Workshop Report: Women and Cybercrime Workshop meeting

Venue: University of Nairobi, Chiromo Campus

Date: 18th May 2010

Synopsis

While 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. Kenya Communications (Amendment) Act 2009 focused on the cybercrime against property and not the person. With increased use of Internet in Kenya with the onset of broadband, it is necessary to create the necessary policy / regulatory and operational frameworks to deal with cybercrime.

Against this backdrop, the Kenya ICT Action Network (KICTANet) organized a workshop using focus group discussion format on 18th May 2010 at the Arziki UNES University of Nairobi, Chiromo Campus to define, share and explore issues surrounding women and cybercrime in Kenya.

KICTANet has launched a study on the issue guided by the following key 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?

The purpose of the meeting was to share case studies of cybercrime incidents in Kenya with a view of getting an idea of its prevalence in Kenya and recommendations for dealing with these forms of crime. The meeting also tried to establish why there was no discussion/dialogue or focus on online cybercrime against women.

Participants were encouraged to be as candid as possible while discussing the issue and share their experiences. To set the discussions in motion, a presentation providing the context of cybercrime was shared with the participants. The presentation provided a background for discussions on definition of cybercrime and explained the issues surrounding it and also sought to begin to develop recommendations on the way forward.

A set of questions from a questionnaire prepared from the ongoing literature survey were presented and discussed interactively with the participants. Finally, following the presentation participants identified commonalities and gaps that exist in Kenya. Recommendations were then made on strategies that can be adopted for long-term advocacy campaign to highlight and sustain the issues revolving around cybercrime against women in Kenya, with an aim of lobbying the relevant actors to come up with policies and legislations that can effectively tackle the issue and ultimately protect women.

Session 1 – Setting the Scene

What is Cybercrime?
Cybercrime can broadly be defined as any activity on the Internet and ICTs generally that offends human sensibilities. Cybercrime can be categorized in three (3) ways:

1. Against government - e.g. cyber warfare, which is very prevalent, and a lot has been written about this crime because the government has a lot of interest in crimes affecting it.
2. Against property - ICT based systems, Denial of service
3. Against the person
   a) Child - child pornography
   b) Women - harassment, cyber stalking

Is cybercrime real?
Cybercrime is indeed real and it happens. Below are two sample case studies cited from a literature review conducted outside Kenya on cybercrime.

Case 1 - India
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).*

Case 2 - USA
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)

Is cybercrime happening in Kenya? Discussions:

Cybercrime is happening in Kenya as evidenced by the following experiences shared by three women who were interviewed in Kenya on condition on anonymity shared .

Woman 1*- She was a contestant in a popular reality show in Kenya called Tusker Project Fame, which showcases musical talent. The woman had this to share "…after project fame, I realized that there was a hate campaign propagated on Face book against me…it injured my reputation, I did not know if these threats would be translated to physical attacks in the streets (she had been told*
That rotten eggs would be thrown at her on the streets)…I did not know which agency could help me…"

Woman 2 *– Some people put her real face and superimposed a nude body on the web. "It's painful, she lamented". This woman's image was no doubt dented by this act.*

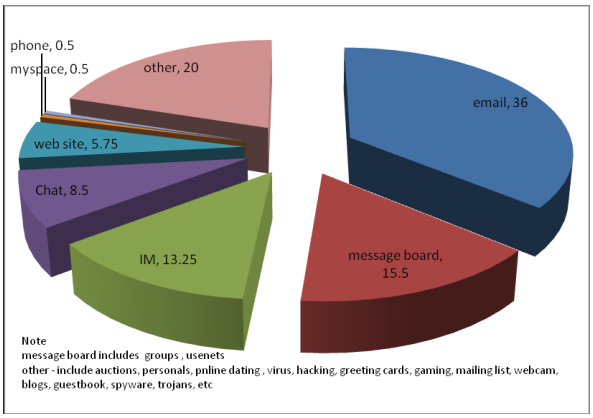
Woman 3 *– She received a blackmailing message stating "we shall distribute mail that you are a lesbian unless you support the course we're interested in."*

Woman 4 *- She would receive hate SMSs from her husband whom she had sought to separate from. The husband would also send the same hate messages to her friends on SMS and e-mail. He had stolen her yahoo e-mail and official passwords and would intercept messages she should send out to friends. He also went ahead and also harvested addresses her message book and would send email; messages to her friends… The police would not help. They did not understand what they would need to do"*

These are just some of many similar stories affecting women out there. Surprisingly however, the common thing with the three women interviewed was that they requested that their identities be concealed and that notwithstanding, it was also a challenge convincing them to share their stories.

