Creating a safer digital world for young women.

PROJECT SHIFT

NEEDS ASSESSMENT REPORT SUMMARY

SEPTEMBER 2015

YWCA CANADA | UN POINT TOURNANT POUR LES FEMMES | A TURNING POINT FOR WOMEN

project shift

Status of Women Canada

Canada

TABLE OF CONTENTS

project shift.

Creating a safer digital world for young women.

Alma Estable & Mechthild Meyer
Gentium Consulting
Submitted to
YWCA Canada

ACKNOWLEDGEMENTS

This research was funded by Status of Women Canada through the Cyber and Sexual Violence: Helping Communities Respond program. YWCA Canada is grateful for their support without which this project would not have been possible. YWCA Canada would like to thank Mechthild Meyer and Alma Estable of Gentium Consulting, the researchers of this project and writers of the needs assessment report, for their expertise, dedication and remarkable work. We would also like to thank the participating YWCA Member Associations, Kids Help Phone and other project partners for sharing their time and knowledge. The project advisory committee, partner groups, and young women's advisory council provided essential guidance in the development of the project and reflections on the research.

Project Hubs:

- YWCA Agvvik Nunavut
- YWCA Lethbridge & District
- YWCA Moncton
- YWCA Montreal
- YWCA Toronto
- YWCA Yellowknife

Project Partners:

- 4Rs Youth Movement
- Canadian Council of Muslim Women
- CYCC Network
- Disabled Women's Network
- Facebook Canada
- Gentium Consulting
- Girls Action Foundation
- Jane Bailey, Associate Professor, Faculty of Law, University of Ottawa
- Kids Help Phone
- Ladies Learning Code
- MediaSmart
- Microsoft Canada
- Nika Naimi, Cybersecurity Expert and Lecturer, École Polytechnique de Montréal
- RCMP Centre for Youth Crime Prevention
- Student Commission
- YWCA Cambridge
- YWCA Halifax
- YWCA Hamilton
- YWCA Kitchener Waterloo
- YWCA Metro Vancouver
- YWCA Peterborough Haliburton
- YWCA St. John's
- YWCA St. Thomas-Elgin

National Cross-Sector Advisors:

- Altus Dynamics
- Atwater Library & Computer Centre
- Behaviour Interactive
- Canadian Women's Foundation
- Kids Help Phone
- Manitoba Crown Attorney
- Office of the Privacy Commissioner of Canada
- UofT Faculty of Information Studies
- Voices of New Brunswick Women Consensus Building Forum

YWCA Canada:
104 Edward Street
Toronto, ON M5G 0A7
Tel: 416-962-8881
Fax: 416-962-8084
national@ywcacanada.ca
www.ywcacanada.ca

This document is also available in French.

This project is funded by the Status of Women Canada. The opinions and interpretations in this publication are those of the author and do not necessarily reflect those of the funder.

ABOUT PROJECT SHIFT

YWCA Canada's PROJECT SHIFT: Creating a safer digital world for young women will engage communities to prevent and eliminate cyberviolence against young women and girls across Canada. Project Shift's diverse stakeholders (YWCA member associations, public sector policy makers, justice and legal professionals, violence against women experts, digital market players) are responding to girls and young women's needs by identifying issues and developing strategies to prevent this form of gender-based violence.

Funded by Status of Women Canada, the 30-month project was launched in May 2014, beginning with a year-long participatory needs assessment, reported here. Its recommendations will be shared through knowledge exchange activities across the country and will inform the strategy implementation phase (Fall 2015).

PURPOSE OF THE NEEDS ASSESSMENT

The Needs Assessment aimed to fulfill the following objectives:

- Identify institutional barriers that make it difficult for communities and individuals to address cyberviolence against women and girls
- Identify approaches to engage youth and communities to prevent and eliminate cyberviolence
- Identify and engage key stakeholders that wish to collaborate
- Identify knowledge gaps and develop strategies for collaboration to address issues of cyberviolence

We incorporated the following principles:

- Fostering participation and input by those affected
- Building on knowledge that already exists to identify knowledge gaps
- Focusing on empowerment
- Engaging new community stakeholders
- Building capacity by sharing expertise
- Considering ethical consequences
- Incorporating evaluative thinking
- Linking process and outcomes

GENDER+ FEMINIST & VIOLENCE AGAINST WOMEN (VAW) ANALYSIS

We refocused gender-based analysis to include feminist analysis combined with a VAW lens. Beyond documenting the gender identity of victims and perpetrators, this encouraged discussion of deeper issues related to cyberviolence:

- How are gender identities created and who benefits if they remain unchallenged?
- What is the role of violence in enforcing gender differences?
- What social and economic purpose is served by reinforcing gender differences?

GENDER + FEMINIST/ VAW ANALYSIS	Considers the context of male violence against women through which men as a group dominate women as a group
	Understands violence and the threat of violence as one of the most direct techniques used by societies to control women and preserve male power
	Links the above to economic structures to maintain unequal relationships that benefit men
	Identifies clear targets for societal transformation

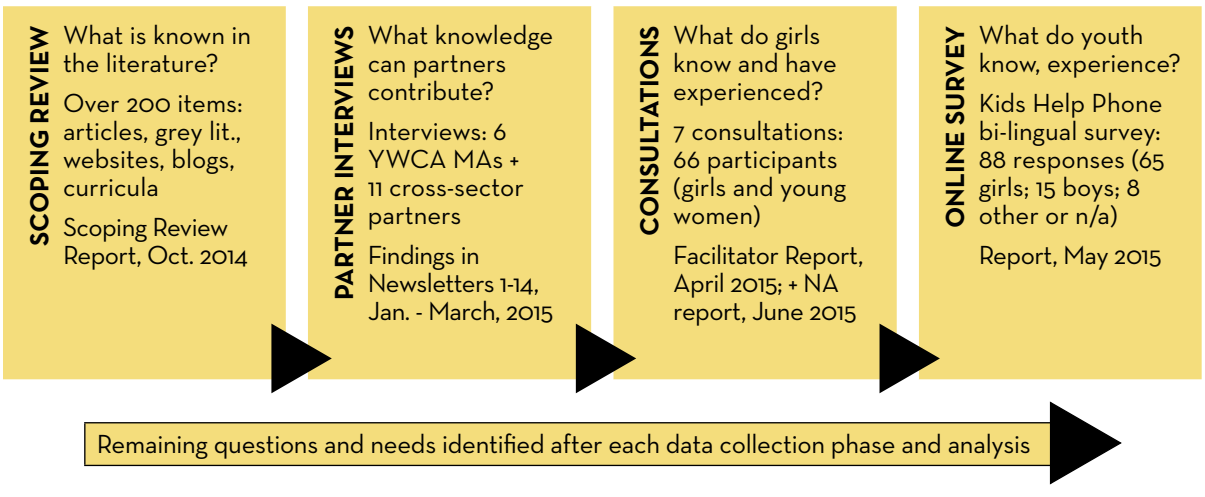
METHOD

The needs assessment sought to answer four key questions:

1. Are there institutional barriers that make it difficult to address cyberviolence against women and girls?
2. Who are the key stakeholders in Canada?
3. What approaches and strategies are being used to engage young women and their communities in prevention of cyberviolence?
4. What are the current knowledge gaps?

