Women and cybercrime in Kenya: the dark side of ICTS

Working document v1

Research Team

Alice Munyua alice@apc.org
Muriuki Mureithi – mureithi@summitstrategies.co.ke
Grace Githaiga- ggithaiga@hotmail.com

- -

Acknowledgements

Table of contents

INTRODUCTION AND BACKGROUND

The use of cyber space and its attendant features of anonymity continue to influence both positively and negatively on social, economic, cultural, and political aspects of every society. Nevertheless, while the cyberspace have provided secure tools and spaces where women can enjoy their freedom of expression, information and privacy of communication, the same benefits of anonymity and privacy also extend to those who employ ICTs for criminal activities and use the internet to commit violence against women. The use of mobile phones and internet to stalk, abuse, traffic, intimidate and humiliate women is palpable in developing countries including Kenya. The lack of specific cybercrime/cyber security legislation makes it even more difficult to punish those who use ICTs tools to conduct violence against women. While, the review of the Kenya Communications Amendment Act, enacted in January 2009, begins to deal with the problem, it does not explicitly deal with all cyber crime and cyber security issues on the person and specifically women.

With increased access to broadband, which will translate to increase in use of ICTs and the internet in particular, it is has become very urgent to ensure that policy and regulation is developed to address issues of cyber violence against women.

This study commissioned by KICTANET as part of the GRACE Project supported by the International Development and Research Center (IDRC) attempts to provide evidence based framework to address cybercrime against women in Kenya and by extrapolation the East African Community Member states.

STATEMENT OF THE PROBLEM

The emergence of the ICTs provides an unrivalled opportunity for women to exploit their capabilities to improve their quality of life as well as the contribution for the welfare of the society.

Development of cyber security policy and legislation that recognises the special needs of women and provides safe space for them to communicate freely and effectively to contribute to their social economic, political and cultural development.

The assumptions is that while ICTs have contributed immensely to addressing gender inequalities they have also exacerbated existing structures of inequality by enabling cybercriminals to access and misuse them to abuse, harass and violate women, and as a result continue to reinforce existing structures of inequality. Women's contribution to social economic, political and cultural development is therefore limited due to fear of virtual harassment abuse, and violence.

Emerging crime threaten to take away the safe and secure space and denying women the ability to appropriate ICTs for their empowerment and development due to safety concerns.

OBJECTIVES OF THE STUDY

The general objective of this study is to contribute to development of cyber security legislation and regulatory framework in Kenya in order to provide a secure safe space, for women to exercise their right to communicate without fear of abuse, harassment, and violence. In order to achieve this larger goal the specific objectives are to:

1. Investigate the prevalence of cyber crime against women
2. Explore how cyber crime affects women differently.
3. Examine measures to address cyber crimes toward women (what are the measures in place or being developed by authorities, regulators, globally etc).
4. Determine mechanisms of engaging stakeholders to begin to address cyber crime against women.

RESEARCH QUESTIONS

The study will seek information to address the following questions:

1. What is the prevalence of cybercrime against women in terms of degree, level, quantity, and distribution?
2. How does cyber crime affect women differently? (Demonstrate spiral effect and determine if women are already intimidated by cyber space e.g. mailing lists, how active do women participate in debates? Is the design of the cyber already woman unfriendly?)
3. What are the current measures and gaps (technological, legal, social, and psychological) to address cyber crime against women (local, regional, and global)? Map the efforts (lessons of best practice).
4. What mechanisms are appropriate for addressing cyber crime against women?

IMPORTANCE OF THE STUDY

The study will provide evidence for development of cyber security/crime policy and regulatory framework that acknowledges and considers cyberspace violence against women and create awareness on cybercrime against women amongst various stakeholders. The study is therefore of importance to the government/ governmental agencies, international organisations, women organisations, media among others as described below.

1. Communications Commission of Kenya (CCK) and the government generally has a specific mandate to facilitate access that leads to increased use of the cyberspace. Any obstruction to access to any segment of the society is of interest to the government with a view to address the obstruction. The output of the study will create the necessary awareness and propose a policy and regulatory framework to begin to address cybercrime

2. ICT Operators/service providers provide the cyberspace intended for gainful applications by their clients. Those engaging in cybercrime affect and indeed inhibit the use of cyber space. Inhibiting use through cybercrime results in increased operational costs occasioned by measures to mitigate the impact (legal, administrative, financial, and social). The outcome of the study will provide a framework to explore a strategy to address threat to increased use of the cyberspace

3. International community (ITU, ICANN, IETF) need to develop global standards for interoperability of networks since by its very nature the cyberspace is global. Cybercrime and the misuse of the cyberspace are global. While the study will draw heavily on the international experiences, it will seek to contribute to the international community that is developing standards and frameworks to enhance its use.

4. Women and their representative organizations are directly affected and access to use of the cyberspace inhibited. In certain cases, women are not able to communicate and have to use meagre resources to mitigate social vice as opposed to development. Most of the previous research efforts have focused on the crime against the child, against property and against government. This work puts the woman at the centre of the study.

5. Legislature needs to enact the necessary legislation to curb misuse of the cyberspace. This study attempts to provide evidence based input to inform legislation development

6. The Media is a critical stakeholder to create awareness to all other stakeholders. This is an opportunity to provide the much needed empirical data as a basis of awareness raising

7. The study will be of interest to the academia. A key outcome is understanding areas of further research that will result out of the study

SCOPE OF THE STUDY

The study is both spatial and the contextual. Primary data will be collected in and around Nairobi. At the contextual level, the study will restrict itself to cyber world. It will review crimes that originate from the brick and mortar world and taken to the cyber, and new ones entirely originating from the cyberspace.

LITERATURE REVIEW

Literature review will seek to bring out the existing body of knowledge relevant to cybercrime and women, critic the work and identify gaps. These gaps motivate the study to advance the body of knowledge on cybercrime and women.

INTRODUCTION TO THE LITERATURE REVIEW

The literature review illustrates the work undertaken in the area of cybercrime and women and the measures taken to address the vice as a deterrent to safeguard use of cyberspace by women. To get a deep insight in this area, the literature review sheds insight on the features of perpetrators of cybercrime, the victims of cybercrime, and the environmental features that foster the commission of the crime and, finally the strategy and measures being taken to address the vice.

Cyber crime is an area of interest and therefore widely addressed by many scholars and stakeholders. This is not the case for the cybercrime against women. The little literature available for the research and virtually nothing for Kenya and Africa generally is a testimony for a need to raise awareness on the issue.

The context of the literature review is to learn from the existing body of knowledge and create awareness of the need for continued investment of resources and time to understand the vice and measures to address it.

