Proceedings of the 2nd World Conference on Women's Studies, Vol. 1, 2016, pp. 1-7

ISSN: 2424-6743 online
DOI: https://doi.org/10.17501/wcws.2016.1101

CYBER VIOLENCE (CRIMES) AGAINST WOMEN AND GIRLS

Nadeesha Adikari

University of Moratuwa, Sri Lanka

Abstract

With the development of Information and Communication Technology, the number of men and women engaged these new technologies is increasing in all over the world including in developed countries as well as developing countries. As Information and Communication Technology plays wider role of their lives, technology related violence also is becoming an issue in the society. According to the report, released by the United Nations Broadband Commission in 2015, reveals that almost three quarters of women online have been exposed to some form of cyber violence. This study is to explain deeply about 'Cyber violence against woman and girls'. The research will help to arouse the public awareness of cyber violence and discus possible approaches to avoid cyber violence. Research methodologies like Literature Review, Meta-Analysis and Systematic Reviews are used throughout this study. This detailed research results the very sensitive statistics of cyber violence against woman and girls and violence avoiding factors like education, laws and appropriate technologies. This study implies a useful source of information and constructive advice for the women and girls who will sense the seriousness and influence of cyber use. Further this topic may have implications on developing e-commence, e-services, social networks and other web-based activities securely.

Keywords: Information and communication technology, cyber, violence

INTRODUCTION

According to (Herring, 2002) Cyber violence is defined as 'online behavior that constitutes or leads to assault against the well-being (physical, psychological, emotional) of an individual or group. What distinguishes cyber violence from traditional off-line forms of violence is that in the former case, some significant portion of the behavior takes place online, although it might then carry over into offline contexts.'

In 1993, the United Nations General Assembly adopted the Declaration on the Elimination of Violence against Women (Yakin, 2009). The Declaration defines violence against women as 'any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life'.

As highlighted by Association for Progressive Communications' statement to the 57th Commission on the Status of Women:

"Violence against women that is mediated by technology is increasingly becoming part of women's experience of violence and their online interactions. In the same way we face risks offline, in the streets and in our homes, women and girls can face specific dangers and risks on the internet such as online harassment, cyber stalking, privacy invasions with the threat of blackmail, viral 'rape videos' and for young women in particular, the distribution of 'sex videos' that force survivors to relive the trauma of sexual assault every time it is reposted online, via mobile phone or distributed in other ways."

As appeared in the above definitions, these cybercrimes can be in several types either in online or offline context due to online behavior. So to control

Corresponding Author: adikari.nadeesha@gmail.com

these kinds of crimes , it is important to check the ways of happening cybercrimes. Then those outcomes will help to distinguish the reasons for the particular cybercrime. Then responsible parties can identify the loop holes on specific areas and work on to avoid those loop holes.

LITERATURE REVIEW

With the advancing of technology , the number of mobile phones users and number of internet users are increasing. Figure 01 shows the variation of internet users among mobile phone users.

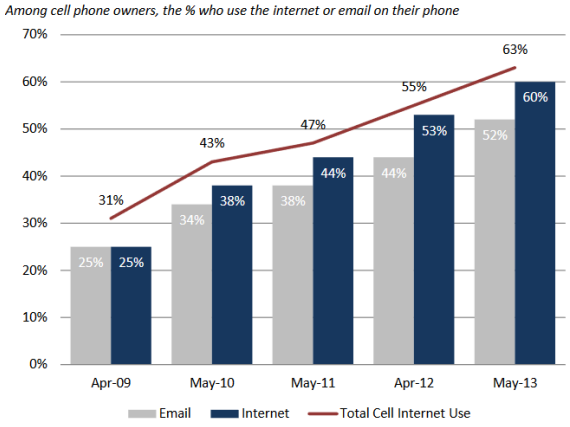

Figure 01: The variation of internet users among mobile phone users

(Source: Pew internet & American Life project spring Tracking survey, April 17 May 2013. Interviews have been conducted in English and Spanish on landline & cell Phones.)

There are more cybercrimes proved in courts all over the world. They are reported in developing countries as well as developed countries. India is a developing South Asian country. There, several cases can be found relevant to cyber violence against women and girls from the literature.

In India's first case of cyber stalking, Manish Kathuria was arrested by the New Delhi Police. He was stalking an Indian lady, Ms Ritu Kohli by illegally chatting on the Web site MIRC using her name. He used obscene and obnoxious language, and distributed her residence telephone number, inviting people to chat with her on the phone. As a result of which, Ritu kept getting obscene calls from everywhere, and people promptly talked dirty with her. The police department traced the culprit and slammed a case under Section 509 of the Indian Penal Code for outraging the modesty of Ritu Kohli (Khurana, 2013).

