Report of the Taiwan Foundation for Democracy Grant

Workshop on Digital based Gender Violence against Women in Manipur

Grantee Organization: Institute of Social Research and Development (ISRD)

Project Coordinator: Mr Ksh. Dinesh Singh

Period of Project: *[2023, 07, 20 to 2023, 08, 20]*

Date of Report: *[2023, 07, 24]*

TAIWAN FOUNDATION for DEMOCRACY
財團法人 臺灣民主基金會

Contents

Executive Summary

Manipur is a small land-locked state in India's north eastern region bordering Nagaland to the north, Assam to the west, Mizoram to the south and a 358 km border with Myanmar to the east, with a population of 23.89 lakhs (2001 Census) and a land area of 22,327 sq.km.

Cyber Crime against women along with general crimes is on the rise in Manipur, as the state recorded a total of 1548 cases of crimes against women in 2021. Cyberspace is the name given to the computer-generated world of the internet, and cyber laws are the regulations that apply there. Due to the fact that this space has a form of universal jurisdiction, all users are governed by these regulations. Cyber law is another area of law that deals with legal problems brought on by the usage of networked information technology.

During the pandemic and lockdown, people were compelled to use the internet for social, professional, recreational, and educational purposes. Through the use of laptops, smartphones, and the internet, working women started working from home. Women who are still in school are compelled to use the internet for online coursework and other academic pursuits.

The rate of cybercrime against women started to increase at this time since the majority of women were using social media sites and one or more online platforms for academic, professional, and entertainment purposes. Criminals started mentally and emotionally tormenting the victim because they could not physically harm them because the entire country was on lockdown.

One Day Workshop on **Digital based Gender Violence against Women in Manipur** was organized by ISRD on 22nd July 2023 at Imphal with a view to create better understanding on cybercrime among the masses for enabling to internalize the magnitude of Increasing Crime Against women in the cyber space. It also aims to promote awareness of existing gaps and challenges in the social system pertaining to crime against women. The program was attended by 55 participants from different sections of the society and they will act as a peer leader to reach out secondary beneficiaries with accurate information. In the larger extent, women will empower to reduce cyber related violences while adopting appropriate skills, precautions and accessing existing legal provisions. On the other hand, the program will enhance the capacities of women to defend violations rights through cyber with timely complaining to the appropriate authority and minimize the unreported cases due to fear and mental weakness.

TAIWAN FOUNDATION for DEMOCRACY
財團法人 臺灣民主基金會

AGENDA

INVITATION

Institute of Social Research and Development (ISRD)

Cordially request the pleasure of your kind presence at

One Day Workshop on Digital based Gender Violence against Women in Manipur

On: Saturday, 22nd July 2023
At: The Castle Hotel, Palace Compound, Imphal
At: 11:00 am

PROGRAMME SCHEDULE

10: 30 a.m.	-	Assemble of participants
11: 00 a.m.	-	Welcome Address by **M. John Singh**, Field Coordinator
11: 05 a.m.	-	Key Note by **Ms H. Loidang Devi**, President, ISRD
11: 15 – 12:00 p.m.	-	*"Overview of Cyber Crime in Manipur"* By **Mr Sanjenbam Jugeshwor Singh** Asst. Professor, JCRE Global College, Manipur
12 to 12:20 p.m.	-	Interaction Programs
12: 20 - 1:00 p.m.	-	Lunch Break
1:00 -1:45 pm	-	*"Manipur Police Response on Cyber Crime in Manipur"* **by Mr Thounaojam Superman Singh**, Sub Inspector, Cyber Crime Department
1:45 – 2:05 pm		Interaction Programs
2:05 to 2:50 pm		*"Women as the Victim of Cybercrimes and Legal provisions"* **by Mr Rakesh Meihoubam** Advocate
2:50 to 3:10 p.m.	-	Interaction Programs
3:10 pm	-	Vote of Thanks

R.S.V.P. +91 7005303385 / 9612569116

CHAPTER 1: INAUGURATION SESSION

A One-day Workshop on **"Digital based Gender Violence against Women in Manipur"** was organized by Institute of Social Research and Development (ISRD) with the auspicious financial assistance from Taiwan Foundation for Democracy, Taiwan at the Castle Hotel on 22nd July, 20223.