The Project Team, with feedback from project partners, selected sources and methods for gathering needs assessment data:

Figure 1 - Needs Assessment Process



FINDINGS

What institutional barriers make it difficult to address cyberviolence against women and girls?

BARRIER	EFFECT ON ADDRESSING CYBERVIOLENCE
Quality and diversity of research and its dissemination	Research literature is of mixed quality, and often includes contradictory claims, making it difficult to know: - The extent of the impact of cyberviolence on women in Canada - Whether strategies being used to combat other types of violence are likely to work to address cyberviolence - Which strategies have been tested and found successful
Prevalence of literature about cyberbullying	Educational sector focuses on cyberbullying; hard to reframe the issue as cyberviolence: - Considering it a VAW issue, and applying a feminist analysis - Recognizing cyberviolence extends beyond the school setting
Role of private enterprise in public digital spaces	Tension between approaches that seek to protect the public and reluctance or inability to regulate cyberspaces Market research drives the search for knowledge about types and incidence of cyberviolence, and proposed solutions Profit motivates companies to develop software to protect users (filters, child locks, teaching guides) Power asymmetries: discrepancy between resources available to communities and organizations seeking to influence girls and young women's experiences with new media, compared to those of corporations that own the digital world
Role of media in re-framing the issues	Moral panic and shifting focus: Media thrive on disseminating sensationalized reports of individual tragedies, including cyber abuse of children, girls' victimization. May contribute to: - Reducing focus on abuse and violence against women where it most often occurs (at home, by people known to them), shifting to 'stranger danger' in the digital world -Changing funding priorities to combating cyberviolence, rather than focusing on violence against women - New and old media promote sexualized representations of women (and men), contribute to cyberviolence through imitation, trivialization, normalization.
Framing the issue as part of cybercrime / anti-terrorist proposals	Inclusion of measures to combat cyberviolence with legislation that permits greater intrusion into private communications (i.e. Bill C-51) limits ability of defenders of civil liberties to align themselves with those concerned with combating cyberviolence

FINDINGS

Who are the key stakeholders in Canada?

- Women's organizations
- Media and software companies
- International organizations
- Legal organizations
- Faith-based organizations
- Child and youth organizations
- Community groups
- Individuals (i.e. blogs, websites)
- Media and communications organization
- Criminal justice, crime prevention, public safety and policing organization
- Academic scholars and centres of research
- Educational sector, including educational institutions
- Health and social service non-profits
- Federal, provincial and territorial governments

What approaches and strategies are being used to engage young women and their communities in prevention of cyberviolence?

The literature lacks precise information about the scope and extent of the problem. Beyond prevalence and incidence, we also need to better understand what causes cyberviolence, to be able to prevent it.

Understanding the problem: Why is this important? Strategies and interventions to address a problem arise from how it is understood. Young women and community organizations will propose strategies and interventions based on how they define and conceptualize the problem of cyberviolence.

Framing the issue: Interventions and strategies addressing cyberviolence have been developed for specific settings (e.g., school, workplace) and within the violence against women discourse.

School-based interventions: Since schools are an accessible setting for intervention research with youth, we know most about cyberbullying in the educational sector.

Most approaches are based on standard health promotion or educational interventions, e.g., awareness raising and behavioural change curricula embedded in whole school approaches.

Some interventions incorporate cyberbullying as one dimension of bullying; others target cyberbullying separately.

Some are peer-to-peer interventions; others have in-classroom educational components delivered by teachers. A few incorporate online methods.

More regulatory approaches (e.g., school board-level policies) sometimes include punitive elements (e.g., suspending offenders). Few of these interventions have been evaluated, although recent research suggests some approaches show promise (especially those focusing on developing empathy).

Other settings: There is less clear and consistent information about ways to work outside of schools and beyond the educational sector, and in relation to other types of cyberviolence.

Types of strategies range from broad-scale social prevention of many types of violence (through education, policies, legislation, regulation, peer pressure, etc.), to supporting criminal investigation and prosecution of individual perpetrators.

Some approaches target behavioural change at different levels: individual, group and/or organizations and companies.

The level of intervention varies considerably. Some simply consist of providing on-line information. A frequent approach is to invite website or social media users to report negative experiences (e.g. filling out a questionnaire). These may or may not be reviewed, go beyond the site, or become formal complaints.

FINDINGS

Gender/VAW lens: The violence against women literature describes approaches that address gender and/or other inequalities at the social level. For instance, cyber-stalking is framed as one form of intimate partner violence. Strategies are proposed to make women's shelters and survivors safer.

Some feminist scholars pose a bigger question: how do women survive and thrive in cyberspace without being attacked? This counter-discourse looks at the issue within the context of addressing violence against women, and considers whether women in an unequal society may need their own space, including online space. Women's safety within cyberspace has similarities to safety for women in physical space.

Other approaches focus on:

- social change strategies to address women's inequality and oppression
- understanding social media bullying as part of dating violence
- sexualization of girls and stereotyping of women
- empowerment of women in cyberspace (e.g. gaming)
- survival of intimate partner violence perpetrated through new technologies
- sexual trafficking of girls and women
- how women's empowerment contributes to image/reality of women as perpetrators of violence (the' mean girl' and 'sluts' discourses)
- shifting the focus back to the setting where violence occurs most frequently (home, family)
- enforcement of current legislation and/or introduction of new laws to address specific issues of cyberviolence.

What were the knowledge gaps after completing the scoping review?

The literature confirms that, despite an increase in attention to the issues of cyberviolence in recent years, important gaps remain. For the next stage of this project, we explored some of these gaps with partners, stakeholders, advisors, and project participants.