Perpetrators World – A literature glimpse
Data gathered from a literature review conducted between 2000 and 2008 garnered the statistics illustrated in the figure 1 below.

Figure 1: How Harassment began (%)



Source: WHOA (www.haltabuse.org)

The above study was compiled over a period of about 10 years (2000-2008), a time when mobile phones and networking sites were not very popular. If a similar study were to be done now, it would reveal a completely different set of data.

Who are the perpetrators?

A study conducted over a 10-year period in the USA revealed that 49.5% of the perpetrators were men while women accounted for 28.5%. Multiple gang perpetrators accounted for 1.5% while 21.5% are unknown. Of the victims, 22% were men while 72.5% were women and 5.5% are unknown.

In 49% of the cases, the victim was acquainted with the harasser who turned out to be an ex (34%), a 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 are significant representing one in three cases.

What motivates the perpetrators?

1. *The rejected stalker*
   - Has had an intimate relationship with the victim
   - A mixture of revenge and desire for reconciliation characterizes behavior.
2. *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.
3. *Incompetent suitors*
   - Seek to develop relationships but they fail to abide by social rules governing courtship.
   - Are usually intellectually limited and/or socially incompetent.
4. *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.

5. *Predatory stalkers*
   - Stalk for information gathering purposes or fantasy rehearsal in preparation for a sexual attack

Motivation of Stalkers

1. Sexual Harassment:
   - Most common and reflects offline experience
   - 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.

3. Revenge and Hate:
   - This could be an argument that has gone out of hand, leading eventually to a hate and revenge relationship.
   - Stalker may be using the net to let out his/her frustrations online.

4. Ego and Power Trips:
   - Stalkers online showing off their skills to themselves and their friends.
   - Have no specific grudge but rather using you to 'show-off' their power to their friends or doing it just for fun and you
   - Mostly weak people who would use the anonymity provided by the virtual worked to harass anyone they perceive to be better.

Prevalence and distribution

A study conducted in universities around Kenya revealed that 13% of the female students in the institutions have fallen victims of cyber attacks or some form of harassment. Anecdotal evidence reveals that stalking is a global phenomena and initial indication reveals that the crime is happening in Kenya and East Africa. The challenge however lies in the fact that the victims remain silent regardless of the seriousness of the attack. Most of the information gathered in Kenya has been through some kind of snowballing approach whereby stories are gathered from victims who have to be coaxed into narrating their experiences. It is a natural phenomenon for the victims to desire to remain silent, preferring to leave the incidents behind them. Common questions that pervade the victim's minds are; *why am I being attacked? Would this translate to an attack in the physical world? What will happen to me when I go out there? What is the Significance of this afterwards?* The nature of cybercrime attacks is very personal and it injures the victim's self esteem and it's about time that victims talked about

Narratives from participants on cybercrime incidents in Kenya

Narrative 1

In this case, the victim was a woman and the perpetrator was a man who was well known to the woman. She was one of the people who started using mailing lists as way of encouraging various stakeholders to get involved in ICT policy making and she established what has become a very popular and successful mailing list discussion forum. The first incident was the perpetrator sending out malicious and character damaging content through the mailing list. Most of the content bordered on tribal insults and derogatory remarks such as *"Unalamba matako ya ….. (which loosely translated means you are an ass-kisser)…you're useless…your Masters degree is not teaching you anything…we'll teach you how to run mailing lists…"*. The victim said that the emails took her aback to the point where she started doubting herself, her capabilities.

Women are not used to expressing themselves openly in public spaces so when they find an online space where they are able to do this freely it is always a welcome relief. But when that right is then abused it can be quite damaging to a woman who have just began using the Internet as a communication tool or otherwise.

