Gender mainstreaming and the proposed cybercrime convention: Commentary on the consolidated draft

December 2022 | Chatham House Cyber Policy team

Introduction

Gender mainstreaming and gender equality have become a component of state discussions on the scope and objectives of the proposed Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (the cybercrime convention), across the first three sessions of the Ad Hoc Committee (AHC) negotiating this convention.

In a previous briefing paper, Chatham House outlined what it means to gender mainstream the cybercrime convention. Key points from that paper include:

- **Gender mainstreaming** is "the process of assessing the implications for girls and boys and men and women [and people of diverse gender identities and expressions] of any planned action, including legislation, policies and programmes".[i]
  The goal of gender mainstreaming is the promotion of **gender equality.**
- Effective gender mainstreaming is **intersectional**: it pays attention to multiple forms of social power relating to class, race, coloniality, nationality, ability, ethnicity, caste, sexual orientation, age and gender expression etc.[ii] An intersectional approach also considers historical, social and political contexts and recognizes the unique experience of individuals based on the intersections of these and other personal factors.[iii]
- Gender mainstreaming also attends to the needs and vulnerabilities of men and boys (particularly from marginalized groups).
- Gender mainstreaming includes the rights of people of diverse gender identities, expressions, and sexual orientations, including non-binary people.
- Gender mainstreaming best practice is **"multi" track**: gender is incorporated into all aspects of policy- and programme-making and pursued as a distinct, stand-alone goal.[iv]

Drawing upon this analysis, this Chatham House briefing paper summarizes AHC discussions on gender to date and analyses the consolidated negotiating document of the proposed cybercrime convention (A/AC.291/16) on general provisions, criminalisation and procedural measures from the perspective of gender mainstreaming and equality.

Summary of AHC discussions on gender

Member States' submissions and AHC discussions on gender have revolved around several key themes: the importance of gender perspectives and gender equality to the overall convention, both on their own and as part of broader human rights provisions; the protection of people, including women and girls in vulnerable situations; and the importance and value of gender mainstreaming the convention, including crime prevention, technical assistance, and capacity-building.

Written submissions to the first session of the AHC (AHC1) noted the importance of gender parity and women experts in drafting the cybercrime convention;[v] the need to address gendered dimensions of

cybercrime (including the needs of women and girls);[vi] and the value of gender-sensitive cybercrime training.[vii] Gender parity was also identified as a priority in Annex III of the report of AHC1 (A/AC.291/7), with respect to expert panel discussions in intersessional consultations.[viii]

Written submissions to the second session of the AHC (AHC2) expanded Member States' engagement with gender and cybercrime. These submissions emphasized: the need to protect human rights and fundamental freedoms (with specific attention to gender);[ix] the importance of the perspectives of women and other people of diverse backgrounds;[x] gendered dimensions of vulnerabilities to cybercrime, including sexual exploitation;[xi] and the importance of gender mainstreaming and a gender perspective in the convention.[xii] Subsequent discussions of gender at AHC2 – notably with respect to Questions 5 and 12 regarding general treaty provisions – indicated support for gender equality and broad openness to incorporating gender into the proposed convention. Several Member States specifically noted their support for provisions that acknowledge the specific risks cybercrime poses to women and girls and/or incorporate gender equality, as a component of human rights, directly into the general provisions of the convention.

Written submissions to the third session of the AHC (AHC3) included more detailed suggestions to promote gender equality and a gender perspective. Member States highlighted the importance of: using evidence to understand and respond to the specific cybercrime needs of people (including women and girls) in vulnerable situations;[xiii] attending to gender equality in measures to prevent crime;[xiv] existing gender mainstreaming efforts to prevent cybercrime, including public awareness and education campaigns;[xv] gender mainstreaming of technical assistance and capacity building activities, and working toward gender parity/closing the gendered digital divide within such activities;[xvi] addressing gender-based violence;[xvii] and writing gender mainstreaming into the implementation provisions of the convention.[xviii]

Discussions at AHC3 regarding preventive measures – especially Question 32 on whether to prioritize preventive measures for "particular groups" – indicated broad support for preventive measures focusing on people in vulnerable positions. Member States defined women, children, the elderly and people with disabilities as vulnerable groups. Discussions about technical assistance at AHC3 – especially Questions 24, 25, and 26 – indicated broad support for including gender equality as a principle and best practice for technical assistance and capacity building. States highlighted the importance of gender mainstreaming, as well as working towards gender parity and closing the gendered digital divide. States also noted the need to include other groups in technical assistance and capacity building, including youth and disabled people.

