

# GENDER APPROACHES TO CYBERSECURITY: INTEGRATING POLICY, RESEARCH AND TECHNICAL STANDARDS DISCUSSIONS



## **Gender approaches to cybersecurity: Integrating policy, research and technical standards discussions**

---

### **Roundtable report**

Author: Alan Finlay

Coordination and review: Verónica Ferrari (APC)

Proofreading: Lori Nordstrom (APC)

Design and layout: Cathy Chen

APC would like to thank Juliana Guerra for the substantial support in organising the roundtable and providing feedback to this report. We also extend our gratitude to the participants who contributed their time and expertise to the roundtable.

Published by the Association for Progressive Communications (APC) 2024

Creative Commons Attribution 4.0 International (CC BY 4.0)

<https://creativecommons.org/licenses/by/4.0/>

## Table of contents

<b>Executive summary</b>	<b>4</b>
<b>1. Introduction</b>	<b>6</b>
<b>2. Case examples from the roundtable presentations</b>	<b>8</b>
<b>3. Creating new parameters for technology design</b>	<b>13</b>
<b>4. Working with standards bodies</b>	<b>16</b>
<b>5. The role of the state: A need for policy responses and regulation</b>	<b>19</b>
<b>6. The role of civil society</b>	<b>20</b>
<b>7. Appendices</b>	<b>22</b>

## EXECUTIVE SUMMARY

In September 2024, APC brought together a group of experts from different regions working on gender, feminist technology, cybersecurity policy and governance, and technical standards to discuss and share viewpoints on gender approaches to cybersecurity. This report presents perspectives and insights shared at this event. The following were key observations made by participants during the roundtable:

- Cybersecurity threats to women and sexually diverse people need to be considered holistically and take into account the nuanced experiences of communities in the global South.
- Threats in regions such as Africa, Asia and Latin America include gendered disinformation attacks, hate speech, smear campaigns, doxing, loss of personal and sensitive data and privacy rights through “scooping”, surveillance and hacking, and harms from states trying to enforce laws that are found to be too restrictive.
- The effects of these attacks on women, female politicians, and gender and sexual rights activists include self-censorship and severe psychological harm. Women politicians have been forced to withdraw from mainstream political life, and activists have been forced offline altogether.
- The use of spyware, stalkerware and the hacking of social media profiles is common, while products such as location tracking devices or features are also being used for abuse and surveillance.
- Threat modelling in the design of new technologies needs to take into account the specific and different kinds of online attacks that are experienced by communities and not assume that there can be a one-size-fits all approach to digital security. An intersectional approach is necessary to help to understand how various identities, whether gender, race or socioeconomic status, among others, intersect and impact cybersecurity experiences. A key concern is the invisibility of marginalised communities in threat modelling because their experiences are not acknowledged in design processes.
- Specific attention needs to be paid by tech companies to algorithmic transparency, increasing the language scope of moderation tools, ease of use of security features, digital literacy training, and strengthening reporting mechanisms.
- Standardisation bodies need to take a human-centric rather than a systems approach to standards setting. Cybersecurity needs to be considered as a societal security issue focusing on societal threats. In this way, human rights and gender equality should be central to standards-setting processes.
- Encouraging a greater level of community participation in standards-setting processes entails making these processes understandable by non-technical participants. Interpretation and the translation of documents in standards bodies is a critical need. Marginalised communities also face administrative and resource challenges when trying to engage in technical standards-setting processes for digital technologies, such as visas and the cost of travelling to venues often in the global North.

- There is a need for stronger regulation and intersectional legal frameworks to complement work done in strengthening the gender responsiveness of standards bodies and design processes. However, states often make use of spyware for surveillance, which can compromise their ability to regulate fairly and in the public interest.
- It is important for activists to take a multi-pronged advocacy approach. Organisations need to engage technology design processes and standards-setting bodies, while also working outside of these structures. Key areas of intervention include producing evidence-based research, developing practical tools to support activists and victims of abuse, and running digital literacy and skills programmes. Collaborating with experts from different fields is also important, given the complexity of the cybersecurity landscape.

## 1. INTRODUCTION

This report summarises the key perspectives and insights shared at a two-hour online roundtable titled “Gender approaches to cybersecurity: Integrating policy, research and tech standards discussions” hosted by the Association for Progressive Communications (APC) on 30 September 2024. The roundtable is a continuation of APC’s work on gender and cybersecurity aimed at promoting an intersectional gender approach to international and national cybersecurity governance that centres people in harm and cyber threat responses. Previous publications on this topic include *When protection becomes an excuse for criminalisation: Gender considerations on cybercrime frameworks*,<sup>1</sup> a GenderIT edition titled “A feminist conversation on cybersecurity”,<sup>2</sup> and a three-part framework for developing gender-responsive cybersecurity policy.<sup>3</sup>

There is increasing recognition that people experience online threats differently depending on their identities and social locations. This implies the need to frame cybersecurity as a gendered and intersectional space. However, gender, human rights and intersectional approaches to cybersecurity at the levels of technological design and standards are still disconnected.