In another case, an engineering and management graduate, facing prosecution in a dowry harassment case, was arrested by Delhi police for sending obscene e-mails in his wife's name to several persons (Jaishankar,2005) .In June 2000, a man was arrested by the Delhi police for assuming the identity of his ex-employer's wife in a chat channel and encouraging others to telephone. The victim who was getting obscene telephone calls at night from strangers made a complaint to the police. The accused was then located "on line" in the chat room under the identity of the, victim and later traced through the telephone number used by him to access the internet (Jaishankar,2005).

United States of America is one of the powerful developed countries. Percentage of internet users is very high.

In the first successful prosecution under California's new cyber stalking law, prosecutors in the Los Angeles District Attorney's Office obtained a guilty plea from a 50-year-old former security guard who used the Internet to solicit the rape of a woman who rejected his romantic advances. The defendant terrorized his 28-year-old victim by impersonating her in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasized of being raped. On at least six occasions, sometimes in the middle of the night, men knocked on the woman's door saying they wanted to rape her. The former security guard pleaded guilty in April 1999 to one count of stalking and three counts of solicitation of sexual assault. (Frankli, 2006)

Impacts of Cyber Crimes

The effects of cyber violence against women are psychological, social, physical and economic. The most widespread are psychological effects, which are felt by most women who experience cyber-violence. According to the result of study on 'Cyber Bullying as Gender-based Violence Online Survey', 65% of the women in the study reported experiencing some kind of psychological effect, ranging from the most

common, anxiety and damaged self-esteem (by about half and 43% of respondents respectively), to the most extreme, thoughts of suicide and engaging in self-injurious behavior (10% of respondents) (West, 2014) . The effects are apparent in the self-published stories about Daisy Coleman, Annmarie Chiarini and Savannah Dietrich describing experiencing all of the above and other psychological effects. Annmarie Chiarini writes about his insomnia, panic attacks, experience of overwhelming fear that kept her from leaving her house, feelings of humiliation, being diagnosed with PTSD, suicidal thoughts and her attempts suicide (Chiarini, 2013). Savannah Dietrich also faced humiliation, struggled with social anxiety and discomfort with physical touch from men, as well as thoughts on suicide (Pesta,2012).

Not only girls and women who experience cyber-violence against women often face suicidal thoughts and suicide attempts, but sometimes they are also completing suicide, such is the tragic stories of Rehtaeh Parsons, Audrie Pott Amanda Todd. Rehtaeh Parsons' mother Leah Parsons describes how her daughter's experiences with sexual abuse and cyber violence made her struggle with depression, mood swings and substance use (Durante et al, 2013). Speaking of her daughter, Leah Parsons commented, "It was not the rape that sent her over the edge, as horrible as it was ... It is the public humiliation and shame of her peers, and everyone saw a picture of her being raped." (Coleman, 2012) an anonymous woman blogged about how she was lured and sexually exploited as a young teenager in the same way as Amanda Todd. She describes how continuous utilization and extortion of men on the internet and cyberbullying and shaming of her colleagues who found out about it got her to experience depression, panic attacks, feelings of shame, substance abuse and thoughts about suicide. Looking back on her experience, she writes, "I lived in a constant state of shame. I felt like I did not deserve to live. There were many times when I thought about suicide, but I never took the final step."

Daisy Coleman writes of her own damaged self-image, how she has engaged in self-harm and attempted suicide three times in response to the violence she experienced but ends with a statement of resilience and resistance. In her own words, Daisy says: "Since this happened, I've been in hospitals too many times to count. I've found it impossible to love at times. I've gained and lost friends. I no longer dance or compete in pageants. I'm different now, and I can't ever go back to the person I once was. That one night took it all away from me. I'm nothing more than just human, but I also refuse to be a victim of cruelty any longer." (Heller, 2013)

Cyber-violence against women can have serious and detrimental economic impacts for women as well, particularly nonconsensual distribution of images and revenge porn. As Danielle Citron explains, women can lose their jobs over things that get posted about them on the internet, and with the impossibility of ever completely erasing things from the internet, revenge porn images and defamation can haunt women forever, keeping them from being hired for new jobs or advancing in their current job. (Citron, 2014) In the Cyber Bullying as Gender-based Violence Online Survey, 13% of women reported some impact on their job (losing their job, being unable to advance in job or being unable to find a new job). Interestingly, a significant number of women (10%) reported that their credit rating was damaged as a result of online abuse.