There are several components of gender equality and mainstreaming that have not yet been raised directly by Member States submissions or during sessions, including: the rights and equality of people of diverse gender identities, expressions, and sexualities (including non-binary people); intersectional analysis of relationship between gender and other forms of potential marginalization; the relationship between gender equality and individual privacy; and the applicability of gender equality (and a gender perspective) to all people in contact with cybercrime governance, in addition to victims (including policymakers, law enforcement actors, citizens, suspects, and the accused). Including these components would significantly strengthen efforts to substantively incorporate gender mainstreaming into the convention.

More generally, while there has been an increase in State submissions and discussions on gender over the previous three sessions, most States have not yet engaged with gender considerations as part of the convention at all. There is, consequently, plenty of further scope for increasing the breadth and diversity of views from Member States on how to best incorporate such considerations in the upcoming sessions.

Summary Table of AHC Discussions on Gender

Meeting	Gender Mentioned in Written Submissions	Related Discussions during AHC Negotiations
AHC1	• gender parity in drafting Convention; • gendered dimensions of cybercrime; • gender and cybercrime training	• openness to consideration of limited, gender-based cyber-enabled crimes
AHC2	• gendered dimensions of cybercrime; • gender mainstreaming the convention; • gender equality as core component of human rights	• broad openness to including gender considerations; • support for provisions addressing gendered cybercrime and inclusion of gender equality in general human rights provisions
AHC3	• gendered dimensions of cybercrime; • gender mainstreaming preventive measures; • gender mainstreaming technical assistance/capacity building; • gender mainstreaming implementation of convention (as provision)	• support for gender perspective in measures to prevent crime; • support for gender mainstreaming technical assistance and capacity building

Analysis of consolidated negotiating document by chapter

In November 2022, a consolidated negotiating document (A/AC.291/16) was published in preparation for the fourth session of the AHC (AHC4), which will take place in January 2023. This section analyzes the three chapters in the negotiating document from the perspective of gender mainstreaming and equality. It does not seek to exhaustively identify all gender considerations regarding either this document or the convention overall, especially as provisions on international cooperation, prevention, technical assistance and mechanisms of implementation are excluded from this document and scheduled for discussion at the fifth session of the AHC. It includes recommendations for alterations to the document, or for further discussion at AHC4, both within the text and summarized at the end.

General Provisions

Article 5.2, which calls for states to make efforts to "mainstream a gender perspective and to take into consideration the special circumstances and needs of vulnerable groups, in particular women, children, and the elderly" is highly significant in its explicit consideration of gender, building on the various state submissions and AHC discussions summarized above. The prominent inclusion of wording relating to gender mainstreaming deserves substantial credit.

The inclusion of gender under General Provisions underlines that gender pertains to the whole of the convention. As a component of Article 5 ("Respect for human rights"), Art. 5.2 accurately positions gender as a matter of human rights.[1] This is an effective instance of **single-track gender mainstreaming** - a

[1] If, as some state members have suggested, the convention eventually lists the relevant human rights instruments enumerating these rights, it is important that the Convention on the Elimination of Discrimination Against Women (CEDAW) be among them.

single clause pursuing some dimensions of gender equality as a stand-alone goal. Art. 5.2 is thus an important step towards gender equality in the future cybercrime convention. Further negotiation regarding this article should consider the following elements.

First, Art. 5.2 contains two components – gender mainstreaming, and special needs and circumstances – that, though related, pertain to distinct dimensions of gender and cybercrime. The goal of gender mainstreaming is gender equality. Gender equality includes, but is not limited to, the particular needs of women and girls in vulnerable situations vis-à-vis cybercrime. There is a risk that, as currently written, the article could inadvertently limit considerations of gender equality and mainstreaming only to the particular needs of women and girls in vulnerable situations. Specifically, as currently written, the article may overlook the gendered effects of cybercrime in boys, men and people of diverse gender identities and expressions, as well as the wider role of women and girls in cybercrime governance (below).

