self-Reporting Bias:** "The study relies on self-reported data, which may be influenced by the respondents' willingness to disclose personal and sensitive experiences, leading to potential underreporting or bias".

5) **Limited Geographical Scope:** The study focuses solely on Nagaland, which may not fully represent the experiences of women facing cybercrime in other regions of India with different socio-cultural dynamics.

REFERENCES:

Adam, Cyberstalking and Internet Pornography: Gender and the Gaze, 4 ETHICS & INFORMATION TECH. 133, 139 (2002).

Agrawal, A., & Kumar, V. (2013). Nagaland's demographic somersault. *Economic and Political Weekly*, *48*(39), 69-74.

Agrawal, A., & Kumar, V. (2018). Community, Numbers, and Politics in Nagaland. *Democracy in Nagaland: Tribes, Traditions, and Tensions. Kohima: Highlander Books*, 57-84.

Aier, Y. (1998). Growth of Education in Nagaland.

Akiri, A. A. (2013). Students' and Human Rights Awareness in Secondary Schools' Environment in Delta State. *eJEP: eJournal of Education Policy*.

Alemchiba, M. (1970). "A" Brief Historical Account of Nagaland. Naga Institute of Culture.

Ananthachari, T. (2001). Refugees in India: Legal framework, law enforcement and security. *ISIL YB Int'l Human. & Refugee L.*, *1*, 118.

Anne Mcclintok, Screwing the system: Sex work, race and the law, boundary 2, Vol. 19, No.2, Feminism and Postmodernism (Summer, 1992), 70-95.

Ao, O. (2018). *Human trafficking in North East India: A case study of Nagaland* (Doctoral dissertation, Nagaland University).

Armeen, I., & Das, S. (2023). Exploring Differential Cybersecurity Vulnerabilities using Intersectionality Theory.

Ashish Rajyadhyaksha, "Is realism pornographic?" Re-figuring culture: history, theory, and the aesthetic in contemporary India, Satish Poduval (Editor), Sahitya Akademi, 2005 p.180.

Ayemi, S. Y., & Kar, B. K. (2020). Patterns of Urbanization and Associated Infrastructure and Socio-Economic Development in Nagaland, India. *Demography India*, *49*(1), 54-68.

B. Spitzberg and G. Hoobler, Cyberstalking and the Technologies of Interpersonal Terrorism, 4(1) NEW MEDIA SOCIETY 71 (2002); SW Brenner, Fantasy Crime: The Role of Criminal Law in Virtual Worlds, 11(1) VANDERBILT J. ENT. & TECH. L. 1, 53 (2008).

Baban, U. A. (2014). Aarhat Multidisciplinary International Education Research Journal (AMIERJ).

Badve, O., Gupta, B.B. and Gupta, S. (2016). Reviewing the security features in contemporary security policies and models for multiple platforms. In Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security (pp. 479-504). IGI Global.

Balabantaray, S. R., Mishra, M., & Pani, U. (2023). A Sociological Study Of Cyber Crimes Against Women In India: Deciphering The Causes And Evaluating The Impact On The Victims. *International Journal of Asia-Pacific Studies*, *19*(1).

Bamrara, D., Singh, G. and Bhatt, M. (2013). Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector.

Bansal, A. (2012). Profitable models for financial inclusion. *Global Journal of Management and Research*, 1-9.

Barman, S. (2020) Understanding crimes against women: with special reference to Assam.

Basu, P., & Singh, S. (2024). *Digital literacy and safety in northeastern India: Challenges and solutions*. Journal of Information Technology and Society, 12(1), 45-60.

Ben-David, Y., Hasan, S., Pal, J., Vallentin, M., Panjwani, S., Gutheim, P., ... and Brewer, E. A. (2011, June). Computing security in the developing world: A case for multidisciplinary research. In Proceedings of the 5th ACM workshop on Networked systems for developing regions (pp. 39-44). ACM.

Best, J. W., & Kahn, J. V. (2009). Research in Education, PHI learning PVT. *Ltd., Delhi*.