Cyber-violence can also coincide, exacerbate or lead to physical violence against women. When the 23-year-old Pennsylvania man's attempts to coerce his ex-partner to return through Facebook threats to expose sexual images of her failed, he waited outside of her house armed with a box cutter and a gun (West, 2014). Likewise, a 31-year-old woman in Seattle who was being cyber-stalked by her police officer ex-partner and found herself the victim of revenge porn, was also choked and pushed to the ground in a physical confrontation with him. 63. 5% of women in the survey reported experiencing physical harm and abuse as a result of online violence, while 3.3% of women reported physical abuse that was exacerbated by online violence. A number of women (12%) also reported experiencing physical illness as a result of violence. The social consequences for women can be very severe, particularly if their entire community is involved with the cyber-violence. In the case of Daisy Coleman, her brother and herself were bullied at school, she was suspended from her cheer leading squad, her mother lost her job, her family was forced to move back to Albany and their home in Maryville was burned

down (Coleman,2012). Likewise for the 33-year-old woman whose ex-partner solicited men on the internet to come rape her, she also moved out of her community, and the affects were felt by her whole family as her children had to switch schools. (Jouvenal, 2013). Rehtaeh Parsons also left school as a result of the cyber-violence and moved to live with her father in Halifax (Durante,2013). According to Focus Group with BWSS Volunteers, interview by the author survey found that 3.3% of women responded that they had to move out of their community as a result of cyber-violence . A common social impact of cyber violence is isolation from friends and family. In that volunteer focus group, one of the volunteers spoke about a caller whose ex-partner was posting things about them on Facebook and how as a result of the things they were saying, some of her friends and family, including her sister, stopped speaking to her. They believed whatever her attacker had posted on Facebook. When the survey conducted by Battered Women's Support Services on "Cyber Bullying as Gender-based Violence Online Survey is considered , this is one of the most commonly reported social impacts with 28% of women responding that they experienced isolation from friends and family as a result of cyber-violence.

Isolation from friends and family is very serious for women, and the threat of exposing information that could potentially cause women's friends and family to turn against them is taken very seriously by women. Often women will comply with their abuser's threats in order to avoid such repercussions, as was the case for one woman who talked to one of our volunteers on the crisis line. Her abuser knew how afraid she was of her family finding out about her work as an escort and used that to coerce her to have sex with him on demand ([8]-71). The most common social impact reported by women is withdrawing from online activity, with 40% of women reporting that they have experienced this as an impact of cyber-violence . (West, 2014) One respondent explains:

"I began blogging as a way of disengaging from an already violent environment for women of color, but over time, while I did manage to gain a support group, it's also negatively impacted my well-being such that I often have to remove myself from the community or "blank out" the blog to be safe from certain people."

According to Focus Group with Women Accessing BWSS Services, interview by the author, Vancouver on April 3,2014 the women in that focus group for women who access services at BWSS also felt this impact the most (West, 2014). Having experienced abusive relationships in the past, all of the women avoided using social media and online platforms in order to keep themselves safe. They were very afraid of the possibility of people online using their personal information against them, violating their privacy and becoming the victims of bullying and violence. However, avoiding online activity to keep safe also meant that they were left out of online social networks and the significant amount of socializing that takes place online in our society. Therefore, the real social impact of withdrawing from online activity is often social isolation.

Cyber Crimes in Sri Lanka

The government is drafting new laws to address emerging crime trends involving cyberspace as they cannot be curtailed under the existing legal framework. The CID (Computer Crimes Division) is to establish 22 new units under each SSP division to address computer related crimes.

The need for Internet privacy laws is felt when the norms of data protection are violated, According to Information and Communication Technology Agency of Sri Lanka (ICTA), emphasizing that Sri Lanka has no specific laws on Internet privacy.

Therefore the government has begun policy level discussions at the initiative of ICTA on Internet privacy laws and data protection. The process of formulating the draft is in progress. Privacy laws count on how information is collected, processed and transferred to the third party.

The Sri Lankan Computer Crimes Division of the Computer Crime Division set up under the Computer Crimes Act 2007 deals with an increasing number of complaints on email scooping and privacy violations. The division has investigated over 100 on internet related crimes, including 50 complaints of cyber deformation, 21 complaints related to obscene publications and another 22 related to email hacking this year on women and girls.

Another 2,000 complaints involving Facebook and Twitter were reported to the Computer Emergency Readiness Team (CERT) in the first seven months of this year. Most incidents had occurred on Facebook, and primarily involved in the use of fake profiles.