CONCEPTUAL FRAMEWORK

The main variables are the perpetrators, the victims, the environmental factors and a strategy to address the vice and its impact on the women's appropriation of the cyberspace. Figure 1 illustrates the interrelations of the variables.

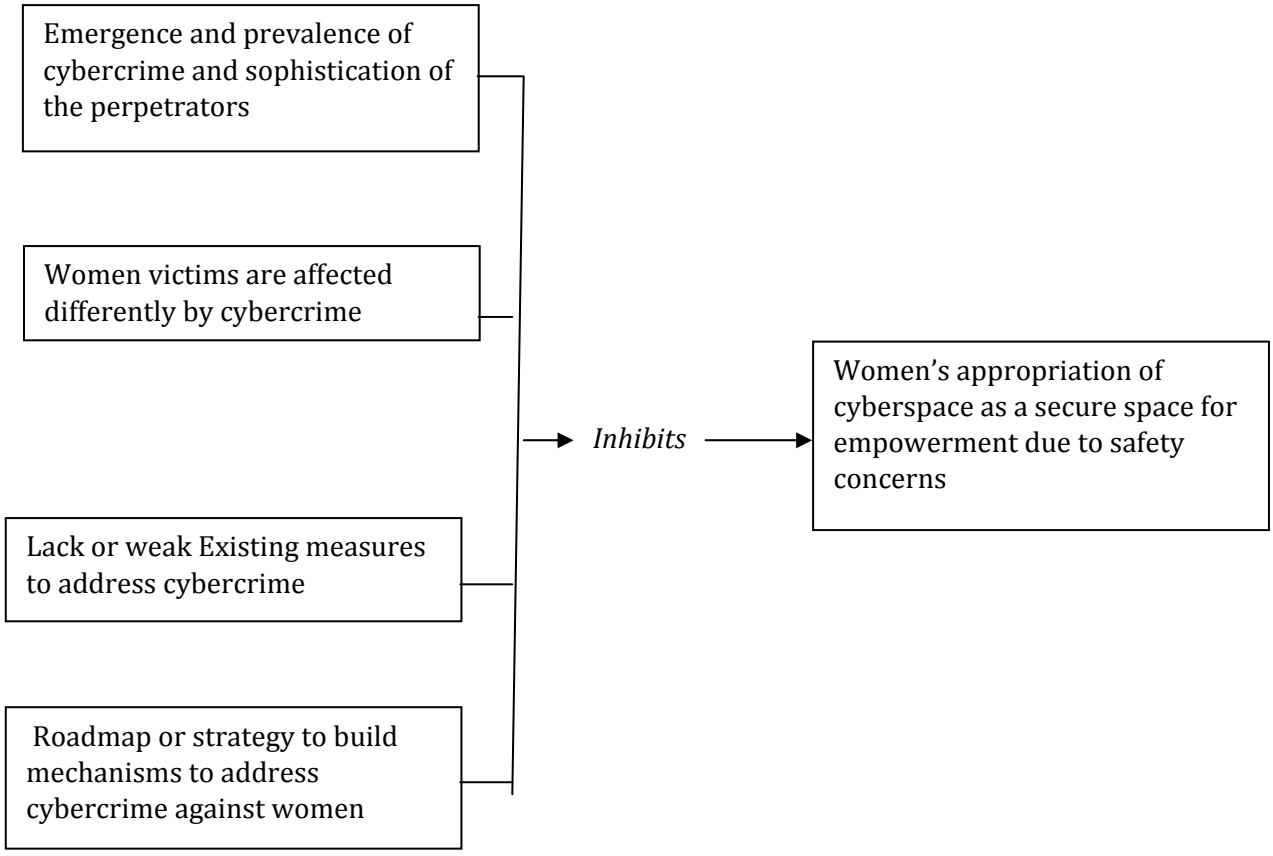


FIGURE 1: INTERRELATIONSHIPS OF VARIABLES ON CYBERCRIME AND WOMEN

REVIEW OF PAST STUDIES IN THE AREA

WHAT IS THE PREVALENCE OF CYBERCRIME AGAINST WOMEN IN TERMS OF DEGREE, LEVEL, QUANTITY, AND DISTRIBUTION?

CYBERCRIME AGAINST WOMEN

Cybercrime can broadly be defined as any activity on the internet that offends human sensibilities. Cybercrime can be divided into 3 major categories namely;

- Against the person
- Against property
- Against government (Dugal n.d)

The focus of this research is cybercrime against the person and in particular against the woman.

Cybercrime against the person includes transmission of child pornography, harassment, and cyber stalking. The latter two are of special interest to the woman and therefore the focus of this paper. The anonymity of the internet provides a safe haven for the perpetrator by hiding their identity. Indeed, cyber stalker's identity can be concealed by using different ISPs and/or by adopting different screen names. More experienced stalkers can use anonymous remailers that make it all-but-impossible to determine the identity of the source of an e-mail or other electronic communication.

Cyber harassment perpetrated through the use of the cyberspace can be sexual, racial, religious, etc. The consequence of harassment is the violation of privacy which the cyberspace grants to a woman.

According to a report by US Department of Justice (USDoJ) cyber stalking is online harassment using Internet, e-mail, or other electronic communications devices to stalk another person. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property. Most stalking laws require that the perpetrator make a credible threat of violence against the victim; others include threats against the victim's immediate family; and still others require only that the alleged stalker's course of conduct constitute an implied threat. While some conduct involving annoying or menacing behavior might fall short of illegal stalking, such behavior may be a prelude to stalking and violence and should be treated seriously (USDoJ 99).

While definitions are still evolving, it is noteworthy that there are similarities and differences between online and offline stalking as illustrated in table 1.

TABLE 1: OFFLINE VS ONLINE STALKING -- A COMPARISON

Major Similarities	**Major Differences**
• Majority of cases involve stalking by former intimates, although stranger stalking occurs in the real world and in cyberspace. • Most victims are women; most stalkers are men. • Stalkers are	• Offline stalking generally requires the perpetrator and the victim to be located in the same geographic area; cyber stalkers may be located across the street or across the country. • Electronic communications technologies make it much easier for a cyber stalker to encourage third parties to harass and/or threaten a victim (e.g., impersonating the victim and posting inflammatory messages to bulletin boards and in chat rooms, causing viewers of that message to send threatening

generally motivated by the desire to control the victim.	messages back to the victim "author.") • Electronic communications technologies also lower the barriers to harassment and threats; a cyber stalker does not need to physically confront the victim.

Source: USDoJ (99)

The incidence of the crime is real and has been proved in courts as cited in India resulting in the convictions:

> In India's first case of cyber stalking, Manish Kathuria was recently (sic) 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 (Indianchild, 2005).
>
> 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 (Mishra, 2001)
>
> 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 (Mishra, 2001).

