Defence on Cyber Crimes Against Women and Laws in India-A Survey

Author : R.Krishnaranjani

Abstract— Though crime against women is on a rise in all fields being a casualty of cyber crime might be most traumatic involvement for a woman. Particularly in India where the society looks down upon the woman, and the law doesn't indeed legitimately perceive cyber crimes. Time is presently here to acquit that our women are secure in cyber world; the memento alarms to halt clowning around activities on web get to because it is an offense and women take umbrage from it. Each moment, one woman in India gets deceived to be a casualty of and the online platform cyber violations and a cyber crime is presently the modern stage where a security, woman's dignity and security is progressively being challenged each minute. Offense, undermining, Trolling, stalking, voyeurism, body-shaming, slandering, watchfulness, exact retribution porn and numerous other shapes of obscene representation of women are uncontrolled within the cyber world. In this paper we organize to examine upon the diverse sorts of cyber crimes that can be caused upon a woman, and they unfavourably influence her. We shall also briefly examine upon the different laws that exist to secure woman in such cases such as the Information Technology Act (2000).

Keywords— Cybercrime; Women; Violence; Information Technology; Internet; Cyber Law; Security.

1. Introduction

Technical measures to forfend computer systems are being implemented along with licit measures to obviate and deter malefactor deportment. But this technology kens no physical boundaries; it flows more facilely around the world subsequently the malefactors are increasingly located in places other than where their acts engender their effects and Cyberspace is no exception to it. Cyberspace is an incipient horizon controlled by machine for information and any malefactor activity where computer or network is utilized as the source, implement, or target is kenned Cybercrime. The mundane types of cybercrime may be discussed under the following heads: hacking, cyber stalking, cyber pornography, phishing, web jacking, software piracy, and cyber terrorism. Cybercrime against women in India is relatively an incipient concept. When India commenced her peregrination in the field of Information Technology, the priority was given to the aegis of electronic commerce (e-commerce) and communications under Information Technology Act, 2000 whereas cyber socializing communications has remained untouched. The Act turned out to be a moiety baked law as the operating area of the law stretched Cyber Victimization of Women and Cyber Laws in India. The present study is an endeavour to highlight the cyber malefactions against women in India.

2. Literature Survey

Indian women aren't ready to report cybercrimes straightaway as they're not extremely aware on wherever to report such crimes or aren't serious regarding coverage an equivalent thanks to social embarrassment they don't wish to face.Their mindset needs to broaden and they must be the whip to curb down by taking derring-do against such perpetrators that is to go ahead and lodge an immediate complaint. Most of the issues will be resolved if women report the crime right away and warn the wrongdoer concerning taking robust action.

Cybercrimes intent typically through fake ids created on Facebook, Twitter and different social media platforms inflicting grave injury to women, as through these platforms, major blackmailing, threatening, bullying, or cheating via person messages and email unit of measurement done by perpetrators. Ill-intentioned men act these cyber-crimes with malafide intention like smuggled gain, revenge, insult to the modesty of a woman, extortion, blackmailing, sexual exploitation, defamation, incite hate against the community, and prank satisfaction of acquiring and to steal data

2.1 Major Cyber Crime Areas

Some of the most important well-known cybercrimes have place thousands of girls into varied health problems like depression, cardiovascular disease and women suffer from anxiety, cardiomyopathy, diabetic and thyroid ailments because of e-harassment[1]. Major cyber crimes area unit as under,

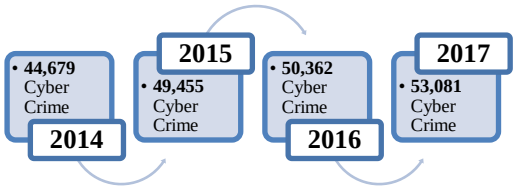

Figure 1:Cyber Crime Cases(2014-2015)

2.1.1 Cyber stalking

Cyber stalking is on the rise and women are the most likely targets. Cyber stalking is a way to use the Internet to stalk someone for online harassment and online abuse. A cyber stalker does not engage in direct physical threat to a victim but follows the victim's online activity to gather information, make threats in different forms of verbal intimidation.