In the context of increasing calls to consider the gendered and differentiated impacts of technology design and technical standards, the roundtable aimed to bring together experts working on gender, feminist technology, cybersecurity policy and governance, and technical standards design and research, with the following objectives:

- To better understand gendered and differentiated harms and impacts of cybersecurity threats, based on real-life cases from the global South.
- To explore the potential gendered and differentiated impacts of technology design and technical standards with respect to cybersecurity, and how these impacts can be addressed.
- To create a space for connecting expert communities working in different ways on cybersecurity issues from a gender and sexual rights perspective.
- To explore potential joint agendas and actionable areas for incorporating gender and intersectional perspectives into policy, as well as technology design and technical standards discussions.

---

1. Derechos Digitales and Association for Progressive Communications. (2023). *When protection becomes an excuse for criminalisation: Gender considerations on cybercrime frameworks*. <https://www.apc.org/en/node/38990>

2. <https://genderit.org/node/5659>

3. <https://www.apc.org/en/node/38507>

About 20 experts participated in the roundtable. It consisted of contributions from seven speakers, and a hands-on session to brainstorm ways of collaborating in the future, identify research priorities and topics, and share resources.

The report below is written under the Chatham House Rule, and therefore contributions are presented anonymously.

## 2. CASE EXAMPLES FROM THE ROUNDTABLE PRESENTATIONS

Presenters shared research and their experiences with technology-facilitated gender-based violence (TFGBV) in Africa, Asia and Latin America, showing the breadth of online harms that need to be considered to properly address cybersecurity threats to women and sexually diverse people.

### 2.1. Supporting women in politics in Uganda

Both harassment and gendered disinformation campaigns have impacted negatively on women participating in politics in Uganda. Women politicians in the country are frequently targeted with personal attacks, “sexualised rumours” and “body shaming”. The intention behind these public attacks is “to weaken their credibility and erode public trust and their legitimacy as public servants.”

“Centring the private life of women has been weaponised against their political participation and aspirations,” the presenter explained. In this respect, civil society had found that the experience of women working in politics is quite different from that of men, who are usually at the receiving end of “banter and jokes”, while women tend to receive thinly veiled threats to their personal safety and privacy.

Two examples were given. The first involved a leader of the opposition in the Ugandan parliament.<sup>4</sup> She constantly had to deal with coordinated disinformation campaigns that focused less on her political competence and more on her “appearance and personal lifestyle”. These attacks were said to have “pushed her out of the system such that there was no way for her to run for office again.” Today she works outside the mainstream political arena, but still organises online, and is outspoken on issues of justice, human dignity and good governance.

The second example – a case of harassment rather than a disinformation campaign – involved a journalist and politician who was also a member of parliament in Uganda. She was stalked by a 25-year-old man who persistently called and texted her to profess his love despite multiple attempts to block his communication. The man was finally arrested, found guilty, and sentenced to two years in jail. While she continues to serve in parliament, and although she could seek legal recourse, the harassment underscores the vulnerability of women entering public life to unwanted advances.


---

4. From May 2016 to August 2018.



The presenter said that civil society strategies to address these gendered attacks on women in politics included:

- Monitoring platforms to properly understand and develop a strategy to navigate gendered attacks on women in politics.
- Building the digital resilience of women working in politics so that they are better able to deal with disinformation campaigns. The focus was on local government leaders who are still vying to get into mainstream politics to build their digital skills for this purpose.
- Developing their profiles on mainstream digital platforms so they can continue to advocate for their causes.
- Attaching women politicians to media houses so they can counteract the rumours.
- The creation of spaces where women in politics can share their stories.



“How do we organise outside mainstream platforms? It may not be possible to remain relevant to this conversation if you do not stay online, so how do you get to your constituents outside the noise? How do you block? How do you avoid being consumed by the trauma of the experience? In the meantime, how do we support them when they are going through such violence so that we deal with the trauma and find rapid responses for their reality online? This is the training and network building that we are engaged in.” – Presenter, commenting on the attacks on women in politics in Uganda

## 2.2. “Gendered fear” created among activists in Thailand

In Thailand, recent research on TFGBV<sup>5</sup> centred on the testimony of 40 activists – 26 LGBTQIA+ people and 14 cis-heterosexual women. It found that there are predominantly two types of TFGBV in the country: online harassment, and targeted digital surveillance, which involves the use of spyware such as Pegasus or Predator, and targeted attacks on people’s individual Facebook accounts. The research found that many activists withdrew from their activism because of these attacks, and even refrained from using social media altogether. The aim of the attacks was to discredit and silence the activists and push them out of civic space.