In another incident affecting the same woman, a man sent her an SMS from Seattle, USA requesting her to rescue his girlfriend stranded in Cote d'Ivoire. The man pestered her for four weeks. When she declined he would become rude and abusive telling her how African women are useless and cannot help anyone. This awakened in her a fundamental issue about protecting personal contacts (shared at meetings etc), which can be easily picked up by would-be harassers. She wondered about protection of privacy and what organizations do when they collect people's details at conferences and meetings, some go ahead to share telephone numbers, and other details on websites, which are accessible to the public.

In yet another incident, the victim would receive insulting SMS's. When she reported the matter to a local police station, the policemen were unhelpful and at one point they told her that they could not help. So grave is the situation that measures to regulate abuse over the Internet were only taken up by the government after tribal websites and mobile phones were used to propagate violence and hatred during the 2008 post-election period. Much more effort is needed to curb the increasing incidents than simply requesting services providers to supply names of offenders to the authorities.

Being actively involved Kenya ICT circle, the victim noted that these incidents made her realize that the law needs to provide protection against cybercrime but this effort can only be realized if people open up and show just how prevalent it is. Another observation made was the tendency to share a lot of personal information that we ordinarily would

not in the real world, for example displaying personal info like telephone contacts on social websites such as Face book. She noted that we seem to share more online than we'd normally dream of telling strangers about (how we live, our lifestyles, our likes, our loves, photographs of quite personal things, our reading habits, who we like, etc Together that information is incredibly powerful in what it can tell someone about us, particularly when analyzed in search of patterns. For example, "project gaydar" (gay radar). Students at Massachusetts institute of technology (MIT) analyzed links on face book they could predict who was gay (I think about 75% accuracy.)

A lot of personal and business data online makes it easy for a hacker to personalize phishing attacks and in some cases, automate the personalization process. Tools and frameworks now exist to gather enough information about you online to custom craft emails that are very credible. It all has to do with the information shared online as well as well as how women use the World Wide Web. Most web browsers retain a history of searching, browsing and buying habits. Google for example analyses search habits of its users to improve its search engine better so it can improve its ads placement.

Most children and teenagers in the modern age are conversant with the Internet and use it to network. They can easily fall prey to predators that fake their personal data and can even woo them in face-to-face meetings. Sometimes such encounters often have unfavorable consequences. While there exist strong child online protection legislations in the UK, US and Europe, Kenya lacks similar policy framework. Perhaps we can speculate that this is due to the fact that no convincing cases have been made to policymakers or that no male politician has fallen victim.

Cybercrime may also not be well understood within the women's circles and most will tend to relegate it to ICT techies. Some women organizations which failed to attend the first meeting called for this project mentioned that they felt the issue was a very ICT technical issue and are yet to fully understand it. Others mentioned that while they agree that cybercrime is an issue, it only seems to affect women who have access to ICTs in the first place and that are a very small percentage in Kenya. So there are other priorities for women.

However, it is important to acknowledge that Kenya is on the verge of an ICT revolution as it works towards becoming part of the global information society. With the national move towards information society initiatives such as digital villages to provide E-government services, telemedicine, e-education, E-agriculture among others, these initiatives will require increased access to the Internet and online services, and as a result increased exposure to cybercrime.

Narrative 2

This narrative is about a woman – a college student who was in an intimate relationship

with two men, one who was her fellow college mate and the other an older man who was paying her school fees. When her college boyfriend learnt of her relationship with the older man, he was furious with her but he did not show his feelings, rather he plotted his revenge. He lured his girlfriend into making an intimate video with him and shortly after, he posted the clip onto the Internet where it spread rapidly within her college and beyond. This traumatized the woman especially because almost everyone in college was talking about her and no one wanted to be associated with her after that incident. She became isolated and her self-esteem was affected.

From the above narrative, it is quite clear that cybercrime actions have negative implications which include injuring one's dignity, isolation from friends, and redefining a person.