- Is there a consensus about what is happening in Canada?
- Are there sound statistics, understood by Canadians as representing what is happening here, which can help us to understand the extent of the problem of cyberviolence directed against girls and women?
- Can we develop a common understanding of the origins and causes of cyberviolence against girls and women in Canada?
- Is there a cyberbullying prevention approach that is gender sensitive, recognizes that girls also can be perpetrators, and actually works?
- Is there any evidence (e.g., program evaluation reports for smaller initiatives) that a particular strategy has had an effect in preventing or reducing cyberviolence against girls and women outside the school setting?
- Should resources focus on individualized response to cyberviolence versus a collective response, e.g. systemic regulation of cyberviolence versus teaching individual girls how not to surf certain sections of the internet?
- Is it possible to shift the culture of cyberspace to diminish cyberviolence against women, without shifting the culture of society at the same time?
- Are there concerns about the criminalization of alleged perpetrators of cyberviolence (youth, minorities) in Canada? Are alternative legal frameworks for dealing with this issue workable?
- What specific policies and strategies have been applied successfully at a community level to address cyberviolence?
- How are communities defined in this project (e.g., geographical, relational, cyberspace, other)?

FINDINGS

HOW YOUNG WOMEN AND GIRLS UNDERSTAND AND EXPERIENCE CYBERVIOLENCE

Girls and young women shared how they understand and experience cyberviolence, through consultations and a survey.

What does cyberviolence consist of, how is it defined?

A common vocabulary to describe and label behaviours can help girls and women to describe their experiences, facilitate knowledge exchange, and support the development of common strategies. Both consultations and the survey specifically asked about the meaning of cyberviolence.

Many girls seemed knowledgeable about various forms of cyberviolence, and were able to describe and illustrate specific cyber-violent behaviours. They often used cyberbullying and cyberviolence as synonymous umbrella terms that cover many forms of online abuse, from online harassment to revenge porn to cyberluring. A few distinguished between the terms cyberbullying and cyberviolence (with cyberviolence being more severe, more harmful).

Three-quarters of survey respondents defined cyberviolence. One quarter (26%) understood it as including online threats and intimidation; 12% described it in terms of harassment (12%) and abuse (12%), including verbal abuse.

Ranking the severity

Consultation participants were asked to rank the severity of different types of cyberviolence. Many used the anticipated impact of an action to determine the severity of some forms of cyberviolence, such as flaming or phishing. Almost all participants ranked some forms of cyberviolence (e.g. cyber-luring) as 'severe' because they targeted young children. Participants, like some survey respondents, explained that their assessment would depend on contextual factors such as:

- Identity of the perpetrator and their relationship to him or her
- Purpose, intended impact that the perpetrator had in mind
- Dissemination: how widely the post could be seen by friends or by others
- Characteristics of the victim e.g., position in the peer group, age

The most cited example of 'depends on the situation' was related to sexting: participants in four consultations pointed out that consensual sexting was neither bad nor violent. On the other hand, distribution of the same intimate photos without consent, or to seek revenge, would be cyberviolence. Survey respondents also emphasized that distributing intimate images without permission was inappropriate and could be considered cyberviolence.

Another example of 'context' related to being pressured to provide intimate images (e.g., male players requesting these for girls to be accepted in the gaming world).

GENDER ANALYSIS: HOW GIRLS AND BOYS EXPERIENCE THE CYBER WORLD

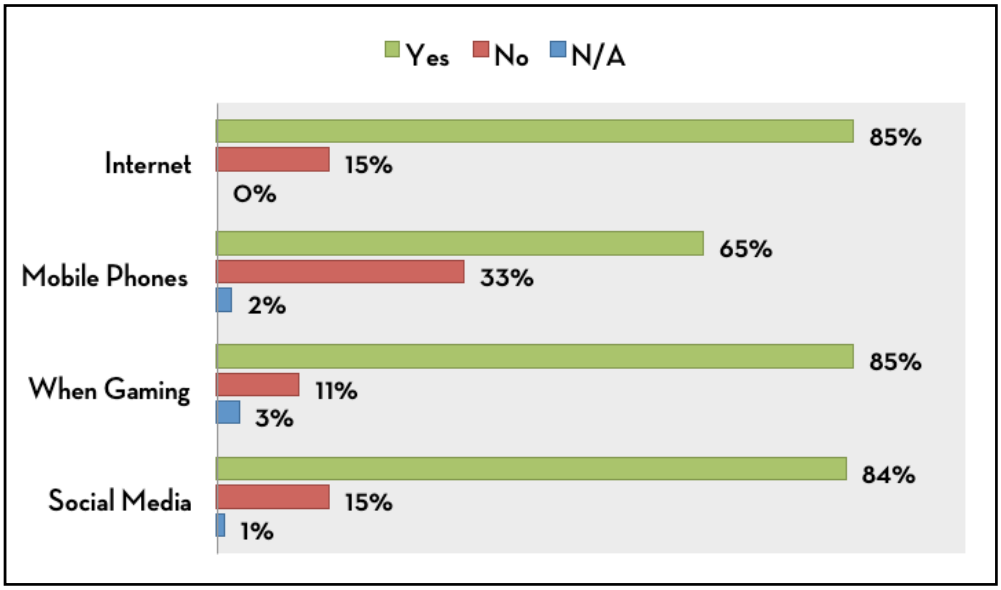
A gender analysis compares how girls and boys experience the cyber world.

Both survey respondents and consultation participants provided rich descriptions of many instances in which girls and boys experienced the online world in very different ways. In the survey, these differences were addressed directly through the following question:

Do you think that girls and boys have different experiences (e.g.: are treated differently):

- On the internet?
- Using mobile phones?
- When gaming?
- On social media?

Figure 2 – Survey: Do girls and boys have different online experiences?



In contrast, in two consultations (with the youngest participants) some participants thought girls and boys had the same experiences online.

The interplay of gender and reported experience is complex, and at times difficult to tease out. In many instances, young people did not specify the gender of those whose actions they were describing: they used the passive tense, or described how 'they' did something. In other examples, the gender of perpetrator, target, and/or witness was specified. For example: girls described their own experiences as perpetrators of cyberviolence targeting other girls both during consultations and in the survey. Information from boys (rather than about boys) is only available through the survey, and includes descriptions of males as targets of cyberviolence, as well as perpetrators.