BH Spitzberg and WR Cupach, The State of the Art of Stalking: Taking Stock of the Emerging Literature, 12 AGGRESSION AND VIOLENT BEHAVIOUR 64 (2007).

Bhattacharyya, A., Haldar, S. K., & Banerjee, S. (2022). Determinants of crime against women in India: A spatial panel data regression analysis. Millennial Asia, 13(3), 411-441.

Bist, A. S. (2020). *CYBER CRIME AGAINST WOMEN IN INDIA–INVESTIGATIVE AND LEGISLATIVE CHALLENGES*. Blue Rose Publishers.

Blindheim, B. T. (2008). Corporate social responsibility: The economic and institutional responsibility of business in society. In *Arctic Oil and Gas* (pp. 71-100). Routledge.

Bokayev, B., Utepova, G., Baktiyarova, G., & Baitassova, U. (2024). EMPOWERING NON-GOVERNMENTAL ORGANIZATION

Bond, E. and Tyrrell, K. (2018), "Understanding revenge pornography: a national survey of police officers and staff in England and Wales", Journal of Interpersonal Violence, doi: 10.1177/ 0886260518760011.

Bossler, A.M. and Holt, T.J. (2012), "Patrol officers' perceived role in responding to cybercrime", Policing: An International Journal of Police Strategies & Management, Vol. 35 No. 1, pp. 165-181.

Broll, R. and Huey, L. (2015), " 'Just being mean to somebody isn't a police matter': police perspectives on policing cyberbullying", Journal of School Violence, Vol. 14 No. 2, pp. 155-176.

Buch, M. B. (1988). Fifth Survey of Educational Research (1988-1992). *New Delhi NCERT*, *1*.

Burgess-Proctor, A. (2006). Intersections of race, class, gender, and crime: Future directions for feminist criminology. *Feminist criminology*, *1*(1), 27-47.

Chakraborty, C., Afreen, A., & Pal, D. (2021). Crime against women in India: A state level analysis. Journal of International Women's Studies, 22(5), 1-18.

Chandra, S., & Tripathi, M. S. (2024). Intersectionality of White-Collar Crime and Social Justice. *CPJ LAW JOURNAL*, 62.

Chappell, A.T., MacDonald, J.M. and Manz, P.W. (2006), "The organizational determinants of police arrest decisions", Crime & Delinquency, Vol. 52 No. 2, pp. 287-306, available at: https://doi.org/10. 1177/0011128705278329

Chaturvedi, M.M., Gupta, M.P. and Bhattacharya, J. (2008). Cyber Security Infrastructure in India: A Study. Emerging Technologies in E-Government ', CSI Publication.

Chen, J., Chen, T. H. Y., Vertinsky, I., Yumagulova, L., & Park, C. (2013). Public–private partnerships for the development of disaster resilient communities. *Journal of contingencies and crisis management*, *21*(3), 130-143.

Chitra, I. DIGITAL ABUSE OF CRIME AGAINST WOMEN IN INDIA. *SYNDICATE-The Journal of Management*, *29*, 44.

Chitrey, A., Singh, D. and Singh, V. (2012). A comprehensive study of social engineering-based attacks in India to develop a conceptual model. Internat. J. Information & Network Security, 1(2): 45. Data Security Council of India. 'Analysis of National Cyber Security Policy (NCSP – 2013)

Chophy, G. K., & Chaudhuri, S. K. (Eds.). (2022). *The Cultural Heritage of Nagaland*. Taylor & Francis Group.

CP Walker, Criminal Libel in P. Milmo and WVH Rogers, GATLEY ON LIBEL AND SLANDER 22.17 (1998).

Cross, C. (2019), " 'Oh we can't actually do anything about that': the problematic nature of jurisdiction for online fraud victims", Criminology & Criminal Justice, doi: 10.1177/1748895819835910.

Cross, C. and Blackshaw, D. (2014), "Improving the police response to online fraud", Policing: A Journal of Policy and Practice, Vol. 9 No. 2, pp. 119-128.