Recommendation 1: *Within Article 5.2, clearly separate the text relating to gender mainstreaming from the text relating to special circumstances/vulnerability, and explicitly advocate an intersectional approach to gender mainstreaming.*

Second, the scope of Art 5.2 as currently written takes into consideration the needs and vulnerabilities of particular groups – including groups categorized by socially constructed and hierarchical gendered differences – in relation only to "measures undertaken to prevent and combat" cybercrime. Gender equality is relevant to the whole of cybercrime policy, including criminalization, procedural measures, implementation, governance and oversight. Likewise, intersectional gender mainstreaming should take into account the particular needs and vulnerabilities of people of all genders who are involved in cybercrime and cybercrime policymaking, including law enforcement officials, citizens, policymakers, suspects and accused.

Recommendation 2: *Explicitly affirm the right of women and people of diverse gender identities and expressions to participate in the governance, implementation, and oversight of cybercrime.*

Third, although gender equality is the goal of gender mainstreaming, gender equality is not explicitly mentioned in the consolidated negotiating document. Moreover, there is a discrepancy between the phrasing of Article 5.1 (states "shall ensure" the convention is implemented in accordance with international human rights law), and Article 5.2 (states "shall make efforts" to mainstream a gender perspective). Given that gender equality is part of international human rights law (via the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), the Universal Declaration of Human Rights (UDHR) and other international instruments), there is some risk that, in its current form, Art. 5.2 actually limits the implied commitment to gender equality in Art. 5.1.

Recommendation 3: *Explicitly refer to gender equality as a component of international human rights that Member States "shall ensure." In addition, explicitly mention the inclusion in the text of a gender definition in its broader sense that encompasses non-binary identities and gender expression as part of gender equality.*

Fourth, Article 5 does not mention the right to privacy, which is held by all people, and is particularly important to ensuring the wellbeing, safety, and broader rights of people of all genders, particularly women and people of diverse gender expressions, identities, and sexualities. While other human rights recognized in international law – such as freedom of expression – are also crucial for the wellbeing and safety of people of all genders, the right to privacy is foundational to gender equality, as it ensures a safe private space in which different gender identities and sexualities can be expressed.

Recommendation 4: *Affirm the right to privacy as a core component of human rights law.*

Fifth, there are downsides to the listing of specific groups as particularly vulnerable to cybercrime in Art 5.2. It is true that women are exposed to specific gendered risks in relation to cybercrime. However, as this is the only direct reference to gender in the consolidated draft, it risks exacerbating **gender stereotypes and biases** that lead to women being understood primarily as potential victims in need of the protection of the criminal justice system, rather than as empowered actors that assume various roles in the criminal justice system, including political leaders, members of the police and the judiciary, and political leaders. Women are not an inherently vulnerable group; i.e., vulnerable by nature and in all times and places.

In connection with Recommendation 3 above, the tendency to see women primarily as potential victims of crime risks the adoption of measures that end up limiting their broader human rights. For instance, in many jurisdictions, national legislation intended to protect women and girls from online harassment has been used to suppress information relating to sex education, expressions of LGBTQI+ identities and rights, the work of women human rights defenders, etc.[xix]

Finally, other groups may experience particular risks related to cybercrime that are not explicitly listed in the consolidated draft – notably people with disabilities and people of diverse gender identities, expressions, and sexualities, as well as neurodivergent people.

Recommendation 5: *Reframe "special circumstances and needs of vulnerable groups, in particular women, children and the elderly" to avoid positioning people, particularly women, as inherently vulnerable. This could be done by referring to the "special circumstances and needs of [groups experiencing particular cybercrime risks\groups in vulnerable situations] particularly women, children, people of diverse gender identities, expressions, and sexual orientations, elderly people, and people with disabilities".*

Criminalization

In addition to the single-track approach to gender mainstreaming represented in Article 5.2, current international best practice advises **multi-track gender mainstreaming**, wherein gender is incorporated into all relevant parts of the convention.[2] Given the differential legal status of diverse gender expressions, identities, and sexualities in various national jurisdictions, it is particularly important to consider the implications of all provisions – criminal and procedural – for the rights and wellbeing of gender and sexual minorities.