FINDINGS

Sexism and gender stereotyping: Consultation participants provided many illustrations of how their experiences of the digital world are gendered, and how their online experiences reinforce offline gender inequalities and stereotypes:

- Sexism in the media and culturally constructed images of women and men.
- Encouraging sexualization online, as a way to attract attention.
- Underlying issues that could contribute to cyberviolence: gender roles, beliefs that women and men should do some things and not others.
- Use of jokes, parodies to degrade women.
- Connection between sexism and the way girls think they need to represent themselves and appear online (internalized sex roles).
- Rating women on their appearances online; women linking self-esteem to number of 'likes' or 'followers' when showing their bodies; taking 'selfies' and asking to be rated on appearance, rather than personality, abilities, or skills.
- Repercussions of experiencing cyberviolence (i.e. eating disorders, depression).
- Degrading comments about women on social media and in online videos.
- Victim blaming: recognizing that when girls present themselves in certain ways, it is a product of gender socialization.
- Challenges reporting violence against women generally; rape culture and victim blaming.
- Impact of gender stereotypes on men: Assumption that men/boys are less equipped to deal with cyberviolence/cyberbullying as they lack supportive social networks and are expected to 'act like men'.
- Boys and men sending images of their own bodies, including their genitalia, to attract the attention of young women, who often found this offensive (also mentioned by survey respondents).

Safety: Some young women believed that young men felt safer in the cyber world than women. As a consequence, some are more cautious in revealing their identity and remain anonymous; in comparison, they observed males more likely to identify themselves.

Double standards: Participants in five consultations were critical of the double standard used to assess the behaviour of young women and men:

- Young women who engage in sex are called 'sluts' when talking online about their sexual activities, whereas boys are considered 'studs'.
- Young women's sexual behaviours are labeled as improper, whereas young men behaving in the same way are celebrated.
- When posting photos, young men are permitted to show how they were engaging in self-pleasure in explicit images, whereas young women are expected to cover up their bodies.

Gender differences in experiences with cyberviolence

Perceived differences of young women and men as targets or victims and perpetrators

AS TARGETS OR VICTIMS	
Young women as targets or victims of cyberviolence are more likely to be :	**Young men as targets or victims of cyberviolence are more likely to be:**
Targeted for their bodies, brains, and abilities (what they can and cannot do)	Bullied if seen as 'weak'
Judged on their appearance, objectified	Mocked for using certain sites (e.g. Instagram) that are assumed to be only for girls
Picked on, disrespected, treated viciously	Mocked for their preferences or the things they say or do
Shamed, slut-shamed	Recipients of rude or inappropriate comments about a boy's mother or family
Manipulated	Bullied in general
Called derogatory names	Victims of internet proxy attacks and DDOS attacks
Put down for displaying confidence	
Not allowed to share their thoughts and opinions	
Harassed during gaming, shut out of games	
Targets of anger when they win at games	
Sexually propositioned or harassed	
Punished for bad behaviour (e.g., sexting)	
Threatened with rape, murder or other violence	
Experiencing backlash (e.g., having their social media profiles searched by employers)	
Seriously affected by online 'hate' (e.g., depressed to the extent of committing suicide)	
Conditioned and intimidated to act in a certain way	
Labelled or put down for confronting inappropriate comments (e.g., not having a sense of humour; called a man hater or feminist)	
Involved in incidents that drag on	
AS PERPETRATORS	
Young women as perpetrators of cyberviolence are more likely to:	**Young men as perpetrators of cyberviolence are more likely to:**
Cyberbully, shame others	Get what they want
Be cruel to one another	Use sexist chauvinistic language
Be manipulative	Get away with bad behaviour; not be held accountable
Be vicious online, call others names	Be in solidarity with each other to protect boys' 'bad' behaviours
Expose weaknesses of their friends	Call boys 'soft', 'weak', 'gay'
Use online technology (rather than in-person confrontation) to hurt each other	Insult, call names, swear (directed at boys)
Commit fraud on the internet	Harass (both boys and girls)
Engage in gossip, spread hateful rumours	Disrespect girls, be rude
Isolate (unfriend, unfollow)	Proposition girls
	Send inappropriate sexts to girls
	Refuse to play with girls

FINDINGS

Experiences of girls and boys as TARGETS of cyberviolence

Both consultation participants and survey respondents provided many examples, and critically examined gender differences, at times with the intention of challenging gender stereotypes. Participants described boys and girls as equally likely to be:

- Stalked
- Affected and emotionally hurt
- Internalizing negative comments

Many participants described male reactions to cyberviolence, often in contrast with those of women and girls. Arising from men's socialization (e.g., showing emotions is a sign of weakness) they believed boys who experience cyberviolence were less likely to:

- Be affected by comments, care what others thought about them
- Be treated with compassion when being hurt or attacked
- Confide in family or friends, or ask for help
- Feel comfortable to talk about their experiences
- Address emotional issues because they should be able to handle online incidents

Consultation participants and survey respondents both noted that boys that fit the 'male' stereotype (confident, dominant, strong) were less likely to be bullied online.

Experiences of girls and boys as perpetrators of cyberviolence

During the consultations, several girls described instances in which they were perpetrators: they had acted in a hurtful, negative or inappropriate ways online. Some also offered explanations of their motivation, the consequences it had, and their learning from those experiences. Motivations included:

- Jealousy, wanting to hurt and seeking revenge
- Anonymity
- Judging others and making fun of them by using gender stereotypes
- Peer pressure, fitting in with the peer group
- Power: to be at the top of the peer group

Their learning included developing empathy by remembering what it had felt like when they had been harassed online. Some realized how they had contributed to escalation of hateful exchanges, which they now regretted.

FINDINGS

Gaming: a special case in cyberviolence against girls and women

Consultation participants and survey respondents were asked about their experiences with gaming online. Just over half (54%) had done online gaming; 12% were daily gamers, and 17%, weekly. There was more content about the different experiences of females and males in gaming than anywhere else (e.g. social media, mobile phones). At two consultations, participants described multiple manifestations of cyberviolence in the gaming world in a particularly pronounced way. Survey respondents consistently described the experiences of girls while gaming as negative.

Participants and respondents, both girls and boys, described sexism that appears pervasive on gaming sites. In the consultations, young women gamers reported experiencing a high level of sexist attacks, to such an extent that some of them had to change their gamer identity, incurring additional costs and/or setbacks in their gaming profile and statistics. Consequently some young women drop out of gaming altogether, feeling they've been "harassed off the internet". Girls who responded to the survey also described being the target of sexual comments and sexual solicitation while gaming.