2.1.2 Defamation

Cyber defamation includes both libel and defamation. It involves publication libellous data regarding the person on a website or current it among the social and friend's circle of victims or organization that is a straightforward methodology to ruin a woman's name by inflicting her grievous mental agony and pain.

2.1.3 Morphing and Cyber Pornography

Morphing is very increasing it's done by redaction the first image to misuse it. Perpetrators because of web access will in few seconds transfer women's footage from Social Media, WhatsApp or alternative resources and transfer morphed photos on other websites like social media website, porno sites or for registering themselves anonymously.

Cyber Pornography is another threat to women as a result of this includes business enterprise sexy materials in erotica websites by exploitation computers and web whereby women won't even bear in mind of such immoral publication of their own terribly image.

2.1.4 E-mail spoofing

It refers to an email that emerges from one source but has been sent from another source. It can cause monetary damage.

Phishing: Phishing is that the plan to gain sensitive data likes username and secret and intent to achieve personal data[10].

2.1.5 Trolling

Trolls spreads conflict on the Internet, criminal starts quarrelling or upsetting victim by posting inflammatory or off-topic messages in an online community such as a newsgroup, forum, chat room, or blog with the intention to provoke victims into an emotional, upsetting response. Trolls square measure skilled abusers, by making and victimization pretend ids on social media, produce a chilly war atmosphere within the cyber area and don't seem to be even straightforward to trace.

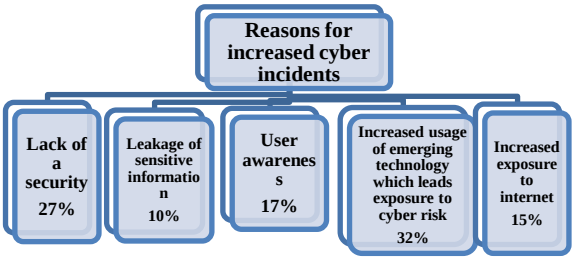

Figure2:Reasons for Increased Cyber Incidents

2.2 Cyber Law under the Information and Technology Act, 2000

The stalkers and cybercriminals can be booked under several sections for breaching of

privacy. **Section 67** deals with publishing or transmitting obscene material in electronic form. The earlier section in **ITA** was later widened as per **ITAA 2008** in which child pornography and retention of records by intermediaries were all included.

a) Section 66A

Sending offensive messages through communication service, inflicting annoyance etc., through associate transmission or causing associate email to mislead or deceive the recipient regarding the origin of such messages normally referred to as IP or email spoofing area unit all coated here. Punishment for these acts is imprisonment up to three years or fine.

b) Section 66B

Dishonestly receiving taken computer resource or communication device with social control up to a few years or one large integer rupees as fine or each.

c) Section 66D

Cheating by person on victimization computer resource or a communication device shall be reprimanded with imprisonment of either description for a term that extends to 3 years and shall even be at risk of fine which can touch one 100000 rupees.

d) Section 66E

Privacy violation-Publishing or transmittal non-public space of somebody while not his or her consent etc. penalisation is 3 years imprisonment or 2 hundred thousand rupees fine or each.

e) Section 66F

Cyber terrorism – intent to threaten the unity, integrity, security or sovereignty of the state and denying access to anyone licensed to get access to personal resource or trying to penetrate or access a computer resource while not authorization.

f) Section 72

Punishment for breaching one's space and confidentiality.

g) Section 72A

Punishment for revealing data throughout lawful contract.

h) Section 441 IPC

This section deals with criminal misdemeanour.

i) Section 354D

This section deals with stalking. It defines stalker as a person who follows women and tries to contact such woman, monitors each activity undertaken by the girl whereas mistreatment digital media.