As noted in our previous briefing paper, the extensive criminalization of online content in the convention poses significant risks to human rights including privacy and freedom of expression, and creates significant potential for both redundancy and abuse. In addition, criminalizing specific forms of online content without considering intermediary liability - in terms of how or when platforms should monitor or remove such content – risks not addressing the major cause of harm, including gendered harms, from such content. In cases of online gender-based violence or non-consensual dissemination of intimate images, much of the harm lies in the continued presence of such content online, almost irrespective of when and whether the original disseminator is prosecuted. In fact, over-criminalization without solving the problem of intermediary liability may actually produce more gendered harms rather than fewer, through re-traumatization of victims and further privacy violations.

Because intermediary liability is appropriately out of scope for both this paper and the convention overall, we therefore believe that avoiding any criminalization of content is the best way to preserve human rights

[2] For example, the UN Sustainable Development Group states that best practice gender mainstreaming is both context-specific and "multiple-track". https://unsdg.un.org/resources/gender-mainstreaming

including gender equality, especially given the existence of other UN processes and international legal instruments to address online gender-based violence.[xx] However, if some forms of online content are criminalized by the convention – as indicated by the consolidated negotiating document – then all criminalization provisions – including those relating to intuitively gendered and/or sexualized harms – should be written narrowly and precisely to avoid inadvertently limiting or negatively impacting gender equality and human rights (including those relating to gender identity, expression, and sexuality).

This section considers the provisions on criminalization in the consolidated negotiating document within the overall caveat above. It is structured in three parts: those relating to online gender-based violence (broadly understood); those relating to cyber-enabled crimes (crimes with offline "analogies", where ICTs are used as part of or exacerbate the impact of the criminal activity); and those relating to cyber-dependent crime (forms of crime targeted at or otherwise entirely dependent on the existence of information and communications technologies).

Provisions relating to online gender-based violence

Article 24 on sexual extortion and Article 25 on non-consensual dissemination of intimate images both pertain to online gender-based violence, in the sense that women and people of diverse gender identities, expressions, and sexual orientations experience particular vulnerabilities to this form of online harm. If drafted narrowly and precisely, with sufficient safeguarding of human rights and protections against misuse, these articles have the potential to improve the security of women and people of diverse gender identities, expressions, and sexual orientations by directing domestic and international law enforcement resources towards countering such activities as cybercrimes, as well as providing increased support to those affected by such activities.

Article 24 and Article 25 together constitute a single "Cluster" (7) in the consolidated negotiating document which, as explained in the negotiating document, suggests they will be discussed together.[3] There are important gender considerations to take into account when comparing sexual extortion (non-consensual sharing of intimate images for *financial gain*) and non-consensual intimate image dissemination in general. For example, men and boys may be more frequently subject to extortion, whereas women, girls and people of diverse gender identities may be more frequently subject to non-financially motivated dissemination.[xxi] For this reason – and in the absence of substantial empirical data – the latter (Article 25) is preferable from a gender perspective, as it includes but is not limited to financially motivated dissemination.

Some reserved options for language in Article 25 (in square brackets) could advantage perpetrators of online gender-based violence, in particular the addition "with the intent to cause serious emotional distress". This may raise the bar for criminalization very high and lead to subjective national interpretations of what constitutes emotional distress, jeopardizing the aims of the article in the first place. The emphasis on reasonable belief in consent to not only the taking but online distribution of the intimate image is current best practice in addressing non-consensual intimate image distribution (NCIID).[xxii]

Recommendation 6: *Support an article that does not depend on a particular motivation or intent (e.g. financial) to criminalize non-consensual dissemination of intimate images (i.e. Article 25 rather than Article 24), and do not include "intent to cause serious emotional distress" in Article 25. These recommendations do not mean that intentionality per se should not be essential to the criminalization of*

[3] The document states that "organization by clusters is only meant to structure discussions held during the formal sessions" (p.3, fn.1).

the act: i.e., the article should still retain the requirement of the act being committed "intentionally and unlawfully".

There are several articles constituting Cluster 5 (18-21) relating to child sexual abuse material (CSAM) and related activity. CSAM is an issue with harmful impacts on people of all genders, including girls and boys. Though there are important gendered dimensions to CSAM, it is important not to conflate CSAM with the protection of women from online gender-based violence. For reasons discussed above, it is problematic to treat women as a vulnerable group analogous to children.