Both survey respondents and consultation participants described an environment in which it is often assumed that girls can't play well, or shouldn't play. Girls reported they experienced more attacks and putdowns when they were winning, including comments that challenged their right to claim their own victories: male players saying that only another male (boyfriend or brother) could have possibly played that well, because women do not possess the skills to game well and win. Participants described how, after winning, women face put downs and harassing comments which may make them reluctant to continue gaming. Participants also described being threatened with physical violence after winning a game.

In summary, the discussions and responses confirmed that gaming is a male-dominated space. Participants explained male reactions to losing as arising from feeling that their masculinity was threatened. By personally attacking women who had beat them in games, males were trying to restore their self-confidence and sense of superiority. Girls and women who game need a great deal of self-confidence, coping strategies and skills in order to be able to function in a recreational space that is hostile toward them.

Why does cyberviolence happen? What do young women think are the root causes?

We analyzed the content of open-ended survey answers and consultation transcripts to identify when, and how, respondents commented on possible causes of cyberviolence. Some considered the motivation of perpetrators (e.g., intent to harm) as a factor.

FINDINGS

LEVELS	CAUSES / MOTIVATIONS
Individual / interpersonal	Needing to fit into a peer group: - Exerting peer pressure, controlling, policing, monitoring others to ensure they conform with group norms - Trying to fit in with a peer group, feel accepted - Demanding proof of trust Lack of social skills: - Feel powerful, exploit another's perceived weakness - Empathy, confidence, coping skills or sense of what is acceptable Unable to differentiate between the digital world and real life Judging, disagreeing with someone Seeking attention, craving 'drama Planning revenge, destroy someone's reputation, hurt or intimidate Get sexual favours Create unsafe spaces Blackmailing
Family	Parents and families contribute to modeling behaviours and attitudes (name-calling, abusive) that may lead to cyberviolence Lack of guidance and supervision
Societal	Gender socialization, inequality and sexism: - Understanding that gender is socially structured category, with gender stereotyping and sexism contributing to cyberviolence in a culture that perpetuates inequality and violence against women. Young women are socialized to be quiet, not to confront others or voice their opinions; - tend to be more interested in friends, relationships, gossip; focused on appearance, competing with one another. - Young men are socialized into privilege giving them greater leeway on how to behave and face less consequences; tend to be more self-reliant and less concerned with relationships other than for sex, but can be vengeful when their pride is challenged (e.g., in gaming). Culture of violence against women: - Violence against women in the physical world can extend to the online world, as a means through which partners or ex-partners use digital spaces or technologies to continue controlling and harassing their partners. - Rape culture: Tendency to blame survivors for acts of violence committed against them; if women do not conform to societal expectations, they placed themselves in a position to be victims.
Technological	Technology is not the cause, but the means through which cyberviolence happens, where societal problems and inequalities are intensified. Anonymity behind the screen: - Permits people to feel powerful in voicing an opinion - Allows people to do something they otherwise might not do - Can easily pass blame onto others - Can directly express feelings without filters - Feel invincible - Large audiences can be reached - Provides illusion of equality; everyone has a voice - Can feel powerful online; contrast with being powerless offline

HOW DO YOUNG WOMEN AND GIRLS DEAL WITH CYBERVIOLENCE?

Consultation participants and survey respondents suggested many different strategies to respond to cyberviolence. They discussed technological options, who they might go to for help, and how well their own actions had worked in the past.

Individual responses/actions

Some respondents didn't know what they would do, or would take a passive approach. In contrast, others suggested engaging or replying to the perpetrator, although this was difficult and took courage, especially if one was not used to speaking up.

Participants assessed whether direct responses to hurtful comments had the desired effect. In several instances, they described how their actions worked to stop the harassment, de-escalate a situation, or change the tone of an online conversation.

INDIVIDUAL RESPONSES	EFFECTIVENESS
Don't know what to do	Participants in three consultations admitted they would not know what to do; some solutions were 'hit or miss'; they were unfamiliar with the technology; not aware of possible responses 24% of survey respondents would not know what to do if there were online threat or problems 50% would not know how to respond if their pictures were circulated online without their permission
Ignore/avoid/do nothing	First action for many participants and respondents; many found it worked well as an initial response.
Staying offline/ disconnecting	Tactic used by some survey respondents. Unrealistic to stay offline; could have potential negative impacts (isolation, missed job opportunities).
Requesting or encouraging the perpetrator to stop	Straightforward request, either in private or offline, was the best way of responding Eliciting empathy from the perpetrator worked sometimes 'Calling out' negative posts or correcting mistakes could be effective in raising awareness, resulting in perpetrators changing their behaviour
Responding with humour, unexpectedly	Responding with humour, sarcasm or in a way that was unexpected had prevented a situation from escalating.

FINDINGS

Acting in support of others - bystander responses

Consultation participants described many instances in which, having witnessed cyberviolence, they chose to act to support the victims or targets in a number of ways:

- Standing up for others (e.g., asking others to stop the bantering on the friend's behalf, speaking out against a negative post)
- Posting positive comments in reply to negative ones
- Creating positive alliances among those who support the victimized friend, working together against this type of behaviour on Facebook
- Confronting hypocritical behaviour directly (e.g., pointing out that someone has been telling others not to bully, but does it herself)
- Refusing to become part of a trend, resisting peer pressure
- Providing support to those who have been attacked (e.g., online or offline, by sharing their disagreement with what had been said about the victims)

Technology-assisted responses

Consultation participants and survey respondents described two types of technology-assisted strategies in response to cyber incidents: blocking callers/users on mobile phones or online (three consultations), and reporting inappropriate content to social media sites or internet providers (seven consultations).

TECHNOLOGY-BASED RESPONSES	EFFECTIVENESS
Blocking	68% of survey respondents had blocked someone and 80% found it to be effective. Participants had varied technological understanding of how to block and hence had varied results. Demonstrates that comments are unwanted, and can be used as a gesture of solidarity with a friend. Some argued it is not effective because perpetrators could simply create a new account to continue the harassment. Does not address the harassment that often continues offline, which can worsen as a result of the blocking. Could also be used as a tactic by a perpetrator to 'out' someone from a group.
Reporting to social media platforms or service providers	20% of survey respondents would use this strategy Discussed in most consultations as a means to deal with more serious cyberviolence issues (not specified). Ineffective: almost never leads to any action. Only one participant could identify an instance in which reporting was successful, and involved several attempts with many people over a long period of time.