2.3 Key points to protect yourself from getting victimized to cyber crimes

- **Don't share passwords**

You may have shared your positive identification with a trusty friend or partner. The concern is affordable whereas friends might not by design because you hurt, they'll accidentally reveal your password to somebody. Use your discretion and keep those passwords non-public and complex.

- **Don't leave your webcam connected**

There square measure too several apps capable of turning on your camera and trickily recording your movements while not your information. As a precaution disable camera permission and keep the lens of your camera closed or coated once not in use.

- **Don't share more than necessary**

Relationships have solely 2 shades spectrum – superb or very dangerous. Even the most effective of individuals will swing from one finish of the spectrum to the opposite, that's why use caution once you share intimate messages, pictures, data or something that has the potential to come back and embarrass you.

- **Don't meet on-line acquaintances alone:**

Perpetually let your friends and family understand wherever you're going and who you're meeting. Confirm you meet the person in a very huddled restaurant or mall.

- **Uncover as it were as much as needed:**

There are as well numerous evil characters browsing social media destinations to start companionship with clueless women. Use caution almost posting points of interest almost your whereabouts and way of life. Stalkers can discover ways to reach you with a basic photo or status update.

- **Update all operating systems on your devices**

They can be a nuisance. But they are very important to keep you safe. Security updates and patches keep the most recent threats away. Invariably install them in spite of however busy you're.

- **Secure your devices with anti-virus software**

Having a portable or a tablet without a security system in its original place is like sitting in a house with the doors unlatched. Each automation and Mac devices are in danger from malicious package offensive and absorbing your life. Continuously introduce a dependable security framework like Norton Security in all your gadgets.

- **Perused the fine print**

Know and get it the security approach and terms of benefit of any benefit you use. A few websites can possess, offer, lease or exchange your information to anybody they need. This will come back as a greater issue and the law may not be able to secure you since you concurred to the terms and conditions.

- **There's no such thing as 'freebies'**

Freebies come as diversions, offers, bargains, etc. They may be perplexed with infection virus, spyware and pernicious computer program. These can get into your gadget and mine all your information.

- **Block individuals you don't need to interact with**

Never feel peculiar declining companion demands from individuals you scarcely know. Believe your intuitive and disregard, unfriend or square them. You get to select who remains on your companion list. When it comes to security, both online and offline, common sense is the primary line of defence.

2.4 Reporting a cyber crime

The strategy for news cyber violations is extra or less a proportionate as for news the other very offense. The nearby police stations can be approached for recording complaints fair as the cyber crime cells specially assigned with the jurisdiction to enlist complaint. In addition, provisions have now been made for filing of 'E-FIR' in most of the states. Women security is a must and the police in our nation must be well prepared to resolve complaints of cyber crime made by women and cognizance of the same must be taken very seriously.

Each police station must have expert-trained police officer who can quickly bargain with cyber crime complaints made. In case a police station denies enlist the complaint, a representation may be given to the commissioner of police/superintendent of police. If in spite of that action isn't taken, the following step seem either be a private complaint before the concerned court or a summons before the high court. "If There's Cyber Crime, Women Begin Reporting Right Now" [2].

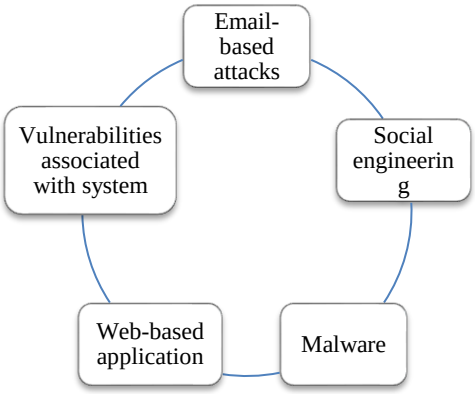

Figure 3:Top Five Attacks Faced

2.4.1 Targets for cyber attackers

There are different frameworks and innovations that are being focused on by attackers, using multiple attack measures. There is steady development towards targeted attacks, which is expanding the like hood of attacks to take place.