Discussion point?
When is the psychological impact likely to be higher in these two scenarios - one depicting the face of a woman with a naked body superimposed on it and the other showing the face of a man with a naked body superimposed on it? Participants unanimously agreed that the picture of the woman was likely to carry more psychological stigma

Narrative 3
This is the account of a woman who was stalked by a man while visiting in a foreign Islamic country. When she reported the matter to the local police in that country, the situation was twisted to favor her offender as it was interpreted that she had brought it upon herself because she was not dressed in a *Hijab*. Being in a foreign country, there was a language barrier but the woman could tell that her interpreter and the police were arguing with the police's apportioning of blame. Sometime later, the woman was required to travel to the same country where the offence had taken place on official mission but her visa request was denied. When she probed it emerged that her name was entered into the police database when a local filed a case against her. The visa was finally issued after intervention by a make relative. Following this experience, the woman realized that sometimes women are made to feel responsible for the injustices they are exposed or subjected to by men. The point being made was that most women would not want to get involved with reporting harassment cases to the police or taking it further, because women are always eventually blamed for having been, sexually harassed, subjected to fraud or violence, including domestic violence. Participants agreed that most often than not a woman will be blamed for having been harassed online. She will be told, she asked for it.

Narrative 4
This account is about a woman who signed up on Face book and as the trend is, she invited many friends including her ex-boyfriend. Happy to link up again through the social website, she exchanged some pleasantries with her ex-boyfriend and his wife came

across their exchanges. His wife then accessed the woman's personal information and started sending extremely offensive and insulting emails to her because of the interaction with her husband. This woman was of course very surprised and could not understand how his wife had accessed her personal information. After searching through Face book, she realized that that the common link was his wife's friend who had invited her as a friend and therefore had access to her personal information. At this point, she warned her ex-boyfriend's wife to stop the abuse and threatened legal action. She also sought intervention of the ex-boyfriend to speak with the wife. The emails ceased after that.

Women are also often quick to believe the worst about other women and are capable of abuse which can be extremely vicious particularly if they feel they have to compete for men and perceived male resources.

General Observations

It is obvious that these issues need to be placed on the public agenda. In Kenya, there is no legislations, policies, or mechanisms provided to address cybercrime incidents such as the ones narrated above. Victims do not therefore feel confident enough to bring the issues into the limelight. Collective measures need to be taken to define the roles of various stakeholders.

Session 2 – Fundamental questions

1. The Spectrum of ICT usage

a. What ICT communications tools do you ordinarily use (rarely/often/frequently?)

- ·Internet email/web surfing
- ·SMS
- ·Twitter
- ·Face book/MySpace
- ·Blog page
- ·Email Mailing Lists
- ·Others (yahoo messenger, Skype, chat rooms etc)

Blog Page – a participant talked of a lady has a blog page which is regularly updated by people. Unfortunately, some people use the blog page to write spiteful things. The woman just brushes off the incidents by saying that she is used to people writing bad things about her on the blog page.

Twitter - a participant said that she has a Twitter page which she rarely uses because she tries to limit the amount of attention it draws on her by people knowing what she is doing or where

she is all the time. Another Twitter user however stated that makes her twitter page public as she cannot afford to be too private due to the nature of her work.

Social networking tools like Face book, MySpace etc – these are changing the fundamental architecture of the Internet and are providing a single hub where people can integrate all of their information into one location, such as photo-sharing, blogs, IM, video-sharing, marketplace listings, etc. This type of networking can be very enjoyable and beneficial, allowing people to reconnect with old friends, share experiences from remote locations, as well as branch out in school or the workplace. However these networking sites do not come without risk. Social networking sites have become a haven for sexual predators because it allows them to lurk through the wormholes of cyber-space anonymously and peruse the profiles of potential victims. Participants noted that Face **book** provides privacy tools and mechanisms that enable a user to vet whom to invite as friends. Most people accept friendship invitations without checking their backgrounds and this could increases the potential of a cybercrime attack. It was noted out that while Face book has the strongest privacy policy statements, most users are not aware that there are ways they can restrict who has access to their personal details. Face book has acknowledged the dangers that exist on its network and have agreed to buckle down on sexual predators by changing the way that it handles complaints on issues of sexual harassment and inappropriate content. Face book has also introduced a much faster process for dealing with complaints about unwanted approaches by strangers, nudity, pornography and harassment. New members are also warned about the dangers to look out for before they sign up for an account.

MySpace on the other hand announced, in July 2009, that it had removed around 29,000 American sex offenders from its network after being pressured by the US government. Now MySpace requires account holders to be 14 years of age and above and automatically restricts these accounts to the highest privacy settings. This is not to say, however that people cannot lie about their age. It is therefore important for an age-verification system to be implemented.