The inaugural session of workshop was graced by M. John Singh, Field Coordinator, ISRD by welcoming all the delegates and participants and wishing for a meaningful participation.

At the outset, Ms H. Loidang Devi, President, ISRD, Institute of Social Research and Development (ISRD) also welcomed the participants and delegates namely Mr Sanjenbam Jugeshwor Singh, Asst. Professor, JCRE Global College, Manipur, Mr Thounaojam Superman Singh, Sub Inspector, Cyber Crime Department and Mr Rakesh Meihoubam, Advocate. She highlighted about the role played by the internet in the 21st century's information technology and advancement. All of us having difficulties as the state has suspended more than 77 days due to some conflict. Internet has positive and negative impacts but we need to assured using in a meaningful aspect while protecting our rights and ethics.

Highlighting the core aspects of the program to empower the womenfolk to understand the cybercrime from the human right perspective and enable to access exiting legal framework to address the violence. In Manipur, due to social stigmatization and fear psychosis, many of us never disclose violation of rights and other forms of violences without punishing the culprits.

She also aspects the meaningful participations from the participants along with in-depth discussion with the delegates to bult a common understanding and collective effort in addressing the digital based violence against women in Manipur.

SESSION REPORT

Session - 1

Session on ***"Overview of Cyber Crimes in Manipur"*** was delivered by Mr. Sanjenbam Jugeshwor Singh, Assistant Professor, JCRE Global College, Manipur. He was well known for his outstanding regular topics related to information technology in regular dailies in Manipur from the last two decades. He describes about Cyber Crime and its effects to generate a common understanding.

Cyber Crime:

- Cyber Crime or Computer oriented Crime is the crime that involved a computer and a network. The computer may have been used in the commission of a crime or it may be the target and

- Cybercrime can be defined as: Offences that are committed against individual or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm or loss to the victim directly or indirectly using modern telecommunication networks such as Internet (networks including chat rooms, e-mails, notice board and groups) and mobile phones (Bluetooth, SMS, MMS).

Effects of Cyber Crime:

- Cybercrime may threaten a person or a nation's security and financial health. Issues surrounding these types of crimes have become high profile, particularly those surrounding hacking, copyright infringement, unwanted mass surveillance, sextortion, child pornography and child grooming.
- There is also problem of privacy when confidential information is intercepted or disclosed lawfully or otherwise. Internationally both governmental and non-state actor engage in cybercrimes including espionage, financial theft and other cross-border crimes.
- Cybercrimes crossing international border and involving the actions of at least one nation state is sometimes referred to as Cyber war fare.

Ranges of Activities in Cyber Crimes:

- Computer crime or cybercrime encompasses a broad range of activities. Any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which cause loss is known as Computer Fraud.
  Other forms of fraud may be facilitates using computer system, including Bank fraud, Carding, identity theft, extortion and theft of classified information.
- A variety of internet scams, many based on phishing and social Engineering target consumers and businesses.
- An act of terrorism committed through the use of cyberspace or computer resources is generally defined as Cyber terrorism.

- As such a simple propaganda piece in the Internet that there will be bomb attack during holidays can be considered as cyber terrorism. Cyber extortion occurs when website- email server or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. Cyber warfare is not the least to mention.

Cyber Crimes in Manipur:

- In Manipur, around forty ethnic communities are living at present in various parts
- Many ethnic groups are separately waging wars of Independence from the Republic of India.
- Manipur has more than forty armed groups actively or inactively operating in the state. Some of these groups are based on ethnic lines and demand for separate state or union territory inside India.
- As these armed groups are operated from outside India, they must be using some form of medium to communicate and execute their agenda. The medium may be telephone, radio, or internets which are optimal in usages.

He further describes about current trend of cyber crime through Social Media tools in Manipur.