With respect to online harassment, the most common type mentioned by the participants in the research was hateful and abusive speech that was often laced with homophobic, transphobic, misogynistic or sexualised content. Activists also experienced smear campaigns through online platforms and doxing (revealing personally identifiable information about a person without their consent) in an attempt to publicly shame and intimidate them.

Participants in the research were often made aware of attacks on their Facebook accounts when they received notifications from Meta saying their accounts may have been targeted by “sophisticated or government-backed attackers”.

The presenter emphasised the structural aspect of these attacks, and that they were part of a continuum of gender-based violence that is perpetuated offline and in digital spaces: “These impacts are influenced by existing structural barriers and gender biases that women and queer people in Thailand already experience due to their gender and sexual orientation.”

The research also found that nearly all the activists experienced more than one form of attack at a time:

It’s like there’s a toolbox of these harms and the perpetrators choose whichever selection in tandem that will have the desired impact against the marginalised person or community; for example, if they are Muslim or trans or whether they are based in Bangkok or in the Southern provinces.

The effects of these attacks on activists included self-censorship, what the presenter referred to as “gendered fear”, anxiety and severe psychological harms: “Some of the activists now suffer from PTSD [post-traumatic stress disorder], depression, anxiety – one woman referred to feeling like she had been raped by Pegasus.”

---

5. Amnesty International. (2024). *Thailand: “Being ourselves is too dangerous”: Digital violence and the silencing of women and LGBTI activists in Thailand*. <https://www.amnesty.org/en/documents/asa39/7955/2024/en>

“There was a real gendered fear and anxiety among those targeted by Pegasus spyware that their data can be weaponised against them in a different and distinct way from cis-heterosexual men. For example, they talked about not wanting to take their phones into the bathroom anymore, not wanting their intimate or families’ photos or videos on their phones, really being nervous and panicking about who’s got their data? What did they take? How long will they have it? How long till they use it against me?” – Presenter, discussing the psychological impact of surveillance on activists in Thailand



### 2.3. A feminist helpline and perspectives on surveillance in Brazil

The third presentation discussed the work of a feminist helpline in Brazil, and the worrying use of off-the-shelf surveillance technology in the region.

The helpline has been set up by a Brazilian NGO that works at the intersection of politics, gender and technology, with a core focus on the digital security of human rights defenders. It is one of several feminist helplines in Latin America and is seen as “a channel to receive reports and to give support to emergency demands on digital security.” It prioritises assistance to women, LGBTQIA+ people and civil society organisations. The most common cases reported to the helpline relate to social media, notably the hacking of social media accounts, as well as the hacking of email. This is often associated with sexual harassment, control and surveillance by partners and ex-partners, including the exposure of intimate photos or videos. Besides offering support, the helpline serves as a way to document and collect evidence of online abuse. In this regard, the project is collaborating with similar initiatives in the region to produce the evidence necessary to advocate for change.

The presenter said that the use of surveillance technologies against human rights defenders in Latin America is also a concern. While recent cases highlighted the use of spyware, surveillance was not limited to spyware but has been carried out using different technologies such as surveillance cameras, indiscriminate use of biometrics, and the use of artificial intelligence, which remains largely unregulated. Hacking and stalking were also considered forms of surveillance, and the role of social media platforms in these instances needs to be addressed.

The marketing and use of stalkerware was highlighted as a growing problem. This is software that has surveillance capabilities but is routinely sold to the general public and then used in cases of TFGBV. This is often marketed as software that can be used for

purposes such as parent-child monitoring and controlling employees, “both of which are problematic in themselves.” However, it can be adapted by abusers and harassers given its surveillance capacities. A study published by The Citizen Lab in 2019 revealed that many companies were actively promoting their software with the aim of facilitating stalking.<sup>6</sup>

Referring to the “gendered political violence” of these attacks – and in line with the experiences in both Uganda and Thailand – the presenter said that the gender bias in cyberattacks against human rights defenders shows that the content of these attacks does not only refer to the political position or activist roles of the targets but also focuses on their “identity or privacy”.

The presenter said that TFGBV is a singular type of violence because of some particularities, like the difficulty in identifying aggressors, the ease of carrying out these actions without advanced technology, limited legal remedies, and the digital permanence of violent content. Aggressors can hide behind anonymity, but the victims continue to be revictimised over time because it is virtually impossible to remove the content from the internet completely.