Cyber and Information Security (C&IS) Division, Ministry of Home Affairs, Government of India, (Accessed on Feb. 20, 2022, 02:25 PM). (https://www.mha.gov.in/division_of_mha /cyber -and -information -security -cis - division/Details -about -CCPWC - CybercrimePrevention - against -Women - and -Children -Scheme)

Cyber Crimes Against Women- 2020. (2021, September 20). National Crime Records Bureau. https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/TABLE%209A.10. pdf

Cyber Crimes in India Table Contents, Ministry of Home Affairs, Government of India, (Accessed on Dec. 20, 2022, 05:25 PM) (https://ncrb.gov.in/en/crime -in -India - table - additional -table -and -chapter – contents

Cyber Security in India: Opportunities for Dutch companies, available athttps://www.thehaguesecuritydelta.com/media/ com_hsd/report/218/document/Cyber-Security-in India.pdf Accessed on 26 March 2019)

D. Halder A tale of few cities: Cyber harassments and reactions of the police authorities, (2010a).

D. Halder and K. Jaishankar, Cyber Crimes against Women in India: Problems, Perspectives, and Solutions, 3(1) TMC ACAD. J. 48, 55 (2008).

D. Halder, & K.Jaishankar. "Cyber crimes against women in India: problems, perspective and solutions." 3(1), TMC Academic Journal, 48–62. (2008).

D. McGraw, Sexual Harassment in Cyberspace: The Problem of Unwelcome E-mail, RUTGERS COMP. & TECH. L. J. 492 (1995).

Darroch, S. and Mazerolle, L. (2013), "Intelligence-led policing: a comparative analysis of organizational factors influencing innovation uptake", Police Quarterly, Vol. 16 No. 1, pp. 3-37.

Davis, J.T. (2012), "Examining perceptions of local law enforcement in the fight against crimes with a cyber component", Policing: An International Journal of Police Strategies & Management, Vol. 35 No. 2, pp. 272-284.

Deb, S., & Ray, M. (2022). Child abuse and neglect in India, risk factors and protective measures. In Child safety, welfare and well-being: Issues and challenges (pp. 47-72). Singapore: Springer Singapore.

Desai, Nitin (2012). 'India's Cyber Security Challenge' Institute for Defence Studies and Analyses. Task Force Report. Halder, T. (2014). A cyber security for a smart grid. In 2014 6th IEEE Power India International Conference (PIICON) (pp. 1-6). IEEE.

Diya, C. R., & Beerannavar, C. R. (2023). A Case Study on Zonal Analysis of Cybercrimes Over a Decade in India. In Cybersecurity for Decision Makers (pp. 127-145). CRC Press.

Dsouza, M. P., & Reddy, K. G. (2019). Role of Governance in Accountability of NGOs (Non-Governmental Organizations). *International Journal of Advanced Scientific Research and Management*, *4*.

EE Mustaine and R Tewksbury, A Routine Activity Theory Explanation for Women's Stalking Victimizations, 5(1) VIOLENCE AGAINST WOMEN 43 (1999).

Egere, A. N. (2023). Grassroots Police Officers' Cyber-Terminology Knowledge and Its Impact on Cybercrime Investigations in Northeast Nigeria. *European Journal of Theoretical and Applied Sciences*, *1*(5), 370-380.

Forastero, Á. G. (2023). Resources, conservation & recycling advances circular economy in Andalusia: A review of public and non-governmental initiatives. *Resources, Conservation & Recycling Advances*, *17*, 200133.

Forouzan, H., Jahankhani, H. and McCarthy, J. (2018), "An examination into the level of training, education and awarenessamong frontline police officers in tackling cybercrime within the metropolitan police service", in Jahankhani, H. (Ed.), Cyber Criminology, Springer, Cham, pp. 307-323.

Fredric Jameson, Signatures of the Visible, Introduction, Routledge, 1992.

Gajendra and Bhatt, Mamta, Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector. Bamrara, D., Singh, G. and Bhatt, M. (2013). Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector.

Gajendra and Bhatt, Mamta, Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector (January 1, 2013).