Getting help

Many consultation participants and several survey respondents would prefer to deal with the situation themselves. However, some participants emphasized that not trying to deal with incidents alone was an important strategy to address experiences of cyberviolence to avoid falling into a depression, prevent situations from escalating or dragging on, and find solutions to the problem.

SEEKING HELP FROM OTHERS	EFFECTIVENESS
Parent or family member	31% of respondents (all under the age of 16) would approach a parent or family member: people who cared for them, would not judge them, and would know what to do. Older participants and respondents would go to their parents as a last resort, because parents would not be understanding or would blame them.
Friends	19% of respondents would ask a friend for help, and this was the most frequently discussed option in the consultations.
Police	16% of respondents would go to the police as their first choice, as they possess the power, authority and capacity to investigate and take action quickly. Participants described when it might be appropriate to approach the police, but questioned the level of effectiveness.
School	One in ten survey respondents said they would seek help at school because they trusted their teachers or the perpetrator was a student. Participants were equally hesitant to seek help at school as they felt that their concerns would not be taken seriously.
Community organizations, others	Few (6%) respondents said they would seek help from community organizations, counsellors or help lines. Some participants might seek out assistance at work or via online communities.
Someone you trust	In the consultations with the youngest age groups, participants explained that they would select the 'right' person to approach based on the level of trust and closeness of the relationship, not necessarily the position they hold.

What strategies do young women propose beyond the individual level?

Recognizing that individual-level strategies alone are insufficient to properly address the wider issue of cyberviolence, participants in all consultations discussed strategies for systemic and social change, including the need for policies at the societal level to regulate cyberspace. They also recognized that it was difficult to know who is responsible for regulating various communications technologies and responding to incidents, and that clarification is needed through policies at different institutional levels, such as schools, social media platforms, and governments. Their suggestions regarding policy interventions, using technology, and raising awareness are presented below.

FINDINGS

SYSTEM/ INSTITUTION	POLICY
Schools	School rules and policies considered to be useful: - Having clear rules about when to report - Blocking the use of certain social media sites because girls had sent compromising photos of themselves around - School suspension as a result of posting hateful comments - Clear protocols to investigate and mediate between perpetrator and victim when an incident has been reported to the school administrator - Ensuring that incidents are taken seriously, including when they happen outside the school setting
Communications technologies (social media platforms, app and game developers, service providers)	Companies should take greater responsibility and be more active to respond to incidents: - One complaint should be sufficient to have a post taken down - Moderators should be responsible for screening posts - Clearer policies and protocols that distinguish between violent, harmful acts versus other incidents
Governments	Increase public discussion about cyberbullying laws, particularly on what constitutes harassment with the inclusion of concrete examples; clarify criminalization of sexting and the implications of it being considered child pornography. While the original purpose of social media had been to connect people in a positive way, it permitted people to harm each other. Many laws exist but they are not well enforced, especially around making physical threats of murder or rape. Government should monitor social media companies more closely, to ensure adequate reporting structures are in place and implemented. The need to respect freedom of speech and privacy must be considered. Governments need to cooperate and work on these issues together across borders.

Using internet technology to identify and address incidents

Participants provided ideas for using technology to deal with cyber incidents:
Building language filters into software, to automatically screen for specific words or phrases and flag posts for review. A committee for the provider, developer or platform could then decide if the comment meets acceptability criteria:

- Blocking violators from signing in to sites.
- A website or chatline where users send copies of inappropriate messages and receive support
- Finding or creating spaces only for women
- Closed groups, moderated by women, to provide safety.

Awareness raising: prevention approach

Many participants believed that education and awareness raising were an important part of the solution, and would lead to specific positive outcomes at several levels. They suggested specific targets, content, and materials to help in raising awareness, and shared what they thought would not work well and should, therefore, be avoided. A certain level of empathy and ability to feel the impact of a hurtful

action was considered essential to preventing cyber incidents. A gender analysis is apparent in some of the proposed strategies:

- Avoid blaming the victim – tell the perpetrator what not to do, rather than emphasize what girls shouldn't do to get attacked
- Define the various forms of cyberviolence
- Avoid becoming too preachy, maintain a casual tone
- Targeting both boys and girls, rather than singling out girls who had been victims.
- During awareness raising activities: Avoid blaming the victim by focusing on what girls shouldn't do, rather than telling the perpetrator what not to do.
- Addressing unintended consequences of laws that have the potential to criminalize under-age sexting, as particularly punitive to girls.
- Taking seriously and enforcing laws that protect girls from threats of rape or murder
- Improving monitoring policies of social media companies to control for rape threats.
- Creating spaces on the internet (such as closed Facebook groups) moderated by women to increase safety, allow open discussion, and reduce risk of harassment
- Integrate raising awareness about cyberviolence with that of sexualization and rape culture
- Encouraging girls to be active online, to use/occupy cyberspace and technology
- Using internet sites to facilitate the exchange of new ideas from all over the world, raise consciousness of women's issues internationally, and provide space to report on sexist incidents and increase feelings of community among women.

TARGET GROUPS	APPROACH TO RAISING AWARENESS
Schools (teachers and students)	Start in primary school to increase openness in talking about the issues and causes. Mandatory content during school assemblies Since many teachers lack experience with new media, better equip them to support students and intervene Schools provide a good venue for awareness-raising activities given the captive audience
Youth	Informal conversations with friends Formation of support groups or clubs at school of local/national networks online Involve young women, including victims, in the development of resources, workshops, etc.
Parents	Address how they may model problematic behaviours Provide parents with skills on how to better recognize when their children may be victims or perpetrators
Other adults	Workshops in the workplace
General public	Resources made available via social media platform that are regularly updated, to teach users about available reporting and blocking functions and how to use them Accessible statistics or data regarding how the platform responded to reports, complaints, etc.

FINDINGS

HOW DOES THIS UNDERSTANDING COMPARE TO THAT OF THE PROJECT PARTNERS?

Project partners and young women involved in the consultations and survey had similar overall understanding of what constituted cyberviolence, using it as an umbrella term for many actions associated with it.

Not all partners felt ready to provide a definition of cyberviolence, and many hope this project would provide opportunities to develop a deeper understanding of the term and the issues. Partners did provide a more nuanced distinction between cyberviolence and cyberbullying, based on their experience working on the issues. Some felt that the terms could be used interchangeably, whereas others explained that the gender dimension was associated with the term cyberviolence, rather than cyberbullying. Several were positive about introducing the term cyberviolence, in contrast to the overuse of cyberbullying, hoping this would generate more interest. Participants, on the other hand, did not raise this issue.