---

6. Parsons, C., et al. (2019). *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry*. The Citizen Lab. <https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry>

### 3. CREATING NEW PARAMETERS FOR TECHNOLOGY DESIGN

Many in the private sector are aware of and responsive to the need for online protections against gender-based violence. For instance, a number of businesses have redesigned their technologies, and incorporated mechanisms such as helplines and flag systems to mitigate the threat of online harms. However, participants pointed out that significant work needs to be done to improve the safety of technologies in their design processes.

In this context, key issues highlighted by presenters included:

**Algorithmic transparency:** It is important to push for algorithmic transparency from social media platforms and tech companies so that they prioritise the ability to filter and suppress harmful content.

**Moderation and language:** There is a need to ensure that multiple language models reflecting different languages and vernaculars are built into content moderation tools so that harmful content in these different languages can be flagged. This is important for the accountability of tech companies in their role in the perpetuation of harmful content online.

**Ease of use of security features:** Privacy and security features need to be easily understandable and straightforward to use so that they are accessible to the ordinary user of digital technologies.

**Digital literacy:** Related to this, it is important for the private sector to invest in digital literacy programmes to help make the use of their technologies safer.

**Strengthening reporting mechanisms:** Platforms also need to strengthen their reporting mechanisms. In Latin America, for instance, there is a general sense that when communities use these mechanisms to report abuse, they are not effective: "You can report as many times as possible and they usually don't care," one presenter said, adding:

These platforms should provide better reporting mechanisms that actually follow through and give users the control back; they should build this into their design. And this is not something that is a breakthrough protocol or like a new encryption algorithm, but rather just thinking from the design perspective of what different user needs are.



“One of the first things that people tell me immediately when we talk about TFGBV is that what we need in order to provide a safe internet is that we need to break end-to-end encryption in order to be able to see who is actually using the specific networks and a specific chat. I advocate for the contrary, because what I have found most of the time when working with communities, is that there’s no need actually to break the network or encryption and security properties of the network, but rather to actually significantly improve the different reporting mechanisms that sometimes already exist on these platforms.” – Presenter, discussing the need for better reporting tools on online platforms

### 3.1. Threat modelling

Underpinning any of these design considerations is the need for more representative threat modelling in the design processes. As one presenter explained:

One of the things that we have found out is that all of the algorithms and protocols that work over the internet in the past were actually designed with a threat model that aims to capture the notion of an attacker that tried to fit all of the models. There was an assumption that everybody is facing the same attacker. But in real life, when we’re actually working with communities, this model of the attacker doesn’t fit all experiences. So when we are trying now to design new technologies, it is way more useful to try to understand what those local attacks on different communities are, and then actually design digital products and services based on the input of the community.

A key concern here is the invisibility of marginalised communities in this modelling, simply because their experiences are not seen or recorded as evidence in technology design or in developing standardisation protocols.

“They are accustomed to only think of one specific size of the world in which everything looks the same, and where people face the same online threats. I would like to see a switch in the paradigm of how we design for the internet [or digital technologies] that doesn’t think that the internet should be the same for all, but rather that the threat models and actors are differentiated by communities.” – Presenter, discussing the need to include the experiences of marginalised communities in threat modelling



An example given of how current threat models generally exclude gendered experiences is in the use of security questions for the purpose of online verification. They are predominantly designed with the idea that it is usually a stranger that tries to gain unauthorised access to a person's account. But, as a presenter put it, "if it's an abusive partner or an ex-partner, then there is no use of these security questions – it defeats the purpose of the design."

Another example given was that of Apple releasing its AirTag location tracking device, which can also be used for abusive surveillance, or to monitor community activists. "It turns out that none of the people who were sitting around the table when they were designing these location features [...] questioned this technology because they have never faced this kind of abuse, hence the limits of their world were too narrow," a presenter said. The participatory design of technology is necessary, where "you have different experiences and communities in the room."

One presenter said that academic colleagues had been involved in some of the initial discussions on AirTags, but that many of their recommendations were not taken into consideration. "This highlights the points about making sure that different perspectives are not just heard, but taken seriously into account," they said.

The filter feature on the social network Mastodon was given as a positive example of an inclusive, bottom-up approach. It was described as a filter that allows the users of the social network to customise the experience that they have, and the posts that they see on their timeline. This means they can avoid topics that they think would be traumatic or upsetting to them. The feature allows easy activation and deactivation, and allows the Mastodon community to give feedback on its functionality. "Of course, there are challenges in terms of scaling this to a larger context, but it's not outside the capabilities of Google and Apple," the presenter said. "They can initiate and receive this feedback at a larger scale and listen to a diverse set of at-risk communities to make sure that their designs are inclusive; it requires being proactive rather than coming at it as an afterthought."