Social Media:

- Social Media is a website that allows those who have an account to communicate with a selected group of friends or people. Facebook, Twitter, Instagram, WhatsApp and 2Go are just some of these Social Media sites.
- Social media has made things easier. With as low as 10 Megabyte of data, one can connect with friends and family members anywhere in the World and for a longer period of time.
- Social media has been very useful when disaster strikes-such as the earthquake, Tsunami that caused untold disaster.
- With social media, one can just pick up his cell phone, access the internet and go the page of his or her loved one and read the information posted or even chat briefly. It's that easy.

Social Media as a tool of Cyber Crimes:

- In the bid to connect with people many youths have added friend requests from people they know absolutely nothing about.
- Some of these friends might be criminals, fraudsters, bullies. Sexually immoral people and bad friends.
- We have many stories of youths who were defrauded, raped, bullied and even murdered by their social media friends.
- Others learn bad things from these so call friends and end up engaging in crime.
- Many teenagers have become addicted to the point that the social media has taken over their lives.

Social Media & Youths:

- Most teenagers think that their privacy is secured while on social media. Hence, they post their pictures of where they are or disclose information that are supposed to be kept to them such as their home address, email address, where they attend the school, the name of their pet, the times when they are at home and when no one is and other sensitive info
- This information is enough to tell criminals or stalkers when to strike. It can also be used for identity thefts, hackers, phishing, scams and virus sending information.

Session - 2

The second session on “Manipur Police Response on Cyber Crime in Manipur” was presented by Mr Thounaojam Superman Singh, Sub Inspector, Cyber Crime Department, Manipur Police. He highlighted Manipur police efforts in mitigating cyber related crimes in Manipur and also reqested cooperation from all the sections of the society. He concerned about the current trends of cyber crimes in the state and people ignorance in reporting cyber crimes.

He mentioned that Cyber Crime Police Station, Manipur was inaugurated on 24th June, 2017 by the Hon’ble Chief Minister of Manipur Shri. N. Biren Singh under the 100 days Programme of the Manipur Government.

The state police has a setup a Social Media Monitoring Cell (SMMC) in the last week of June, 2021. It works, round-the-clock, and scrutinize posts/comments on platforms like Facebook, Twitter, Instagram, Youtube, etc for any Cyber Crime Post . On the reports submitted by the SMMC, Cyber CrimePoliceStation, Manipur takes up necessary action.

He further urged the partcipants to report any cyber related cases at the earliest to enable track the culprits with following evidences:

Financial Fraud Cases:

- Bank Statement highlighting the Fraudulent Transactions;
- Screenshot of the chats with the Fraudsters – Whatspp/FB/IG/SMS and
- Screenshot of payments – UPI.

Social Media Related Cases:

- URL of the Account; .
- Screenshot of the Account and the concerned posts/messages and
- Screenshot of the chats– Whatspp/FB/IG/SMS

He also mentioned key points for incidents are Under reported which needs to be more focus for improvements.

- Woman and child cyber harassment and related cyber-crimes remain overwhelmingly underreported due to associated stigma and propensity of parents/guardians to not involve police in such matters;
- Perpetrators know their victims well or they are related to them;
- Women are mostly unaware about privacy policies and safety

tips for using social media sites and

- The Manipur society is such that a woman is expected to tolerate a certain degree of harrying, in the fear of social humiliation.

Cyber Crime on Women further categories - Sending Obscene email, Stalking using chat room, WhatsApp, FB, online dating site, matrimonial sites, Morphing, Pornography, revenge porn, Trolling, Cyber bullying-3rd in the world, Online Sexual solicitation and harassment Online Grooming, Online sexting-self generated sexual images and Online Commercial fraud.

To prevent the cyber crimes, the Ministry of Home Affairs, Government of India has setup 'Indian Cyber Crime Coordination Centre (I4C)' to deal with cybercrimes in a coordinated and comprehensive manner.

