HM Government

UKaid
from the British people

Cybersecurity, Gender Equality & Social Inclusion

Strategic Research Paper

Faraz Hassan, Anna Gawn, Lola Gani-Yusuf & John Ashdown

December 2022

KPMG

Social Development Direct

Table of Contents

1. Introduction & Definitions

Globally, women and men face different barriers to accessing and controlling assets and economic resources, information, as well as disparities in decision-making power. Diverse expectations around roles and behaviours for women and men, intersecting with other characteristics such as race, disability, or sexual orientation, determine the choices, decisions and actions they have and the risks they face. These disparities are reflected in the digital world, where one's gender and other intersecting identities can increase risk to cyber harms. Understanding the differences in the capabilities, needs, and priorities across genders and how gender norms underpin cybersecurity designs are crucial in maximising their effectiveness (Haciyakupoglu and Wong, 2021). The Foreign, Commonwealth & Development Office (FCDO) is committed to incorporating Gender Equality and Social Inclusion (GESI) as part of its programmes.

This research aims to provide practical guidance on how GESI could be incorporated into cyber capacity building (CCBs). It has been compiled through a combination of desk research, Key Informant Interviews (KIIs) and from the authors' own experience, including in mainstreaming GESI as part of the Digital Access Programme DAP. More details on methodology can be found in Annex A.

This paper is divided into two parts. The first illustrates the types of harms experienced by women and excluded groups online and through technology. It identifies overarching trends, and important opportunities or constraints to be aware of when designing programmes. It also explores what data is available in terms of how CCBs can be more responsive in addressing causes and mitigating impacts of online harms experienced by women and excluded groups, and thereby boosts resilience of target populations as a whole.

The second part of the paper looks at how CCBs can better incorporate GESI, including providing examples of what GESI-responsive cyber capacity building interventions could look like.

GESI in cyber security is relatively under researched,[1] but available data shows it is an important issue that must be considered as part of CCB design. Ignoring it leaving the most excluded groups at risk which risks undermining investments in cyber security and efforts to increase cyber resilience.

Technology and the harms it can facilitate often evolve faster than programmes can respond. Therefore, solutions proposed in this paper are not intended to be comprehensive, but rather aim to equip those delivering programmes with the tools needed to analyse and monitor impacts on excluded groups. This will enable interventions to be designed to be responsive to their needs and mitigate the harms they experience.

1.1 **Definitions & Prevalence**

Cyberviolence in general is defined by Council of Europe (2018) as 'the use of computer systems to cause, facilitate, or threaten violence against individuals that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities.' Although online violence can affect women, men, girls and boys, women and girls experience different and more traumatic forms of cyberbullying (Cybersafe, 2020; Van der Wilk, 2021). Crucially, these are positioned as part of a continuum of violence across the online and offline worlds (Powell and Henry, 2017, p. 206; Powell, Henry and Flynn, 2018; McGlynn, Rackley and Houghton, 2017, p. 36). (UNODC, 2019).

Definitions of cyber Violence Against Women and Girls (VAWG) are therefore useful as they go beyond understanding it as technology-facilitated violence to highlight i) a continuum of offline violence, ii) that women and girls are more likely to experience these harms and iii) the impact is greater on women and girls.

Reports suggest 73% of women have been exposed to some form of online violence. (UN Broadband Commission, 2015). A recent survey by Plan International found that 58% of women using the internet have been trolled and a joint study by the World Wide Web Foundation and the Girl Guides and Scouts found that 84% of women think that the problem is getting worse. It is estimated that 1 in 10 girls have already experienced a form of cyber violence by age 15 (European Union Agency for Fundamental Rights, 2014). Another study from the Economist Intelligence Unit (2021) estimates that more than a third of women worldwide have experienced abuse online, rising to almost half for younger women (classified as Generation Z and Millennials) (Martellozzo et al, 2021).

1.2 Types of Targeted Harms

Cyber VAWG can take on various forms, including but not limited to cyber stalking, impersonation, hacking, non-consensual pornography (or 'revenge porn'), gender-based slurs and harassment, 'slut-shaming', unsolicited

[1] See Annex A on data gaps.

pornography, ‘sextortion’, rape and death threats, ‘doxing’, and electronically enabled trafficking (EIGE, 2017; Faith & Fraser, 2018).

These threats are characterised by a specific intention to target women and girls, as well as other minority groups. They are enabled by technology.

Often these types of harms are do not have clear legal definitions and many forms overlap. Similarly, most social media platforms have very limited definitions available to their users, with unclear approaches to recourse. (Van der Wilk, 2021).

A list of definitions, who is at risk, and what interventions could be deployed against them are included in Annex B. However, it should be noted that it is difficult to link these harms to specific solutions or identify groups of perpetrators. This is in part due to the complexity of causes for these harms, which often extend beyond the remit of cyber security alone.

1.3 The Continuum of ‘Online’ and ‘Offline’ violence and harms

Research into Cyber VAWG finds that it is closely linked to offline harms and violence, which was found to be particularly true for women and girls. For example, cyber stalking by a partner or ex-partner follows the same patterns as offline stalking and is therefore intimate partner violence, simply facilitated by technology (EIGE, 2017).

Evidence confirms this continuum:

- A UK study of cyber stalking found that over half (54%) of the cases involved a first encounter in a real-world situation (EIGE, 2017).
- Data from the 2014 FRA survey shows that 77 % of women who have experienced cyber harassment have also experienced at least one form of sexual or/ and physical violence from an intimate partner (European Union Agency for Fundamental Rights, 2014).
- 7 in 10 women (70 %) who have experienced cyber stalking, have also experienced at least one form of physical or/and sexual violence from an intimate partner (EIGE, 2017).
- A survey found that 45% of domestic violence victims reported experiencing some form of abuse online during their relationship; 48% reported experiencing harassment or abuse online from their ex-partner once they’d left the relationship. 38% reported online stalking once they’d left the relationship (Women's Aid, 2014).
- An analysis of documented cases in the Philippines disclosed that victims/survivors of online GBV experienced emotional harm (82%), sexual assault (63%), physical harm (45%) and damage to their reputations (37%). (UN Women, 2020).

Notably, most of the forms of online and technology-facilitated violence against women are existing crimes and offences, however, they are ‘expanded, amplified or generalised’ by the internet (Van der Wilk, 2021).

The linkage to offline harms has implications for designing responses to address the issue. For example, 75% of respondents to a survey on domestic violence and online abuse reported concerns that the police did not know how best to respond to online abuse or harassment. This includes 12% who had reported abuse to the police and had not been helped. (Women's Aid, 2014). These highlight the importance of addressing cyber harms, abuse and harassment as part of offline measures to tackle gender-based violence.

2. Disproportionate impact of untargeted cyber-attacks on women and excluded groups

While there are forms of harm aimed at women and excluded groups facilitated by technology, women and excluded groups can also suffer disproportionately from cyber harms that may not be targeted at them. This is largely because people access and use digital technologies in different ways and these dynamics, and the implications for different groups notably women, girls and excluded groups, have not been fully considered in the design and delivery of digital technologies.

2.1 Internet shutdowns

Access to the internet can be an important recourse for women to access services, information, or economic opportunities. Cyber incidents that limit access or disrupt these services can have knock-on impacts on women or excluded groups due to their relative dependence on them. Evidence from India, where the state has used internet shutdowns in the name of "national security and public safety" or in "fighting fake news and hate speech", found that shutdowns had disproportionate effects on women who relied on cyberspace to access public services compared to men. Women sharing a home with their abusers could struggle to reach for help when the internet is down (Haciyakupoglu and Wong, 2021).

2.2 Data breaches

Even when there is a data breach or intentional disclosure of personally identifiable information that is not targeted at women, women can experience differential impacts because of underlying inequality and discrimination. For example, in 2017 WikiLeaks released massive databases containing sensitive and private information of millions of ordinary Turkish citizens, which included a special database of almost all adult women in Turkey (Tufekci, 2016). Offline violence against women could be exacerbated by the availability of personal information for stalkers, ex-partners, or perpetrators of domestic violence from the release of such sensitive personal data.

Women can be more severely affected than men by personal data breaches. For example, studies have shown that in many contexts women manage most households' finances, including paying bills and managing bank accounts. This means that they are disproportionately affected by threats targeting financial services, such as phishing and malware like banking trojans (Rollo, 2021).

2.3 Disproportionate impact of other cyber harms

While more research is needed, differentiated impacts can also be inferred from the disparity in access and use of digital technologies by gender. Only 52% of women are online (compared to 62% of men), (ITU, 2021), and across low and middle-income countries, women are less likely than men to use the internet, which translates into 264 million fewer women than men. (GSMA, 2022).