Yahoo messenger and Skype – another participant stated that she uses yahoo messenger to chat but she sometimes controls whom she interacts with by changing the status to busy when some friends pop up to chat. One participant noted that she had been receiving Skype chat messages from someone she does not know guiding her to a pornographic websites.

Email Messages – has received emails that are quite offensive. Initially she would just delete such messages and on one occasion when such a message came, she forwarded it to a friend to read and summarize it for her. This forced her to pay attention to the content and she found herself responding to it thereby creating a cycle of messages. Unlike before when she would delete the emails, she has now learnt that she can archive

the message as evidence for to report the cybercrime incident.

Discussions on Cybercrime incidence affecting you or aware of

i. Incident 1

A male participant narrated how a former college-mate – a lady was being stalked through emails by someone commenting on her good looks and telling her how intimate he would like to get with her. She would receive messages telling her how good she looked while walking around the university, what she was wearing, etc and how much he liked watching her walking around the campus. The emails scared her to the point where she involved her parents and they would drop her and pick her from school. She also contemplated dropping out of college for a semester because it appeared that her stalker was someone who knew her quite well. Together with two of his friends, the participant requested the lady to share with him the emails and they were able to trace the source of the emails. A simple search on the Internet returned a match from MySpace complete with a photo. The lady was able to recognize the man in the photo as her classmate. This incident happened in the Western world and the authorities therefore took charge and the culprit was apprehended. Closer back home in Kenya, there is a complete disconnect between the law enforcers and technology. The Kenya police still records criminal reported offences in an occurrence book (OB), handwritten. The police need to be trained on basic evidence collection mechanisms by for example collecting the emails cited in Narrative 1 above and engaging experts to verify the validity and genuineness and using the same to apprehend cybercrime perpetrators. One need not be a cybercrime expert to be able to handle some of these situations, such as conducting an Internet search.

ii. Incident 2

This was an incident revolving around three (3) women who were close friends and shared very personal details about each other. One of the women fell pregnant and her husband offered to throw her a baby shower to be hosted at one of her friend's house. Shortly after, the would-be host started receiving malicious SMS texts questioning why she was offering to host a baby shower for a woman who was having a child out of wedlock, thereby calling into question the mother to be sexual monogamy. Fortunately, in Kenya there is a system whereby an SMS can be traced to the sender's phone through the International Mobile Equipment Identity (IMEI) number. Through the intervention of a mobile service provider, the malicious texts were traced to the phone of one of the three women. This cast a dark cloud on their friendship which eventually broke up and degenerated further because their families got wound of the situation. This is another incident where the perpetrator was well known to the victim. This incident happened in 2008 and again confirms that women can be abusers as well.

iii. Incident 3

This is the story of lady who subscribed to a dating sight where she met a German man. They developed a relationship which progressed very fast and eventually, she relocated to Germany. However, when she arrived in Germany, she discovered that the man had mis-represented himself. He was not who or what he had portrayed himself to be on the website and during their online courtship. He soon enslaved her in his apartment, withholding means of communication, or meeting other people.

Women are very vulnerable to online dating. It is hard to gauge who the person on the end is online. The physical cues we use in life - body language, dress, personal hygiene, and tone of voice - the way we judge the truth of statements, are lost in cyberspace. Some services monitor the online behavior of members to a certain extent. Sites such as Match.com provide second-party regulation to track complaints and terminate the access of those who violate standards. Ultimately however, each user is in control of what information they transmit on virtual spaces and for women who have been marginalized in the use of ICTs and the internet in particularly they are more likely to be gullible when using online dating facilities and as a result likely to be victims of not only cybercrime but also trafficking, among other crimes.

iv. Incident 4

One participant gave an account of a woman who received a "face book be my friend" request from a man based in Qatar and just for the fun of it, accepted. The man somehow gained access to her work details including her telephone number and he called her directly on her extension asking for her hand in marriage. The man was persistent and she got scared and reported the incident to her employer. They had to subscribe her to a new email account and change her extension. The stalker stopped. A lot of women innocently divulge their information which is contained in the footer of email messages and also update it for Face book.