Cyber Violence (Crimes) Categorizing

By considering literature and selected case studies, cybercrimes can be identified under main categories in higher level. These categories are defined with under different names. Therefore this study will describe these different types of cybercrimes. Although these violence categories have been described in simple terms , some of the outcomes of this kind of incidents are very crucial.

- Malicious Distribution

Manipulating and Distributing defamatory and illegal materials related to women and girls can be identified as malicious distribution. There are threatening or leaking intimate photos/video using the advance of cyber space.

- Recruitment

Recruitment is lure potential victims (girls and women) into violent situations using the technology. As examples sharing fake advertisements and postings, traffickers using chat rooms

- Harassment/Spamming

Harassment or Spamming is most probably not an isolated incident. It is an ongoing behavior to continuously contact, annoy, threaten, and/or scare the victim using the freedom of advance of technology freedom.

- Surveillance/Tracking

In this type of cybercrime, the technology is used to stalk and monitor a person's activities and behaviors either in real-time or historically. GPS tracking via mobile phone without permission is a better example for this type of cyber violence.

- Impersonation

Impersonation is the use of technology to assume the identity of the victim or someone else in order to access private information, embarrass or shame the victim, contact the victim, or create fraudulent identity documents. Calling victim from unknown number to avoid call being blocked.

- Hacking

Hacking is the most common violence appeared through technology. It can be defined as gaining illegal or unauthorized access to systems or resources for the purpose of acquiring personal information, altering or modifying information, or slandering.

- Cyber-stalking

cyberstalking is a violation of privacy is a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant messaging (IM), or messages posted to a Web site or a discussion group. A cyber-stalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected.

- Cyber Bullying

Cyberbullying is the act of harming or harassing via information technology networks in a repeated and deliberate manner. According to U.S. Legal Definitions, "cyber-bullying could be limited to posting rumors or gossips about a person in the internet bringing about hatred in other's minds; or it may go to the extent of personally identifying victims and publishing materials severely defaming and humiliating them

- Morphing

Morphing is a special effect in motion pictures and animations that changes (or morphs) one image or shape into another through a seamless transition. Most often it is used to depict one person turning into another through technological means or as part of a fantasy or surreal sequence by an unauthorized user. As an example, It was observed that female's pictures are downloaded from websites by fake users and again reposted/uploaded on different websites by creating fake profiles after editing them.

- Email spoofing

E-mail spoofing is a term used to describe fraudulent email activity in which the sender's address and other parts of the email header are altered to appear as though the email originated from a known or authorized source. By changing certain properties of the email, such as its header, from, Return-Path and Reply-To fields etc., hostile users can make the email appear to be from someone other than the actual sender.

ANALYSIS AND RECOMMENDATION

Each The main challenges in facing cyber space are not having cyber security or cyber strategies. Because Information communication systems and their usage is becoming very complex. But the attention paid for information security is insufficient.

- Improving knowledge about cyber space

When some cases are carefully analyzed, it is possible to convey that some of those violence has occurred due poor knowledge on cyber usage. The Figure 02 show the results of online survey conducted related to opinions on the internet in year 2014 over average of seventeen years by BBC world and GlobeScan Poll. There we can see that 13% of users believe that the internet is a safe place to express their opinions.