Limitations in digital literacy make women and girls more vulnerable to online risks than men and boys (EIGE, 2019). For example, when women or girls experience harmful or negative digital experiences, they often report a sense of helplessness and may have little information, knowledge, or resources about staying safe online (UNICEF, 2021). A study in Brazil found that girls do not know how to proceed or where to turn for help when faced with online harassment or non-consensual sharing of nude photos (EQUALS, 2019).

3. Impact of cyber harms on women and excluded groups

Violence happening online and via new technologies has a serious impact on women's lives, their physical and psychological health (and that of their dependents), their livelihoods, their reputation, their political participation and their presence online (Van der Wilk, 2021). There are also broader economic and political impacts on society when women, girls and excluded groups are shut out from the benefits offered by digital technology. Impacts and evidence are summarised in Table 1 below.

Table 1 Impacts and evidence of cyber harms on women and excluded groups

Type of Impacts	Evidence
Social impacts and personal safety Cyber violence can result in lasting trauma for women and girls ranging from mental health challenges; anxiety; depression (Sargent et al. 2016); diminished self-esteem; all the way to self-harm and suicide (Pashang et al 2018; Cybersafe, 2020). It can also lead to physical threats to women and girls safety, due to the links illustrated in section 1.3 between online and offline violence.	• 41% of women in one survey who experienced online abuse feared for their personal safety because of this abuse and harassment (Amnesty International, 2017) (UNODC, 2019). • Cyberbullying in Azerbaijan has been linked with child suicide, where an average of 50 children commit suicide every year (Orujova, 2015). • In Pakistan, online harassment has led to suicide, murder, physical assault, emotional distress and women leaving their jobs and online spaces (UN Women, 2020). • Publishing of nonconsensual pornography, particularly if posted with a real name and corresponding contact information, can lead to physical confrontations from strangers (Citron & Franks, 2014).
Economic impacts Online cyber violence against women and girls and perceptions of safety can have a profound impact on limiting technology driven economic growth. Women's access to technology and internet enabled services can be inhibited by safety and privacy concerns. This means that ignoring women's cyber security needs could exclude them from new labour market requirements. Business and markets will be unable to capitalise on the full potential of a female workforce in the digital sector. Conversely, closing the gap in mobile ownership and use in low- and middle-income countries would result in US$ 140 billion in revenue to the mobile industry and generate an additional US$ 700 billion in GDP growth (GSMA, 2019c).	• A report on "Women's Rights Online" of 2015 54 – covering nine cities in Africa and Asia – identified online harassment as one of the constraints limiting the use of technology by women (World Wide Web Foundation, 2015). • GSMA found that across 19 low- and middle-income countries, 4% to 65% of women who do not own a mobile phone were concerned about being contacted by strangers as one of the main reasons stopping them from owning a mobile (GSMA, 2018). • Technology enabled harassment or abuse can prevent women from engaging with online content and has led to women leaving their jobs (UN Women, 2020). • Women in general have been found to be more concerned about the privacy of their personal data than men (World Wide Web Foundation, 2020), so a lack of data protection legislation could deter women from using digital products and services. • The disclosure of personal information discourages women from engaging in e-commerce at a higher rate in comparison to men (Michota, 2013).
Impacts on freedom of speech and democratic participation Gendered disinformation and campaigns of harassment that often build on existing stereotypes can be used to deter women and excluded groups from participating in politics and the public sphere (17), which in undermines democracy (Haciyakupoglu and Wong, 2021).	• In Brazil, online harassment of feminist campaigners and an LGBT politician led to the need for police protection and, eventually, the individuals fleeing the country in 2018 (Cortez, 2018). • Research in 2019 found that online violence and harassment against women in Ukraine is pervasive and debilitating, focusing particularly on how it undermines their political participation (IFES, 2019).

4. Specific Groups at risk

Specific groups of were identified to be more at risk of cyber harms and specific forms of cyberviolence. As in the offline world, women, girls and minority groups in general are at higher risk or cyber harms. Women with intersecting identities face additional exclusion on account of race, ethnicity, sexual orientation and identity, disability, religion, migrant status, and more. (Fraser & Martineau-Searle, 2018; Van der Wilk, 2021).

4.1 Women with a high public profile. Women in the public sphere, including those in politics, human rights campaigners, and journalists are often subjected to targeted cyber-harassment and cyberstalking. (IGF, 2015; Human Rights Council, 2018; OHCHR, 2018). (Al-Nasrawi, 2021) Research has shown that simply being a female public figure can result in threats of physical and sexual violence, as well as misogynistic comments. (UNODC, 2019) These activities are aimed at delegitimizing, depersonalizing, and ultimately dissuading them from being politically active. (Women Around the World and Women and Foreign Policy Program, 2019)

4.2 People from ethnic minority groups. A study from the US found that people from ethnic minorities are more likely to have their identities stolen compared to white people (21% vs 15%), and least likely to avoid financial impact due to cybercrime (47% vs 59%). (MalwareBytes, 2021) 21 percent of women and 23 percent of BIPOC (Black, Indigenous, and People of Colour) respondents said they experienced "substantial" stress in dealing with online suspicious activity, compared to 17 percent of all respondents. (MalwareBytes, 2021) The same research also revealed a stronger link between online activity and physical attacks on respondents from ethnic minorities or women.

Moreover, in South Africa, research with 1,726 young people aged between 12 and 24 years found that "race appears to be more significant than gender" (Burton and Mutongwizo, 2009: 6). Black children and youth reported the highest incidence of cyber aggression. (Fraser & Martineau-Searle, 2018) Similarly Plan International found that 37 percent of girls who are from an ethnic minority *and* have suffered abuse say they are targeted because of their race or ethnicity. (Van der Wilk, 2021)

4.3 People of diverse sexualities and gender identities. Research by Plan International into victims of online harassment found that more than half (56%) of respondents who identify as LBTQI say they are harassed because of their gender identity or sexual orientation (Van der Wilk, 2021).

4.4 Children and young people. Due to their age and different development stages, children in general are at high risk of cyber harms, particularly bullying, harassment, and sexual exploitation and abuse. For example, research has exposed Instagram's negative impacts on the mental health of younger users, teenage girls in particular. (Duggan, 2014) Girls appear to be at higher risk of online harms than boys, and minority groups, notably sexual minorities, are at heightened risk of abuse. (WePROTECT Global Alliance and Economist Impact, 2021) At the same time, evidence suggests that the specific harms on boys should be explored further. Further, women aged 18-24 were found to be at a heightened risk of being exposed to every kind of Cyber VAWG, including cyber stalking and online sexual harassment, while simultaneously being at risk from other types of harassment that affect young people in general.43 (UN Broadband Commission, 2015).

4.5 People with disabilities. Plan International (2022) highlighted that the harassment of girls in various countries is amplified if they have a disability. This was echoed by reports from the UK which confirmed online hate crime and abuse of people with disabilities as widespread; a 33 percent increase in online hate crime was recorded between 2016 and 2017 (Leonard Cheshire). Further, DFAT notes that where decisions about critical services, such health, education, insurance, are made by artificial intelligence, with algorithms, data sets and screening tools people with disabilities, as well as women and other minority groups, can be marginalised.

5. How GESI is being integrated into existing cyber security programmes

Despite the different user experiences in digital settings described above, the research shows limited evidence of GESI being considered in the design and delivery of cyber security programmes. Ambitions towards "digital inclusion" and a "whole of society approach" in cyber security programmes are clear; some preliminary steps taken in this direction and lessons are listed below.

5.1 Building a skilled, gender-diverse cybersecurity workforce. Based on the premise that women and other excluded groups bring different and vital priorities, skills and perspectives, a range of organisations and initiatives encourage women's participation in cyber security delegations, policy discussions and related decision making (cited in consultations with: OAS, GFCE, KPMG). Examples of initiatives include women in cyber fellowships, coaching programmes for women, ensuring proportional representation or a gender balance in trainings, policy discussions and networking opportunities in cyber security. Also, as well as upskilling women who are already in the workforce, some initiatives have created pathways for women's engagement in cybersecurity over the long-term.

However, it is not clear if women actively participate more, have the space to share ideas and are listened to in cyber policy and procedure discussions because ofbe because the initiatives are relatively new and/or these initiatives. This may such outcomes may not be monitored. But also, it is noteworthy that no examples were identified of accompanying initiatives looking at the structural barriers to active participation when enough women are already "in the room" or of initiatives with all delegation staff on how and why it is valuable to enable and embed GESI in cyber security policies and strategies.

5.2 Building skills of younger generations. Other initiatives aim to encourage the participation of (younger) women and girls into science, technology, engineering and maths (STEM) studies as a way of building a more balanced future cyber security workforce. Examples include scholarship funds and academic programmes for women on cyber security with accompanying conditions to work in their own country.