From an intersectional gender perspective, a precise and narrow definition of CSAM, as in Article 18, is preferable to the less well-defined definitions in Articles 20 and 21. In addition to the general advantages explored in this paper, precise and narrowly criminalized activities will reduce the risk that such articles could be misused when applied to educational resources or other emotional or medical support related to gender and sexuality available online. This especially pertains to jurisdictions where particular gender expressions, identities, or sexual orientations – as well as access to sexual and reproductive health care and sexual education – are illegal or highly restricted under national law.[4]

***Recommendation** 7: Ensure that CSAM provisions are drafted sufficiently narrowly to ensure appropriate and necessary access to educational, medical, and emotional support information relating to gender, sexuality, and sexual and reproductive health remains available.*

Provisions relating to cyber-enabled crimes

Article 15 criminalizes "the accessing, sale, provision or otherwise making available of any material containing personal information about a person", as long as this is done "with the intent of obtaining a financial benefit". People of different gender identities and expressions are vulnerable to the leaking of personal information (for example, pertaining to reproductive history or other medical records) in different ways. For example, people of diverse gender identities and sexualities are at risk of being involuntarily outed, and people who may become pregnant risk having their reproductive history made public. Such leaks make victims vulnerable to stigmatization and violence. Furthermore, as discussed above, when such information leaks occur as part of gender-based violence, they do not necessarily have a financial motive. From a gender perspective, the best way to counter such risks is the implementation of strong legal protections for privacy as a human right for people of all genders (see **Recommendation 4**).

Articles 26, 27, 28 and 29 include provisions regarding subversive or armed activities, extremism- and terrorism-related offences, and crimes of genocide and crimes against peace and humanity. From a gender perspective, it is important to recognize that human rights defenders, including women and activists for the rights of people with diverse gender identities and sexual orientations, are often mislabelled under these categories, especially when national laws also criminalize their activities. Such criminalization leads to further gender-based harms, such as the over-incarceration of young men, particularly from marginalized groups, and their exposure to abuse in the prison system. Consequently, these articles pose substantial risks to gender and sexual equality.

More specifically, Article 27, which criminalizes "political, ideological, social, racial, ethnic or religious hatred, the advocacy and justification of such acts and the provision of access to such materials", could easily be subject to misuse. Article 27 is written so broadly it may be used to criminalize legitimate political dissent (including advocacy for gender and sexuality equality) – notably by journalists, whistleblowers, and human rights defenders – as well as access to information about feminism, diverse gender identities,

[4] https://www.hrw.org/news/2020/10/19/submission-human-rights-watch-un-special-rapporteur-right-privacy

expression, and sexual orientations. On the other hand, despite its breadth, it does not include hatred on the basis of gender or sexuality.

***Recommendation 8**: Omit Articles 26, 27, 28, and 29 from the Convention.*

Article 33 on money-laundering may have gendered implications for sex workers, who often are women, people of diverse gender identities or sexual orientations, or come from marginalized or minoritized communities.[5] Where sex work is criminalized under national law, Article 33 may make it more difficult for sex workers to access financial services that lead to increased security or stability. Article 33 may also put at further risk financial support for gendered healthcare provision, including access to abortion, where such provision is criminalized under national law.

***Recommendation 9:** consider how Article 33 both relates specifically to the use of ICTs - especially in clause 2b) - and how it improves on existing international legislation on anti-money-laundering. If there is no additional value, given the risks to sex workers, remove the article.*

Provisions relating to cyber-dependent crimes

In the consolidated negotiating document, cyber-dependent crimes are criminalized in Cluster 1 (Articles 6-10),[6] with the language of these articles taken largely from the 2001 European Convention on Cybercrime (the "Budapest Convention"). These articles focus predominantly on threats to the confidentiality, availability, and integrity of computer data, systems, and networks, although several terminological choices are offered throughout the consolidated negotiating document.