Table 1: Targets for Cyber Attackers

Targeted Attacks	Percentage(%)
Identity impersonation	22%
Phishing attacks	61%
E-mail based attack	75%
Malware/Ransom ware	69%
Web-Based applications	33%
Vulnerabilities associated with system	22%
Physical theft of computing devices	22%

2.4.2 Motives of Cyber attackers

Table 2:Motivation Behind Attacks (June-August 2018).

Motivation behind attacks	JUNE 2018(%)	AUGUST 2018(%)
Cyber crime	84.4%	77.5%
Hacktivism	1.0%	1.3%
Cyber Warfare	2.1%	2.5%
Cyber espionage	12.5%	18.8%

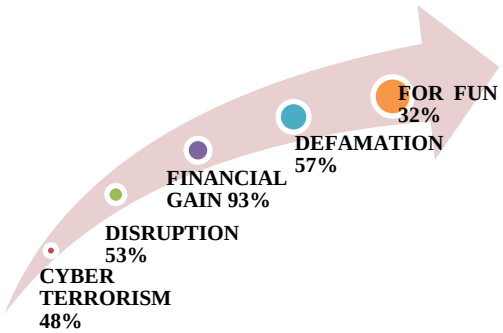

Figure4:Reasons for Cyber Attacks

2.5 NCRB (National Crime Record Bureau)

NCRB information reveals violations against women and outsiders, cases of sedition have diminished whereas human trafficking, cyber crimes have expanded. Human Trafficking-Implies sale of people like goods, including devadasi system, forced labour, sexual slavery and other kind of exploitation.

2.5.1 Reasons for human Trafficking.

1. Poverty
2. Illiteracy and unemployment
3. Political instability and Natural Disasters
4. Demand.

Measures needed to reduce human Trafficking

A. Reducing the vulnerability to potential victims.
B. Holding anti Trafficking festivals in rural areas.
C.Creating sensitisation programme for stakeholders.
D. NGOs can be a game changer in raising awareness campaign in vulnerable areas regarding FIR lodgement and rights for the trafficked.
E. Providing employment and education opportunities to the victim person.
F.A special investigation agency for co coordinating the work between states and collect intelligence on Trafficking.

All such measures require will of all the stakeholders to effectively implement the above-mentioned measures to curb the menace of cyber crimes and human Trafficking.

2.5.2 Cybercrime

Violation of cyber laws and gaining access to personal information for harassing people.
Measures needed

- **Technical -** Recruit cyber specialists for strengthening the cyber security infrastructure of the country.
- **Security**- Establish anti-cyber terror cells in Police stations to take action against offenders.
- **Social**- Increase awareness among people and educate them about loopholes that can be exploited.
- **International**- Sign Mutual Legal Assistance Treaties with countries to punish offenders in case of cross border crimes.

Avoiding human trafficking and cyber crime is within the interest of the country. It will ensure human rights to the individuals and will avoid assaults on basic infra of the country. NCRB information reveals violations against women and non-native's, cases of rebellion have decreased whereas human trafficking, cyber crimes have expanded [5].

2.5.3 Reasons for increased cyber crimes

1. No dedicated cyber laws in India.
2. Cyber security infrastructure in India still missing.
3. Unclear obligation of different stakeholders dealing with data.

2.5.4 Measures needed to Reduce Cyber Crimes

1. Drafting of National Cyber Security Policy of India as soon as possible.
2. Dedicated cyber security laws in India keeping in mind contemporary cyber security threat.
3. Cyber security awareness must be improved in order to involve all the stakeholders for the proper
implementation of cyber security initiatives of GOI.
4. Greater emphasis on R&D of indigenous security technology.
5. PPP VIA a VIS technical and operational co-operation aimed at encouraging organisation to adopt individually tailored IT regulations and infrastructure in conformity with international best practices.
6. Creation of new agency such as National Critical Information Infrastructure Protection Centre to charge with protecting assets in sensitive areas such as defence, telecommunications, finance,energy etc.

