

Gender Dimensions of Cybercrimes: Why Do Women Get More Easily Trapped in Cyberspace?

Irene George

Adjunct Faculty,

Emirates Institute of Finance, UAE

irene.george155@gmail.com

and

Moly Kuruvilla

Senior Professor of Women's Studies (Retd),

University of Calicut, Kerala

molykuruvilla14@gmail.com

Abstract

Though men and women are equally susceptible to cybercrimes of various forms, they have a gendered dimension, which has not yet received due attention from development scholars or law enforcement officers. The authors have heavily relied upon the analysis of various reports of government agencies and case studies of cyber victimization in the Indian context, especially during the Covid-19 pandemic, to support their arguments. All instances are looked at with a gender perspective that unfolds the actual reasons for women's increasing vulnerability in the cyber world. Gender digital divide; lack of cyber awareness and digital skills; undue victim-shaming against women; and lack of adequate laws against cyber abuse are highlighted as the factors contributing to the escalating cyber abuses against women in the tradition-bound Indian society. The objective of this paper is to critically examine the gendered dimensions of cybercrimes and to propose awareness and policy measures that strengthen women's digital security and empowerment. The authors propose the need for more cyber awareness programmes to women of all ages, along with having a gender perspective while enacting laws and implementing policies to address cybercrimes.

Keywords: Gender Digital Divide, Cyber Victimization, Victim Shaming, Online Education, Cyber Awareness

Introduction

Three major forces influence the development discourses of the 21st century: the web or the internet, women, and the weather or global warming. It has become imperative to discuss the interconnectedness between two of such great forces, especially in a context where the web force happens to be problematic to the women force not only in developing but also in the developed countries. The web or the internet represents a gateway to new ideas and opportunities, a means of self-expression and empowerment, a driving force for innovation and, increasingly, sustainable growth and has become a critical digital tool helping both men and women across the globe (UNESCO, 2013).

ICT and Women Empowerment

ICT has made the global village concept a reality and has provided immense potential for women's empowerment. The ICTs include a gamut of tools like mobile phones, internet, kiosks, community radio, LAN, WAP applications, etc., which enhance the efficiency and productivity of the process by saving on cost, energy and time. Several researchers have acknowledged the vitality of ICTs in women empowerment and overall development (Hegazy Shehata, 2017; Laizu et al., 2010; Nath, 2001; Rauch & Kostyshak, 2009). Whether it be online education, online purchase, calling taxis, net banking, e-ticket booking or e-tax filing, socializing and networking, accessing health facilities or online marketing, the internet has given wings to women to overcome the centuries-old restrictions imposed on them in various spheres and activities.

The webinars at national and international levels and the Google Meets of families and women's groups have become a dream come true for women worldwide. The internet also provides a platform for socializing with like-minded people in the cyber world that actually serves as an opportunity to ventilate the suppressed feelings and issues (Halder & Jaishankar, 2009). This, in turn, has become one of the reasons for the "Me Too campaign" to be so prominent and welcomed by women all over the world and has gained so much momentum. Women today have lots of friends of all genders in their networking sites and groups. Women get connected to large sections of society through social networks like Facebook, WhatsApp, etc. (Bimber, 2000; Ono & Zavodny, 2003; Vijayalakshmi & Bhavani, 2006). Thus, social networking sites have offered women a space to voice their dreams, desires, and dislikes and expose their real selves to what they are and what they want- which, in most cases, is contradictory to the existing notions about womanhood prevalent in society. As opined by Balagopal, 'easy and low-cost availability of the hitherto luxury electronic products like mobile phones have made the life of women richer....it is as though a brave new world is opening for women'(2020, p.128).

The ITU Facts and Figures for 2020 estimates that during the Covid-19 pandemic, the internet bandwidth usage has grown globally by 38%, exceeding the previous year's growth rate by six percentage points (ITU, 2020). The international bandwidth use is much higher in developing countries than in developed ones during 2019-2020. It is also stated that the highest use occurs in Asia and the Pacific, followed by Europe and the Americas.

With the wider use of the internet, the instances of cyber victimisation have also been increasing and have hit alarming rates during the Covid -19 pandemic. Cyber abuse takes different forms and dimensions like phishing scams, ransomware, data breaches, cyber defamation, cyberstalking, cyberbullying, child pornography, sexting, cyber grooming, sextortion, etc. "During this time of emergency and isolation, technology is a fundamental tool for access to information, education, work, and even facilitates access to services for women victims of violence, but it also opens new paths for perpetrators"(World Bank, 2019). Children of all ages spend more time online for education; most employed women work online from home; people of all ages spend more hours online for e-shopping and e-banking; for communication and entertainment purposes, women and men also spend more time on social networking sites. While being confined at home, social media like WhatsApp,

Facebook, Twitter, Instagram, etc., serve as the only means of solace for lonely and frustrated human beings. Spending more time online paves the way for cyber misuse and abuse. During the pandemic, “India was the second most attacked country in the Asia Pacific. Attacks on India made up 7 per cent of all attacks that IBM Security X-Force has observed on Asia in 2020” (Press Trust of India, 2021a, p.1).