One presenter added:

So my trade-off will always be that maybe you need to sit more time in the room to actually think of all of the design decisions that you need to take; it will take a little bit longer to actually put this protocol or a specific system into practice, but it will turn out that you are actually thinking of the different users that your protocol aims to serve.

## 4. WORKING WITH STANDARDS BODIES

Standards bodies such as the International Telecommunication Union (ITU) and the International Organization for Standardization (ISO) have taken cognisance of gender in their work, for instance, through the ITU's Women in Standardization Expert Group and the ISO's Gender Action Plan. However, the extent to which these have meaningfully impacted on the specific discussions related to cybersecurity needs to be questioned. Moreover, as a presenter explained, advocating for gender issues in cybersecurity discussions is much more complex than working on other standards:

Cybersecurity is considered a relatively hard case. So you have often not very powerful, not very well-supported movements towards gendering standardisation, but they try and pick the lower hanging fruit, or the easiest case to play. This obviously needs to be gendered, too; but they look at cybersecurity and they think, ah, not only is it really hard to make a case for gender, it's also really hard to make a case for gender and technology and cybersecurity.

There is also resistance in standards bodies to change. While regions around the world are passing legislation that attempts to account for the specificities of the threats encountered in those regions, standards bodies are falling behind, and civil society organisations face "a lot of opposition [...] any time we talk about human rights or new threat modelling in any standard body settings."

One of the challenges with current cybersecurity discourse and practice is that, firstly, standards are focused too tightly on systems and IT devices, and, secondly, cybersecurity is mostly considered a corporate and national security topic. To remedy this, one presenter argued, a human-centric rather than systems approach is necessary. Cybersecurity needs to be considered "as a societal security issue focusing on societal threats." In this way, "a much broader idea of cybersecurity [is created] where gender issues are really at the heart of it rather than something that is tackled from the outside."

But taking this approach implies a greater participation of marginalised communities in standards-setting discussions. As one presenter explained, as with the design of technology by companies, the kinds of unique threats different communities in the global South face are often unrecognised and therefore not catered for in these discussions and processes. However, the "threats, models and actors are different in different communities [and] even the idea of a perpetrator is different." The result is an internet that has been created to work "just for a limited subset of the population."

"Right now, if you go to any of the standards bodies of the Internet Engineering Taskforce (IETF) or the World Wide Web Consortium (W3C), you will see a very homogeneous body of participants, so the technology does not reflect all of the variety and diversity that the world has," one participant said.



## 4.1. Challenges with inclusive participation

Civil society organisations have found that inviting representatives from different communities to standardisation bodies, and giving them the power to speak about the threats that they face, has helped to push for new threat models to be considered and more understanding of what kind of threats marginalised communities face. However, encouraging a greater level of community participation in standards-setting processes entails making these processes understandable by non-technical participants, who have to navigate complex and sometimes alienating institutional dynamics, and have to grapple with opaque technical jargon.

A key challenge is the lack of interpretation and translation in standards bodies, even when it comes to the documents for foundational protocols such as the Internet Protocol. The Internet Engineering Task Force (IETF) is said to have considered translating its Requests for Comments (RFCs) and drafts of its existing documents, but this has not yet materialised. As one participant put it: “We want more people at the table but we also want them to understand what’s being discussed, and that’s not really possible at present.”

“This is a battle,” one participant said. “When we invite [participants from communities to the standards-setting forums] we provide live interpretation – but this is an individual effort, and there is no support from the standardisation body.”

Power imbalances are also implicit depending on where the standards-setting discussions take place, as they are often geographically inaccessible and expensive for marginalised communities to participate in. For example, the majority of IETF meetings take place in North America, Europe or some countries in East Asia. This perpetuates existing power structures, because many people who would want to participate are limited by resources and other barriers such as visa and travel restrictions. Bodies such as the World Wide Web Consortium (W3C) are even more difficult to access, because you have to pay to attend, which means sourcing sponsorship for your attendance.

Moreover, long-term, sustained engagement in standards-setting discussions is also important, which implies a time and resource commitment:

The other issue is just the slowness of these bodies. By the time they introduce a standard, most of the practitioners in the industry think it’s already outdated, and then they immediately start to renew it. So if you’re dealing with a standard like ISO27k<sup>7</sup> and you’re trying to introduce some kind of gendered acknowledgement or relevance, you have to do it seven years before it’s even happened.