Source: Jaishankar, & Sankary,

The USA leads in cybercrime against the person largely because of the high usage of the internet. As early as 1999, the US Attorney General reported convictions on cybercrime. A typical cyber stalking case is cited below:

> 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. Source; USDoJ (99)

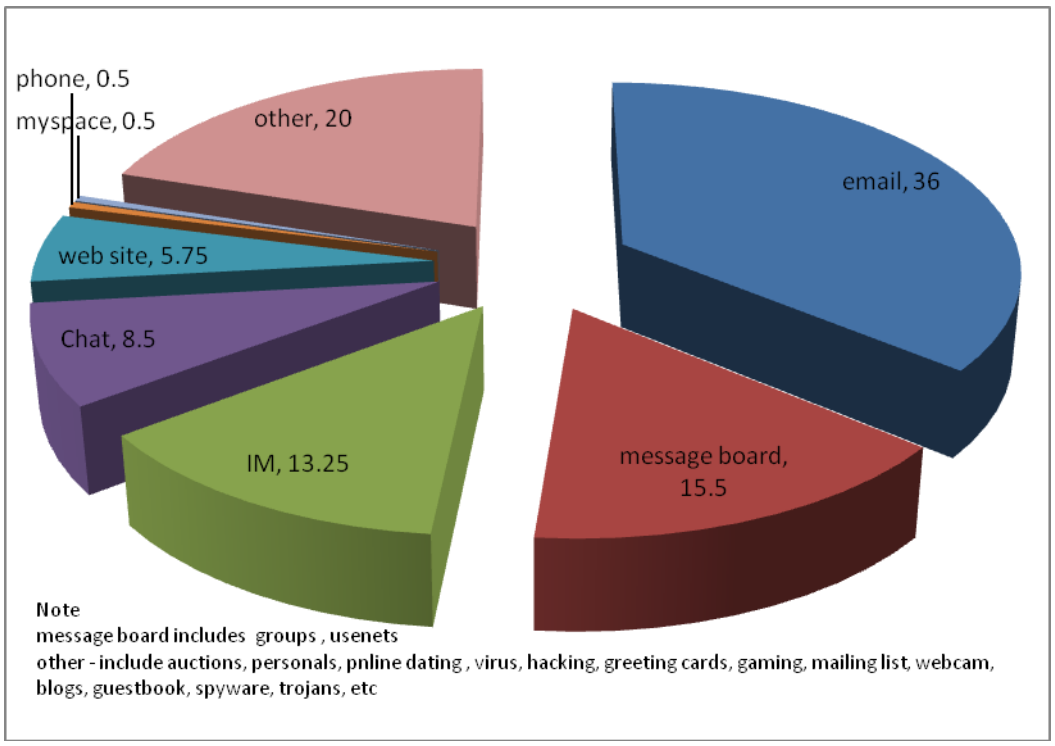
Cybercrime against women is real as demonstrated in foregoing using a range of tools to perpetrate the crime.

TOOLS OF PERPETRATION

Cyber stalkers use increasingly sophisticated means to target and harass their victims using websites, chat rooms, discussion forums, open publishing websites (e.g. blogs) and email. There are three primary ways in which cyber stalking is conducted

- Email Stalking: Direct communication through email.
- Internet Stalking: Global communication through the Internet
- Computer Stalking: Unauthorized control of another person's computer (Jaishankar, & Sankary, nd)

In terms of the prevalence of use depicting how the harassment begin, a a volunteer organization founded in 1997 to fight online harassment through education of the general public, education of law enforcement personnel, and empowerment of victims Working to Halt Online Abuse (WHOA) provides statistics of self reported cases on cyber stalking. The data between 2000-2008 indicate that the email is the most popular method used by online perpetrators to commence harassment as illustrated in fig 2:



Source; WHOA (www.haltabuse.org)
FIGURE 2: HOW HARRASSMENT BEGUN (%)

According to the statistics published by WHOA, phone and MySpace are a recent phenomena reported first in 2008. Other tools have been reported since 2000.

A report by US Attorney the Vice President in 1999, illustrates how the cyber stalker use internet tools for cyberstalking. A cyber stalker may send repeated, threatening, or harassing messages by the simple push of a button. Cyber stalkers that are more sophisticated use programs to send messages at regular or random intervals without being physically present at the computer terminal. In addition, a cyber stalker can dupe other Internet users into harassing or threatening a victim by utilizing Internet bulletin boards or chat rooms. For example, a stalker may post a controversial or enticing message on the board under the name, phone number, or e-mail address of the victim, resulting in subsequent responses being sent to the victim. Each message -- whether from the actual cyber stalker or others -- will have the intended effect on the victim, but the cyber stalker's effort is minimal and the lack of direct contact between the cyber stalker and the victim can make it difficult for law enforcement to identify, locate, and arrest the offender (USDoJ 99).

CHARACTERISTICS OF PERPETRATORS AND THE VICTIMS

Self reports to WHOA between 2000 -2008 indicate that the cyber stalkers are predominantly men representing 49.5% while women cyber stalkers were

significant at 28.5%. Thus, women are a significant contributor to cyber stalking. The victim is clearly the women, 72.5% of the victims were women while men accounted for 22% of the cases as illustrated in table 2

TABLE 2: GENDER OF THE HARRASSER ADN THE VICTIM (%)

	Harasser	**Victim**
Men	49.5	22
Women	28.5	72.5
Multiple gangs	1.5	
unknown	21.5	5.5

Source: WHOA (www.haltabuse .org)

Other reports concur that men are predominantly the perpetrators and the women are the victims (see USDoJ, Kathar, Duval). Other features of the crime include:

- Up to 44% of the victims were between 18-30 years with the rest being over 31 years old.
- Of the victims, 34.75% were single while 25.25% were married.
- In 49% of the cases, the victim knew the harasser who was an ex (34%), friend (14.25%) or online acquaintance (17.25%).
- In 71% of the cases, the cyber stalking did not result in offline threats. Nevertheless the 29% offline threats is significant representing one in three cases.
- In 67.75%, the victim reported the threat and the most important reporting agency was to the law enforcement followed by harassers' ISP and the web administrator.

The data suggest that the cyber stalking is significant and needs serious attention.

TYPOLOGY OF STALKERS:

According to Jaishankar & Sankary(nd), cyber stalkers can be categorized into five types. This is based on a A multi-axial typology developed by Mullen et al (1999) who assessed convicted stalkers in an Australian mental health unit. The axes included an examination of the stalkers' predominant motivation and the context in which stalking occurred, information about the nature of the prior relationship with the victim, and finally, a psychiatric diagnosis. They classified five types of stalkers:

- The rejected stalker has had an intimate relationship with the victim (although occasionally the victim may be a family member or close friend),

and views the termination of the relationship as unacceptable. Their behavior is characterized by a mixture of revenge and desire for reconciliation.