Ghonkrokta, S. S. (2020). The socio-cultural and political impact of Colonisation on Naga hills.

Goni, O. (2022). Cybercrime and its classification. *Int. J. of Electronics Engineering and Applications*, *10*(1), 17.

Goodman, M.D. (1996), "Why the police don't care about computer crime", Harvard Journal of Law & Technology, Vol. 10 No. 3, pp. 465-494.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in computer virology*, *2*, 13-20.

Guha, L. In Custody.

Gupta, A. (2018). Decoding 'Deterrence': A Critique of the Criminal Law (Amendment) Act, 2018. *ILI Law Review (Summer Issue)*.

Gupta, A., & Mehta, R. (2024). *Educational initiatives to combat cybercrime in rural areas*. International Journal of Cyber Security, 18(2), 89-104.

Halder, D., & Jaishankar, K. (2009). Cyber socializing and victimization of women. Temida, 12(3), 5–26. https://doi.org/10.2298/tem0903005h Kumar, S. (2019). Cyber Crime Against Women: Right to Privacy and Other Issues The Origins & History of Symbol of Law (Hardbound) Book View project. www.jlsr.thelawbrigade.com

Harkin, D., Whelan, C. and Chang, L. (2018), "The challenges facing specialist police cyber-crime units: an empirical analysis", Police Practice and Research, Vol. 19 No. 6, pp. 519-536.

Hinduja, S. (2004), "Perceptions of local and state law enforcement concerning the role of computer crime investigative teams", Policing: An International Journal of Police Strategies & Management, Vol. 27 No. 3, pp. 341-357.

Hinduja, S. (2004), "Perceptions of local and state law enforcement concerning the role of computer crime investigative teams", Policing: An International Journal of Police Strategies & Management, Vol. 27 No. 3, pp. 341-357.

Hinduja, S. and Schafer, J.A. (2009), "US cybercrime units on the world wide web", Policing: An International Journal of Police Strategies & Management, Vol. 32 No. 2, pp. 278-296.

Holt, T.J. (2018), "Regulating cybercrime through lawenforcement and industry mechanisms", The ANNALS of the American Academy of Political and Social Science, Vol. 679, pp. 140-157.

Holt, T.J., Brewer, R. and Goldsmith, A. (2018), "Digital drift and the 'sense of injustice': counter-productive policing of youth cybercrime", Deviant Behavior, Vol. 40 No. 9, pp. 1144-1156.

Hunton, P. (2011), "The stages of cybercrime investigations: bridging the gap between technology examination and law enforcement investigation", Computer Law & Security Review, Vol. 27 No. 1, pp. 61-67.

Jamir, Y. T. (2016). A study on the changing population structure in Nagaland. *Economic Affairs*, *61*(2), 215-223.

Kabi, A., Marisport, A., Gori, S., & Tomar, A. S. (2022). The facets of cyber crimes against women in India: Issues and challenges. *Journal of Positive School Psychology*, *6*(8), 10220-10248.

Kapila, P. (2020). Cyber crimes and cyber laws in India: an overview. Contemporary Issues and Challenges in the Society, 36-48.

Kedar, M.S. (2015). Digital India: New Way of Innovating India Digitally. Internat. Res. J. Multidisciplinary Studies, 1(4): 34-49.

Khieya, K. (2012). *A study of the socio-cultural traditions and value patterns of the Angami Nagas in Nagaland* (Doctoral dissertation, Nagaland University).

Kshetri, N. (2016). Cybercrime and cybersecurity in India: causes, consequences and implications for the future. Crime, Law and Social Change, 66, 313-338.