Such initiatives have been challenged as limiting cyber security to STEM when a diverse range of skills and experiences (sociology, technology, business etc.) and a "whole of government approach" is needed for successful cyber security.

5.3 School based interventions. Evidence was found to suggest that school-based interventions that engage both boys and girls can have lasting impact (UN Broadband Commission, 2015), and can reach scale (Cybersafe, 2020) in shaping positive changes to behaviour - this could be extended to tackling cyber VAWG and cyber bullying. There is an opportunity to use interventions focused on raising awareness and influencing social norms as an avenue to integrate cyber VAWG sensitisation and prevention. While there is a lack of evidence on the long-term impact of school-based interventions, short-term and initial evidence indicates these can be an effective way to prevent Cyber VAWG and cyberbullying. (Cybersafe, 2020).

5.4 Public awareness campaigns. Examples of public awareness campaigns focused on cyber hygiene basics and the responsible use of technology across society were shared (DAP conference, Chatham House, 2022). Some campaigns target particular social groups, for example children of a certain age, parents, and teachers, whilst others take a general approach aiming to reach across society. Reflections suggested that it is important to identify any gaps relating to who is not being reached in public awareness campaigns, how to reach specific groups and key messages for specific groups so they feel encouraged and safe online. Also, it is important to understand that some social groups may not be online for reasons beyond a lack of opportunity or access, for example some may feel scared or unsafe online. Understanding barriers and decisions relating to digital access will be crucial for reaching and effectively increasing the cyber resilience of different social groups.

6. Opportunities & Constraints for embedding GESI in cyber security programmes

6.1 Opportunities

- There is a clear need for GESI-sensitive cyber security. Across low- and middle-income countries, 300 million fewer women than men use mobile internet (GMSA, 2020). This disparity in online access is partly due to women's concerns over privacy and security (UN Broadband Commission, 2015).

- Technology can help transform existing stereotypes in a positive way. Examples of women taking and adapting technology in their own way and for their own purposes are impressive and growing. Such initiatives and progress can be sought out, encouraged and promoted to amplify reach.

- There is momentum and will. There is growing recognition that cyber security programmes do not deal with one default user group and that people have distinct experiences, take different decisions, and face diverse risks online. Terms like "digital inclusion" and "a whole of society approach" set this ambition.

- We are moving towards common definitions. Common definitions of cyber harms against women, girls and excluded groups and a shared understanding of how technology facilitates those harms could increase visibility and facilitate prevention and response.

- Extensive lessons from offline ODA programmes are available. Using and adapting experiences of embedding GESI and respecting rights in other sectoral national strategies and ODA programme design, programme cycle management and system development is crucial. Also, ODA programmes have vast experience tackling key aspects of GBV. Seeing cyber harms as an extension of offline harms presents opportunities to tackle the root causes through ODA spending.

6.2 Constraints

- Structural gender inequality and social exclusion go beyond cyber security. Where harmful social norms exist in schools, workplaces and homes, it is likely that they will exist or be heightened in digital settings. TFGBV stems from societal misogyny, exclusion, gender stereotypes and relations. Cybersecurity programmes alone are not sufficient in tackling the root causes of online harms (The Diplomat, 2022).

- The link between cyber security programmes, GESI and human rights is not always clear. Strategies do not clarify how cyber security capabilities can have different impacts on women, girls and excluded groups.

- The 'tick-box' risk. "Identifying candidates and promoting their *meaningful participation* in training, policy dialogue and cyber security interventions remains a … significant challenge" (DFAT, GEDSI strategy).

- Social norms change takes time. The cyber security area of work is moving quickly; there is a relative urgency to get the basics right and to do them well. It is perhaps inevitable therefore that integrating GESI, a step-by-step and slow process into cyber security programmes will require careful balancing.

- The digital access gender gap can perpetuate exclusion. Online security concerns for women and may remain on the margin of political agendas simply because there are fewer women online.

- Limited legal recourse for victims of cyber harm. Legislative reforms cannot keep up with tech changes and perceptions that cyber harms are less harmful that offline harms are common (The Diplomat, 2022).

- The cyber security field is still largely viewed as gender neutral. Some crimes against women perpetrated online are not conceptualised in cybercrime frameworks (Van der Wilk, 2021). Those who work in cyber security are governed by their own social norms, which are mirrored in cyber security infrastructure, software, data sets, scanning tools and artificial intelligence (Feminist internet).

7. Recommendations

Recommendations are provided in two areas. The first are programme design recommendations. These build on I) findings from desk research and KIIs II) experience of the team delivering GESI mainstreaming as part of the Digital Access Programme and III) general good practice in GESI mainstreaming. Figure 1 outlines a general approach to mainstreaming GESI in CCBs. Table 2 illustrates how CCB interventions can be designed in a way responsive to the risks and cyber harms experienced by women and excluded groups. These are not comprehensive, but illustrate the types of approaches that could be taken.

Implement GESI mainstreaming good practice in cyber security programmes. This includes requiring dedicated GESI resource and expertise, a GESI analysis, a GESI action plan or strategy, internal targets on gender and inclusion, regular reviews and reporting, data disaggregated by sex, age, disability, and integration into the programme's MEL approach. See Figure 1.

Train cybersecurity experts on GESI as part of cyber programmes. The pace of change in technology moves faster than its social impacts can be tracked. In addition to programmes having dedicated GESI expertise, cyber security experts should also be trained on GESI at the outset of a programme. This collaborative, multi-disciplinary approach will facilitate co-creation of solutions in response to cyber harms, and will also build ownership for GESI across delivery teams.

Convene diverse teams to design cyber security solutions as part of interventions. Women and excluded groups are underrepresented in the cyber security field and in the ICT industry as a whole. The FCDO's cyber security programmes could be a catalyst for more diverse teams to design and deliver cyber security interventions. Commitments to diversity and inclusion could be incorporated into procurement and scoring of providers.

Generate, capture, and share learning on GESI and cybersecurity through effective Knowledge & Learning strategies. This paper found a lack of resources that look specifically on the gendered impact of cyber-attacks and women and excluded groups. FCDO programmes could contribute to the global evidence base by implementing knowledge and learning strategies as part of cyber security programmes, that capture and disseminate key learnings.

Design cybersecurity programmes around grassroots, bottom up approaches that reflect local contexts. This is especially important given the continuum with offline harms and cyber harms. Local women's groups, or civil society groups will be best informed about the impact of cyber harms in the communities they represent, and should be involved in helping to shape cybersecurity interventions wherever possible. Programmes should adopt meaningful consultation throughout the project life cycle.

Align cyber security programmes with existing programming that addresses root causes of cyber violence and 'offline' violence against women and excluded groups. Programmes responding to gender-based violence, violence against women and girls, organisational safeguarding or protection from sexual exploitation, abuse and sexual harassment or programmes (PSEAH) and Women, Peace and Security (WPS) all connect in some way to cyber harms. The FCDO should draw on learning and evidence from existing programmes; adjust activities in its own programmes to incorporate an 'online' component on cyber violence; and engage overlapping stakeholders such as schools or women's groups.

Leverage FCDO's convening power to coordinate with other stakeholders including donors, governments, civil society, and the private sector. This paper found that the integration of GESI into cyber security programming is relatively unexplored; yet there is significant recognition of gendered cyber harms and the necessity of responding. FCDO could use its experience from existing programmes such as DAP, and programming on areas such as Gender Based Violence, to convene multi-stakeholder learning and knowledge exchange and champion this issue at a global level. It could also encourage other donors to incorporate GESI as part of their cyber resilience programmes. The FCDO could consider the generation of comparable data and definitions of cyber harms as an initial step.

Figure 1 Integrating GESI across a cyber programme life cycle

Analysis

Conduct **a gender and social analysis** to understand the context & inform programme design. The analysis should identify:

- How do women and excluded groups **use and access digital technology and connectivity?** Patterns and access, as well as barriers, in women and excluded groups' use of digital technologies and connectivity (e.g. access to internet, devices, digital literacy, etc).
- **What cyber harms and risks exist for women and excluded groups?** Potential digital risks and harms associated with the proposed intervention, including any existing data on prevalence or documented occurrence of cyber violence in the country of intervention. E.g. is there an increased risk of cyber VAWG (annex 2) that the intervention could address?
- **Who is likely to be impacted?** Excluded groups likely to be impacted by delivery of the intervention, based on existing datasets and consultation with stakeholders (see section x.x)
- How might women, men, and excluded groups be **impacted differently?** Could there be differentiated impacts on women, men, and excluded groups as a result of the harm the intervention is seeking to address?

Identify and **consult with relevant women's groups or grassroot organisations** representing excluded groups to analyse potential harms, needs, and solutions that can inform programme design.