The negotiating document contains several differences from the Budapest Convention, including the addition of targeting critical infrastructure as a potential aggravating factor. While this is likely to be a point of negotiation at AHC4, from a gender perspective it is important to define critical infrastructure in a way that includes services and facilities that are necessary for people of all genders, gender identities and expressions and sexual orientations. This is an intersectional consideration, overlapping with the problems created by differential infrastructural provision in much of the world, especially for poor, rural, aging, or minoritized communities. For example, the provision of sanitary facilities in public spaces that are appropriately sized and gendered and include spaces for non-binary people, as well as appropriate waste treatment for those facilities, is a matter of critical infrastructure with significant gender implications.

Aside from this, the gendered implications of articles 6-10 are less obvious because they are more mediated, meaning that the gendered effects of misuse of computer data, systems, and networks will depend significantly on the use and purpose of those data, systems, and networks. **Given the dependence of these effects on context, we stress again that general provisions on human rights, gender mainstreaming and, as advocated above, privacy are essential to ensuring these articles**

---

[5] While the UN refers to "minority communities" using a primarily numerical definition (https://www.ohchr.org/en/special-procedures/sr-minority-issues/concept-minority-mandate-definition),
the term "minoritized" acknowledges that "status as a minority is a systemic function within a racialized hierarchy that advantages and disadvantages groups differently" (https://www.brandeis.edu/diversity/resources/definitions.html). Minoritized communities include but are not limited to Indigenous, Black, and other racialized communities.

[6] With the exception of Article 14 on the illicit use of electronic payment instruments, which is also a cyber-dependent crime.

have a positive, rather than negative, effect on gender equality (see Recommendations 3, 4 and 5).

Overall, parties should consider carefully the gendered implications of different forms of criminalization, particularly with respect to: privacy; confidentiality of medical information (including sexual orientation, gender identity and expression, and sexual and reproductive health); access to information relating to sexual education; access to information relating to diverse gender identities, expressions, and sexual orientations; the safety of people engaged in sex work; incarceration of particular groups of young men; and protections for whistleblowers, human rights defenders, and journalists.

Procedural Measures and Law Enforcement

In the consolidated negotiating document, the chapter on procedural measures and law enforcement includes a key article on privacy, which, as we have argued above (Recommendation 4), should be repeated or emphasized in the earlier general provisions and throughout the criminalization chapter. More specifically, Article 42 on conditions and safeguards requires that relevant domestic law "shall provide for the adequate protection of human rights and liberties, including rights and fundamental freedoms arising from… obligations under applicable international human rights law", and also "shall incorporate the principles of proportionality, necessity and legality and the protection of privacy and personal data".

Article 42 is crucial to the overall gendered implications of the consolidated negotiating document. It is laudable that this article explicitly mentions privacy protections in addition to general human rights obligations. However, considering the best practice of multi-track gender mainstreaming discussed above, it is best practice to also mention gender - including sexuality, gender identity and expression - as private personal data that requires protection. Specific and strengthened privacy protections for protected forms of communication, including medical, legal, religious, or public interest, would also ensure the article adequately safeguards people of all genders in vulnerable situations. This is particularly important to ensuring the rights and wellbeing of women and people of diverse gender identities, expressions, and sexual orientations both broadly and in jurisdictions where access to abortion and/or the expression of LGBTQI+ identities is currently not legally permitted.

Recommendation 10: *In Article 42: explicitly mention gender mainstreaming; explicitly include gender and sexuality as part of privacy protections; provide stronger, specific protections for privileged communications; and connect the whole article to privacy and gender provisions earlier in the document.*

Article 40 includes multiple references to jurisdiction for offences. As noted above, some activities relating to gender identity, expression, and sexuality, as well as access to/provision of abortion and reproductive healthcare, are criminalized by domestic legislation in some Member States and not others. While this discussion will return in the negotiating document for AHC5 under international cooperation, for example, we note that this is a specific gendered consideration within a broader issue with inconsistent criminalization present in the convention, with significant human rights implications for extradition, trial, and punishment of cybercrime.

Regarding Articles 43-50 (Cluster 2), these articles seek to provide relevant state agencies with significant powers, including on: the search, seizure and preservation of computer data; the real-time collection, preservation and partial disclosure of traffic data; the production of subscriber information and other data; and the interception of content. While these powers are necessary to collect intelligence and evidence regarding cybercrimes, from a gender perspective it is vital that they are accompanied by appropriate conditions and safeguards, both in the overall sense in Article 42, and within the specific articles discussing these powers.