- Intimacy seekers attempt to bring to fruition a relationship with a person who has engaged their desires, and whom they may also mistakenly perceive reciprocates that affection.
- Incompetent suitors tend to seek to develop relationships but they fail to abide by social rules governing courtship. They are usually intellectually limited and/or socially incompetent.
- Resentful stalkers harass their victims with the specific intention of causing fear and apprehension out of a desire for retribution for some actual or supposed injury or humiliation.
- Predatory stalkers stalk for information gathering purposes or fantasy rehearsal in preparation for a sexual attack (Jaishankar & Sankary n.d).

The other types of stalkers are (Bully online, 2002):

- Delusional stalker: this one has a history of mental illness which may include schizophrenia or manic depression. The schizophrenic stalker may have stopped taking his or her medication and now lives in a fantasy world composed of part reality and part delusion, which he or she is unable to differentiate. If they're not careful, targets of the delusional stalker are likely to be sucked into this fantasy world and start to have doubts about their own sanity, especially if the stalker is intelligent, and intermittently and seamlessly lucid and "normal."
- Erotomaniac: this stalker is also delusional and mentally ill and believes he or she is in love with you and will have created an entire relationship in their head.
- Harasser stalker: some stalker types like to be the centre of attention and may have an attention-seeking personality disorder; they may not be stalkers in the strict sense of the word but repeatedly pester anyone (especially anyone who is kind, vulnerable or inexperienced) who might be persuaded to pay them attention. If they exhibit symptoms of Munchausen Syndrome[1] they may select a victim who they stalk by fabricating claims of harassment by this person against themselves.
- Love rats: these may not be stalkers in the strict sense of the word but they have many similar characteristics. Love rats surf the web with the intention of starting relationships and may have several simultaneous relationships. The targets of a cyber stalker may know little about the person they are talking to (other than what they've convincingly been fed) and be unaware of a trail of other targets past and present.

[1] Munchausen syndrome is a type of factitious disorder, or mental illness, in which a person repeatedly acts as if he or she has a physical or mental disorder when, in truth, they have caused the symptoms. People with factitious disorders act this way because of an inner need to be seen as ill or injured, not to achieve a concrete benefit, such as financial gain. They are even willing to undergo painful or risky tests and operations in order to get the sympathy and special attention given to people who are truly ill. Munchausen syndrome is a mental illness associated with severe emotional difficulties (http://my.clevelandclinic.org/disorders/factitious_disorders/hic_munchausen_syndrome.aspx

- Troll: the Troll's purpose is to be given more credibility than (s)he deserves, and to suck people into useless, pointless, never-ending, emotionally-draining, ranting discussions full of verbal loops and "word labyrinths", playing people against each other, hurting their feelings, and wasting their time and emotional energy.

STALKERS MOTIVATION:

The motivation of the cyber stalkers are varied as described by (Indianchild.com, 2000) and include:

1) Sexual Harassment: Sexual harassment is also a very common experience offline. The internet reflects real life and consists of real people. The very nature of anonymous communications also makes it easier to be a stalker on the internet than a stalker offline;

2) Obsession for love: this could begin from an online romance, where one person halts the romance and the rejected lover cannot accept the end of the relationship. It could also be an online romance that moves to real life, only to break-up once the persons meet. One of the problems with obsession stalking is that since it often starts as real romance, much personal information is shared between persons involved. This makes it easy for the cyber stalker to harass their victim. Some users online enjoy "breaking hearts" as a pastime, and so may well set up obsessions for their own enjoyment - games that they may later regret having played. Sometimes, an obsession can also be a fixation by a stranger on another user for no valid reason. Since these obsession stalkers live in a dream world, it is not always necessary for the target to have done anything to attract her (or his) attention in the first place. Obsession stalkers are usually jealous and possessive people. Death threats via email or through live chat messages are a manifestation of obsession stalking.

3) Revenge and Hate: this could be an argument that has gone out of hand, leading eventually to a hate and revenge relationship. Revenge vendettas are often the result of something you may have said or done online which may have offended someone. Vendettas often begin with arguments where you may have been rude to another user. Sometimes, hate cyber stalking is for no reason at all (out of the blue)- you will not know why you have been targeted nor what you have done, and you may not even know who it is who is doing this to you & even the cyber stalker does not know you. In fact you have not been individually targeted at all - you have been chosen as a random target by someone who does not know you!! This stalker may be using the net to let out his frustrations online.

4) Ego and Power Trips: these are harassers or stalkers online showing off their skills to themselves and their friends. They do not have any grudge against you - they are rather using you to 'show-off' their power to their friends or doing it just for fun and you have been unlucky enough to have been chosen. Most

people who receive threats online imagine their harasser to be large and powerful. But in fact the threat may come from a child who does not really have any means of carrying out the physical threats made (Jaishankar & Sankary n.d)

PREVALENCE OF PERPETRATION

A study conducted through telephone by the University of Cincinnati on sexual victimization of college women surveyed 4,446 randomly selected women attending two- and four-year institutions of higher education. It was conducted during the 1996-97 academic year. In this survey, a stalking incident was defined as a case in which a respondent answered positively when asked if someone had "repeatedly followed you, watched you, phoned, written, e-mailed, or communicated with you in other ways that seemed obsessive and made you afraid or concerned for your safety." The study found that 581 women (13.1 percent) were stalked and reported a total of 696 stalking incidents; the latter figure exceeds the number of victims because 15 percent of the women experienced more than one case of stalking during the survey period. Of these 696 stalking incidents, 166 (24.7 percent) involved e-mail. Thus, 25 percent of stalking incidents among college women could be classified as involving cyber stalking (USDOJ 99).

DISTRIBUTION OF CYBER STALKERS

No data is available to indicate the distribution of cyber stalkers. Anecdotal evidence suggests that this is a global phenomenon. The perpetrator could be from a neighbour, across the street or from overseas.

DOES CYBER CRIME AFFECT WOMEN DIFFERENTLY?

My daughter Katie and I were targeted for harassment via the internet by a multiple convicted felon in July 1996. Katie was only five years old when this case began, but that didn't stop the stalker from sending obscene email messages addressed to her via her page on my web site. The harassment turned into stalking, moved offline, and never really stopped. Due to threats, we lived in three different homes in the first two years after initial contact with the criminal, and I lost track of the number of times I had our phone numbers changed. I also greatly reduced my presence on the internet for many months, hoping he would lose interest and leave us alone. He did not. (Cynthia L. Armistead, http://www.cyberstalked.org/ourstory/).