Identify other existing programmes or interventions that deal with violence against women and girls, or excluded groups, either offline or online. Identify any lessons learnt, and align activities if possible.

Design

- How can the intervention account for, respond to, and mitigate **identified barriers** to women and excluded groups that would prevent them from participating in intervention activities, or from benefitting from the intervention?
- What features can be designed into the intervention that would address **identified cyber harms** that women and excluded groups are at risk of experiencing, such as cyber violence?
- What features can be designed as part of the intervention that would mitigate any **disproportionate impact** on women or excluded groups as a result of cyber attacks?
- Can **local women and women's groups** be involved in planning, design, and decision-making related to the intervention?
- Identify how the intervention can **promote impact on gender equality and women's empowerment** even if it is not the main purpose. For example, what opportunities are there to provide training and capacity building to women and girls in the cyber sector?

Implementation

- Integrate gender equality and social inclusion objectives into **procurement documents, processes, scoring, and assessment.** This helps to ensure that ambitions identified in analysis and design are carried throughout the project and do no dissipate.
- Assess whether implementing teams have **dedicated social and gender expertise** or capacity that can ensure achievement of gender equality and social inclusion outcomes.
- Ensure gender and exclusion is being assessed throughout the programme as part of **progress reports and reviews.**
- Identify relevant opportunities for ongoing **participation and empowerment of women and excluded groups** in delivery of interventions, e.g. involvement in training and capacity building, user testing, and feedback

Monitoring & Evaluation

- Identify relevant metrics or **indicators** to measure impact on GESI
- Ensure monitoring and evaluation data and indicators are **disaggregated by sex, age, disability,** and other characteristics as appropriate
- Identify to what extent the intervention has **benefitted different groups of women** as compared to men
- Involve women, women's organisations, and organisations representing excluded groups in **beneficiary feedback**
- Capture, share, and **disseminate relevant data or learning** in relation to the intervention and impact on women or excluded groups to support and grow the evidence base on what works

Table 2 Examples of GESI cyber capacity building measures

	Challenges	Example GESI features	Potential Outcomes
Law enforcement	-Cyber VAWG is underreported -Tendency for victim-blaming -Capacity to identify, gather evidence, and prosecute perpetrators is limited	• Sensitiation of law enforcement personnel to causes & impacts of cyber violence and links to 'offline' violence • Build capacity of law enforcement to gather digital evidence of cyber VAWG & strengthen digital tools to identify perpetrators • Strengthen reporting mechanisms available to the public • Work with the judicial system to support prosecution of perpetrators of cyber VAWG	• Enhanced sense of safety of women and girls online • Mitigation of social and personal harms experienced by women and excluded groups
Working with SMEs	Women cite safety concerns as one of main reasons for not using technology; and can be more at risk of hacking and scams	• Engagement of women-owned SMEs in analysis of security needs and risks • Targeted interventions to enhance capability of women-owned SMEs to safely use technology such as e-commerce, mobile banking, etc. • Partner with SME enabling organisations (banks, gov, charities) to provide training to female owned business.	• Enhanced Women's Economic Empowerment Women owned SMEs are better able to use technology and generate more jobs and income
Incident Response	Needs of women and excluded groups often not understood or prioritised in incident response	• Analysis of how women and excluded groups are impacted differently by cyber incidents • Targeted engagement of women and excluded groups to inform improvements in incident response and how to support them after an incident	• Most vulnerable sections of the population are better protected during cyber incidents and supported in responses
Banking and financial services	Women and excluded groups, such as minorities, are more frequently victims of cyber attacks related to banking and fraud	• Inform banking and financial service providers the effects cyber attacks have to excluded groups and the benefits of collecting customer data disaggregated by gender, age, disability, etc. where possible. • Targeted digital literacy and safety capacity building for women and excluded groups	• Customers of banking and financial services are better protected from cyber harms • Losses to banking and financial service providers from cyber incidents minimised
E-platforms	Women and excluded groups are often more reliant on e-platforms to access important services & loss of access can have higher impact	• Identify specific risks and needs are in accessing e-platforms, and incorporate into intervention design • Train women and excluded groups on how to engage with e-services securely and the potentials threats they face e.g phishing	• Women and excluded groups are less impacted by cyber incidents targeting e-platforms • E-platforms are more secure through understanding of how they are used by different groups
Training activities	Women and excluded groups are underrepresented in cyber security training	• Context-appropriate quotas for participation of women and excluded groups; facilitation to ensure they are given equal opportunities to learn and gain skills • Women-only training sessions • Delivery of training in partnership with grassroot organisations.	• Enhanced participation and voice of women and excluded groups • Solutions are more responsive to the needs of the whole population
School-based learning	Unique opportunity to shape what is acceptable in terms of online behaviour	• Incorporate awareness of cyber violence, bullying, harassment in school-based learning for girls and boys • Provide tailored content, including apps and tools, for girls and boys on how to deal with cyber abuse	• Young people's understanding of acceptable online behaviour is strengthened • Young people and children are more resilient to cyber abuse and harassment if it does occur
Communication Campaigns	Women and excluded groups may access information differently and are a key audience for cyber awareness campaigns	• Design appropriate communication materials and relevant content for girls and boys, • Identify and use dissemination channels that are likely to reach both women and men, and other excluded groups (i.e. people with disabilities)	• Cyber awareness campaigns reach wider sections of the population, including vulnerable groups at risk, enhancing their resilience
Data protection	Women and excluded groups can suffer disproportionately from data breaches – both large scale and personal	• Support data protection institutions to understand the impact of personal data on women and excluded groups	• Women and excluded groups suffer reduced harm in event of data breaches

References

Adriane van der Wilk (2021) Protecting Women and Girls from Violence in the Digital Age: The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women, Available at: https://rm.coe.int/the-relevance-of-the-ic-and-the-budapest-convention-on-cybercrime-in-a/1680a5eba3

APC (2017) Online gender-based violence: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences, Available at: https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf

APC (2020) Why Gender Matters in International Cyber Security, Available at: https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf

Azmina Dhrodia | World Wide Web Foundation (2021) OPINION: To stop online abuse against women, we must reform digital spaces, Available at: https://news.trust.org/item/20210409123542-l58r0

Bassan, Laura - Università Ca' Foscari Venezia (2019) Cyber Violence as Violence against Women and Girls: Taking a Step Forward for Female Inclusion in the Digital Era, Available at: http://dspace.unive.it/handle/10579/15315

Becky Faith and Erika Fraser (2018) What Works to Prevent Cyber Violence against Women and Girls?, Available at: https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/14764/vawg-helpdesk-report-212-what-works-cybervawg.pdf?sequence=1&isAllowed=y

Bonnie StabileORCID Icon,Aubrey Grant,Hemant Purohit &Kelsey Harris (2019) Sex, Lies, and Stereotypes: Gendered Implications of Fake News for Women in Politics, Available at: https://www.tandfonline.com/doi/abs/10.1080/10999922.2019.1626695

Council of Europe (2018) Mapping study on cyberviolence, Available at: https://rm.coe.int/t-cy-mapping-study-on-cyberviolence-final/1680a1307c

Cybersafe (2020) Cyber Violence against Women & Girls, Available at: https://www.stoponlineviolence.eu/wp-content/uploads/2020/06/Cybersafe_Report_200623_web.pdf

Danielle Keats Citron & Mary Anne Franks (2016) Criminalizing Revenge Porn, Available at: https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=2424&context=fac_pubs

Deborah Brown & Allison Pytlak (2020) Why Gender Matters in International Cyber Security, Available at: https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf

Economist Intelligence Unit (2021) Measuring the prevalence of online violence against women, Available at: https://onlineviolencewomen.eiu.com/

EIGE (2019) Gender equality and youth: opportunities and risks of digitalisation, Available at: https://eige.europa.eu/publications/gender-equality-and-youth-opportunities-and-risks-digitalisation

Elena Martellozzo, Paula Bradbury, Emma Short (2021) Speaking Up: Contributing to the fight against gender-based violence online, Available at: https://blogs.lse.ac.uk/medialse/2021/12/17/speaking-up-contributing-to-the-fight-against-gender-based-violence-online/

Emily A. Vogels (2021) The State of Online Harassment, Available at: https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/

End Violence Against Women Coalition (2021) Experts call for online VAWG to be addressed in the Online Safety Bill, Available at: https://www.endviolenceagainstwomen.org.uk/experts-call-online-vawg-online-safety-bill/

End Violence Against Women Coalition (2022) Ofcom steps up to urge tech firms to do more to ensure women are safe online, Available at: https://www.endviolenceagainstwomen.org.uk/ofcom-steps-up-to-urge-tech-firms-to-do-more-to-ensure-women-are-safe-online/