Such safeguards should include strengthened privacy protections for privileged communications as discussed above (see **Recommendation 10**), as well as considering the gendered internet and community access issues created by law enforcement actions like device seizures. Victims of domestic and intimate partner violence, for instance, might be made further vulnerable by the seizing of their devices as evidence; children may rely on such devices for schooling, small traders for banking, and LGBTQI+ people for online resources and support.

Safeguards should also include narrow and precise criminalization provisions that underpin their use. There is significant risk of over- or mis-use of law enforcement powers provided in this chapter of the consolidated negotiating document to collect data on a wide variety of vulnerable or high-risk individuals or communities, especially minorities, as well as access to sexual and reproductive health care by people of all genders and ages. In addition to exposing people of diverse gender identities, expressions and sexualities to the dangers of being involuntarily outed, such provisions could, for instance, be used to monitor location data and/or the use of fertility tracking apps by people who may become pregnant to determine proximity to sexual and reproductive health services.

Recommendation 11: *Ensure the implementation of adequate and effective safeguards and conditions on law enforcement powers in Cluster 2, including protections of the rights of gender and sexual minorities, as well as access to sexual and reproductive health care by people of all genders and ages.*

Other important personal protections, in addition to safeguards against misuse of collection, interception, and seizure powers, are considered elsewhere in this chapter, for example in Article 52 on protection of witnesses. From a gender perspective, Art.52.2.b sets out important alternatives to in-person testimony that can help protect victims in legal cases concerning online gender-based violence. This article would be further strengthened if it explicitly included whistleblowers and journalists within its definition of witnesses, as such individuals often play a key role in identifying and highlighting instances of gender inequality.

Recommendation 12: *Explicitly include protection of whistleblowers and journalists in Article 52.*

Article 53 on assistance to and protection of victims is another important addition to procedural measures. From a gender perspective, a focus on victims is itself helpful, especially on enabling the "views and concerns of victims to be presented and considered". It is important to ensure this is balanced with due process and respect of the rights of the accused (also a matter of intersectional gender equality, given the frequent over-incarceration of young and/or minoritized men). While it is important to recognize that the protection of victims depends on capacity building and training for relevant personnel in law enforcement and the judicial system, the issue of capacity building will be addressed in the next session (AHC5) and so we do not address it further here.

Recommendation 13: *Explicitly refer to importance of gender mainstreaming in reference to the rights of the accused and rights and wellbeing of victims. Explicitly commit to gender-, sexuality-, and age-sensitive training for legal and judicial personnel interacting with victims of cybercrime, including training on trauma-informed and culturally-relevant practices for legal and judicial personnel interacting with victims and accused people.*

Conclusion

Since AHC1, the Ad Hoc Committee has moved forward discussions on incorporating gender and gender equality. The current consolidated negotiating draft, which designates gender mainstreaming as a core component of cybercrime prevention, and highlights the specific needs and vulnerabilities that may be experienced by women and girls, reflects this.

This paper has emphasized the importance of ensuring the protection of groups in vulnerable situations – including but not limited to women and girls – and securing broad protections for equality and human rights. This includes the rights to privacy and access to sexual and reproductive healthcare and related information. This paper has also emphasized the specific and substantial risks faced by people of diverse gender expressions, identities, and sexualities when encountering cybercrime and cybercrime governance, particularly but not exclusively in jurisdictions where LGBTQI+ identities and expressions are not legal. The paper provides gender commentary and recommendations on specific articles in the consolidated negotiating draft.

We hope that this paper will be of value to state members as they consider the next iteration of the consolidated draft. We also note that many of the issues raised here – notably the inconsistent legality of LGBTQI+ identities and expression, sex work, and access to sexual and reproductive healthcare (including abortion) – have substantial implications for the discussions of dual criminality to come at AHC5. Likewise, the specific implications of much of the consolidated draft – particularly those provisions not explicitly relating to gender – depend significantly on the way such articles are interpreted and enacted. Alongside the human rights dimensions of dual criminality, it is therefore also essential that gender mainstreaming feature prominently in AHC5 negotiations on implementation.