DEFINITION

The internet has opened up a world of new opportunity for gender activists and development actors working in the arena of information and communications

technologies (ICT). The need for access, connectivity and relevant content has been well argued by researchers and advocates alike, but as the reach of the internet expands, new issues arise in bridging the 'digital divide'. Invasions of privacy, objectionable and malicious content, cyber harassment and other forms of 'cyber crimes' undermine the internet's potential as a great equalizer and threaten autonomy and security of individuals, organizations, communities, and nations.

What is the meaning of “cybercrime”? Often when we talk about cybercrimes, the first thing that comes to mind - and that is stamped on many laws - are crimes such as fraud, theft of credit card numbers and hacking. Rachid Traoré, the Communications Officer for the Burkina Faso Ministry of Posts and New Technologies says that cybercrime is all the crimes committed by persons using information technology and the internet, including sending spam, hoaxes, worms and viruses, to design and create false documents, or to develop and watch pornography, and paedophilia.

HOW DOES CYBER CRIME AFFECT WOMEN?

It is estimated that 95% of aggressive behavior, harassment, abusive language and denigrating images in online spaces are aimed at women and come from partners or former male partners (UN 2006). In addition, many ICT tools such as spyware, wireless technology, webcams etc. are used to perpetrate violence against women. Mavic Cabrera-Balleza, in *Finding a difficult balance: human rights, law enforcement and cyber violence against women* (2008) points out that Women's groups and individuals have reported cases of e-mail harassment, "flaming" (online verbal abuse), cyber-stalking, online prostitution and pornography. Despite this alarming reality, cybercrimes seem absent from the agenda of feminist movements.

According to Weiting Xu (n.d), the increasing availability of and ease of access to personal information online, especially through popular social networks such as Facebook, also facilitate incidences of cyber harassment, with minority and marginalized groups often at the receiving end. Further, while both men and women are affected by cyber stalking, a survey of the characteristics of 'victims' finds that amongst users from the ages of 18-32, victims are predominantly female. Weiting further points out that in India, Delhi police confirm this observation, noting that nearly half of cyber crime cases reported are filed by women who discover their faces morphed onto pornographic images and posted online, usually accompanied by a personal phone number and an invitation for strangers tocall.

For marginalized[2] groups, cyber crimes can threaten the very communication rights that have been one of the most democratizing aspects of the internet. The creation

[2] The term will be operationalized for the purpose of the study.

of secure online spaces has provided fora where marginalized groups can feel safe from harassment and enjoy freedom of expression and privacy of communication. Unfortunately, the benefits of anonymity and privacy also extend to those who employ ICT to threaten the communication rights of others, and often to target groups that are already marginalized on the basis of age, sexuality, race, or religion, among others (Weiting n.d).

Cabrera- Balleza (2008) raises the issue of laws on cybercrime lacking consideration of their social impact. Often pushed by the private sector to regulate intellectual property matters or by the State to enforce control and surveillance on citizens, it is uncertain whether women's rights stand to be protected or traded in this debate. Particularly with the acute lack of broader women's rights engagement, or even awareness, in this issue, claiming the boundaries and definition of the issues at stake – moving it beyond arguments of "terrorism", "national security" and "crimes against capitalism" - can be challenging. This then raises concerns on whether cybercrime laws will simply be mobilized to restrict communication rights of individuals and communities. As such, their different approaches and stances clearly demonstrate the difficulty of drawing a clear line between protection of women's rights from violation and empowering their status as users and definers of ICT and the information society.

The Convention on Cybercrime adopted by the Council of Europe on November 8, 2001 and signed by other countries including South Africa, addresses the issue of child pornography but is silent on violence against women.

The 2006 UN Secretary General report and in-depth study on all forms of violence against women recognized the new forms of violence against women that have developed with the advent of the new information and communication technologies (ICTs). The report calls on Member States to acknowledge the evolving nature of violence against women and respond to new forms as they are recognized. With increasing access to ICTs, the cases of cyber violence against women and girls are also increasing. However, the statistics on this issue are very uneven if not sketchy. The weakness in data collected may also be linked to the fact that most of the existing laws and policies on ICTs do not cover cyber violence against women therefore provide segregated data.

IS THE DESIGN OF THE CYBER ALREADY WOMAN UNFRIENDLY?

Lesley Ann Foster, founder and Executive Director of Masimanye Women's Support Network in South Africa is of the opinion that cybercrimes against women are increasing because more people are gaining access to the information and communication technologies. Women and particularly girls are targeted for cybercrime because of their vulnerability. Her stand is echoed by Charlotte Bunch, founder and Executive Director of the Centre for Women's Global Leadership at Rutgers University in New Jersey, who feels that there is a new level of cultural violence against women that is becoming more prominent because of cybercrime (www.genderIT.org).

“Even as women try to master communications and media as a way to expose this violence and use the internet as a tool to expose it, sometimes it gets turned around and used by people who want to titillate sexuality with violence. The new media extends the access to women that men have, particularly young women who may be vulnerable, and creates new forms of abuse that are not necessarily different in character but require new responses”. Says Bunch

A report by the Association of Progressive Communications (APC), *Dealing with fraud and internet "love": women and cybercrime in Burkina Faso*, Frédéric Robert Ilboudo, a journalist, conceives of the net as a fertile ground for cybercrime. As discovered by young women, the internet is a viable vehicle to make money and become involved in sex work, specifies Rachid Traoré, the Communications Officer for Burkina Faso’s Ministry of Posts and New Technologies. With regards to sex work, the women offer their services to clients, who directly enquire about their descriptions to find out whether they are “to their taste.” Moreover, emphasizes Traoré, some individuals, under the pretext of loving them, exploit their naiveté and ask them to send nude photographs of themselves. Then these photographs are published on the worldwide web without the women's consent. As far as Traoré is concerned, the dignity of women has come under attack with the development and popularization of instant communication technologies. “In Burkina Faso, cybercrime is not linked to gender. It is practiced by men as well as women. However, women are most often the victims, even if there are cybercriminals amongst them.” As no statistics exist, Rachid Traoré considers it difficult to assess the impact of cybercrime on women.

DEALING WITH CYBER CRIME

Many Internet service providers offer tools that filter or block communications from specific individuals.

As soon as individuals suspect they are victims of online harassment or cyber stalking, they should start collecting all evidence and document all contact made by the stalker. Save all e-mail, postings, or other communications in both electronic and hard-copy form. If possible, save all of the header information from e-mails and newsgroup postings. They should record the dates and times of any contact with the stalker. They should also document how the harassment is affecting their lives and what steps they have taken to stop the harassment.

Victims who are being continually harassed may want to consider changing their e-mail address, Internet service provider, a home phone number, and should examine the possibility of using encryption software or privacy protection programs. Any local computer store can offer a variety of protective software, options and suggestions. Victims may also want to learn how to use the filtering capabilities of email programs to block e-mails from certain addresses.