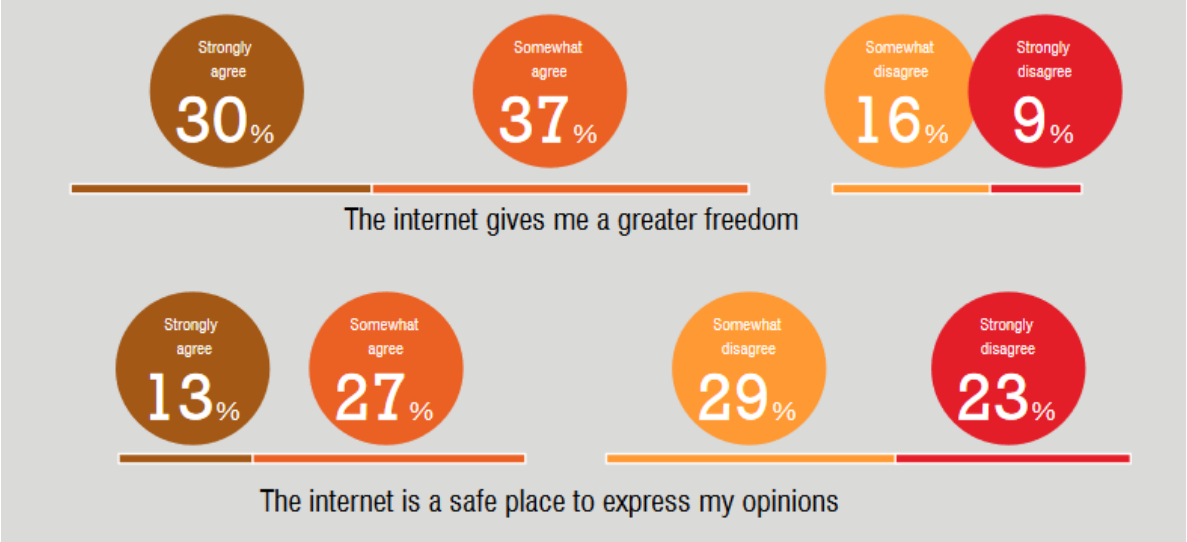

Figure 02: The results of online survey conducted related to opinions on the internet in year 2014

- Make victims to report the cyber crimes

Cybercrimes are happening daily all over the world. But few of them are reported. Some severe crimes are also not reported. Sometimes they are reported late. Then the actions that can be taken to avoid those crimes are limited. Therefore all the victims should allow to report the crimes.

- Increase and monitor quality of applications and systems in cyber space

With the development of technology , various systems and applications are increasing in the cyber space . But quality of some of those application are not guaranteed. Some system developers only focus on earning money through these. These kind of matters lead to the low quality of the applications. Therefore the quality and security of cyber space should be thoroughly accessed.

- Weakness and unavailability of law

Countries in all over the world have different acts laws within the countries. But there are no proper

laws to overcome the cybercrimes in some countries. On the other hand some legal coverages are not up to date. The relevant laws and acts on cybercrimes must be upgraded and changed with the time, because with the development of the technology, nature of the crimes is changing.

REFERENCES

Chiarini A, 2013, The Comment is free, Date of access: 01/04/2016 http://www.theguardian.com/commentisfree/2013/nov/19/revenge-porn-victim-maryland-law-change

Citron D, 2014, 'Revenge Porn' Should Be a Crime, CNN, Date of access: 01/05/2016, http://www.cnn.com/2013/08/29/opinion/citron-revenge-porn/index.html?hpt=hp_t4.

Coleman, 2012, "Like Amanda Todd, I Was Blackmailed with Naked Pictures at 16," Date of access: 20/04/2016

http://www.xojane.com/it-happened-to-me/it-happened-to-me-i-was-blackmailed-with-naked-pictures-at-16-years-old.

Durante T, Bates B (2013), MailOnline, Date of access: 20/04/2016

http://www.dailymail.co.uk/news/article-2308762/Rehtaeh-Parsons-Tragic-tears-Rehtaeh-Parsons-mother-buries-teenage-daughter-killed-bragging-rapist-posted-picture-ordeal-online.html

Franklin, C. J., 2006, The Investigator's Guide to Computer Crime, (USA, Charles C Thomas).

Herring, S. C., 2002. Cyber Violence: Recognizing and Resisting Abuse in Online Environments. Asian Women 14 (summer): 187-212.

Jaishankar, K., Sankary, V. U., 2005, Cyber stalking: A global menace in the information super highway, ERCES Online Q.Rev. , 2(3). Jouvenal J, 2012 "Stalkers Use Online Ads as Weapons Against Victims," Washington Post, Date of access: 01/05/2016, http://www.washingtonpost.com/local/i-live-in-fear-of-anyonecoming-to-my-door/2013/07/14/26c11442-e359-11e2-aef3-339619eab080_story.html

Khurana, R., 2013, Dispute Settlement for Cyber Crimes in India: An Analysis for Interdisciplinary Perspectives on Business Convergence, Computing, and Legality, (IGI Global, India) pp. 161- pp163.

Li y, 2014, Morphing communications of Cyber-Physical Systems towards moving-target defense, 2014 IEEE International Conference on Communications (ICC), Sydney, pp 592 – 598.

Pesta, A. (2012), Thanks for Ruining My Life, News week, Date of access: 30/03/2016 http://www.newsweek.com/thanks-ruining-my-life-63423

Statement to the CSW 57th Session, The Association for Progressive Communication, Date of access: 01/04/ 2016. https://www.apc.org/en/pubs/briefs-technology-related-violence-against-women-2

West, J., 2014, Cyber-Violence Against Women,Battered Women's Support Services Report. Date of access: 01/04/ 2016. Available at http://www.bwss.org/wp-content/uploads/2014/05/CyberVAWReportJessicaWest.pdf

Yakin E, 2009, 15 Years of The United Nations Special Rapporteur On Violence Against Women, Its Causes and Consequences (1994-2009) - A Critical Review, UN Human Rights Council, Report of the Special Rapporteur on Violence against Women.