---

7. <https://www.iso.org/standard/iso-iec-27000-family>

While token representation needs to be guarded against, having the “right people at the table” is also not enough:

There have to be structures and processes that are affirmative, that make voices heard and ensure that they are taken into consideration. I’ll say from personal experience that you can be in the room and be very much ignored. We have to find ways to make sure those voices are not just present, but actively participating.

As one participant put it: “Standards development organisations are interested in looking like they are inclusive and that they are universal because that makes it easier to adopt and to accept, but that does not necessarily mean that it is willing to be more inclusive.”

“We want to change a lot of things, but every change that we do is really small because it turns out that all of these standardisation bodies were built with some systematic power structures that we have to break little by little. And it shouldn’t have been this way; it should have been that diversity and inclusivity should have been built into the beginning.” – Presenter, discussing the difficulties in engaging standards bodies



These power dynamics are important to address, because although some standards-setting bodies promote a “consensus-based” process, it is clear that “at the end of the day, if a big tech company wants to push one way, and a small human rights organisation wants to push another way, we will likely end up going the way big tech wants to go.” What is needed is structures and systems to address these inevitable imbalances in power as they occur.

Change is possible, for instance, by engaging in early stages of the standards development. This allows civil society “to have influence over the structure of standards development.”

“One of the first ways that we did that was by establishing binding guiding principles around misuse and abuse; and because we did that at the very start we were able to push very strongly for human rights-focused harm assessment,” the participant said. However, standards-setting bodies are also limited. Standards are “base-level infrastructure”, cannot address all the prevalent harms, and can only respond to an extent to human rights concerns.

## **5. THE ROLE OF THE STATE: A NEED FOR POLICY RESPONSES AND REGULATION**

Appropriate regulations and other mechanisms such as intersectional legal frameworks – including, for example, writing TFGBV into the Sexual Offences Bill in Uganda – were also necessary to comprehensively address gender-based harms online. As one participant put it: “A large part of digital surveillance against HRDs and TFGBV takes advantage of big tech’s business plan and the gap in regulation of surveillance tools. If data monitoring is the rule, how is it possible to protect this information and these people?”

In Latin America and in Asia, a shared concern is the role of spyware in gender-related harms online, including the use of AI in surveillance. Some organisations make a distinction between spyware and “highly invasive” spyware (such as Pegasus and Predator) that was designed to “scoop up all of the data by default.” Highly invasive spyware can never be human rights-compliant, because the digital tools used cannot be independently audited. There is therefore a need to consider technical amendments to regulations and standards to bring the use of the tools in line with law. With any form of spyware, there is nevertheless a role and duty of the state to examine the different impacts on women and sexually diverse people. Currently this is not happening, one presenter said.

So-called “stalkerware” was also identified as a critical issue that needs more regulatory attention. As mentioned earlier, this software is often marketed for purposes such as parent-child monitoring and controlling employees, both of which are problematic in themselves, but can be adapted to facilitate online gender-based violence given its surveillance capacities. One presenter suggested that some stalkerware products were even marketed discreetly as being useful for intimate partner surveillance. These products take advantage of the gaps in big business regulation.

While highly invasive spyware should be banned, technical amendments, or technological guardrails, that limit its functionality could also be explored to make its use lawful. This is currently being explored in different processes. However, it was suggested that when it comes to regulation, states are often complicit in its use, including in targeting human rights defenders, making human rights-based regulatory changes difficult to achieve.

## **6. THE ROLE OF CIVIL SOCIETY**

It is important for activists to think about their advocacy on gender and cybersecurity holistically. Despite the obstacles, it remains critical to engage technology design processes and standards-setting bodies, and to push for better policies, laws and regulations, while also working outside of these structures. Key areas of intervention include producing evidence-based research, developing practical tools to support activists and victims of abuse, and running digital literacy and skills programmes. Collaborating with experts from different fields was also highlighted as important, given the complexity of the cybersecurity landscape.

### **6.1. Building long-term collaborative relationships**

A cross-field approach to advocacy and learning means working with individuals and organisations active at the intersection of gender and cybersecurity policy and governance, as well as experts in technical standards and technology design. This includes engaging organisations that “work on trade and other corporate accountability issues, because most of what we see is motivated by the dominance of the largest tech companies.” Many in the private sector can also be considered allies in this process given that technology service providers are seen to be best positioned to address gender-based harms.

The voices of participants from the global South need to be amplified. Practical areas of collaboration in this respect include translation and outreach, and even collaborating on administrative needs such as dealing with visa requirements and other travel restrictions so that underrepresented communities can participate in standards-setting processes – which, as mentioned earlier, typically take place in North America, Europe or some East Asian countries.