2.6 NATIONAL COMMISSION FOR WOMEN (NCW):

NCW(The National Commission for Women) was set up as statutory body in January 1992 beneath the National Commission for Women Act.

• Survey the Protected and Legal shields for women.
• Prescribe medicinal administrative measures.
• Encourage redressal of grievances and.
• Prompt the Government on all approach things
influencing women.

In keeping with its command, the Commission started different steps to progress the status of women and worked for their economic strengthening amid the year beneath report. The Commission completed its visits to all the States/UTs but Lakshadweep and arranged Sex Profiles to survey the status of ladies and their strengthening. It had gottena expansive number of complaints and acted suo-moto in a few cases to supply rapid equity.

According to official sources, the number of complaints of cyber wrongdoing against ladies gotten in National Commission for Ladies (NCW) and the closed appeared that in 2014, complaints gotten were 2009 and closed were 53,223 and 86 in 2015, 311 and 119 in 2016 whereas they were 370 and 250 in 2017 respectively [3].

As per laid down method these complaints are taken up with specialists concerned including police. National Commission for women had given comments on extend" Cyber Wrongdoing Avoidance against women and Children (CCPWC)"beneath Nirbhaya Fund.

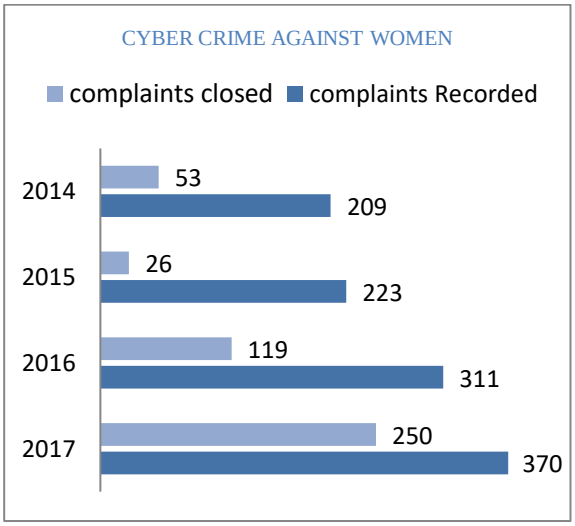

Figure5:Cyber Crime against women by NCW (2014-2017)

The Enabled Committee constituted beneath the Chairmanship of secretary, Service of women and Child Improvement has as of now endorsed the venture" Cyber Wrongdoing

Anticipation against Ladies and Children" (CCPWC) of Service of Domestic.

2.7 Cyber Crime Prevention against Women and Children (CCPWC)

The primary objective of Cyber Crime Prevention against Women and Children (CCPWC) Plot is to have an effective mechanism to handle cybercrimes against women and children within the country.

The plot encompasses a total evaluated cost of **Rs. 223.198 crores** and primary highlights of the scheme are given below

• Online cybercrime detailing platform
• One national level cyber measurable laboratory
• Training of Police officers, judges & prosecutors
• Cybercrime mindfulness activities
• Investigate & Development

The online cybercrime detailing entry www.cybercrime.gov.in has been operationalized and since initiation, more than 3800 complaints have been gotten on it. The helpline for announcing of such complaints beneath the said conspire is however to be operationalized [4].

2.7.1 Most affected

A major consequence of online abuse is the silencing effect it has on women, sometimes forcing them to shut themselves out of online spaces. A survey by Feminism in India, a digital platform, found that 28% of women who experienced online abuse said they intentionally reduced their online presence. Amnesty International conducted a study on online violence against women in 2017 which showed that more than 75% of women surveyed across eight countries *(Denmark, Italy, New Zealand, Poland, Spain, Sweden, the UK and USA)* who had experienced abuse or harassment made changes to the way they used social media platforms. A third of women said they even stopped posting their opinion on certain issues altogether.