Just like in most other Internet tools, new subscribers to Yahoo are required to provide detailed personal information such as date of birth, surname and first name, gender, etc. A female subscriber gave an account of how someone accessed her account and changed her password because he was privy to her personal information. By so doing, he made her inaccessible through her yahoo email and even had access to very personal details such as confirmation of a monetary transaction. This incident happened back in the year 2000 and afterwards, she stopped putting her real personal details when she signs up to any site.

Extortionist scams (commonly known as 419 scams) have become rampant. Most of these scams have West African origins and East Africans easily fall prey to such scams which

promise huge monetary benefits. As genuine as the scams may seem or sound, people should listen to trust their instincts and prevail on common sense to safeguard themselves from falling victims of such scams.

General Observation
Going by the above incidents, women appear to be more vulnerable to cybercrime incidents and either men or women can orchestrate the attacks.

2. What is the impact of cybercrime on the victim's reputation, ICT usage behavior and social networking?

Most women who shared their experience or shared others' experiences reported to have been weakened, rendered vulnerable and sometimes become easy target for subsequent attack/slander etc. Most became scared of fully exercising their right to communicate using the Internet or phones, being forced to change phone numbers and e-mail addresses.

For those who dared to share and /or report their experience like the two cases studies observed that the consequences were ostracism, disconnection, loss of status, and in one cases affected their career adversely. Seems like telling the truth about cyber violence against women apparently offends startles and endangers and women and resulted in subsequent slander and scapegoat. As a result rather than risk this, most women would prefer to maintain silence rather than continue to be abused or bullied.

An example was cited of a cyber bully who continues to use Google groups to subscribed people to a mailing list called "bidii Africa" by harvesting email addresses from other people's mailing lists. When requested to unsubscribe someone, the administrator would often result to insults. He would then use the forum to channel and perpetrate hate campaigns against person the he had grudges with, sometimes degenerating to very personal attacks. It has taken the intervention of Google to block the forum completely after the administrator refused to unsubscribe people from the mailing list.

Such bullies create a hostile environment for mailing users and this may affect the way women would then use the internet and indeed SMS to exercise their right to communicate.

Participants agreed that cyber violence against women can destroy reputations break spirits, impoverish by making it difficult for women to access information and communicate, in some case even end lives.

General Observation
Perpetrators of cybercrime are well known to their victims.

3. Do you have any idea on why you are being harassed by this person(s)?

Participants agreed that;

- ·when a person decides to harass or stalk another person, there is usually a motive behind which can be revenge, retribution or just plain jealousy.
- ·Women are easy targets for cybercrime due to how they are socialized. There is usually a level of judgment placed upon women as we saw in Narrative 3 above, where authorities lay blame s on the woman who was being stalked by a man.
- ·Others perpetrators of cybercrime maybe suffering from a psychological disorder or some other form of sickness and this is especially prevalent
- ·it's not just men who harass and sexually abuse, women too have been known to bully, harass and abuse. Women tend to judge and treat other women in patriarchal ways (they would have internalized sexist values) like observed in incident 2.

Additional attributes typology of stalkers

In addition to the typology of stalkers the following attributes were also identified by participants/discussants.

- ·Women against women – women too are perpetrators of cybercrime against their fellow women
- ·Fraudsters – those who attempt to fleece other through SMS texts purporting that you have won a prize but you need to top up the senders phone with airtime for instructions on how to get the prize
- ·Poverty mainly related to extortion scams
- ·Perception – when you appear in the press or public forums that are perceived to be high profile, it can trigger a situation where people bombard you with calls or emails mostly trying to seek a favor from you
- ·SMS – in Kenya, this has been used lately in hijacking incidents

Additional attributes on the motivation of stalkers

- ·Extortion - the desire to get favors (sexual, monetary, etc) quickly and effortlessly
- ·Ignorance and Fear – an example was given of a man who conducted fraudulent activities through a phishing scam that was introduced to him by someone from Russia. Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. The FBI was however hot on his trail and eventually tracked him down to Thika Road in Nairobi. When he was arrested and interrogated, he appeared to be just an ignorant victim used by the real offender to perpetrate his crimes.

- ·Fear that someone else may get better than they, so they hit out at others to bring them down. This is mostly attributed to women's abuse against women.
- ·Opportunities were there.