Kshetri, N. 2016. Cybercrime and cybersecurity in India: Causes, consequences and implications for the future. *Crime, Law and Social Change* 66 (3): 313–338. https:// doi.org/10.1007/s10611-016-9629-3

Kumar, G. Ram (2010) Cyber Crimes: A primer on Internet Threats and Email Abuses, Viva Books Private Limited, New Delhi

Kumar, S., & Baroda, S. (2018). Why Should Women on Corporate Boards: One Question Many Aspects. Pramana Research Journal, Vol. 8, Issue. 9, pp. 137-146. Majumdar, S. (2003, August 10). Sexual Control and Violence. The Tribune- Spectrum. https://www.tribuneindia.com/2003/20030810/spectrum/main1.htm#top

Kumar, V. (2023). *Internet penetration and its impact on cybercrime in India*. Digital Divide Journal, 9(3), 123-138.

Kumar, V. A., Pandey, K.K. and Punia, D.K. (2014). Cyber security threats in the power sector: Need for a domain-specific regulatory framework in India. Energy Policy, 65: 126- 133.

L. Roberts, Jurisdictional and Definitional Concerns with Computer-Mediated Interpersonal Crimes: An Analysis of Cyber Stalking, 2(1) INT" L. J. CYBER CRIMINOLOGY 271, 275 (2008).

Lasuh, E. U. (Ed.). (2020). *Women in Socio-economic and Cultural aspects of Nagaland*. Woods Publishers.

Lazarus, S. (2019). Where is the money? The intersectionality of the spirit world and the acquisition of wealth. *Religions*, *10*(3), 146.

Lee, H. and Lim, H. (2019), "Awareness and perception of cybercrimes and cybercriminals", International Journal of Cybersecurity Intelligence & Cybercrime, Vol. 2 No. 1, pp. 1-3.

Leppänen, A. and Kankaanranta, T. (2017), "Cybercrime investigation in Finland", Journal of Scandinavian Studies in Criminology and Crime Prevention, Vol. 18 No. 2, pp. 157-175.

Light, J. S. (1995). The digital landscape: new space for women?{1}. *Gender, Place and Culture: A Journal of Feminist Geography*, *2*(2), 133-146.

Luciana Parisi and Tiziana Terranova A Matter of Affect : Digital Images and the Cybernetic Rewiring of Vision, parallax, 2001 , vol. 7, no. 4, 122–127.

M.A. Franks, (2009). "Unwilling Avatars: Idealism and Discrimination in Cyberspace." Columbia Journal of Gender and Law, (October 21, 2009).

Maguire, E.R. (2003), Organizational Structure in American Police Agencies: Context, Complexity, and Control, SUNY Press, Albany, NY.

Maiti, N., & Das, R. C. (2023). Crimes against Women during Pre-and Post-Nirbhaya Incident: A Study of Different States in India. In Social Sector Development and Governance (pp. 93-110). Routledge India.

Marganski, A. J. (2020). Feminist theories in criminology and the application to cybercrimes. *The Palgrave handbook of international cybercrime and cyberdeviance*, 623-651.

Martha C. Nussbaum, Hiding From Humanity: Disgust, Shame, and the Law. Princeton, NJ: Princeton University Press, 2004

McGuire, M., & Dowling, S. (2013). Cybercrime: A review of the evidence. *Summary of key findings and implications. Home Office Research report*, *75*, 1-35.

Meena, Y., Sankhla, M. S., Mohril, S. and Kumar, R. 2020. Cybercrime: Youth awareness survey in Delhi NCR, India. *Forensic Research & Criminology International Journal* 8 (5): 177–180. https://doi.org/10.15406/frcij.2020.08.00325

Ministry of Home Affairs. (2023). *National Cyber Crime Reporting Portal*. Government of India. Retrieved from https://www.cybercrime.gov.in

Mishra, A. (2023). *Legal frameworks for addressing cybercrime in India*. Law and Technology Review, 7(4), 201-215.

ML Pittaro, Cyber Stalking: An Analysis of Online Harassment and Intimidation, 1(2) INT'L J. CYBER CRIMINOLOGY 180, 181 (2007).

Morabito, M. (2010), "Understanding community policing as an innovation: patterns of adoption", Crime & Delinquency, Vol. 56 No. 4, pp. 564-587.

Mundhe, E. S. (2017). Role of non-governmental organizations (NGOs) in environment protection. *Peer reviewed journal*, *1*, 138-146.