Cybercrimes against Women in India

The issues related to availability and access to ICT are getting resolved to a larger extent in recent days, but pose major hurdles to women in developing country contexts. The very enabling environment of ICT and its cyberspace is being turned into a debilitating and dangerous world for girls and women, of all ages across the globe, by the techno-savvy miscreants through cybercrimes. Halder and Jaishankar (2011a) define cybercrime from the perspective of gender and describe ‘cybercrimes against women’ as “crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as the internet and mobile phones”. Both men and women are equally susceptible to cyber attacks of various forms. But these cybercrimes have a gendered dimension, which has not yet received due attention from the development scholars, the public or the law enforcement officers. The present paper analyses such gendered aspects, especially pertaining to Indian society. This paper heavily relies upon the analysis of various reports of government agencies as well as the case diary reports of the second author, who is also a feminist counsellor to whom a large number of women, families and educational institutions seek guidance at times of girls and women confronting a cyber abuse situation. All instances are looked at with a gender perspective that unfolds the actual reasons for women’s increasing vulnerability in the cyber world.

Next to China, India accounts for the largest digital population of 688 million internet users, of which 40% are women. As per the 2019 report of Thomson Reuters, India is the most dangerous place for women to live in. Though the reality behind this statement is being questioned, it is a fact that in India, there is an alarming rise in violence against women in the physical world. This is true in the case of the virtual world also. World statistics show that the majority of victims of sexual cyber abuses are women, and India too is no exception. Internet accessibility has spread all over India, covering the urban, semi-urban, and also under-developed rural areas through the 983 million active mobile phone users (TRAI, 2020) and the 502 million active smartphone users (TechArc, 2020). In India, as elsewhere, with the proliferation of smartphones and social media, women, especially of a young age, are overwhelmingly the victims of rising cybercrimes.

In India, the National Commission for Women received 23,722 complaints of crimes committed against women in 2020, the highest in the last six years (Press Trust of India, 2021b, p.1). The lockdown period has witnessed the ‘cyber pandemic’ with a tremendous rise in cyber attacks, and the number of complaints filed with the police and the National and State Commissions for Women has also increased. According to National Commission for Women (NCW) data, 54 cybercrime complaints were received online in April 2020 in comparison to 37 complaints - received online and by post -- in March, and 21 complaints in February 2020.

The panel is taking complaints online due to the lockdown (Athar, 2020). A hike in the number of cybercrimes is clearly visible during the period March-July 2020, the initial months of Covid -19, as shown in Table 1.

Table 1: Complaints Received by National Commission for Women in 2020

Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
32	21	37	55	73	103	110	68	59	48	42	56	704

Source: National Commission for Women, India (2020)

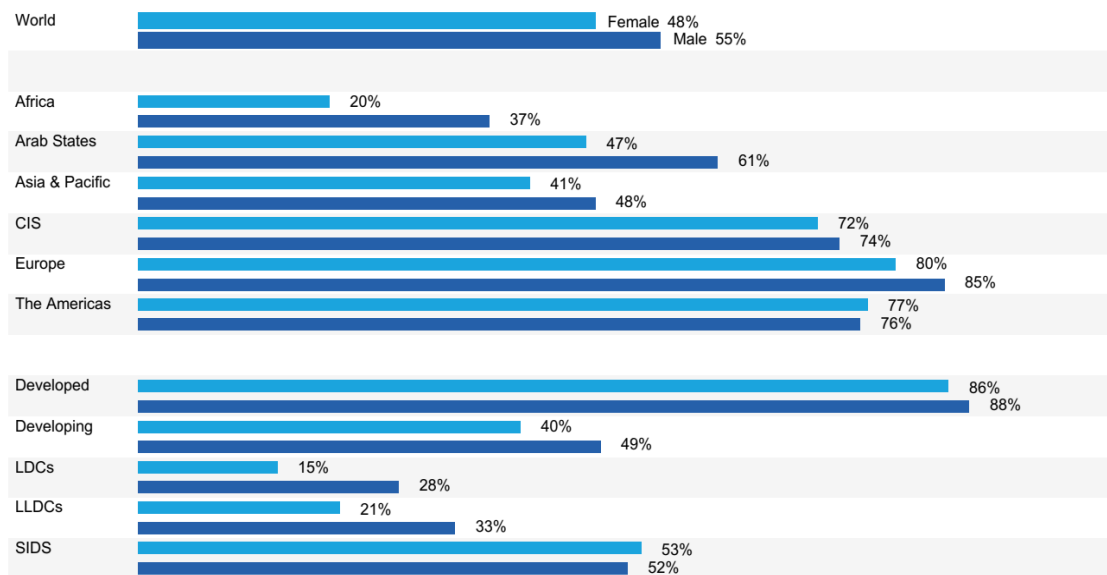
“We received a total of 412 genuine complaints of cyber abuse from March 25 till April 25. Out of these, as many as 396 complaints were serious ones from women (and these) ranged from abuse, indecent exposure, unsolicited obscene pictures, threats, malicious emails claiming their account was hacked, ransom demands, blackmail and more,” said the founder of the Akancha Foundation (Athar, 2020, p.4). It is also reported that “sextortion” (extorting money or sexual favours from someone by threatening to reveal evidence of their sexual activity through means like morphed images) has increased during the lockdown (Athar, 2020). But according to cyber experts, the number of complaints filed is only the tip of the iceberg. The majority of cases remain hidden and unreported because of the stigma mentioned earlier. The authors argue the gender digital divide and the cultural stigmatization attached to women victims as the major reasons for the hike in cybercrimes against girls in developing countries with conservative societies like India.