A key component of addressing the cybercrime is education and empowerment: If individuals are given clear direction about how to protect themselves against

threatening or harassing communications, and how to report incidents when they do occur, both industry and law enforcement will be in a position to cooperate to conduct investigations

Cyber violence is more difficult for police to handle because people do it in the privacy of their homes. People can use the internet and email facilities wherever they find themselves and in this way hide what they do. It can be anonymous and therefore more dangerous.

There is need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights. Such rights also include the right to freedom of expression and the rights concerning the respect for privacy. However, given the free and boundary-less nature of ICTs, the lines are often blurred and finding the right balance between becomes an extremely difficult task (Cabrera-Balleza 2008).

WHAT ARE THE CURRENT MEASURES AND GAPS (TECHNOLOGICAL, LEGAL, SOCIAL, AND PSYCHOLOGICAL) TO ADDRESS CYBERCRIME AGAINST WOMEN (MAPPING THE EFFORTS AND BEST PRACTICE?

Cybercrime is not a rigorously defined concept, according to the Berkman Center for Internet & Society (2008). However, cybercrime is cheap to commit, difficult to detect and often hard to locate in jurisdictional terms, given the geographical indeterminacy of the internet.

According to Goodman and Berner (2000), cybercrimes differs from terrestrial crimes in four ways: “They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal.” With this in mind, cybercrime present new challenges to lawmakers, law enforcement agencies, and international institutions. This therefore calls for the existence of effective national and international legal, technical, and social mechanisms, that not only monitor the utilization of ICTs for criminal activities in cyberspace but also protects users, particularly those vulnerable like women.

A 2008 paper by Gender IT.org, notes that individuals from minority and marginalized groups are particularly vulnerable because ‘often they already face information deprivation – not only online but also offline – and may not have knowledge of the protections that exist to guard their basic human rights. Thus they do not have the resources to seek legal or technical recourse when their communications rights are violated in cyberspace. Further the limitations and in some cases lack of cybercrime laws make it very difficult for women to deal with these cybercrime.

Kenya, for example has no specific provisions for crimes such as cyber stalking, chat room abuse, impersonification and identity theft, among others, in the Kenya Communications Amendment Act (2009). The Act focuses primarily on offences

committed against information technology infrastructure, like data interference and misuse of the technical aspect of devices. The Act fails to address crimes committed against the person. According to Goodman and Brener (2000), this could be because it is difficult to define laws that need to be put in place for the apprehension and prosecution of cybercrime because it raises some difficult issues, for example the scope of cyber-offences a country needs to define. Another is the extent to which these laws should be cybercrime specific. They question whether it is necessary for a country to add a 'computer fraud' offence if it has already outlawed fraud.

What makes it even more challenging is that many victims of cybercrime are unwilling to report their cases with the authorities, therefore the true magnitudes of cybercrime, as well as demographic statistics on victims and perpetrators is unknown. Gupta(2007), suggests that the reason for this could be that victims are either scared of police harassment or wrong media publicity. She goes on to add that for minority and marginalized groups who already bear the brunt of media bias, reporting online harassment to the police may simply draw further unwanted attention. Gender IT.org also notes that the lack of cooperation from foreign-based websites is another challenge to dealing effectively with and resolving cybercrime cases.

Another difficulty, noted by Schjølberg and Hubbard (2005) is that although Internet Service Providers (ISPs) began to receive increasingly more complaints about harassing and threatening behavior on-line, they have yet to pay much attention to these types of complaints. Many on-line industry associations state that providing more attentive protection against their customers (informing them as to the ISP's complaint procedures, the policies as to what constitutes prohibited harassment, and the ISP's follow-up procedures) would be costly and difficult. They argue that "no attempt to impose cyber stalking reporting or response requirements should be made unless fully justified," yet at the same time contend that "the decentralized nature of the Internet would make it difficult for providers to collect and submit such data.

Another approach being used by ISP's has been advising internet users to stay away from social networks as a possible social strategy against cybercrime. This according to Gender IT.Org (2008) insinuates that users are 'victims' who do not know how to protect themselves and should therefore minimize their online interactions. As a result, marginalized groups vulnerable to cybercrime are further discouraged from participation and there is a risk that this approach would widen the digital divide as more business, leisure, governance and other activities take place online.

In the United States, the State Office of Cyber Security and Critical Infrastructure partnered with a volunteer organization the 'Alliance of Guardian Angels to promote online safety in New York communities and in classrooms'. APC (2008) notes that this initiative is another example of funding being provided for men to protect women from violence rather than empowering them to protect themselves. In

addition, they note that most of the social approaches being proposed fail to take into consideration the need to empower women to effectively use and appropriate ICTs while protecting themselves from criminals. They propose a a multi pronged approach, which would involve, raising awareness and capacity building would be better strategies of addressing cybercrime from a social perspective.

The Internet Corporation for Assigned Names and Numbers (ICANN, 2008), has held a series of workshops aimed at creating awareness on Domain Name System Security (DNS) . These workshops also aimed at creating awareness and developing capacity of various stakeholders to begin to address issues of cybercrime and security from a technical perspective.

ICANN also maintains a WHOIS[3] data system (ICANN 2005). This, it is believed would assist towards identifying owners of domain names.

INTERNATIONAL LEGAL EFFORTS

A McConnell International 2001 report notes that the Internet has made cybercrime a trans-border problem. The global dimension of cybercrime is now universally perceived even in countries that do not have a large percentage of people using the internet. The reports suggest that international coordination and cooperation are therefore necessary in fighting offences, which are commonly prohibited by every country in the physical world.

Several international organizations have recognized the trans border nature of cybercrime, the limitations of domestic, national approaches and the need for international collaboration and harmonization of legal, technical, and other solutions. The main organizations engaged in this field are the European Union, Commonwealth of Nations, Organization for Economic Cooperation and Development (OECD), United Nations, the Interpol and more recently the African Union. These organizations continue to play an important role in harmonization of criminal law as well as of underlying civil and administrative law in all of the above-mentioned areas of computer-related criminal law reform.

The International Criminal Police Organization (Interpol), the international law-enforcement organization notes that harmonized legislation is the prerequisite for the coordinated law enforcement. They provide technical guidance for combating cybercrime, among them, detection, forensic evidence collection, and investigation. They have produced an Information Technology Crime Investigation Manual, which provides a technological law-enforcement model to improve the efficiency of combating cybercrime. Interpol also takes distinct actions to prevent cybercrime, cooperating with credit-card companies to combat payment fraud and by building a database on Interpol's web site.