One informant found the distinction between cyberbullying and cyberviolence useful for policy development, but less significant in the context of direct work with women clients. She explained that women who feel the impact don't care what it is called.

Partners also acknowledged how the quick evolution of the cyber world requires them to update their knowledge, and the terms used, on an ongoing basis, by consulting young people who are 'digital natives'. Partners seemed to be more concerned about legal definitions, and aware that there are implications to using particular terms, such as harassment, in certain situations.

Both young women and partners explored the impact that cyberviolence could have (shame, embarrassment, loss of reputation, humiliation) when discussing and defining the terms.

Participants described a wider range of feelings and behaviours resulting from unwanted comments directed at them, and analyzed to a greater extent contextual factors (intention, relationship to the victim, dissemination) to assess the severity of an incident.

Comparison: gendering the cyber world

This issue was approached differently with partners and young women. Partners were asked whether or not they knew how to apply a gender analysis to the issues, whereas participants were asked to share their experiences and talk about how their own might differ from boys.

Partners varied greatly in their assessment of whether or not they themselves or their organizations were applying a gender analysis to the issue of cyberviolence: those working in women's organizations all did, whereas for others it varied. Their responses can be placed on a continuum: from 'no gender analysis/gender neutral', to 'emerging understanding', to 'consistent application of a gender analysis'.

Overall, partners expressed a great interest in learning from young women how they experience the cyber world as compared to boys. They emphasized that girls and women should explain cyberviolence on their own terms, to increase everyone's learning.

In the context of exploring prevalence, partners also reported on some incidents of cyberviolence that they had heard about. These included cyberbullying based on faith, shaming, sexting and sexual exploitation, and emotional abuse endured by women victims of violence. The issue of faith bullying was the only issue that was not raised by participants. They in turn told many detailed stories about

how sexualization and stereotyping had shaped their experiences, both as perpetrators and recipients of cyber incidents. Attacks on young women during gaming were particularly vicious and widely reported by survey respondents, whereas partners did not bring up the issue of gaming.

Girls and boys (NB: small number of boys) in the survey also confirmed that their experiences differed. Several partners emphasized the importance of including the experiences of boys and men as part of a complete gender analysis of cyberviolence. Both boys and girls who responded to the survey also wanted to ensure that both boys' and girls' experiences were taken into account.

Comparison: Explaining the root causes of cyberviolence

Partners and young women attributed cyberviolence to similar causes that can be categorized into three main types: not significantly different from other types of negative social interactions; a unique consequence of modern communications technology; and resulting from unequal access of men and women to social power and control.

As described in a previous section of this report, girls explored the issues related to negative social interaction in great detail. The motivation to hurt someone and the many different reasons why someone would want to do that were identified as causes. Partners and participants mentioned specific features inherent in internet technology: possibility to remain anonymous; capacity to spread and replicate information quickly; ability to reach enormous audiences with little effort. On the other hand participants also expressed their belief that technology is not responsible for cyber-tactics: the people who use the technology are ultimately responsible.

Both partners and participants spoke of social structures as contributing to or causing cyberviolence. Partners spoke of a patriarchal or misogynist society, with power dynamics that favour men and control women. Participants used slightly different terms, talking about men being brought up to dominate women; their pride being challenged when women are successful (e.g., winning in gaming). They talked about a culture in which boys were privileged, able to act violently against women, and about rape culture. Both partners and participants spoke about society enforcing a 'double standard' for acceptable behaviours of men and women.

Those working with girls and women in groups talked about addressing cyberviolence through group dynamics, education and raising awareness. Those working in the field of communications described specific strategies related to particular platforms that users could use to protect their privacy and reduce exposure to negative communication. Partners involved in research about the issue shared their insight about the current state of the literature, including the extent to which interventions have actually been assessed and evaluated.

Partners and participants linked cyberviolence to gender stereotyping and sexualization of girls in the media. Partners also saw a connection with racial stereotyping. Girls did not address racism, but a few mentioned homophobia in the discussions.

CONCLUSIONS: WHAT ARE THE NEEDS?

Below is a summary of the key needs as they emerged from the analysis of all sources of data, reported above. We have taken a pragmatic approach to selecting the areas of need included below, limiting them to what might be feasible for the project to consider addressing.

- Needs of those who work directly with girls and young women
- Programs and resources (tailored and tangible resources to share with communities)
- Support systems for women who experience cyberviolence
- Mechanisms to report cyberviolence including concrete actions that can be taken
- Resources, programs to involve parents in any awareness or education strategies for the younger age groups
- Peer-led intervention strategies for those working with the older age groups

For girls and young women: Building knowledge, skills, attitudes

- More nuanced understanding of cyberviolence, applying a stronger gender analysis, and distinguishing between cyberbullying and cyberviolence
- Understanding the legal framework that governs cyberspace, including what actions are forbidden by what laws, what isn't, what the consequences are
- How to appropriately access policing, limitations, what can and can't be accomplished by 'calling the police' in relation to different types of cyberviolence
- Computer literacy skills, including concrete, hands-on strategies to help them make decisions about, and implement specific actions.
- Capacity to analyze the nature of comments directed at them, situate these on a continuum of their own values, tolerance, possible harm or legality. Consider possible responses and the consequences that might ensure a decision-aid for how to respond to various types of situations.

Safety

- Understanding and skills to use the existing mechanisms provided by internet and mobile phone providers, and social media platforms to block individuals and report inappropriate content, as well as strategies to protect their own privacy.
- A gaming space free of sexism and harassment
- A sexism-free support system that makes it easy for them to ask and receive help
- Online spaces in which they can express their opinions freely without fear of harassment.

RECOMMENDATIONS

The project team, partners, and young women linked to the project were provided with the draft recommendations for their input, in June 2015. The recommendations were refined, based on their input. The result is the following project recommendations.