The Gender Digital Divide

The existence of a gender digital divide is a global reality, and it refers “to the gender gap existing in the structure of opportunities, cultural attitudes and skills related to the use of ICTs” (UNESCO, 2014, p. 50). As suggested by Kularski and Moller (2012), “there are two primary ways in which the gap is enacted, through lack of technical skill and through a physical limitation on access to technology. The digital divide is caused by and reinforces traditional systems of inequality such as race, socioeconomic status and gender” (p.1). Intel’s Report on Women and the Web (Intel, 2012) shows that only 21% of women and girls in developing countries have access to the internet compared to 27% of men, which means that there is a huge gap of around 200 million women who are still not connected to the internet. International Telecommunication Union (ITU) states that the proportion of men using the internet is higher than that of women in two-thirds of the countries worldwide (ITU, 2017) and is estimated as 58% and 48% respectively (ITU, 2019). The gender gap is wider in developing countries, as shown in Figure 1.

Figure 1: Internet gender gap across developing and developed countries

Percentage of female and male population using the Internet, 2019*



Source: ITU, 2020

Differential Access to ICT

Even though the technology itself does not innately discriminate against women, the human context of its usage and application makes access more challenging for women users (UNESCO, 2013). The barriers to successful access and use of ICT's by women users are deeply rooted in the socio-cultural context of the societies where they belong and thus are influenced by factors such as nationality, class, ethnicity, age, and position in society (Purushothaman, 2013). Men start getting access to the cyber world at an age much earlier than their counterparts. Even parents who deny a smartphone to their daughters are happy to secure one for their sons, sometimes much younger than the daughters (George & Kuruvilla, 2021). The fear of traps in the cyber world and ensuring the safety of daughters is a major reason projected by such parents. Thus, women have less access to the digital world, and the majority who don't have a smartphone are women.

The nationwide rapid assessment survey undertaken by the authors in March 2021 (George & Kuruvilla, 2021) has confirmed the existence of the gender digital divide among men and women students in higher education in India.

The gendered roles defined by the culture also strongly influence how women use the technology (Purushothaman et al., 2017). However, it cannot be ignored that there are numerous cases where girls and women are gifted with smartphones by their male friends and the internet connection expenses are also met by the same friends. Very often, the family comes to know about this when the girl gets caught up in some form of cyber or physical abuse.

Lack of Digital Skills

Due to various reasons, women are not as smart as men in protecting themselves from cyber traps. Men engage in more interactions on defence mechanisms and cybersecurity tips than women. Several researchers have revealed how men have better computer literacy, computer efficacy (Stein & Lajmi, 2019; Todman, 2000), lower computer anxiety (Chou, 2003; Jackson et al., 2001; McIlroy et al., 2001) and positive attitudes towards ICT (Durndell & Haag, 2002; Durndell & Thompson, 1997; Jackson et al., 2001; Liaw, 2002). What is suggested by Vekiri and Chronaki (2008) regarding the situation in Greece, where boys report more perceived support from their parents and peers to use computers and more positive computer self-efficacy and value beliefs than girls, is quite true in the Indian context also. Parental support and, to a lesser extent, peer support are the factors more strongly associated with boys' and girls' computer self-efficacy and value beliefs. Also, the majority of those women who know how to browse on the internet or post on social networking sites may not be fully aware of their privacy protection measures or how to use the web effectively and judiciously.

Societal Attitudes towards Women

Morphing and the production of pornography are more centred on women's bodies because of the market value attached to it as a commodity in the globalized society. Also, women's bodies are treated as the sites and objects for victimization in the cyberattacks, just as they are treated in the real world. Such attacks on the body and its features are not applicable in the case of men. Even those who lack a mobile phone or are unaware of the cyber world are at risk of being abused in cyberspace by others who have access to cyber technologies. A typical example is an abuse that happened to the Jarawa tribal women of Andaman and Nicobar islands in 2012, where the innocent and ignorant tribal women were forced to dance completely nude in front of a few visitors. Without their knowledge or consent, their videos were taken and circulated through YouTube (Halder & Jaishankar, 2014). Such abuses are part of the daily lives of several women whose snaps and videos are taken without their knowledge and misused. Even while travelling in a bus or sleeping on the train berth, cameras of miscreants might be haunting women.

There exists a disproportionate stigma and shame between the cyber victimization of men and women in the tradition-bound society of India. If it happens to a woman, she is blamed for it, while if it is a man who is victimized, there is no such shame or blame. This is a matter of socio-cultural beliefs, norms and attitudes where 'moral policing' by society is stricter on women even in cyberspace. Several studies report the non-consensual use of images to shame and blacken the character of women, blackmail and harass young girls. This is especially prevalent in traditional societies that emphasize the chastity of girls.