[3] **WHOIS** (pronounced as the phrase *who is*) is a query/response protocol that is widely used for querying databases in order to determine the registrant or assignee of Internet resources, such as a domain name, an IP address block, or an autonomous system number (http://en.wikipedia.org/wiki/WHOIS)

The Organization for Economic Cooperation and Development (OECD) adopted Guidelines for the Security of Information Systems and Networks in July 2002. OECD has encouraged their member governments to "establish a heightened priority for security planning and management," and to "promote a culture of security among all participants as a means of protecting information systems and networks" (OECD 2002a, Part I). The Guidelines established nine principles, including awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment (OECD 2002a, Part III).

The Commonwealth of Nations through the Commonwealth Secretariat developed a Model Law on Computer and Computer Related Crime in October 2002 and covers the offences of illegal access, interfering with data, interfering with computer systems, illegal interception of data, illegal data, and has very strong provisions for child online protection.

The European Convention on Cybercrime and its Protocol has been widely accepted as a landmark, providing for both the substantive and procedural legal frameworks, both at the domestic and international level nd has been ratified by 19 countries, including non-member states, the United States of America, Canada, Japan, and South Africa. South Africa is the only African country to have signed the Convention.

The United Nations General Assembly has endorsed several resolutions dealing with cybercrime. According to Schjølberg and Hubbard (2005), there are several resolutions on Combating the Criminal Misuse of Information Technology all calling on member states "to promote the multi-lateral consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats." The UN has gone further with the 2006 UN Secretary General report and in-depth study on all forms of violence against women, which recognized the new forms of violence against women that have developed with the advent of the new information and communication technologies (ICTs). The study calls on member states to acknowledge the evolving nature of violence against women and respond to new forms as they are recognized.

The UN, through the International Telecommunications Union (ITU) has developed a tool kitIt is important to note that most of the existing international laws and policies on ICTs, and cybercrime do not have provisions for cyber violence against women.

KENYA

Kenya enacted the Kenya Communications Amendment Act 2009 (KCA 2009), which recognizes cybercrime and sets out legal protection for government and businesses. The Act defines cybercrime as offences against the information technology infrastructure, from unauthorized access to and interpretation of

computer services, modification of computer material, data, and unauthorized change of mobile telephone equipment.

It does not acknowledge cybercrime against persons and as a result cyber crime committed against women for example would not be a priority within this legislative framework.

As a technical strategy to fight cybercrime, Kenya is in the process of developing a national Computer Emergency Response Team (CERT) (CCK 2008) and is part of the ITU Global Resource Centre (GRC)/International Multilateral Partnership Against Cyber Threats (IMPACT). Its objective is to support ITU member States in dealing with Cybercrime through the establishment of national CERTs, capacity building and information sharing.

The CCK also notes that at the national level, there is a process in place to develop a framework that will facilitate for setting up Certification Authorities for the issuance of digital certificates to protect online transactions in the country to encourage electronic commerce. Other technical approaches at the national level include, Domain Name System Security (DNSSEC) and Internet Protocol version 6 (IPv6), which is the new Internet protocol that provides enhanced end-to-end Internet Protocol security.

At the East Africa level (EARPTO 2008), Kenya chairs the Cyber security Taskforce whose main objective is to facilitate the development of national CERTs in the East Africa region. This effort is expected to lead to more harmonized regional efforts led by regulatory authorities.

As noted in international cybercrime initiatives, there seems to be more focus on child online protection and less on cybercrime against women and their protection . An issue paper by Women of Uganda Network (2009) suggest that this could probably be because of the low penetration of the Internet, as a result the current focus is on expanding accessibility than focusing on issues of abuse.

Individuals from minority and marginalized groups such as women are left especially vulnerable by cybercrime laws limitations because they are often information deprived and may not have knowledge of the protections that exist to guard their basic human rights (Gender IT 2008). They do they do not have the resources to seek legal recourse when their communications rights are violated in cyberspace.

This challenge extends to the use of the mobile phone, where, notes WOUGNET (2009) mobile phones have been used extensively to commit violence against women in Uganda, yet there are no laws that focus on their protection, nor technical or social solutions made available. In Kenya, a BBC study (2008) noted that mobile phones were used extensively during the post election conflict in 2007-2008 to spread hate speech and inflammatory messages. The Kenya Communications Amendment Act 2009, fails to make provision of hate messages or crime committed against the person using mobile phones.

Gender IT (2008) cautions that while legislation is certainly required to ensure the realization of communication rights for both internet users and non-users, the impact of increased regulation and policing of the internet on marginalized groups must be clearly examined. The report notes that from the current legal provisions made to protect children online for example in the United Kingdom and Australia, the provisions extend to regulating other broad range of content including information on women's sexual and reproductive health, and in some cases, notes the report to state censorship to stifle freedom of expression.

CRITICAL REVIEW OF MAJOR ISSUES

- Data available is more than five years old. Cyber space is a dynamic space and there is need for more recent/current statistics.
- Lack of comprehensive national data/statistics on women and cybercrime. Availability of this would allow for development of response strategies.
- Ways in which cybercrime restrict the exercise of individual rights to privacy, freedom of expression and civil liberties need to be acknowledged and discussed.
- Cyber crime against women not yet an agenda item on the women's movement.
- Lack of appropriate legal and regulatory measures against cybercrime specific to women.

SUMMARY AND GAPS TO BE FILLED BY THE STUDY

Encouraging developers to produce appropriate technologies that create secure empowering online spaces for women. Creating an internet that enables and ensures the social, economic, cultural, and political participation of minority and marginalized groups.

Governments can facilitate these processes by taking legislative measures that ensure human rights are protected online just as they are physical spaces. Legislation should not just protect users, however, creating awareness and educating individuals on how to exercise their communication rights is imperative

Cybercrime legislation must become flexible and evolve as cybercrime evolves. Legislation must be developed to anticipate the needs of all that well-being depend on the internet eco system.

Further, there is a need to recognize that violence against women is anchored within the broader societal systems that privilege men over women. These systems are nurtured by structures such as the family, the state, religious institutions, the legal regimes, the policies etc (WOUGNET 2009). A sustained effort should therefore be made at enabling capacity of ICTs to foster awareness at all these levels.

CONCEPTUAL ISSUES /OPERATIONALISATION OF TERMS

DESIGN AND METHODOLOGY

STUDY DESIGN

This is a descriptive research to demonstrate the phenomena of cyber violence against women in Kenya and how the vice is manifested. The research is qualitative.

TARGET POPULATION

The study population is women in Kenya

SAMPLING DESIGN

Through exploratory research and will seek out real life stories identified through purposive sampling.

DATA COLLECTION PROCEDURES AND INSTRUMENTS

Data will be collected though Interviews using structured and unstructured questionnaires

DATA ANALYSIS

Once data is collected and checked for completeness, the same will be analysed for emerging themes to form the basis of the report.