Women often find it difficult to report online abuse to the police for several reasons, ranging from not knowing the law to not trusting the criminal justice system. Of the women surveyed by Feminism in India who reported harassment to the authorities, only one in ten said they had received a helpful response**.** The National Crime Records Bureau says that around 12,000 incidents of cyber-crimes were reported in 2016**,** and nearly the same number that were reported the previous year were still pending investigation.

Social media platforms, which are uniquely positioned to take quick and effective action against abusers, are also known to fail to act. **Amnesty's survey** indicated that women feel social media companies need to do more. Just 18% of women polled across all countries said that the responses of social media companies were very, fairly or completely adequate. In India, there have been a number of reports in the media about women who reported online abuse to social media platforms, but received highly unsatisfactory responses.

2.8 Cybercrime Tools

2.8.1 Analysis Tools

These tools are utilized to measure hazard. They measure what an incident did and how it was done and what the results were. Cases of investigation tools include the Coroners Toolkit that runs beneath NIX and Encase that runs beneath windows.

These include a specialized awareness through information of specialized suggestions of activities, an understanding of how data can be modified, cleverness, open-mindedness, deviousness, a tall standard of morals, proceeding instruction and the utilize of excess information sources. In case one doesn't altogether get it or meet the over necessities, the framework can be left distant more regrettable than when at first compromised from a legal angle. It is like a activity cop investigating a murder scene. I would deliver a case of one of the told**" EcCase".** It gives a recognizable Windows Explorer fashion view. The view shows records without changing them in any way, counting free space that contains erased records. The see sheet is additionally exceptionally supportive when sorting through many records. It contains a solid Report see which offer assistance agents

construct a case as they continue. It too permits point and tap record hashing; a priceless apparatus to verify records afterward.

The reason of the ultimate organ of the cyber crimesdivision is to police the web to guarantee that certain cyber crimes can be stopped some time recently their commission. For this reason, the Network Monitoring Centre has been provided with a Network Monitoring Tool, created by I.I.T. Kanpur. It is additionally utilized to permit comparative devices to attain such a purpose.

2.8.2 Machine Learning & Deep Learning basedTools

a) SIEM tool

Machine Learning & Deep Learning based SIEM tool for numerous professionals, SOC still implies SIEM tool and security observing and to a few degrees that's redress as the SIEM tool acts as a core engine of the SOC, which collects the logs from the integrated log sources, forms those logs as per the predefined rule and give the alerts[6].

Since the beginning of the SIEM tool security engineers/analysts are putting in parts of distinctive rules to screen and relate the log information pumped into the SIEM instrument. These rules are included one by one as per the environment necessities[7].

Since of the amount of log data that must be prepared by the SIEM apparatus, it is impossible to generate the rule that can distinguish the anomalies. The next generation SIEM tools will be utilizing machine learning which is basically marrying the rules or algorithms with the measurements that can be utilized for making knowledge-based, intelligent investigation that will deliver prescient noteworthy results [8].

b) Wearing the Hackers Hat — AI primarily based Sandbox

Hackers are constantly ahead of security defence bunches, utilize the innovation to perform investigation of focused on client's environment to spot the vulnerabilities to anticipate exploitability. This same technique security analyst will use by utilizing AI and ML-based sandboxing tool, which will be a proactive approach and a defensive one too. this could offer knowledge-based inputs to the analyst to counter the probable security attacks and shield the system from potential security risks.

A Security Operations Centre (SOC) is characterised each as a group, typically operating in shifts round the clock, and a facility dedicated to and arranged to stop, detect, judge and respond to cyber security threats and incidents, and to fulfil and survey administrative compliance.