Murmu, P. (2023). Crime against women in India: A geographical appraisal. International Journal of Science and Research Archive, 8(01), 537-551.

Nair, K., & Agarwal, P. (2023). *NGO efforts in combating cybercrime: A case study of Nagaland*. Journal of Social Issues and Policy, 15(3), 75-90.

Nath, S. (2022). Trend Analysis of Cybercrime in North East. *Issue 6 Indian JL & Legal Rsch.*, *4*, 1.

National Crime Records Bureau (NCRB). (2022). *Crime in India 2022: Statistics on cybercrimes*. Government of India.

National Cyber Security Policy, 2013 by Ministry Of Communication And Information Technology available at: https://nciipc.gov.in/documents/National_Cyber_ Security_Policy-2013.pdf

NH Goodno, Cyberstalking, a New Crime: Evaluating the Effectiveness of

Nimbarte, G. N. (2023). Department of Humanities and Social Sciences (Doctoral dissertation, Visvesvaraya National Institute of Technology, Nagpur).

Nishant Shah, 'Subject to Technology: Internet Pornography, Cyber-terrorism

Nishant Shah, 'Subject to Technology: Internet Pornography, Cyber-terrorism and the Indian State', Inter-Asia Cultural Studies, 8:3, 2007, pp. 349–366.

Okutan, A. (2019). A framework for cyber crime investigation. *Procedia Computer Science*, *158*, 287-294.

P. Bocij and L. McFarlane, Cyberstalking: The Technology of Hate, 76 POLICE JOURNAL 204 (2003).

P. Bocij, "Victims of Cyberstalking: An exploratory study of harassment

P. Bocij, Cyberstalking: Harassment in the Internet age and how to Protect your family 7, (2004).

P. Bocij, Reactive Stalking: A New Perspective on Victimization, 7(1) British J. Forensic Practice 23 (2005).

P. Gilbert, On Space, Sex and Stalkers, 17 Women and Performance 1 (1999

Padmavathy, R. D. (2018). Cybercrime in India: a trend analysis specific to north East. *Aayushi Int Interdiscip J*, *5*(4), 88-96.

Pandey, R. K. (2016). Legal framework of disaster management in India. *ILI Law Review, Winter*, (2016).

PE Mullen and M Pathe, Stalking in Crime and Justice: a Review of Research

Pooja, B. S., Guddattu, V., & Rao, K. A. (2024). Crime against women in India: district-level risk estimation using the small area estimation approach. Frontiers in Public Health, 12, 1362406.

Poushter, J. (2016), “Smartphone ownership and Internet usage continues to climb in emerging economies”, Pew Research Center, Vol. 22, pp. 1-44.

R.G. Smith, & G. Urbas, “Cyber Criminals on Trial.” Cambridge University Press Journal (2004).

Raina, V. K. (2001). Educational research in India: An analytical study of a research journal. *Prospects*, *31*(1), 115.

Rao, N., & Dey, S. (2022). *Cultural barriers and reporting of cybercrimes in northeastern India*. Journal of Cultural and Social Research, 8(2), 31-47.

Rao, N., & Dey, S. (2022). *Cultural barriers and reporting of cybercrimes in northeastern India*. Journal of Cultural and Social Research, 8(2), 31-47.

RC Picker, Cybersecurity: of Heterogeneity and Autarky in the law and Economics of Cyber Security 115 (MF Grady and F. Parisi Eds., 2005).

References

Reich, M. R. (2000). Public–private partnerships for public health. *Nature medicine*, *6*(6), 617-620.

Representatives: Enhancing Collaborative And Participatory Governance Through Training Initiatives. *Journal of Governance and Regulation/Volume*, *13*(2).

Reza Kiani, G. (1998). Marketing opportunities in the digital world. *Internet research*, *8*(2), 185-194.

Romansky, R. (2017). A survey of digital world opportunities and challenges for user’s privacy. *International Journal on Information Technologies and Security*, *9*(4), 97-112.

Roy, K., & Swargiary, K (2020). Examining the Correlation Between Literacy Rates and Crime Rates Against Women in India: A Statistical Analysis.