The fear of being blamed by parents and elders holds back adolescent girls from conveying the threats they face in cyberspace. They may have to succumb to the whims and fancies of the predator who uses the contents of chats and snaps for blackmailing them. The

victim is blamed for the crime, accessing social media and posting pictures, which is considered an inviting or seducing element (Rajendran, 2017). Numerous cases come up daily where married girls are blackmailed with snaps and dialogues they have had during their college days. The purity and chastity that is expected of a girl in Indian society and the double standards followed in this regard are applicable in the cyber world also. Nobody is bothered about the cyber chats of a boy or a man but is much concerned about those of a girl or a woman. It has become a usual pattern in arranged marriages that the chastity of the girl in her thoughts, words and actions are checked on her Facebook by the boy and his family. In some cases, the girl is gifted with a mobile phone by the prospective bridegroom or his family and her online interactions are monitored by them. Meanwhile, the techno-savvy might have cleared his Facebook account neat and clean in accordance with the societal standards of morality.

Lack of Confiding Relationships

In addition to all these, women fall easy victims because of their longing for confiding relations to open up. Because of their secondary social status with restricted mobility and comparatively fewer social relations, women, especially the housewives with a busy husband and children who are all the more engaged in their world of education and career-building and interested in interacting more with their friends only, may face much loneliness and depression. As a consequence, they resort to the internet as a space for recreation and chatting with friends. Still more research is required to unearth the complex reasons why women turn to the internet as a space for solace. Adolescents in broken families or those who crave love and friendship due to a multitude of reasons like lack of love and care from busy parents, parents' indifference, etc., are more vulnerable to the traps in cyber chats.

The tenth-class daughter of highly employed, busy parents was gifted with a mobile phone by the tuition teacher. The chats went on secretly as the girl used to reach home early in the evenings and was left alone with the mobile phone. The parents had cut off the TV cable to facilitate the daughter's intensive studies. They could not foresee the actions of the tuition teacher in providing solace and company to his student (A case study report).

In the modern world, women increasingly find themselves alone and prone to loneliness and depression. Not only adolescent girls but also adult employed women and housewives fall easy prey to cybercrimes in their attempts to overcome loneliness through social networking sites. As opined by Saha and Srivastava (2014), "they have more inclination to spend time on the internet and the social media as a source of entertainment and comfort, but invariably find themselves trapped in a whole new world". With the cyber world opening up to them through ICT, they easily get the chance to interact with strangers through online chat portals, video chat on social media, instant messages, etc., while sitting at home. The privacy of mobile space provides courage to the most introverted and least spoken girls and women to chat with strangers. Women who otherwise are restricted from speaking or

mingling with strangers start confiding in virtual friends without any delicacy and reveal a lot of their personal information, which in turn is used against the women for causing harm through blackmail and through various other ways (Saha & Srivastava, 2014). Most of the time, women are forced to give in to their demands and end up getting victimized. Due to sheer ignorance, women quickly disclose their identity, bank details, property details, details about family members, and exchange photos with a newly found friend on social networking sites.

Citron (2009) proposes the provision of anonymity in cyberspace as a reason for the victimization of women. The mystic sense of secrecy associated with mobile phones motivates both the predator and the prey to open up and discuss issues they dare not do in the real world. Often girls and women are unaware of the fact that there is nothing private or secret in cyberspace.

Lack of Awareness

Girls and women are often confused as to where to stop the unpleasant cyber chats and how to do it. Here starts the cyberbullying, threatening and blackmailing. Women, in general, lack voice and the courage to say 'no' whether it be the physical world or cyberspace. Only when they end up in a real issue do girls and women reveal what has happened. By this time, the harasser will have either escaped or secured ample proof to defend himself. In several complaints of cyber abuses, the miscreants come up with long pages of conversation that the complainants have had with them. The woman won't have any evidence to support her innocence except the last conversation, which has totally shaken her trust.

There are numerous instances where women jump into traps on their own. There are girls and women who know the consequences of interacting with online strangers, but when they feel lonely, they dare to take up and pursue dialogues with miscreants and entertain them to any extent. A typical case study is as follows:

In an engineering college, an M.Tech boy had simultaneous relations with a B.Tech and M. Tech college mate. Both the girls used to send him nude photos in the smartphone handed over by the boyfriend without knowing each other. But when the issue was caught up, the M.Tech girl argued that it is her body, her rights, and she will do whatever she wanted and that the college authorities have no right to question her (Case study report).

Legally, what she said is correct, but the dangers involved in the matter are multidimensional. Without foreseeing the aftermath, girls and women happen to get involved in cybercrimes against themselves.