Educational institutions:

a. All schools and/or school boards must develop and enforce clear policies to encourage positive digital space, good digital citizens and that outline:
   - The encouraged uses and restrictions of ICT of students in the school;
   - How teachers, faculty and other staff will engage students in delivering lessons, courses, workshops or other activities aimed at promoting positive digital spaces and good digital citizenship;
   - Who will monitor online behaviour of students and investigate complaints or problematic online activity, including attacks based on gender, orientation or any intersectional of identity thereof;
   - What measures will be taken regarding inappropriate or violent online behaviour, including attacks based on gender, orientation or any intersection of identity thereof; and,
   - That require follow-up meetings with students that report to gage whether the situation has improved or not.

b. A digital literacy curriculum should be found (from existing sources) or developed (if no appropriate curriculum with a gender lens exists) for students at the primary and secondary level, and could include:
   - Digital citizenship and the positive use of digital spaces, including techniques for reflecting on privilege, critical thinking and being mindful of language;
   - That defines cyberviolence and equips students with tools to deal with cyberviolence when it does occur;
   - Topics such as building self-confidence/esteem, empathy, healthy relationships, conflict resolution and consent (starting at an earlier but appropriate age; need to differentiate between 'normal conflict' and bullying or violence);
   - Promote careers in information and communications technology, particularly to girls and young women that have traditionally been discouraged from pursuing careers in such fields; and,
   - Inviting guest speakers to share their experiences, related to the topics above.

c. All schools/school boards should ensure adequate guidance and support staff equipped with expertise to identify and work with students that may face mental health issues.

d. Student leaders should be empowered to create safe online environments (blogs, Twitter, etc.) monitored by staff and/or administration to provide examples. Schools should embrace social media and get involved by positive promotion of school spirit.

e. Schools should continue to survey students about the experience of young women online and invest effort in developing tools and campaigns based on the evidence.

Parents, teachers, guidance counsellors, police and other adults:

a. Develop digital media literacy training based on existing and/or new materials for parents and other adults to familiarize them with social media sites, apps, tools and digital culture more generally so that they can better understand how these can be used to empower young women or to engage in cyberviolence against girls and women.

b. Develop a woman-centered training based on existing and/or new materials, along with a toolkit for parents and other adults to build capacity to effectively support young women experiencing cyberviolence in a way that is non-judgmental and supportive, and that addresses the mental health of victims/survivors.

c. Police should work with parents, teachers, schools and school boards to do prevention work such as delivering presentations to define cyberviolence, how to prevent it and outline the potential consequences of engaging in it (mental health, social and criminal consequences). Young people need to be made aware of their rights and responsibilities online, and understand when police intervention is appropriate or necessary.

d. School counsellors, social workers, and others working with girls and young women should engage in 'online counselling' to meet them 'where they are at' in order to facilitate positive online communications, mentor young women and girls, and counsel those that are experiencing cyberviolence.

RECOMMENDATIONS

Legal and legislative systems

a. Police must investigate all reports seriously, and enforce existing laws when reported. In order to do so:
   - Police and the legal community need woman-centered training on how to work with victims in a way that is supportive and non-judgmental (i.e. not blaming the victim);
   - Police need training and to be encouraged to become familiar and engage with social media, apps, tools and better understand the digital world generally; and,
   - Police need training on techniques for working with the tech sector more effectively for the purpose of conducting more effective and timely investigations (ex. what to include in a warrant/ subpoena).

b. Legislation needs to be enacted where current gaps exist that is responsive to the needs of girls and women, on an ongoing basis, to protect young women from cyberviolence.

Information and communication technology (ICT):

a. Advocating for more effective reporting and blocking policies that are enforced quickly and efficiently (ideally results in immediate removal of the post or suspension of the user). These need to be easy to find and use, and should include clear consequences for violators.

b. Abuse or harassment need to be more widely defined than current categories found (i.e. limited list of options to select from when reporting) to include harassment, unpermitted use of identity, oppressive language (based on gender, orientation or any intersectional identity thereof), etc.

c. Social media sites and game and app developers need to commit to ensuring that their sites, games and apps are safe by being proactive in building tools and resources that allow for the reporting of offensive content, the education of users to the risks and consequences of posting offensive content, and cooperation with law enforcement as appropriate under the law.

Public awareness and education:

a. Create large-scale educational campaign(s) using mass and social media to address cyberviolence that support rather than blame victims should be developed, using online 'celebrities' (i.e. people with existing followings on YouTube, blogs, Twitter, etc.) to deliver messages and increase reach, and:
   - Should also address sexism, hypersexualization, women's equality and oppression.
   - Should challenge stereotypical definitions of masculinity, and may include campaigns directly aimed at young men and boys.
   - Should clearly demonstrate cyberviolence as a form of violence against women.
   - Should raise awareness about warning signs of abusive relationships and how online violence can translate into the real world, dating violence on dating sites and apps, and online human trafficking.

b. Create sustainable networks of community service and other organizations to work on awareness campaigns/projects to for local delivery in communities and to support victims/survivors and:
   - Should also address sexism, hypersexualization, women's equality and oppression.
   - Should challenge stereotypical definitions of masculinity, and may include campaigns directly aimed at young men and boys.
   - Should clearly demonstrate cyberviolence as a form of violence against women.
   - Should raise awareness about warning signs of abusive relationships and how online violence can translate into the real world, dating violence on dating sites and apps, and online human trafficking.

c. Use existing or develop new youth-tested online resources for youth and adults to raise awareness among young women and girls regarding how to be safe online and report when cyberviolence occurs. This may include providing information on apps available to help stay safe online or have emergency functions and alerts, such as YWCA Canada's Safety Siren.

d. YWCA Member Associations across Canada should support the distribution of materials to support a multi-organization campaign.

RECOMMENDATIONS

Safe spaces:

a. A community of peer and/or youth mentors should to be created and fostered in school, online and elsewhere. These youth should be given the tools needed to:
   - Promote safe online spaces where young women and girls can feel empowered, receive support and mentoring, engage in safe online gaming and the like.
   - Call out cyberviolence, and encourage others to do the same, including when they witness attacks based on gender, orientation or any intersection of identity thereof.

b. Promote existing and create new safe online spaces (where needed) where young women and girls can feel empowered, receive support and mentoring, engage in safe online gaming and the like. Such sites, apps, games and online tools will have multi-stage registration procedures, strict guidelines and enforcement regarding terms of use and other measures in place to ensure safety of the space for young women and girls.

c. Foster support groups that use the power of storytelling and art therapy to empower young women to tell their story on/offline. This could also be used in the classroom.

The final stage of this participatory needs assessment – what strategies will be used to implement some of the above recommendations – requires input from the project team, partners, and the girls and young women who are linked to the project. To this end, we will review each identified need, and discuss criteria for setting project priorities (e.g. the size of the need, the consequences of ignoring the need, the impact of barriers, etc.). This will form the basis for decisions regarding recommended actions to address needs that can be met by the project, and an eventual action plan for the project as a whole.