Erika Fraser and Laura Martineau-Searle (2018) Nature and Prevalence of Cyber Violence against Women and Girls, Available at: https://assets.publishing.service.gov.uk/media/5c597613ed915d045f3778a2/VAWG_Helpdesk_Report_211_CyberVAWG.pdf

European Institute for Gender Equality (2017) Cyber violence against women and girls, Available at: https://eige.europa.eu/publications/cyber-violence-against-women-and-girls

European Union Agency for Fundamental Rights (2014) Violence against women: an EU-wide survey – Main results., Available at: http://fra.europa.eu/en/publica-tion/2014/violence-against-women-eu-wide-survey-main-results-report

Feminist Internet, Your Feminist Guide to AI Bias, Available at: https://f-xa.co/

Geneva Centre for Security Sector Governance (DCAF) (2021) Cyber Violence against Women and Girls in the Western Balkans: Selected Case Studies and a Cybersecurity Governance Approach, Available at: https://www.dcaf.ch/sites/default/files/publications/documents/CyberVAWG_in_WB.pdf

Global Cyber Security Capacity Centre (Unknown) Why We Need More Women in Cybersecurity Capacity, Available at: https://gcscc.ox.ac.uk/article/why-we-still-need-more-women-in-cybersecurity-capacity

Gulizar Haciyakupoglu and Yasmine Wong (2021) Gender, Security and Digital Space: Issues, Policies, and the Way Forward, Available at: https://www.rsis.edu.sg/wp-content/uploads/2021/12/PR211213_Gender-Security-And-Digital-Space.pdf

Holly Rollo (2021) 3 Ways Women Are Uniquely Impacted by Cyber Threats, Available at: https://www.spiceworks.com/it-security/cyber-risk-management/guest-article/4-ways-women-are-uniquely-impacted-by-cyber-threats/

IASET (2021) Cyber Violence Against Women and Girls (CVAWG), The Algorithms of the Online- Offline Continuum of Gender Discrimination, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3953292

ICRW (2018) Technology-Facilitated Gender-Based Violence: What is it, and how do we measure it?, Available at: https://www.svri.org/sites/default/files/attachments/2018-07-24/ICRW_TFGBVMarketing_Brief_v8-Web.pdf

InsureGood (n.d.) Cyber Attacks – Women and Minorities are Top Targets, Available at: https://insuregood.org/cyber-attacks-women-and-minorities-are-top-targets/

Japleen Pasricha (2016) Violence Online in India: Cybercrimes Against Women and Minorities on Social Media, Available at: https://www.comminit.com/content/violence-online-india-cybercrimes-against-women-and-minorities-social-media

Maeve Duggan (2014) Part 4: The Aftermath of Online Harassment, Available at: https://www.pewresearch.org/internet/2014/10/22/part-4-the-aftermath-of-online-harassment/

MalwareBytes (2021) Demographics of Cybercrime, Available at: https://www.malwarebytes.com/resources/2021-demographics-of-cybercrime-report/index.html

Millar, Katharine; Shires, James; and Tropina, Tatiana (2021) Gender approaches to cybersecurity: design, defence and response, Available at: https://s3.eu-west-2.amazonaws.com/igc-production/5VmjuiWvoa7oVEK1Y2ErHT4HxYMu2lUJ.pdf

Nehal Johri (2020) India's internet shutdowns are like 'invisibility cloaks', Available at: https://www.dw.com/en/indias-internet-shutdowns-function-like-invisibility-cloaks/a-55572554

Neo Chai Chin (2021) Helplessness, hopelessness: The human cost of India’s Internet shutdowns, Available at: https://www.channelnewsasia.com/cnainsider/helpless-hopeless-human-cost-india-internet-shutdowns-kashmir-275701

Nina Jankowicz, Jillian Hunchak, Alexandra Pavliuc & 3 more (2021) Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online, Available at: https://www.wilsoncenter.org/publication/malign-creativity-how-gender-sex-and-lies-are-weaponized-against-women-online

Plan International (2022) Free to be Online, Available at: https://plan-international.org/uploads/2022/02/sotwgr2020-commsreport-en-2.pdf

Sukaina Al-Nasrawi (2021) Combating Cyber Violence Against Women and Girls: An Overview of the Legislative and Policy Reforms in the Arab Region, Available at: https://www.emerald.com/insight/content/doi/10.1108/978-1-83982-848-520211037/full/html

Sum of Us (2022) Metaverse: another cesspool of toxic content, Available at: https://www.sumofus.org/images/Metaverse_report_May_2022.pdf

The Diplomat (2022) Southeast Asia Must Be Wary of Gendered Cyber Abuse, Available at: https://thediplomat.com/2022/06/southeast-asia-must-be-wary-of-gendered-cyber-abuse/

The Economist (2020) Measuring the prevalence of online violence against women, Available at: https://onlineviolencewomen.eiu.com/

The Tahrir Institute for Middle East Policy (2022) Cyber Violence and Women in Egypt, Available at: https://timep.org/commentary/analysis/cyber-violence-and-women-in-egypt/

UK Home Office (2021) Policy paper, Annex 2: protecting against online exploitation, violence and abuse (accessible version), Available at: https://www.gov.uk/government/publications/g7-interior-and-security-ministers-meeting-september-2021/annex-2-protecting-against-online-exploitation-violence-and-abuse-accessible-version

UN Broadband Commission (2015) Cyber Violence Against Women and Girls: A World-Wide Wake-Up Call, Available at: https://en.unesco.org/sites/default/files/genderreport2015final.pdf

UN Studies Association (2019) Femicide Volume XI - Cyber Crimes Against Women & Girls, Available at: https://www.unsavienna.org/sites/default/files/2020-01/FEMICIDE%20Volume%20XI.pdf

UN Women (2020) Take five: Why we should take online violence against women and girls seriously during and beyond COVID-19, Available at: https://www.unwomen.org/en/news/stories/2020/7/take-five-cecilia-mwende-maundu-online-violence

UNDP (2022) UNDP Digital Strategy, Available at: https://digitalstrategy.undp.org/documents/Digital-Strategy-2022-2025-Full-Document_ENG_Interactive.pdf

UNICEF (2021) What we know about the gender digital divide for girls: A literature review, Available at: https://www.unicef.org/eap/media/8311/file/What%20we%20know%20about%20the%20gender%20digital%20divide%20for%20girls:%20A%20literature%20review.pdf

UNICEF (2022) Global Insight: Protecting Children in Cyberconflicts, Available at: https://www.unicef.org/globalinsight/media/2856/file/UNICEF-Global-Insight-Rapid-Analysis-Protecting-Children-in-Cyberconflicts-2022.pdf

UNODC (2019) Gender-based interpersonal cybercrime, Available at: https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/gender-based-interpersonal-cybercrime.html

WePROTECT Global Alliance (2021) Global Threat Assessment, Available at: https://www.weprotect.org/global-threat-assessment-21/#report

WMC Speech Project (Unknown) Online Abuse 101, Available at: https://womensmediacenter.com/speech-project/online-abuse-101

Women Around the World and Women and Foreign Policy Program (2019) Gendered Disinformation, Fake News, and Women in Politics, Available at: https://www.cfr.org/blog/gendered-disinformation-fake-news-and-women-politics

Women’s International League for Peace and Freedom and the Association for Progressive Communications (2020), Why Gender Matters in International Cyber Security, Available at: https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf

Women's Aid (2014) Virtual World, Real Fear, Available at: https://www.womensaid.org.uk/evidence-hub/research-and-publications/virtual-world-real-fear/

World Economic Forum (2022) Global Cyber Security Outlook, Available at: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

World Web Foundation (2021) Facebook, Google, Tik Tok and Twitter commitments, Available at: https://webfoundation.org/2021/07/generation-equality-commitments/

World Web Foundation (2021) Online Gender-Based Violence and Abuse: Consultation Briefing, Available at: https://assets.website-files.com/617a5f094309b93ce9ab25b9/618c0360cf5fd081bd6f0b5a_OGBV_ConsultationBriefing.pdf

World Web Foundation (2021), The Costs of Exclusion Report, Available at: https://webfoundation.org/research/costs-of-exclusion-report/

World Web Foundation, Tech Policy Design Lab: Online Gender-Based Violence and Abuse, Available at: 618c03493db5a4df42017dc8_OGBV_Report_June2021.pdf (website-files.com)

World Wide Web Foundation (2015) Women's Rights Online Translating Access into Empowerment, Available at: http://webfoundation.org/docs/2015/10/womens-rights-online21102015.pdf

Zeynep Tufekci (2016) WikiLeaks Put Women in Turkey in Danger, for No Reason (UPDATE), Available at: https://www.huffpost.com/entry/wikileaks-erdogan-emails_b_11158792

Annex 1: Methodology

The paper was compiled using findings from a literature review and a series of Key Informant Interviews / consultations. The organisations identified for the consultations were chosen based on their recent experiences working on cyber security and GESI. We spoke to: USAID, World Bank, UNICEF, Organisation of American States (OAS), Global Forum on Cyber Expertise (GFCE) and Plan International. See Annex 1 for the consultation guide.