Differential Nature of Victimization

Men and women are equally susceptible to cyber attacks. Various researchers have found that boys are more likely to be victims of cyberbullying and cyber aggression (Huang & Chou, 2010), whereas others have found that girls experience more types of victimization when

compared to boys (Wachs et al., 2015). In addition, some researchers have found gender differences in cyber victimization to be dependent on cultural contexts. Most women who get victimized are not aware of the consequences of their actions and are naïve and gullible; they fall into various traps, often at the cost of their marriage and family life. This is particularly true in a patriarchal society like that of India (Saha & Srivastava, 2014). Women are often considered the 'weaker' sex by the world at large and are relatively more vulnerable when dealing with attacks through technology and communication in the cyber world. Whatever field a woman may be working in, as a reporter, a politician, or an actress, they are the victim of various types of degrading comments, both in the physical and cyber worlds. Being on social media is never really easy because a woman's public profile can be misused by miscreants to a greater extent than that of a man. Moreover, pictures and photos of a woman's profile on social media or the internet are sometimes photoshopped with the intention of blackmailing and taking revenge. High-profile women who are more vocal are thus silenced by cyberbullies (Pandey, 2020).

Women who lead very silent and lonely lives are also equally vulnerable to cyber abuse, especially cyber grooming. Online grooming (or cyber grooming) is the process of manipulation, rapport building, deception and misuse of trust by which a significantly older offender prepares sexual abuse of a minor by means of ICTs. Here, the ignorance of women is taken advantage of by the bullies (Whittle et al., 2013). In most cases, the cyber harassers have a common pattern of approaching their prey. Beginning with very simple, gentle, positive and motivating conversations, the chats start. This will be followed by sharing of snaps, which is then followed by comments on looks and dresses, then to personal beliefs, feelings and value systems, which gets gradually shifted to sexually coloured remarks, followed by a further exchange of nude snaps and sexual chats. In an age of curiosity and self-appreciation, adolescent girls do whatever is demanded to please the cyber friend, and they dare to do that happily without a second thought. As mentioned earlier, the youngsters seem to be bolder and conscious of their rights regarding bodily integrity and bodily autonomy to go to any extent of impulsive behaviours. But finally, the friendship becomes problematic when the chats end up in unwelcome favours, requests and advances.

There are numerous instances where girls get ready to marry virtual friends they have never met and whose identity they know nothing about except what is told by the cyber friends.

There are also cases where even adult employed females lose all their bank balance and assets to the virtual friends who vanish immediately after handing over all the cash and gold.

Lack of Effective Laws

According to Halder and Jaishankar (2011b), one of the main reasons behind the increase of cybercrimes against women in India is the lesser legal protection. Laws related to cybercrimes in India mainly cover commercial and financial crimes, including hacking, deception, etc. Some laws have been designed for email spoofing, cybersex, trespassing into others' privacy, etc. (Citron, 2009; Halder & Jaishankar, 2011a). "However, the laws related to cybercrimes

against women are correlated to sexual crime and abuses on the internet, but there are many practical difficulties associated with punishing the miscreant” (Saha & Srivastava, 2014, p.63). Studies also show that women are not often aware of the existing laws against cybercrimes (Halder & Jaishankar, 2008). Unfortunately, Section 66A of the IT Act of India 2000, which dealt with “punishment for sending offensive messages through communication services” that could be invoked in complaints of cyber abuse and insults, was struck down by the Supreme Court of India in 2015 on the grounds that it violates the right to freedom of expression. This has created a legal vacuum in addressing cybercrimes against women in the country.

Despite the cyber laws implemented in the country, the delay in getting justice and the fear of getting exposed make women withdraw from filing complaints. Even if the source from which the offensive matter has been posted could be detected, the police find it difficult to trail the offender as it is quite easy for skilled miscreants to manipulate their identities and hide in cyberspace. In addition to this, a girl harassed in cyberspace is further victimized by the media and the public. Recently, a dubbing artist in Kerala had to face a lot of criticism and character assassination in the incident of cyber abuse (Ayyappan, 2020). The lack of effective laws to prevent cybercrimes was widely discussed in this context (Jayarajan, 2020).

Impacts of Cybercrimes

Cybercrimes have a disproportionate toll on women’s mental health and well-being. The study by Cripps and Stermac (2018) in a Canadian context examined cyber-sexual violence, which included non-consensual pornography and other image-based sexual exploitation, online sexual harassment, cyber-stalking, online gender-based hate speech, and the use of a carriage service to arrange/attempt a victim’s sexual assault. It was found that experiences of cyber-sexual violence are associated with symptoms of depression, anxiety, stress, and posttraumatic reactions, regardless of individuals’ disclosure experiences. Culturally, a victim of a morphed picture uploaded on the internet is seen as impure and damaged in the Indian context. The stigma and shame due to cyber victimization have led to the suicides of several girls and women. However, there is a new change through cybersecurity that can help to counter these cyber-attacks on gullible women and even young children. While more and more school and college-going children, adolescent girls and university students are online in the ‘new normal education’, any kind of cyber abuse is likely to demotivate them from further accessing the classes. It can also develop anxiety and depression among youngsters.

Suggestions to Curb Cybercrimes

ICTs are an essential pathway to gender equality and facilitating the attainment of SDG 5. It is necessary to understand that the cyber world is as dangerous and deceptive as it is useful. In order to prevent the proliferation of cybercrimes, measures both at the state level and individual levels are required. A gender perspective must be central to the policies and laws formulated to prevent and redress cybercrimes.