Following are seven components of the centre:

- National Cybercrime Threat Analytics Unit (TAU);
- National Cybercrime Forensic Laboratory (NCFL);
- National Cybercrime Training Centre (NCTC);
- Cybercrime Ecosystem Management;
- Platform for Joint Cybercrime Investigation Team;
- National Cybercrime Reporting Portal and
- National Cyber Research and Innovation Centre (NCR&IC).

Ministry of Home Affairs launched the Cyber Crime Reporting Portal (www.cybercrime.gov.in) under Cyber Crime Prevention Against Women and Children (CCPWC) scheme in September 2018 for CP/RGR cases. NCRP(National Cyber Crime Reporting Portal) – improved version in August 2019.

Session - 3

The third session on “Women as the Victim of Cybercrimes and Legal provisions” was delevered by Mr. Rakesh Meihoubam and he is a well known legal practissioner and human right activist. He mentioned about most common cyber crimes in relation to women as most of the women victimized and underported.

Sextortion: The most common cybercrime performed against women during the pandemic was sextortion. By using their victims' private photos or altered images as blackmail, the offenders started demanding money or sexual favors from them. In order to express their aggravation about the epidemic, the offenders threatened women and asked for sexual videoconferencing or letters from them. Additionally, as they had no money, they felt empowered to threaten victims with their altered images in order to get money from them.

Phishing: To make money during the lockdown, criminals send fake e-mails with a link to a particular webpage in an effort to coerce the victim into entering personal information like contact details and passwords or with the purpose of infecting the victim's device with dangerous viruses as soon as the link is clicked. These texts and emails appear to be authentic. The attackers then carry out shady transactions from the victim's bank account to their own using the victim's bank account and other private information.

Pornography: During the pandemic, offenders indulged in online sexual attacks against women, altering the victim's image and using it in pornographic material.

Cyber stalking: It included, among other things, contacting or trying to engage the victim via social media sites or phone conversations despite her obvious lack of interest, posting messages on the victim's page (often threatening in nature), and persistently bothering the victim with emails and phone calls.

Cyber hacking: During the pandemic, people started reading the news online. There are more examples of false news and information now than ever before. After clicking on malicious URLs, the women were the victims of cyber hacking. The malware downloaded all of their personal information to their phones, turned on the microphone and camera, and took their intimate photos and videos. Then, criminals use these bits of information and pictures to carry out extortion and other offenses.

Cyber-bullying: This includes, sending rape and death threats to the victim and posting false, misleading, and abusive statements about the victims on social media sites, and demanding money to have them removed. It also includes leaving hurtful comments on the victim's posts. A computer, cell phone, or laptop are examples of digital or communication technology that are used for harassment and bullying.

Cybersex trafficking: It is different from physical sex trafficking in that the victim does not physically engage with the perpetrator. Cybersex trafficking is when a dealer broadcasts, records, or takes pictures of the victim engaging in sexual or intimate activities from a central location and then sells the content online to sexual predators and clients. The criminals have forced, manipulated, and blackmailed women into participating in cybersex trafficking, which constitutes sexual abuse of women.

Legal provisions regarding Cybercrime: Although a comprehensive regulatory framework for laws governing the cyber realm, including such actions, has not yet been developed, some legal remedies under different statutes can help victims of cyber violence.

The Indian Penal Code 1860: Before 2013, there was no law that dealt directly with cyberbullying or crimes committed against women online. Sections 354A to 354D are added to the Indian Penal Code, 1860 as a result of Section 354A of the 2013 Criminal Amendment Act.

Section 354A: According to Section 354A, a male who engages in any of the following acts-demanding or pleading for sexual favors; showing pornography against a woman's will; or making sexual remarks-commits sexual harassment and may be punished with rigorous imprisonment for up to three years, a fine, or both. In the first two cases, there is a possibility of up to one year in imprisonment, a fine, or both.

Section 354C: Voyeurism is defined in Section 354C as the act of taking a photograph of a woman engaging in a private act and/or publishing it without the lady's permission. The circumstances must be such that the woman would "usually expect not to be seen, either by the offender or by anyone else acting at the perpetrator's direction" for it to qualify as "voyeurism." If found guilty under this section, the offender may be fined and sentenced to up to three years in prison on the first conviction and seven years on subsequent conviction.