4. Why the harasser would chose to use ICTs instead of the other means?

Participants observed that;

- ·ICTs are impersonal and allows for anonymity.
- ·ICT allows one to be bold and feel powerful because the cyberspace provides a shield.
- ·Others just have do it because they have the opportunity and means and engage in it as a hobby
- ·The African cultural and social system is predominantly patriarchal, whereby men feel that they must be in control and always ahead or above women. One participant cited an incident whereby a man who felt threatened career wise by a female colleague resulted to humiliating her using emails sent to her copied to other employees. However when confronted face-to-face over his email content, he does not portray the same boldness as his email portrays.
- ·most believe they can get away with it and in Kenya many have.

5. How did you respond when harassed (– report to the policy/system administrator etc and what was the outcome? Communicate to the harasser?)

- ·a representative of (association for Media women in Kenya)AMWIK noted that Kituo cha Sheria, a legal aid organization has very good linkages with the police. Some of these legal aid organizations have links with police departments and cybercrime victims should be encouraged to consider presenting their cases through such organizations rather than approaching the police departments directly, because our police do not understand the phenomenon, do not have the capacity nor skills to deal with this kind of crime and the law while clear on ethnic related hate messages does not deal with cybercrime against women or the person. Participants noted how long it has taken Kenya to institute legal measures to deal with physical violence against women and sexual harassment.
- ·**KENIC (Dot ke ccTLD)** has established policies to attempt to deal with cybercrime from a Domain Name System (DNS)abuse perspective. The level of implementation, however, is hampered by lack of firm legislations to back their efforts. up. KENIC receives a lot of complaints on DNS abuse. An example is a case in which someone registered a domain for the Kenya Revenue Authority (KRA) and proceeded to upload malicious content attacking the Director of KRA.

KENIC's domain registration policies are clear, however, the content carried on such websites/face book pages, etc would be the responsibility of the police, the Communications Commission of Kenya (CCK) etc. When such information of abusive offensive content is reported, the police are not able to do much with it due to lack of established procedures to handle such cases. Another example is the registration in Kenya of domain for "Barclays.co.ke". Barclays is a registered international trademark but KENIC cannot do much to protect the copyright because it does not have existing partnerships with the copyright society which can assist in blocking copyrighted trademarks. Omissions such as these create loopholes and create a thriving environment for cybercrime.

PREVENTION AND PROTECTION

6. **Which actors have and /or should have a role to combat cybercrime against women? What are their roles?**

Government

When referring to the government, it is important to define which government agency should take the responsibility. The National Communications Secretariat (NCS) is the policy arm of government that engages in research regarding ICTs and it should be lobbied to actively assist in conducting research on the prevalence of cybercrime in Kenya.

Participants observed that it seems like the NCS do not update themselves on global trends on communications.

NCS should be engaged actively in forums such as these, ICANN, IGF, etc because they need continuously update themselves on global communication trends to be part of the dialogue process that will eventually lead to the drafting of appropriate policies. Cybercrime policy must be flexible and evolve as cybercrime evolves.

The Regulatory authority the CCK, needs to take the issue of cybercrime seriously. Currently, the commission has drafted regulation on various sections relating to the recently revised Kenya Communications Amendment Act 2009, but do not seem to be clear on convergence and how that will impact on content regulation as a way of dealing with cybercrime.

We must however, be careful about calling for increased regulation of content, because this could end up infringing on our rights to communicate.

Government also needs to build capacity of law enforcement institutions to enable them to deal with issues of cybercrime.

Parliamentarians

Review of existing acts including communications act, sexual harassment, etc to include provisions to deal with cybercrime against women.

Private Sector (ISPs etc)

Private sector entities and industry in general must also play a role. From developing technical solutions for dealing with cybercrime for example, solutions for women to use to protect themselves, solutions that make it easier to track cybercriminals, creating awareness of the issue, among others.

Civil society

The civil society has a great role to play and should take a first step and compile a database of all the prevailing issues on cybercrime so that a case can be built as this will prompt the government to act. Civil Society always tend to fill in the gaps left by industry and governments and therefore always ahead in terms of understanding the issue and being able to articulate it and propose technical, policy solutions.

Civil society organizations must also continue to create awareness about the issue, advocate for policy frameworks as well as place the issue on the policy and public agenda. They can continue to research on the issue to monitor the trends.