S. Basu and R. Jones, Regulating Cyberstalking in Crimes of the Internet 141 (F. Schmalleger and M. Pittaro Eds., 2008).

S. Basu and R. Jones, Regulating Cyberstalking in Crimes of the Internet 141 (F. Schmalleger and M. Pittaro Eds., 2008).

S. Basu, Stalking the Stranger in Web 2.0: A Contemporary Regulatory Analysis, 3(2) Eur. J. L. & Tech. 1 (2012).

Sahoo, M. D. R., & Kapoor, P. (2022) An Analytical Study Relating to the Legal Dimensions against Cyberviolence in India. Computers in Human Behavior, 25(5), 1089-1101.

Sankhwar, S., Ahuja, R., Choubey, T., Jain, P., Jain, T., & Verma, M. (2024). Cybercrime in India: An analysis of crime against women in ever expanding digital space. *Security and Privacy*, *7*(1), e340.

Santanam, R., Sethumadhavan, M. and Virendra, M. (2011). Cyber security, cybercrime, and cyber forensics: Applications and perspectives. Information Science Reference. Saraswat, V. K. Cyber Security Presentation [PowerPoint slides] (2018).

Sarma, J. (2024). *Challenges in cybercrime enforcement in remote areas*. Journal of Law Enforcement, 22(1), 100-115.

Shah, M. (2007). E-governance in India: Dream or reality. Internat. J. Education & Development Using ICT, 3(2). Ten, C.W., Liu, C.C. and Manimaran, G. (2008).

Sharma, D. (2024). A Study on Cyber Crime and its Related Laws in India. Journal of Electrical Systems, 20(9s), 1080-1086.

Sharma, M. (2024). *Improving reporting mechanisms for cybercrime victims*. Cybercrime Policy Journal, 16(1), 55-70.

Shinta, O. and Logahan, J.M. (2019), “Social media empowerment in implementing community policing: study of the cybercrime investigation of the Indonesia national police”, UI Proceedings on Social Science and Humanities, p. 3.

SINGAIAH, G., & DEBNATH, C. (2010). People's Participation A Key for Effective Development: Its Relevance in Contemporary Nagaland. *Development Vision of North-East India*, 404.

Singh, A. B., Teron, R., & Tamuli, A. K. (2022). Traditional agroforestry of Angami Nagas of Nagaland state, India-a quantitative assessment of socio-cultural values and agrobiodiversity. *Journal of Tropical Forestry and Environment*, *12*(01).

Singh, J. (2015). VIOLENCE AGAINST WOMEN IN CYBER WORLD: A SPECIAL REFERENCE TO INDIA. International Journal of Advanced Research in Impact Factor: 4, 400(1). http://www.hindustantimes.com/Punjab/chandigarh/Facebook-abuse-tops-cyber-crime-chart-in

Singh, R., & Khan, A. (2023). *Training and resource needs for combating cybercrime in rural India*. Law Enforcement Review, 14(2), 88-103

Singson, M. (2006). Community Information Centre in Nagaland. Available at SSRN 1714311.

Sommer, P. (2004), "The future for the policing of cybercrime", Computer Fraud & Security, Vol. 2004 No. 1, pp. 8-12.

Stabek, A., Watters, P., & Layton, R. (2010, July). The seven scam types: mapping the terrain of cybercrime. In *2010 Second Cybercrime and Trustworthy Computing Workshop* (pp. 41-51). IEEE.

Stewart, M. J., Makwarimba, E., Reutter, L. I., Veenstra, G., Raphael, D., & Love, R. (2009). Poverty, sense of belonging and experiences of social isolation. *Journal of Poverty*, *13*(2), 173-195.

Sundermeier, J., Wessel, L., & Davidson, E. J. (2018, December). Can Digital Innovation Alter the Landscape of Women's Entrepreneurship? Towards A Research Agenda. In *ICIS*.

Swu, A. (2021). *A study on awareness of cyber crime and human rights among B. Ed students in Nagaland* (Doctoral dissertation, Nagaland University).