A. Measures to be adopted at the individual level:

- Always protect one’s accounts with a strong password and change passwords as frequently as possible.

- Never disclose personal matters more than what others essentially need to know
- Do not add strangers as friends
- Do not transfer cash or card details to anyone, however close they may seem
- Do not reveal sensitive data like passwords
- Do not discuss things with cyber friends that one does not want to share with parents or teachers
- The moment danger is sensed in cyberspace, it must be reported to parents/teachers /police. Do not wait till the last minute when things get out of control.
- Always remember Google knows everything about a person online- the age, income, qualifications, languages spoken, location, the content and contexts of Google search, the content of emails, the products purchased and a lot more about persons which they themselves might have forgotten.

B. Measures to be adopted at the institutional level:

- As a way forward, girls and women must become aware of the forms and possibilities of traps in the cyber world to prevent the proliferation of crimes against them.
- Both men and women must get familiarized with the privacy protection tips. Awareness campaigns like webinars and workshops are required in large numbers.
- The underrepresentation of women in cybersecurity should be addressed, as more girls and women will be free to open up to women security professionals than the present male officers.
- The cyber laws must be strictly implemented, and speedy measures need to be developed to avoid delays in granting justice, as delayed justice is justice denied.
- The women blaming in instances of women's victimization is to be stopped both in the real world and cyber world, for which gender sensitivity and change in mindsets are inevitable.
- As suggested by Interpol, parents' role in serving as role models and educating the youngsters cannot be underestimated. Awareness generation needs to be a shared responsibility of all concerned, like the parents, teachers, and the public, including the police and the social justice departments.

Conclusion

Despite the IT Act of India, 2000, cybercrimes against women and children are on the rise. In a world of digital technology, denial of mobile phones or other digital means to children and girls is not the solution to prevent the hike in crimes. Each and every individual should be made responsible for his/her safety. This can be done only by having a better and more accurate understanding of cyberspace, the nature of traps and crimes, and the cybersecurity measures to be taken. The 'Digital Literacy Programme' for college/ university students initiated by the National Commission for Women (2018) in India is a positive step in this regard.

It is also necessary to relate cybercrimes to terrestrial crimes, thereby comprehending them better. Those with criminal tendencies utilise much of the technology available today for crimes, whether in the real or virtual world. As far as women are concerned, it is better safe than sorry to avoid disclosing any personal information on the internet. The youngsters, especially girls, should be equipped with better digital skills through awareness campaigns and training to educate them about the legal landscape for reporting cybercrime and safe digital practices to prevent it. For this, a lot more inputs into capacity building of girls and women through legal literacy, media literacy, and digital literacy are essential. Cybercrimes against women should be handled seriously so that the miscreants can no longer hide in the shadow of anonymity.

It may be summarized that the cyber community has to find a way to avoid illegal activities without having to control the freedom of speech and expression. What suggested by the Inter-American Commission of Women (2020) for ensuring women's rights in the western hemisphere seems fully applicable for countries across the globe:

Measures known as the 3 "S" should be adopted to: (i) sensitize, to prevent cyber violence against women and girls through training, learning, campaigning and community development to promote changes in attitudes and social behaviours; (ii) generate safeguards for supervising and maintaining a responsible Internet infrastructure, and having well-founded user care practices; and (iii) enforce sanctions through laws, regulations and governance mechanisms to discourage and/or punish violators from committing these crimes. (p.10)

Gender-responsive measures are to be formulated to stop the cybercrimes that can have demotivating effects while countries worldwide engage in the pursuit of Sustainable Development Goals, especially Target 5.b., which calls for enhancing the use of enabling technology, in particular information and communications technology, to promote the empowerment of women. In the 'new normal' conditions of the Covid-19 pandemic, massive awareness campaigns are essential to straighten the 'cyber pandemic' curve.

References

- Athar, U. (2020, May 1). "Significant" increase in cybercrime against women during lockdown: Experts. *Outlook*. <https://www.outlookindia.com/newsscroll/significant-increase-in-cybercrime-against-women-during-lockdown-experts/1820444>
- Ayyappan, R. (2020, September 29). Bhagyalakshmi and friends versus cyber bullies: What's wrong with law and police. *ONmanorama*. <https://www.onmanorama.com/news/kerala/2020/09/29/youtuber-assault-case-bhagyalakshmi-and-friends-vs-cyber-bullies.html>
- Balagopal, B. (2020). Gender digital divide and technology enabled inclusive strategies. In M. Kuruvilla & I. George (Eds.). *Handbook of research on new dimensions of gender mainstreaming and women empowerment* (126-141). USA: IGI Global. <http://doi:10.4018/978-1-7998-2819-8.ch008>