Collaboration should be seen as a long-term commitment in terms of engagement and capacity building: “It is crucial to sustain influence across the standards or design life cycle,” one participant said. What was referred to as “post-standardisation corporate advocacy” is also necessary to make sure that companies actually implement the standards that we help to create.

### **6.2. The need for intersectional research**

There is a growing need to raise awareness about the nuanced intersections of gender and cybersecurity, especially in the global South. Research is important because it provides the evidence necessary to influence standards-setting processes and helps to ensure that the experiences of women and sexually diverse people online are not overlooked in the design of technology. Evidence is also necessary to build appropriate regulations, policies and laws, and to advocate for better responses from the private sector to online harms.

It is important to encourage community-led research so that it is not only the perspectives and voices of experts that influence tech policy and design. This needs to take an intersectional approach that helps to understand how various identities, whether gender, race or socioeconomic status, among others, intersect and impact cybersecurity experiences. As one participant put it, it is important to “frame cybersecurity as a human-centred issue, rather than merely a matter of disputes between companies or countries.”

### 6.3. Priority topics for research

The roundtable also identified priority research topics going forward.

One approach proposed to prioritising research was to firstly focus on the “greatest harm”, by identifying what can be considered the greatest and most widespread threat to women and sexually diverse people online at the moment, and secondly, by considering “ease of policy intervention”, or where the most effective change is likely to be possible. Research methods and outputs proposed include evidence-based participatory research, developing how-to guides, and storytelling, which is necessary to reach “unlikely” stakeholders, “not just highly visible internet users but people from other organisations, movements, and even those with limited tech use and presence.”

Proposals for research included the intersection between gender and spyware; guides that demystify the processes at standardisation and other technical bodies and processes; research visioning feminist digital futures for women in politics; and elaborating on the difference between “gendered targeting” and “gendered impacts”.

Research that explores the connection between cybersecurity and broader gendered structures that produce discrimination and support patriarchy is also necessary.

“At this moment, we are conducting national research on security and developing a study on digital forensics with an intersectional and feminist perspective in order to improve the response of feminist helplines in Latin America. Much of the assistance on TFGBV is done by feminist organisations and collectives that are part of the digital care community. Our goal with this research is to improve case documentation, to learn about advanced digital threats, and to develop protocols for vulnerabilities, education, and rapid response. In the case of Latin America’s feminist helplines in recent years, we share a digital security and feminist perspective that puts the needs of survivors first.”  
– Presenter, commenting on their organisation’s collective research agenda in Latin America

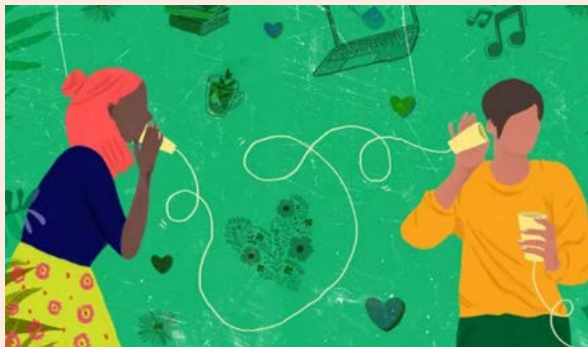


## 7. APPENDICES

### 7.1. Feedback from participants

During a hands-on exercise, the roundtable participants were asked to provide feedback on a number of questions. Their responses are presented here verbatim, as well as anonymously.

#### What type of collaborative relations should we build among individuals and organisations working at the intersection of gender and cybersecurity policy and governance, or technical standards/design?



Create a coalition or cross-body group that works together -- Public Interest Technology Group (for example)

Service providers might be best placed to proactively measure and act on the abuse of their services. So collaborating with the government or support services to inform them about harms from emerging technologies would also be quite helpful in preventing such harms. Basically, some form or resource or knowledge exchange between the stakeholders involved can be quite useful.

Online campaigns can be a collaborative efforts for organisations working at the intersection of cybersecurity policy, governance and technical standards.

I agree, support for longer term projects is crucial to sustain influence across the standards/design lifecycle.

Translation, localization and outreach of research and work in the different fields

Getting more local groups to engage in their national SDOs as a way to get more views and leadership in the global south.

Joined projects to investigate specific questions that the organizations are also reflecting about.

Ensure proper visa support for many underrepresented communities so that they can attend.

Ensure travel funding and support for anyone or organisations to engage in the longer term.

## How can research better inform tech policy and design agendas to mainstream gender and intersectionality in cybersecurity?