The literature review covered materials available online. Materials from the last five years (2017-2022) were prioritised due to how rapidly issues may shift based on evolving technology, and digital access and usage patterns.

Gaps in data and evidence

The majority of literature on cyber harms and women, girls and excluded groups pertains to cyber violence against women and girls (VAWG). This is a prevalent issue with a range of implications (as illustrated in section 3) but it should also be noted that other forms of cybercrime may also have a disproportionate impact on women and excluded groups. However, these types of harms are much less documented and there is a lack of data and evidence.

Consultations and Key Informant Interviews also suggest that institutions are in early stages of engaging with the nexus of cyber security and social inclusion. While there is enthusiasm and some work has been done in these spaces, there is relatively little past experience to draw from to be able to draw definitive conclusions on what works in tackling cyber harms experienced by women and excluded groups.

Because of the above and the implications they have on availability of evidence, it has been difficult to make recommendations based on what has worked elsewhere. Therefore this paper should be treated as a snapshot of issues at a current moment in time, rather than a comprehensive collation of evidence. In some cases, where there are gaps in evidence or data, suggestions have been made based on inferred or possible outcomes.

Annex 2: Targeted Cyber Violence against Women and Girls

Type	Definition & Occurrence	Who may have heightened risk?[2]	Indicative Interventions	Barriers/Risks[3]
Cyber Stalking	Unwanted and repeated attention or surveillance in a digital setting. This can lead to control and psychological abuse.	Victims/Survivors of Intimate partner violence (IPV)	• School-based interventions • Training of law enforcement • Development of referral mechanisms • Communications Campaigns • Development of apps and tailored online content to support victims	• Cultural norms around online harassment, victim blaming • Lack of definition of crime in local laws • Difficulty in collecting evidence of harassment • Root causes, including structural gender inequality and social exclusion go beyond cyber security
Non-consensual pornography (or revenge porn)	Revealing or sexually explicit images or videos of a person posted on the internet or in a digital setting, typically a former partner, without the consent of the subject.	Victims/Survivors of Intimate partner violence (IPV)	• School-based interventions • Training of law enforcement • Development of referral mechanisms • Communications Campaigns • Development of apps and tailored online content to support victims	• Cultural norms around online harassment, victim blaming • Root causes, including structural gender inequality and social exclusion go beyond cyber security
Gender-based slurs and harassment	Harassment, discrimination, demeaning and abusive language and jokes shared publicly or privately in a digital setting, due to a person's gender or gender identity.	Women from racial or ethnic minorities, women with disabilities, women from sexual minority groups, women with high public profile	• School-based interventions • Development of referral mechanisms • Training of law enforcement • Communications Campaigns • Development of apps and tailored online content to support victims	• Not always clearly defined according to law • Lack of transparency in enforcement from social media companies • Root causes, including structural gender inequality and social exclusion go beyond cyber security

[2] While all women were found to at risk from these types of violence, where other intersecting identities may heighten risk is indicated here. This does not mean these are the only groups at risk.

[3] Many barriers and risks are common across these types of harms. However, some harms are more explicitly recognised than others, for example in legal settings.

Sextortion (or blackmailing online)	When someone threatens to distribute your private and sensitive information in a digital setting (including videos, photos) if you don’t provide them with images of a sexual nature, sexual favours, money or something else.	All	• School-based interventions • Development of referral mechanisms • Training of law enforcement • Development of apps and tailored online content to support victims • Cyber security awareness and cyber hygiene training • Data protection interventions	• Cultural norms around online harassment, victim blaming • Lack of definition of crime in legal context • Difficulty in collecting evidence of crime or information on perpetrators • Root causes, including structural gender inequality and social exclusion go beyond cyber security
Rape and Death threats	Statement or communication in a digital setting that intends to inflict rape or murder on someone. This is normally anonymous.	Women with high public profile	• Development of referral mechanisms • Training of law enforcement	• Difficulty in tracking anonymous perpetrators online • Root causes, including structural gender inequality and social exclusion go beyond cyber security
Doxing (also doxxing)	Identifying and sharing someone’s personally identifiable information via digital settings.	All	• Training of law enforcement • Development of referral mechanisms • Communications Campaigns • Development of apps and tailored online content to support victims • Cyber security awareness and cyber hygiene training • Data protection interventions	• Cultural norms around online harassment, victim blaming • Lack of definition of crime in legal context • Difficulty in collecting evidence of crime or information on perpetrators • Root causes, including structural gender inequality and social exclusion go beyond cyber security
Electronically Enabled trafficking	Use of technology to lure potential victims into violent situations; e.g., fraudulent postings and advertisements (dating sites; employment opportunities); traffickers using chat rooms, message boards, and websites to communicate/ advertise.	Children and young people; women aged 18-24; people from minority groups; girls (aged 13-17)	• School-based interventions • Training of law enforcement • Development of referral mechanisms • Communications Campaigns and awareness raising • Development of apps and tailored online content to support victims	• Digital Gender Divide • Root causes, including structural gender inequality and social exclusion go beyond cyber security

Hacking	The use of technology to gain illegal or unauthorized access to systems or resources for the purpose of acquiring personal information, altering or modifying information, or slandering and denigrating the victim and/or VAWG organizations. e.g., violation of passwords and controlling computer functions, such as freezing the computer or logging off the user	People from racial or ethnic minorities	• Digital literacy training • Cyber security awareness and cyber hygiene training • Data protection interventions	• Digital Gender Divide • Difficulty in tracking anonymous perpetrators online
Impersonation	The use of technology to assume the identity of the victim or someone else in order to access private information, embarrass or shame the victim, contact the victim, or create fraudulent identity documents; e.g., sending offensive emails from victim's email account; calling victim from unknown number to avoid call being blocked	All	• Digital literacy training • Cyber security awareness and cyber hygiene training • Data protection interventions	• Digital Gender Divide • Difficulty in tracking anonymous perpetrators online
Mal/Mis/Disinformation (MDM)	**Misinformation:** False but not created or shared with the intention of causing harm. **Disinformation:** Created to mislead, harm or manipulate a person, group, organisation or country.	Women with high public profile	• Targeted support for female journalists, politicians or campaigners including additional security measures, psychological support, personal data protection measures.	• Potentially used as a state tool, so law enforcement may not be sympathetic in some cases • Can per perpetuated by online trolls and bots which are hard to track and prevent • Root causes, including structural gender inequality and social exclusion go beyond cyber security

	Malinformation: Based on fact but used out of context to mislead, harm or manipulate. Deep fakes can be used for all the above.			
Surveillance/ Tracking	The use of technology to stalk and monitor a victim's activities and behaviours either in real-time or historically; eg. GPS tracking via mobile phone; tracking keystrokes to recreate victim/survivor's activities on computer	Victims/Survivors of Intimate partner violence (IPV)	• Digital literacy training • Cyber security awareness and cyber hygiene training • Data protection interventions • Digital forensic training for law enforcement	• Digital Gender Divide • Difficulty in tracking anonymous perpetrators online
Cyber Dating Abuse	CDA is defined as the control, threatening, harassment, stalking, and abuse of dating partners via technology and social media (Zweig et al., 2014).	Victims/Survivors of Intimate partner violence (IPV); Young people	• School-based interventions • Development of referral mechanisms • Development of apps and tailored online content to support victims	• Root causes, including structural gender inequality and social exclusion go beyond cyber security • Data on occurrence is based mainly on studies in North America

Annex 3: Regional trends in cyber security and GESI

Summary

Data looking at regional trends of cyber violence against women, girls and other vulnerable groups is relatively scarce especially in low and middle income countries. Available evidence suggests that in low and middle-income countries, digital literacy and cyber safety are still considered the biggest barriers to achieving gender equality and social inclusion in cybersecurity programmes. In addition, social-cultural barriers also affect both the activities of women and girls online as well as the types of cyber harms experienced by these groups in different regions.

For the purpose of analysis, we have looked at key areas that have been identified as critical to the way GESI is mainstreamed in current and future cyber security programmes. These areas include prevalence of GBV (online and offline, cyber incidents, E-commerce, women and entrepreneurship, women in cybersecurity sector, accessibility, variations of cyber VAWG, as well as legal and regulatory frameworks. The analysis also focuses on five regions namely Sub-Saharan Africa, Asia and Asia Pacific, Middle East and North Africa (MENA), Latin America and the Caribbean, Eastern Europe. A look at the global trends provided useful comparison between these regions.