TIMELINE

12/12/09	Framework/Task sharing
22/12/09	Share literature sources
12/01/10	Present literature review/develop tools and methodologies.
15/01/10	Confirm methodology and tools/Plan validation workshop dates.
16/02/10	validation Workshop
February	Data collection
March	Break fast meeting during the ICANN meeting 9 March 09 at 8.30-10.30 am.

REFERENCES

(DoJ) US Dept of Justice (1999) Cyber stalking: A New Challenge for Law Enforcement and Industry, A Report from the Attorney General to the Vice President August 1999 viewed at **http://www.cybercrime.gov/index.html viewed** on January 6 , 2010

. Governor Announces Partnership with Guardian Angels to Promote Online Safety. Retrieved on August 10, 2008 from http://www.guardianangels.org/pdf/1610.pdf

Bourne, R. (2002). *Commonwealth Law Ministers' Meeting: Policy Brief*. London: Commonwealth Policy Studies Unit.

Cabrera-Balleza, Mavic. 2008. *Finding a difficult balance: human rights, law enforcement and cyber violence against women*, http://www.genderit.org/en/index.shtml?w=a&x=96169

Commission of the European Communities (2002). *Proposal for a Council Framework Decision on Attacks against Information System*, COM (2002) 173 final, 2002.

Communications Commission of Kenya (CCK) www.cck.go.ke

Council of Europe. 2001. *Convention on Cybercrime*. http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

Council of Europe. 2001. Convention on Cybercrime. Retrieved on August 8, 2008 from http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

Cyber crime legislation and gender: http://www.genderit.org/en/index.shtml?apc=f--e--1&x=96162 http://www.genderit.org

Cybercrime legislations and gender Aug 2008 Flavia Fascendini http://www.genderit.org/en/index.shtml?apc=f--e--1&x=96162

David Goldstone & Betty Shave, *International Dimensions of Crimes in Cyberspace*, 22 Fordham Int'l L.J. 1924 (1999).

Dealing with fraud and internet "love": women and cybercrime in Burkina Faso. http://www.genderit.org/en/index.shtml?apc=a--e96160-1

Duggal,Pavan Cyberlaw Consultant pduggal@vsnl.com, pavanduggal@hotmail.com

Gupta, Vinta 19 November 2007. No End to Cyber Crime. Express Computer.

Interview conducted by Marvic Cabrera- Balleza with Charlotte Bunch, founder and Executive Director of the Center for Women's Global Leadership at Rutgers University in New Jer Lesley Ann Foster, founder and Executive Director of Masimanye Women's Support Network in South Africa sey, USA. www.GenderIT.org

Interview with Lesley Ann Foster, founder and Executive Director of Masimanye Women's Support Network in South Africa. www.GenderIT.org

Jaishankar, K, Sankary, V. U Cyber Stalking: A Global Menace in the Information Super Highway*

M. D. GOODMAN and S. BRENNER, *The Emerging Consensus on Criminal Conduct in Cyberspace* (Oxford, International Journal of Law and Information Technology), [2000] Vol. 10, n. 2 p. 3.

McConnell International (2000). Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information: Archaic Laws Threaten Global Information. http://www.witsa.org/papers/McConnell-cybercrime.pdf

Mcconnell International E-Lert, *Combating Cybercrime : A Proactive Approach* [Feb. 2001], <http://www.mcconnellinternational.com/pressroom/elert.cfm>

Organization for Economic Cooperation and Development (2002). *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*

Schjølberg, S., & Hubbard, A.M. (2005). Harmonizing National Legal Approaches in Cybercrime, 10 June 2005, *International Telecommunication Union, WSIS Thematic Meeting on Cyber security*, Geneva, 28 June-1 July.

United Nations Crime and Justice Information Network (UNCJIN) (1999). International Review of Criminal Policy -United Nations Manual on the Prevention and Control of Computer-Related Crime. *International Review of Criminal Policy*, nos. 43 and 44

United Nations. 2006. *In-depth study on all forms of violence against women*. Report of the Secretary-General. http://daccessods.un.org/TMP/7121883.html

United Nations. 2006. In-depth study on all forms of violence against women. Report of the Secretary-General. Retrieved on August 10, 2008 from http://daccess-ods.un.org/TMP/7121883.html

WHOA (2008) Online Harassment/Cyber stalking Statistics viewed at http://www.haltabuse.org/resources/stats/2008Statistics.pdf on Jan , 6th , 2009

Xu,Weiting. *Unequal protection, cyber crime and the internet in India* http://www.genderit.org/en/index.shtml?apc=a--e96161-1

KICTANET QUESTIONAIRE
Cybercrime and Women

Age:

☐ 18-30 ☐ 31-40 ☐ 41 or over ☐ Not saying

Marital status:

☐ Single ☐ Married ☐ Life Partner ☐ Divorced ☐ Separated ☐ Widowed ☐ Not Saying

Questions

1. Describe fully how the harassment began.

Thoughts

2. What did you think was happening and why did you think it was happening?

3. Did you have any relationship or contact with the harasser, online or offline, before the harassment began?

If not how do you think the perpetrator got your details? Please provide as much information as possible.

4. Do you know why you are being harassed by this person or persons? Please explain this in as much detail as possible.

5. Type of first known interaction with harasser (email, mailing list, yahoo messenger, Skype, chat rooms, telephone, other)

6. Has the harassment escalated since it began? For instance, have the communications become more frequent, or has the content of those communications become more overtly threatening or defamatory? Yes No

7. Have you been threatened with physical offline harm? (e.g. violence, kidnapping, rape, death) Yes No

b) If yes, how were these particular threats communicated to you?

8. Has your reputation been attacked, e.g. have lies been spread about you to others? Yes No

9. Have you sent any communication to the harasser yourself, or made statements about the harasser in a public place? Yes No

If yes, please describe. Give type of communication e.g. any email messages, chat or IM exchanges, messages directed to or about the harasser, etc. Who did you share this information with?

10. Have you taken any steps to protect yourself?

11. Do you think this is different from any criminal phenomenal in the physical world?

12. What measures do you think should be put in place to protect you? (social or regulations, to curb cybercrime?)

Feelings

13. What level of internet user are you:

☐ Consumer - You can check your email, surf the web and chat, but that's about it. You might have a web site, but you don't really know HTML.

☐ Power User - You can also install and configure different programs so that they work with your internet access. You know HTML. You know how to get the full headers of messages in your email program(s).

☐ Expert - You can accurately trace email and messages to their origin, get registration information for domains and find out who owns IP addresses.

☐ Guru - You are a sysadmin, or you train other to be advanced users. You know all about firewalls, proxies, anonymizers, daemons, etc.

14. How would you say the harassment affected you? (your feelings)

15. Could you explain the impact? (e.g. stopped using internet).