Research into proposals for regulatory solutions to curtail GBV facilitated by spyware is one area that could support policy development. For example is a risk-based approach (taking inspiration from the EU's AI act) best suited here? Or a more capability-based approach (such as the distinction between spyware and highly invasive spyware as Becka mentioned)?

Research should aim to influence tech policy and design in govts and private sector at the same time. As each stakeholder cares more about each other than about researchers (!), showing each of them that the other cares would be more effective.

Research removes the shadow of doubt on what the issues and problems are in the tech policy and design agenda; research also provides evidence-based solutions in building secure platforms, especially in making sure that the experiences of women online are not overlooked in the design agendas.

Expose the anti-competitive trends within standards bodies that align with our issues-- they aren't as concerned with inclusion as they are with avoiding anti-trust complaints.

Research training in order to facilitate community-led research — cybersecurity doesn't have to be the domain of schooled 'experts' especially when schooling and education is a spectrum for internet users

Research on intersectionality or intersectional frameworks to examine how various identities (e.g., gender, race, socioeconomic status) intersect and impact cybersecurity experiences can be quite useful. Similarly coming up with educative resources or guidelines can also inform engineers on how to design safer products or services.



Research can be used to push back against narratives that the work of SDOs is just 'technical' and therefore not relevant to gender or other considerations. This publicity can have an impact (thanks sofia for putting this so eloquently!)

Research can provide evidence to frame cybersecurity as a human-centered issue, rather than merely a matter of disputes between companies or countries.

the difference between gendered targeting and gendered impacts

demystifying standardization and other 'technical' bodies and processes --> maybe how to guides for participation?

Post-standardization corporate advocacy is necessary to make sure that companies actually implement the standards that we help to create.

Work with orgs that work on Trade and other corporate accountability issues because most of what we see is motivated by the largest tech companies dominance.

Echoing my response to Q2, further research on the intersection between gender and spyware would be particularly interesting

storytelling methodologies from 'unlikely' stakeholders — not just highly visible internet users but people from other orgs, movements, and even those with limited tech use and presence (e.g. people who mostly engage with tech through mobile money)

Change the thread model and security framework so that we don't continue to use a "model that fits all".

cybercrime / cybersecurity debunking !

## Can we identify priority topics, methodologies, or contexts for future research?



Prioritization could be based on 1) greatest harm - i.e. what is causing the most harm at the moment, or 2) ease of policy intervention - i.e. where effective change is likely. One priority topic is the connection between broader gender structures (discrimination, patriarchy) and gendered cybersecurity - e.g. South Korea, deepfakes, and NCIID.

There's a growing need to raise awareness about the intersections of gender and cybersecurity, especially in global majority contexts. Research can play a crucial role in shaping decisions and informing standards bodies.

Visioning Feminist Digital Futures for Women in Politics

Navigating emerging technologies for women in politics especially in the last mile countries



## 7.2. Resources

Several resources were shared by the participants, including:

- [A framework for developing gender-responsive cybersecurity policy](#) – APC
- [A feminist conversation on cybersecurity](#) – GenderIT (APC)
- [Amplified Abuse: Report on Online Violence Against Women in the 2021 Uganda General Election](#) – Pollicy
- [Inclusive Cyber Norms Toolkit](#) – Global Partners Digital
- [Feminist Helplines Index](#) – Community of Feminist Helplines
- [Maria d'Ajuda](#) – The first digital security helpline created by feminists from Brazil
- [Submission to call for input: The relationship between human rights and technical standard-setting processes for new and emerging digital technologies \(2023\)](#) – WITNESS
- [Request "Off the Record"](#) – Brave Privacy Team
- ["Being ourselves is too dangerous": Digital violence and the silencing of women and LGBTI activists in Thailand](#) – Amnesty International
- [Gender Approaches to Cybersecurity](#) – Katharine Millar, James Shires and Tatiana Tropina (UNIDIR)
- [Navigating Human Rights in the Digital Environment: The World Telecommunication Standardisation Assembly](#) – Global Partners Digital
- [A Guide to the Internet Engineering Task Force \(IETF\) for Public Interest Advocates](#) – Center for Democracy & Technology and ARTICLE 19
- [Internet Standards Almanac](#) – ARTICLE 19
- [Internet Exchange newsletter](#) – Mallory Knodel
- [Internet Draft: Intimate Partner Violence Digital Considerations](#) – IETF
- [Digital Security Resource Hub for Civil Society](#) – Amnesty International
- [The role of the private sector in combatting gendered cyber harms](#) – Chatham House





**GENDER APPROACHES TO CYBERSECURITY:  
INTEGRATING POLICY, RESEARCH AND  
TECHNICAL STANDARDS DISCUSSIONS**