- Bimber, B. (2000). The study of information technology and civic engagement. *Political Communication*, 17(4), 329-333. <https://doi.org/10.1080/10584600050178924>
- Campbell, N. J. (1990). High school students' computer attitudes and attributions: Gender and ethnic differences. *Journal of Adolescent Research*, 5, 485-499.
- Chou, C. (2003). Incidences and correlates of internet anxiety among high school teachers in Taiwan. *Computers in Human Behavior*, 19(6), 731-749. [https://doi.org/10.1016/S0747-5632\(03\)00010-4](https://doi.org/10.1016/S0747-5632(03)00010-4)
- Citron, K. D. (2009). Cyber civil rights. *Boston University Law Review*, 89(61), 69-75. *Michigan Law Review*, 108, 373-415.
- Cripps, J., & Stermac, L.(2018).Cyber-sexual violence and negative emotional states among women in a Canadian University. *International Journal of Cyber Criminology*, 12(1):171-186. <https://doi.org/10.5281/zenodo.1467891>
- Durndell, A. & Thompson, K. (1997). Gender and computing: A decade of change? *Computers in Education*, 28, 1-9.
- Durndell, A. & Haag, Z. (2002) Computer self-efficacy, computer anxiety, attitudes towards the internet and reported experience with the internet, by gender, in an East European sample. *Computers in Human Behaviour*, 18, 521-535.
- George,I., & Kuruvilla, M. (2021). From conventional classrooms to online platforms: experiences of women students and faculties in Indian higher education during Covid-19 pandemic. In I. George& M.Kuruvilla (Eds.), *Gendered Experiences of COVID-19 in India*(pp.167-195). Springer Nature, Switzerland AG (Palgrave Macmillan). <https://link.springer.com/book/10.1007/978-3-030-85335-8>
- Halder, D., & Jaishankar, K. (2008). Cybercrimes against women in India: Problems, perspectives and solutions. *TMC Academic Journal*, 3(1), 48-62.
- Halder, D., & Jaishankar, K. (2009). Cyber socializing and victimization of women. *Temida*, 12(3), 5-26. <https://doi.org/10.2298/TEM0903005H>
- Halder, D., & Jaishankar, K. (2011a). *Cybercrime and the victimization of women: Laws, rights and regulations*. Hershey, PA, USA: IGI Global.
- Halder, D., & Jaishankar, K. (2011b). Cyber gender harassment and secondary victimization: A comparative analysis of US, UK and India. *Victims and Offenders*, 6(4), 386-398. <https://doi.org/10.1080/15564886.2011.607402>
- Halder, D., & K. Jaishankar, K.(2014). Online victimization of Andaman Jarawa tribal women: An analysis of the 'Human Safari' Youtube videos (2012) and its effects. *The British Journal of Criminology*, 54(4), 673-688. <https://doi.org/10.1093/bjc/azu026>
- Hegazy Shehata, A.M. (2017). Role of information and communication technology in closing gender employment gap in MENA Countries. *The Business and Management Review*, 8(4), 168-178.
- Huang, Y., & Chou, C. (2010). An analysis of multiple factors of cyberbullying among junior high school students in Taiwan. *Computers in Human Behavior*, 26, 1581-1590.

- Intel. (2012). *Women and the web*.
<https://www.intel.com/content/dam/www/public/us/en/documents/pdf/women-and-the-web.pdf>
- Inter-American Commission of Women. (2020). Covid-19 in women's lives: Reasons to recognize the differential impacts.
<http://www.oas.org/en/cim/docs/ArgumentarioCOVID19-EN.pdf>
- INTERPOL. (2020, August 4). *INTERPOL report shows alarming rate of cyber attacks during COVID-19*. <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>
- ITU. (2017). *ICT facts and figures 2017*. <https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx>
- ITU. (2019). *Measuring digital development: Facts and figures 2019*. International Telecommunication Union. <https://news.itu.int/measuring-digital-development-facts-figures-2019/>
- ITU. (2020). *Measuring digital development: Facts and figures 2020*. International Telecommunication Union. <https://www.itu.int/en/itu-d/statistics/pages/facts/default.aspx>
- Jackson, L. A., Ervin, K. S., Gardner, P. D., & Schmitt, N. (2001). Gender and the internet: Women communicating and men searching. *Sex Roles*, 44(5), 363–379.
- Jayarajan, S. (2020, September 29). Why FIRs are delayed in cyber abuse and harassment, Kerala top cop explains. *The News Minute*.
<https://www.thenewsminute.com/article/why-firs-are-delayed-cyberbullying-and-harassment-kerala-top-cop-explains-134138>
- Kularski, C.M., & Moller, S. (2012). The digital divide as a continuation of traditional systems of inequality. *Sociology*, 5151, 1-23.
- Laizu, Z., Armarego, J., & Sudweeks, F. (2010). *The role of ICT in women's empowerment in rural Bangladesh*. In F. Sudweeks, H. Hrachovec & C. Ess (Eds.). *Proceedings of Cultural Attitudes Towards Communication and Technology*, Murdoch University, Australia, 217-230.
- Liaw, S.S. (2002). An internet survey for perceptions of computers and the World Wide Web: Relationship, prediction, and difference. *Computers in Human Behavior*, 18(1), 17–35. [https://doi.org/10.1016/S0747-5632\(01\)00032-2](https://doi.org/10.1016/S0747-5632(01)00032-2)
- McIlroy, D., Bunting, B., Tierney, K., & Gordon, M. (2001). The relation of gender and background experience to self-reported computing anxieties and cognitions. *Computers in Human Behavior*, 17, 21-33.