---

[i] UN Women, "Gender Mainstreaming", https://www.unwomen.org/en/how-we-work/un- system-coordination/gender-mainstreaming.

[ii] K. Crenshaw, "Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Colour", Stanford Law Review, vol. 43, no. 6, July 1991, pp. 1241–1299, https://doi.org/10.2307/1229039; and Combahee River Collective, "A Black Feminist Statement", Women's Studies Quarterly, vol. 42, no. 3/4, fall/winter 2014, pp. 271–280, https://www.jstor.org/stable/24365010, pp. 210–218.

[iii] See e.g. https://www.ohrc.on.ca/en/intersectional-approach-discrimination-addressing-multiple-grounds-human-rights-claims/introduction-intersectional-approach

[iv] Moser, Caroline, and Annalise Moser. "Gender mainstreaming since Beijing: a review of success and limitations in international institutions." *Gender & Development* 13, no. 2 (2005): 11-22.

[v] https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/USA_National_Statement_-_Cybercrime_AHC.pdf

[vi] https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/MEX-Initial_Position_to_UN_Cybercrime_Convention.pdf; https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/UK_AHC_National_Statement.pdf

[vii] https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/UK_AHC_National_Statement.pdf

[viiiviii] Annex III, Art 15, https://documents-dds-ny.un.org/doc/UNDOC/GEN/V22/016/71/PDF/V2201671.pdf?OpenElement

[ix] https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/New_Zealand_written_contribution.pdf

[x] https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/New_Zealand_written_contribution.pdf

[xi] https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Mexico_Contribution.pdf; https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Canada_Contribution.pdf; https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/United_Kingdom_contribution_E.pdf; https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_intersessional_consultations/Revised_Indian_Text_for_UN_AHC_published_on_12.5.2022_-Revised_.pdf;

https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Egypt_contribution_A.pdf;
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Colombia_Contribution_S.pdf

[xii] https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Canada_Contribution.pdf;
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/United_Kingdom_contribution_E.pdf;
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Switzerland_Written_Contribution.pdf;
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Colombia_Contribution_S.pdf

[xiii] https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/New_Zealand_AHC3.pdf;
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/Australia_-_25_August_2022.pdf;
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/Canadian_Submission_for_AHC3_July_6.pdf;
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/EU_AHC3.pdf;
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/Japan.pdf

[xiv] https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/UK_AHC3.pdf;
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/EU_AHC3.pdf

[xv] https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/Canadian_Submission_for_AHC3_July_6.pdf;
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/EU_AHC3.pdf;
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/Norway_AHC3.pdf;
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/United_States.pdf

[xvi] https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/EU_AHC3.pdf;
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/Canadian_Submission_for_AHC3_July_6.pdf;
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/UK_AHC3.pdf

[xvii] https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/EU_AHC3.pdf;
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/Ghana_AHC3.pdf;
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/UK_AHC3.pdf;
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/United_States.pdf

[xviii] https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/Canadian_Submission_for_AHC3_July_6.pdf

[xix] See, for instance, https://www.hrw.org/news/2020/10/22/online-harassment-women-pakistan; https://www.independent.co.uk/news/world/americas/us-politics/dont-say-gay-bill-florida-ron-desantis-b2057359.html; https://www.hrw.org/news/2020/08/17/egypt-spate-morality-prosecutions-women; https://feministinternet.org; https://www.hrw.org/news/2021/05/05/abuse-cybercrime-measures-taints-un-talks

[xx] https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_35_8267_E.pdf

[xxi] Dueck-Read, A. (2020). Judicial constructions of responsibility in revenge porn: judicial discourse in non-consensual intimate image distribution cases a feminist analysis. Manitoba Law Journal, 43(3), 357-390; Chicago 17th ed; Rackley, E., McGlynn, C., Johnson, K. et al. Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse. Fem Leg Stud 29, 293–322 (2021). https://doi.org/10.1007/s10691-021-09460-8

[xxii] https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/07/Intimate-Image-Abuse-summary-of-report.pdf; Dueck-Read, A. (2020). Judicial constructions of responsibility in revenge porn: judicial discourse in non-consensual intimate image distribution cases a feminist analysis. *Manitoba Law Journal, 43(3),* 357-390.