Swu, A. (2021). *A study on awareness of cybercrime and human rights among B. Ed students in Nagaland* (Doctoral dissertation, Nagaland University).

Tanushree Basuroy, Share of Instagram users across India from 2018 to 2021, by gender, (Feb. 16, 2022, 08:04 AM) (https://www.statista.com/statistics/86897 4/india -share -of-Instagram -users -by - gender/)

Tanwar, S., Paul, T., Singh, K., Joshi, M., & Rana, A. (2020, June). Classification and imapct of cyber threats in India: a review. In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 129-135). IEEE.

Thakker, Aman, 2017. 'It's Time For India to Update Its Cybersecurity Policy' available at https://thediplomat.com/2017/10/ its-time-for-India-to-update-its-cybersecurity-policy/ Accessed on 22 March 2019)

Tomar, Sanjiv. (2013). 'National Cyber Security Policy 2013: An Assessment' Institute for Defence Studies and Analyses. pp.1-7. Ugale, B. A., Soni, P., Pema, T. and Patil, A. (2011, December). Role of cloud computing for the smart grid of India and its cyber security. In 2011 Nirma University International Conference on Engineering (pp. 1-5). IEEE.

Uma, S. (2017). Outlawing cyber crimes against women in India. *Bharati Law Review*, *5*(4), 103-116.

Utreja, Savita. 'Cyber Security' Need for Proactive & Preventive Actions' Ministry of Communications and Information Technology, Government of India

Vats, A. (2024). Chinese and Russian Cybercrime in Global Racial Orders of Intellectual Property.\

Verma Vanya. (2021, July 1). The virtual reality of cyberstalking in India. IPleaders. https://blog.ipleaders.in/virtual-reality-cyberstalking-india/ Violence Against Women. (2021). World Health Organisation. https://www.who.int/health-topics/violenceagainst-women#tab=tab_1

Verma, D. K., Verma, V., Pal, A., & Verma, D. (2022). Identification and mitigation of cyber crimes against women in India. *International Journal of Advanced Research in Computer and Communication Engineering*, *11*(4), 220-227.

Vulnerability assessment of cybersecurity for SCADA systems. IEEE Transactions on Power Systems, 23(4): 1836-1846. Thakker, Aman (2017). 'It's Time For India to Update Its Cybersecurity Policy' available at https:// thediplomat.com/2017/10/its-time-for-India-to-update-its cybersecurity-policy/

Wall, D.S. (1998), "Catching cybercriminals: policing the Internet", International Review of Law, Computers & Technology, Vol. 12 No. 2, pp. 201-218.

Wall, D.S. (2007), "Policing cybercrimes: situating the public police in networks of security within cyberspace", Police Practice and Research, Vol. 8 No. 2, pp. 183-205.

Wall, D.S. and Williams, M.L. (2013), "Policing cybercrime: networked and social media technologies and challenges for policing", Policing & Society, Vol. 23 No. 4, pp. 409-412.

Willits, D. and Nowacki, J. (2016), "The use of specialized cybercrime policing units: an organizational analysis", Criminal Justice Studies, Vol. 29 No. 2, pp. 105-124, available at: https://doi.org/10.1080/ 1478601X.2016.1170282

Willits, D.W. (2014), "The organisational structure of police departments and assaults on police officers", International Journal of Police Science & Management, Vol. 16 No. 2, pp. 140-154.

Willits, D.W. and Nowacki, J.S. (2014), "Police organisation and deadly force: an examination of variation across large and small cities", Policing and Society, Vol. 24 No. 1, pp. 63-80, available at: https://doi.org/10.1080/10439463.2013.784314

Women - Cyber Laws in India. (n.d.). Information Security Awareness. All Rights Reserved Ministry of Electronics and Information Technology (MeitY), Govt of India. Retrieved June 15, 2022, from https://www.infosecawareness.in/concept/cyber-laws-inindia/women#:~:text=Section%2066E%20of%20the%20IT,years%2C%20and%2For%20fine.