Prevalence

Literature reviewed suggest that data on technology-facilitated GBV (cyber VAWG) and those that occur offline is scarce and best patchy in virtually all the regions reviewed. However, there is evidence to suggest that obtaining actual percentages of victims of cyber VAWG and the prevalence of harm across each region is a herculean task due to low reporting, none criminalisation of cyber VAWG, challenges in surveying survivors, and where limited data exist, such data lacks the disaggregation by sex of the victim and perpetrators and the relationship that exist between them.

Cyber incidents

The most common cyber-attack trend for 2022 remains credential theft (19%) then phishing (16%), misconfigured cloud (15%) and vulnerabilities in third-party software (13%)`. The biggest among these cyber-attacks include the Ukraine war (Eastern Europe); the Costa Rica Conti ransomware attack (Central America) but also linked to Russia; the Lapsus$ group' chaotic spree that targeted Ubisoft, Samsung, Nvidia and Microsoft (North America); Ransomware attacks and Data theft of healthcare providers (North America and Europe); Cryptocurrency theft by North Korea's Lazarus Group (worldwide); Data breach in Marriot hotel (North America); Targeted industry attacks of steel companies by Predatory Sparrow linked to Iran (Southwest Asia); Drone-based intrusion of a financial services company (unnamed and region unknow). On a positive note, the Dutch National Police managed to launch a counter ransomware attack that led to the notorious DeadBolt ransomware gang into handing over 155 decryption keys.

E-commerce, women and entrepreneurship

Increasing global digital transformation has equally the tendency to transform e-commerce and the lives of women entrepreneurs globally. E-commerce growth across all the regions analysed is being used by women to advance gender equality and social inclusion by leveraging e-commerce to open up more markets and enter sectors (e.g. electronics) where women have been traditionally underrepresented.

It has been argued that the rise of ecommerce in the pandemic created a lucrative window of opportunity for cybercrime to flourish. This window was created as businesses sought to reduce supply chain strain through ecommerce without necessarily strengthening their cyber defences. As a result, the pandemic led to a sales dip for many women-owned entrepreneurs whilst increasing online threats for both female entrepreneurs and consumers alike. Some of the online threats faced by women and girls in ecommerce have been linked to security issues, privacy issues, trust issues, digital threats, social networking worms, phishing bait, trojan, data leaks, shortened links, botnets, advanced persistent threats, cross-site request forgery impersonation, pornography, human trafficking, censorship and cyber VAWG (Ismail & Al. 2020).

These threats and cybercrime are a particular concern for Women, girls and other vulnerable groups face due to the fact that they may be less attentive and perceptive when it comes to identifying unusual online behaviour. Their lack of expertise and access to the internet further makes them a high risk to technology related violence. A combination of the highlighted risks, access to the internet, low awareness and expertise of the ecommerce and cybersecurity landscape has created a barrier for women, either as entrepreneurs or customers in developing e-business entrepreneurship and empowerment activities (Michota, 2014).

Women in the cybersecurity

Due to structural, infrastructural, or social cultural inequalities, the fact remains that women are strongly underrepresented not only in the cybersecurity sector, but also in the debates and the decision-making processes related to cybersecurity programmes and defence. A 2020 survey projected that women who work in cybersecurity represent only 28% of the total workforce globally. According to the World Bank, two out of 10 cybersecurity professionals are women. This percentage is 9% in Africa, 30% in Asia and Asia Pacific, 32% in South East Asia alone, 20% in the Middle East, 24% in Latin American and the Caribbean.

Asia Pacific

- **Cyber threats.** Common cyberthreats in the region include ransomware, scams, phishing, e-commerce data inception, cryptojacking, crimeware-as-a-service, and denial-of-service attacks. The top countries prone to incessant cyberattacks in the Asia-Pacific region are Japan, Singapore, Indonesia, and Malaysia with a 40%, 30%, 25%, and 22% increase, respectively (Security Brief Asia, 2022; INTERPOL, 2022).
- In 2022, Asia was the most targeted region; one in four cyberattacks worldwide occurred in the region. The most common of these attacks are ransomware, server access and data theft. The most targeted countries were Japan, Australia and India (Zdnet.com, 2022).
- In Asia Pacific, 59% of business have experienced cyber incidents, 36% of organisations do not have a response plan, data loss is the most reported impacts of cyber incidents and malware is the most common cause of cyber incidents (Kroll, 2022a).
- **E-commerce and women entrepreneurship**. Asia has more women entrepreneurs than men. Women-owned businesses tend to be smaller with lower average sales and fewer employees (World Bank 2019). COVID-19 disproportionately impacted women; women sales dropped by 27% in the Philippines and 44% in Indonesia.
- More female online consumers, compared to male online consumers in Southeast Asia have made more e-commerce purchases since the pandemic started and will continue to shop at newly discovered online stores post pandemic (Kantar, 2020).
- **Access**. In India, around 12 % of women report not to use the Internet because of the negative social perception associated to its use, and 8% due to the lack of acceptance by family members (OECD, 2018).
- **Related social factors**. Key societal factors relevant to technology-facilitated GBV in the Asia region include: patriarchal social norms, familial power dynamics, taboos surrounding sex and sexuality, varying levels of digital literacy, cultural taboos surrounding sex and sexuality leading to sexual frustration, societal perception of cyber VAWG as ‘not serious’, victimisation of women participation in both social and political debates and the normalization of GBV (USAID, 2022).

Africa

- **Prevalence of cyber VAWG.** In 2021, over 81 million cyber attacks were recorded in Kenya (32.8%), South Africa (31.5%) and Nigeria (16.7%). 80% of these attacks are categorised as criminal, 19.9% are categorised as targeted while 0.1% are categorised as advanced. Organisations prone to cyber attacks include government, telecommunications, diplomatic, education and healthcare (The Fintech Times, 2021)
- A 2018 study by UN Women revels that 73% of African women have already been exposed to or have experienced some form of cyber violence (UN Women, 2018). By 2020, there was a 17% increase thereby making 90% of women in Africa to have personally experienced or know someone who has experienced cyber VAWG (EIU, 2020).
- A 2021 survey of low-income women in Malawi revealed that 67.1% of respondents say that they experience cyber harm on a daily basis while 26.4% say they experience cyber harm on a weekly basis (Arxiv.org, 2021).
- In spite of this gender disparity in digital access between men and women in Kenya, more than one in five Kenyan women surveyed had experienced cyber VAWG (Web Foundation, 2016).
- **Cyber threats.** The top cyberthreats in Africa are online scams, digital extortion, business email compromise, ransomware, and botnets. The lack of cybersecurity policies, standards and infrastructure further exposes the population to these online risks (INTERPOL, 2001).
- Consequently, there are growing concerns about the inability of African governments to protect its cyberspace. For instance, in June 2020, it was estimated that South Africa has the third highest number of cybercrime victims globally. In Nigeria, one in nine Android mobile phones has malware-infected

applications. This year, Ethiopia, home to the headquarters of the African Union reported an increase in cyber attempts (Tony Blair Institute, 2022).

- **E-Commerce and Women Entrepreneurship**. Women are active participants in e-commerce in the region. For instance, women own between one-third (in Côte d'Ivoire (31%) and just over half in Kenya (51%) and Nigeria (51%) of companies on Jumia, one of Africa's largest e-commerce platforms. Women vendors are more likely than men to use social commerce tools like WhatsApp and this is where many women get their start selling online However, the COVID-19 pandemic reversed or stunted many of these early successes as women sales fell by 7% while men's sales rose by 7% (Foresight Africa, 2022).
- Studies have shown that legal constraints, access to finance, digital connectivity, logistics, digital skills and low uptake of fintech offerings have been identified as major barriers that impacts on women's ability to effectively participate in e-commerce and entrepreneurship in the region (IFC.org, 2021).
- Platforms where cyber harm occur for women. Cyber VAWG are often perpetuated on social media platforms (62%) especially Facebook and WhatsApp or entertainment and dating sites (31.3%) (Arxiv.org, 2021).
- **Access**. The internet access growth rate in Africa is estimated to be 27% per annum while the percentage use of social media by women and girls is relatively higher than this access rate (UN Women, 2019). A Kenya study found that in the slums of the capital Nairobi, only 20% of women were connected to the internet, compared to 57% of men (Web Foundation, 2016). In Uganda, 43% of men are more likely to be online than women.