All these progressions within the innovation zone don't dispose of the require for making the natural educated decisions by the human brain. We still need to have security investigator to see into the occurrences and finalize the activity plan. The life of these analysts will be made simple by liberating them from the tedious unremarkable tasks and they can utilize their time and intelligence in characterizing and executing the occurrence reaction arrange to decrease the impact.

c) AI and machine learning can boost cyber defences

• As artificial intelligence and machine learning gathers pace, and begins to affect increasingly businesses, it's beyond any doubt to play a greater part in cyber security[11].

• Since the fight with cyber criminals moves so rapidly, machine learning models that can anticipate and accurately identify attacks quickly may well be a genuine boon for InfoSec experts [12].

These models got to be prepared and sharpened. In any case, there's moreover a risk that AI and machine learning may be misused by attackers [9].

3. Conclusion:

According to a survey every month 7000 cyber crimes are happened, but in national crime record bureau less than 1000 crimes have been reported. So, there is huge mismatch between actual crime happen and crimes reported. Cybercrime reporting in India is still in its nascent stage though cyber violence is fast growing. Our laws need to be changed to make them cyber-sensitive as well

as gender-sensitive. Words like lascivious and prurient should be dropped from the concerned Act to make them better secure women's equality and dignity. The perspective of the laws should be to ensure dignity of women and not being in a paternalistic role. Cybercrimes against women needs a holistic approach with change in laws, change in approach of officials and more intense sensitization campaigns involving different sections of society. Indian women netizens are still not open to quickly report the cyber mishandle or cyber-crime. This nature gives the guilty parties the chance to elude after the commission of cyber-crime. The issue would be unravelled only when the victimized woman at that point and there report back or indeed caution the abuser around taking strong activities.

References

[1]The Economic times."Cyber Security Incidents observed in 2017 ", February 2018. [Online]. Available: https://economictimes.indiatimes.com/tech/ites/over-53000-cyber-security-incidents-observed-in-2017/articleshow/62852008.cms

[2] Dhruti M Kapadia." CyberCrimes against Women and Laws in India", November 2018. [Online]. Available: https://www.livelaw.in/cyber-crimes-against-women-and-laws-in-india/

[3]Live mint."cybercrime registered in India" April 2017. [Online]. Available:
https://www.livemint.com/Politics/ayV9OMPCiNs60cRD0Jv75I/11592-cases-of-cyber-crime-registered-in-India-in-2015-NCR.html

[4] United news of India. " cybercrime against women closed in past 4 years", December 2018. [Online]. Available: http://www.uniindia.com/~/more-complaints-of-cyber-crime-against-women-closed-in-past-4-yrs/India/news/1452774.html

[5] Press Information bureau."Cyber Crime prevention against Women and Children ", January 2019. [Online]. Available:http://pib.nic.in/newsite/PrintRelease.aspx?relid=187328

[6] Taslet security." The Rise of Next Generation Security Operation Center**",** December 2017. [Online]. Available: https://medium.com/taslet-security/the-rise-of-next-generation-security-operation-center-ng-soc-266d0522681b

[7] Yash Technologies."Managed Security Operations Centre (SOC) in Cyber security", [Online]. Available: https://www.yash.com/blog/managed-security-operations-center-in-cybersecurity/

[8] LewanTechnology blog. "Reason you need a Security Operations Center(SOC)" may 2018. [Online]. Available: https://www.lewan.com/blog/5-reasons-you-need-a-security-operations-center-soc

[9] Dr VK Saraswat member, NITI ." Cyber Security" .

[10] Panda Security. "Types of Cyber Crimes", August 2018.
[online].Available:https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/

[11] Harold Kilpatrick ,"How will AI and Machine Learning affects Cyber Security " January 2018. [Online]. Available:https://bigdata-madesimple.com/how-will-ai-and-machine-learning-affect-cyber-security/

[12] Kgaogelo Letsebe, portals journalist, "AI and Machine Learning boost Cyber Security Efforts" march 2018.
[online].Available:https://www.itweb.co.za/content/5yONP7EEpGr7XWrb