- Nath, V. (2001). Empowerment and governance through Information and Communication Technologies: Women's perspective. *International Information & Library Review*, 33, 317-339. <https://doi.org/10.1006/iilr.2001.0175>
- National Commission for Women. (2020). *Nature-wise report of the complaints received by NCW in the year: 2020* (Report generated through 43.229.89.174 at 17/07/2021 00:27:47). <http://ncwapps.nic.in/frmReportNature.aspx?Year=2020>
- National Commission for Women. (2018). *Digital Literacy and Online Safety Programme*. <http://ncw.nic.in/basic-page/digital-literacy-and-online-safety-programme>
- Ono, H., &Zavodny, M. (2003).Gender and the internet. *Social Science Quarterly*, 84(1), 111–121. <https://doi.org/10.1111/1540-6237.t01-1-8401007>
- Pandey, G. (2020, July). Sulli Deals: The Indian Muslim women' up for sale' on an app. *BBC News, Delhi*. <https://www.bbc.com/news/world-asia-india-57764271>
- Press Trust of India. (2021a, February 24). India 2nd biggest target of cybercriminals in Asia Pacific in 2020: IBM. *Business Standard*. https://www.business-standard.com/article/current-affairs/india-2nd-biggest-target-of-cybercriminals-in-asia-pacific-in-2020-ibm-121022401585_1.html
- Press Trust of India. (2021b, January 3). NCW received 23,722 complaints in 2020, highest in six years. *The Indian Express*. <https://indianexpress.com/article/india/ncw-received-23722-complaints-in-2020-highest-in-six-years-7131099/>
- Purushothaman, A. (2013). *Empowering women through learning to use the internet: An ethnographic action research project to address the second order digital divide*. Aalborg University, Denmark. http://vbn.aau.dk/files/195244502/Aparna_Thesis_VBN_Upload.pdf
- Purushothaman, A., Holmfeld, L. D., & Kuruvilla, M. (2017). Second order divide in internet usage in developing countries: An overlooked issue? *International Journal of Digital Literacy and Digital Competence*, 8(2), 1–13. <https://doi.org/10.4018/IJDLDC.2017040101>
- Rajendran, A. (2017). *Cybercrimes_and victim_shaming_in_India*. <https://www.researchgate.net/publication/330753191>
- Rauch, J. E., & Kostyshak, S. (2009). The three Arab worlds. *Journal of Economic Perspectives*, 23(3), 165–188.

- Saha, T., & Srivastava, A.(2014). Indian women at risk in the cyber space: A conceptual model of reasons of victimization. *International Journal of Cyber Criminology*, 8(1), 57-67.
- Stein, J., & Lajmi, L. (2019). The impact of self-efficacy and gender on computer performance. In Stephanidis, C., & Antona, M. (Eds.). *HCI International 2019 – Late Breaking Posters. HCII 2019. Communications in Computer and Information Science*, 1088. Springer, Cham. https://doi.org/10.1007/978-3-030-30712-7_16
- TechArc. (2020). *India smart phone trends 2020*. www.techarc.net/reports
- Todman, J. (2000). Gender differences in computer anxiety among university entrants since 1992. *Computers & Education*, 34(1), 27-35.
- TRAI. (2020). Press Release number 17/2020, Telecom Regulatory Authority of India, New Delhi.
- UNESCO. (2013). *Doubling digital opportunities: Enhancing the inclusion of women & girls in the information society*. <http://www.broadbandcommission.org/documents/working-groups/bb-doubling-digital-2013.pdf>
- UNESCO. (2014). *Media and gender: A scholarly agenda for the global alliance on media and gender*. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/publications/media_and_gender_scholarly_agenda_for_gamag.pdf
- Vekiri, I., & Chronaki, A. (2008). Gender issues in technology use: Perceived social support, computer self-efficacy and value beliefs, and computer use beyond school. *Computers & Education*, 51 (3), 1392–1404. <https://doi.org/10.1016/j.compedu.2008.01.003>
- Vijayalakshmi, P., & Bhavani, D. (2006). Internet use, Indian culture and gender variations. *Media Asia-Singapore*, 33(3/4), 202–211.
- Wachs, S., Junger, M., & Sittichai, R. (2015). Traditional, cyber and combined bullying roles: Differences in risky online and offline activities. *Societies*, 5, 109–135. <https://doi.org/10.3390/soc5010109>
- Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of online grooming: Characteristics and concerns. *Aggression and Violent Behavior*, 18(1), 62–70. <https://doi.org/10.1016/j.avb.2012.09.003>
- World Bank. (2019). *The good, the bad and the intersection of gender-based violence and technology*. [https:// blogs.worldbank. org/voices/good-bad-and-intersection-gender-based-violence-and-technology](https://blogs.worldbank.org/voices/good-bad-and-intersection-gender-based-violence-and-technology)