Middle East and North Africa (MENA)

- **Prevalence of online threats for women and girls**. Cybercrime is the biggest source of concern for 76% of internet and mobile phone users in MENA. 40% of online shoppers have been victims of cybercrime while 71% have witnessed or have been aware of a cyber-attack (Cosumer international, 2019).
- One in 10 Moroccan women has reported cyber harm to authorities. In spite of these statistics, many of the cyber harms experienced by women and girls in MENA region go unreported (MiddleEast Eye, 2020).
- One third of wone in Arab countries have been subjected to violence and harassment online such as sexual assault, as well as threats and blackmailing to publish indecent pictures of women (GendderIt.org, 2018).
- **Cyber Incidents**. In 2022, cyber attacks in the Middle East have increasingly targeted civilians. Examples of such threats include the hacking of Iran's national fuel distribution network consequently disrupting the smart payment system that the government uses in distributing subsidised petrol. Another major cyber incident was linked to Black Shawdow (an Iran-affiliated hacker group) which leaked the personal data of Isreali users of the LGBTQ dating app Atraf (Equal Times, 2022). These cyber attacks have contributed to increased social and political tension within the countries in the region.
- Kaspersky reported a 17 per cent increase in malware attacks in the Middle East ion an annual basis. Oman recorded the biggest increase in malware attacks(45%), followed by Egypt (32%), and Qatar (16%). It is interesting to note that UAE, which is the second biggest economy, recorded only 7% rise in malware attacks. These attacks have been linked to the Covid-19 pandemic and the rapid digital transformation of the regions economy. Hospitals and medical centres are also the targets of most of these attacks using advanced persistent threat-type attacks that are intended to steal sensitive data (The National News, 2021).
- **E-Commerce and Women Entrepreneurship.** With a growing population and high smartphone penetration, online retail has been slow to take off in the Middle East and North Africa due to cultural reasons (ZEDNET.COM, 2015). When COVID-19 struck, many people found themselves shopping online for the first time in the Middle East, a region where e-commerce was weak (UNCTAD, 2022).
- Research has shown that women entrepreneurs in MENA are not making the most of what e-commerce has to offer them as only one quarter of women entrepreneurs in the region reports using digital technologies at some stage in their business operations and sales. The low uptake of ecommerce has been attributed to the relative high cost of buying an ICT device, poor internet connectivity, privacy and safety concern, digital literacy, language barriers, low understanding of the benefits of ecommerce and the disapproval by family and friends. On average, 44% of rural areas in MENA countries benefit from 4G mobile network coverage, compared to 76% of urban areas (OECD.ORG, 2022)
- As women in MENA continue to tackle the cultural restrictions and the impact of the pandemic, women entrepreneurs formerly excluded and underserved are increasingly moving from exclusively cash-based transactions to embracing e-transactions supported by social commerce and e-commerce (Fast Company, 2022)

- The rise of women in tech with half of all STEM graduates coming from the MENA region, it is not surprising that a quarter if digital startups in the region (Middle East in particular) were founded by women (Fast Company, 2022). Despite the fact that between 34% to 57% of STEM graduates in the Middle East are women, this has not increased the percentage of women in the cybersecurity and tech workforce in the Middle East. Available statistics estimate that in 2017, only 11% of the cybersecurity in the Middle East were women, and this figure rose to about 20% in 2021 (CIO, 2021).
- **Access.** MENA region is undergoing a digital boom with 71% of people with online access as at 2019. The region also has the fastest mobile phone growth rate outside Sub-Saharan Africa and the region also has one of the most youthful populations in the world with 60% of its population aged under 30 (Cosumer international, 2019).
- When compared to other world regions, the gap between men and women with respect to the internet penetration rate is largest across Arab States. Therefore its not a coincidence that the region has the world's worst performance in narrowing the gender gap. The digital divide across the Arab States region pertains not only to gender, but also to the elderly, the less educated and lower income individuals, who are also less likely to use the Internet than their younger, more highly educated and higher-income counterparts (Arab Barometer, 2020).

Latin America and the Caribbean

  - **Prevalence of online threats for women and girls.** Research in Latin America suggests that attacks on media workers via Twitter are fueled by hostility to journalists, especially women journalists, perceived as expressing opinions in a polarised society (UNESCO, 2021).

- In Cuba and the rest of Latin America, there is evidence to suggest that Covid-19 and the pandemic led to an increase in use of the internet and social media to perpetuate cyber harms with women and girls in the region becoming the victims of crimes such as cyberbullying and revenge porn (Havana Times, 2020).
- **Cyber Incidents.** In 2019, the region has faced different types of incidents such as DoS (denial of service) and multiple ransomware cases. Since the rise of COVID-19, we have seen around three million cyberattacks in Latin America and the Caribbean. In March 2020, computer virus incidents in the region increased by 131% compared to the same period in March 2019. The increase in computer virus has been attributed to the increase in web traffic activities in multiple Latin American countries within the same period (ISJ, 2020).
- **E-Commerce and Women Entrepreneurship**. In 2020, mobile data traffic increased by 25% and more than 50 million Latin Americans became online consumers for the first time. While this digital transformation has expanded access to financial, medical and educational services to people across the region, it has also increased privacy and cybersecurity concerns (Wilson Centre, 2021).
- Data from the Digital Economy in Latin America and the Caribbean project indicate that between April and May 2020, business websites increased by 800% in Colombia and Mexico and by around 360% in Brazil and Chile. In spite on this jump, barriers such as connectivity issues, insufficient logistics infrastructures, limited access to capital, and lack of digital skills (with large discrepancies between rural and urban areas) still persist in the region (UNCTAD,2021).
- **Variations of cyber harm for women, girls and excluded groups**. Ethnopornography, which is a type of sexual exploitation of indigenous girls and women is said to be prevalent in the region and currently on the rise in Mexixo. This type of cyber VAWG uses extortion, and erotic images and videos that have be obtain from indigenous women, girls and other vulnerable groups to exploit or harras victims. This illicit content are shared on the Internet, on social media and in the corporate environment. This is the most common type of online violence in the region to the extent that (Havana Times, 2020).

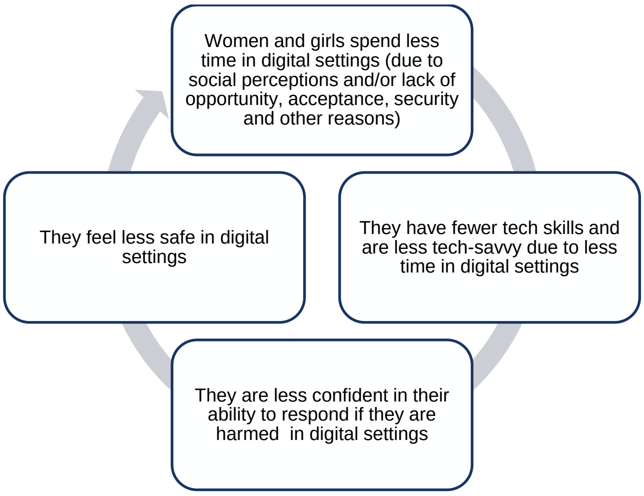
Annex 4: Categorising ODA programmes that connect to cyber security

Due to the broad scope and varied definitions of cyber security programmes, different actors and programmes can target different areas, or dimensions, of cyber security. For example, different actors may engage on different dimensions of the GCSCC cyber security capacity maturity model for nations (CMM). Also, other ODA programmes, that are not defined as cyber security programmes per se, can also respond to different cyber harms within a particular country, region or at a global level.

As different actors use diverse definitions of the term "cyber security programmes" there is a lack of consistency in what is included across this emerging area of work. Based on the literature and consultations, this paper has broadly categorised the ODA programmes and initiatives that connect in some way to the different cyber harms outlined above.

Type of ODA programme	Objective	Connection to cyber security programmes	Connection to gender equality and social inclusion (GESI)
ODA cyber security programmes	To strengthen cyber security capacity and resilience of a nation, community, organisation or individual	A cyber security programme	GESI is / should be embedded in every dimension of the programme
ODA programmes which aim to respond to cyber harms, e.g., TFGBV programmes, child protection online	Specific objectives related to cyber harms, such as TFGBV prevention and response	Respond to one or some cyber harms	It is likely that GESI is a core consideration of the programme design, and that social change transformation in a particular community is a core consideration of the programme design
Non-cyber security ODA programmes which use technologies as a core part of their delivery, e.g., online education programmes or large-scale financial distribution programmes.	Specific topical objectives, such as education attainment or number of finance distributions	Use different technologies as core for their delivery. As digital technologies are increasingly intertwined with our offline lives, this category includes the large majority, if not all, ODA programmes.	Poor cyber capabilities and resilience in general can lead to more and different harms for women, girls and other excluded groups. GESI is / should be embedded in every dimension of the programme

Annex 5: Negative cycle - women and girls in digital settings


Women and girls spend less time in digital settings (due to social perceptions and/or lack of opportunity, acceptance, security and other reasons)
They have fewer tech skills and are less tech-savvy due to less time in digital settings
They are less confident in their ability to respond if they are harmed in digital settings
They feel less safe in digital settings

HM Government