Section 354D: The addition of Section 354D states about stalking prohibition that covers online stalking. The act of stalking is defined as when a man pursues or approaches a woman despite the woman's obvious disinterest in the interaction, or when a guy observes a woman's online behavior, use of the Internet, or electronic communication. If found guilty of stalking, a man might spend up to three years in jail and a fine, and subsequent convictions could land him in prison for up to five years and a fine.

In addition to the specific changes to the Code, there are a number of other provisions that provide for the reporting of cyber-attacks and the prosecution of those who are responsible.

Section 499: To slander is to do something with the intent to harm someone's reputation. Defamation through the publication of an instant and unambiguous portrayal of imputation is punishable by up to two years in prison, a fine, or both when done with the intent to harm a woman's reputation.

Section 503: Criminal intimidation occurs when a person is threatened with reputational injury in an effort to make her panic or force her to do what she ordinarily does or does not do. This rule can be applied to situations where someone is cyber-blackmailed, as was done in the aforementioned scenario.

Section 507: This section specifies the maximum punishment for criminal intimidation done by a person the victim does not know. This clause sanctions any anonymous communication that violates Section 503's prohibition on criminal intimidation.

Section 509: Anyone who speaks, gestures, shows an object, or makes a sound with the intent that it be heard or seen by a female and offends her modesty or invades her privacy may be charged with violating this section and punished with up to three years of imprisonment and a fine. This provision may impose penalties for instances of sexually explicit images and content that are forcibly distributed online, as well as for remarks or comments made in a similar vein.

The Information Technology Act 2000

Section 66C: Identity theft is a crime that is punishable under Section 66C of the IT Act. This provision would be applicable to scenarios of cyber hacking. According to this clause, whoever falsely or dishonestly uses another person's electronic signature, password, or other distinctive identifying feature risks up to three years in prison and a fine of up to Rs. 100000.

Section 66E: If someone's right to privacy is breached, Section 66E addresses that issue. A person can face up to three years imprisonment and/or a fine for taking, sharing, or sending a picture of their private area without their consent or in a way that violates their privacy.

Section 67: Obscene content must not be published, transmitted, or made to be distributed under Section 67, which carries a maximum sentence of three years imprisonment or a fine for a first conviction and up to 5 years imprisonment and a fine for the second.

Section 67A: Publishing, transmitting, or aiding in the transfer of sexually explicit material is a misdemeanor under Section 67A, punishable by up to five years in prison and a fine for a first conviction and up to seven years of imprisonment and a fine for the subsequent conviction.

RECOMMENDATION AND WAY FORWARD

- Social media can do well, it can also do badly. The bottom line is just moderation. Youths should learn to use the social media with moderation. This will help to make the world of social media a great place. So, let's use social media usefully;
- Even though Manipur is plagued with separatists' movements, civil unrest, drug trafficking, ethnic conflicts, communalism; Manipur police Cyber Crime units have been able to solve more than sixty-five percent of registered cyber cases using IT Acts and IPC Sections. There are instances where the Manipur Police Cyber Crime unit unable to solved or registered cases of communal nature, which may be due to political pressure and which they will deny;
- Government must implement awareness generation initiatives to educate women on cyber related violences;
- Government must operate helpline for easy cyber related crimes probably female functionaries;
- Government must modernize existing cyber police stations in order to ensure quick response and
- Adoption of cyber crimes related chapters in the school curriculum in order to educate children.

Acknowledgement

This is a report of a project that was supported by a grant from the Taiwan Foundation for Democracy (TFD). The Grantee agrees to acknowledge the sponsorship of the Foundation and print the approved Foundation logo where feasible and practical in project proceedings or similar publications and reports and on conference banners, program materials, and any other significant forms of publicity, including periodic public reports and press releases.

In addition, the Grantee consents to the use of the content of this report and any accompanying photographic and/or video documentation materials in future publications or publicity materials of the Foundation.