KENIC

KENIC receives cybercrime complaints mainly related to the abuse of DNS. However, lack of a legal framework in Kenya to adequately address DNS abuse makes it difficult to deal with the issue. KENIC does what it can based on its internal policies and procedures but these efforts are hampered by the lack of legal frameworks to guide the process. Forums such as this can fast track the policy formulation process.

Media

The media also needs to take an active role in sensitizing the public on cybercrime issues. A positive step on this front is the invitation extended by Kiss FM, one of the most popular FM stations in Kenya, to appear on one of their shows to discuss the issue, a first step towards placing on the public agenda.

FINAL SESSION: ADDITIONAL VIEWS

Should the focus of the forum be around women? Are women affected by cybercrime differently?

- ·Most women are affected differently mainly due to the way they are socialized.
- ·other studies conducted reveal that most women who fall victims have had very limited or have not had access to ICT and are thus vulnerable and gullible.

- ·Women are also more trusting and tend to have a softer approach to appeals for help
- ·Most women who are victims of cybercrime are not aware that what is happening to them is wrong.
- ·Women would not report incidences of abuse to avoid being ostracized, etc. This is a huge problem because it then means that the issue will take longer to be acknowledged as critical to women's exercise of their rights to communicate.

Does the sexual harassment act in Kenya cover cybercrime? Can we begin to advocate for an amendment in the act to cover cybercrime?

In relation to sexual harassment, attendees from the Coalition of Violence Against Women (COVAW) noted that they attended to many victims of abuse through SMS. On average, COVAW revealed that they handle 30-50 complainants per month. An interesting aspect that emerged was that most victims of sexual offences afflicted over the internet usually channel their cases directly to the police, where as the meeting established, they get limited assistance. While those who report to COVAW for help will usually report abuse having started on mobile phones, using sms's, which has then led to physical abuse? COVAW has recovery centers at the Kenya National Hospital (KNH) and Mbagathi hospital which cater for most victims who are from the Kibera slum area. Most of the complainants only visit the centre after they have been violated physically – they do not register their complaints immediately when the abuse starts on sms's. By the time they visit the centre, they are desperate and harm has already been inflicted upon them. The meeting agreed that there is need to engage COVAW more in the research as it is an important data source especially on SMS crimes affecting women as well as further advocacy work.

Challenge in getting Women's organizations to participate

It has been challenging for the research team to mobilize women's organizations. The issue does not seem to be that important to attract sufficient attention from the women's movements that have cited other issues like health, education as more pressing. Participants were informed that the upcoming 2010 Commission on the Status of Women (CSW) conference in New York, USA will first time will focus on Science and Technology and this presents a good international platform for women's organizations in Kenya to begin to deal with the issue of women a cybercrime. A participant from the Kenya ICT board offered to assist with making the connections and advocacy efforts on the same.

Way Forward

It was proposed that a working group be established consisting of the participants (women's organizations, private and public sector, media and technical community) to continue to advocate and place this issue on the public and policy agenda.

A mailing list would be developed immediately to continue these discussions, to begin the work of the working group. It was also agreed that a website would be developed as both an advocacy tool.

Other points for consideration

- ·the ongoing study should consider the role of prisoners who perpetrate some of the cybercrime offences behind prison walls.
- ·another factor that needs to be evaluated is the controversy that is generated by cybercrime.
- ·The judiciary it seems has shown an interest in cybercrime cases especially those pertaining to SMS abuse and seems to have persecuted a few cases since last year, thereby sending a strong message that cybercrime is illegal. These cases need to be highlighted by the media and the links made.

Concluding remarks

To maintain the momentum, the conveners of the meeting received consensus to set up a mailing list and developed a website to encourage continued dialogue and engagement on this topical issue. Participants were requested to contribute as much as possible to the research process by sharing experiences and ideas as this will build up a database.
It was agreed that the report will be posted to the mailing list for further comments/additions.

Vote of thanks
Conveners of the meeting thanked

- The International Development and Research Centre (IDRC) for supporting the research study
- Internet Society (ISOC) for supporting initial advocacy activities including this workshop
- Carol Thuku and Dr. Catherine Adeya for coordinating, organizing, not taking and the final workshop report writing.
- All participants for their energy and valuable contributions.