



Inter-Parliamentary Union
For democracy. For everyone.



146TH IPU ASSEMBLY
المنامة، البحرين
MANAMA, BAHRAIN
11-15 MARCH 2023 – ١٥-١١ مارس ٢٠٢٣

146th IPU Assembly Manama (11–15 March 2023)

Forum of Women Parliamentarians
Item 4

FEM/35/4.Inf-1
6 February 2023

Contribution to the work of the 146th Assembly from a gender perspective

Saturday, 11 March 2023, 11:30 – 13:00

I. Arrangements for the debate

Participants will be invited to discuss the draft resolution that is on the agenda of the 146th Assembly, entitled *Cyberattacks and cybercrimes: The new risks to global security* (Standing Committee on Peace and International Security). Participants will discuss the draft resolution from a gender perspective and issue recommendations on gender-related amendments to be submitted by the Forum of Women Parliamentarians to the Standing Committee.

After a short presentation on the draft resolution, the Forum will debate it in plenary. On the recommendation of its Bureau, the Forum will designate a rapporteur, who will present recommendations from the debate to the Forum later in the afternoon.

II. Focus of the debate

The debate will focus on the main gender aspects of the topic of the draft resolution.

As the internet and technologies have advanced and become woven into the fabric of our daily lives, research shows that women and girls are disproportionately impacted by cyberattacks and cybercrimes.

This is the case, for instance, with cyberviolence against women and girls, which occurs as part of a continuum that is often connected to offline violence against women and girls. One study found that 38% of women have personal experience of cyberviolence, and that 85% of women who are online have witnessed such violence against other women.¹ This violence can take many forms, including cyberstalking, the non-consensual distribution of intimate images, sextortion, threats of violence, online sexual harassment and misogynistic hate speech.

Women in politics, journalism and activism and those defending human rights, as well as young women and girls, and women with intersecting identities, are at heightened risk. Women and girls are also disproportionately victims of technology-facilitated trafficking and online child sexual exploitation and abuse.

Cyberviolence and technology-facilitated gender-based violence share the same root causes and drivers as their offline forms, such as structural gender inequality, deep-seated cultural and social norms, and patterns of harmful masculinities.² Moreover, laws fail to take into account the specific features of digital spaces that create a conducive environment for gender-based violence. Evidence also shows that victims/survivors often face challenges when seeking access to justice, and when navigating the investigation and prosecution of cybercrimes against them.

¹ <https://onlineviolencewomen.eiu.com/>.

² <https://www.unwomen.org/en/digital-library/publications/2022/10/accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls>.

With the gender digital divide, women have unequal access to the Internet and to information and communications technology. This results in them being less digitally literate than men and can also place them at greater risk of other types of cybercrimes such as identity theft and bank account fraud. Digital access and training are therefore prerequisites for reducing the disadvantage women often face because of this divide. Another factor is the lack of a gender perspective in cyber defence and protection strategies. Artificial intelligence is playing an increasingly important role in cybercrime detection and prevention, which raises an important question: are algorithms being developed with a gender perspective?

On a final but no less important note, only 25% of cybersecurity experts globally are women.³ This statistic underscores the need to involve more women in devising and implementing prevention strategies and cyber defence systems that reflect and respond to their needs.

Parliamentarians can prevent and address cyberattacks and cybercrimes against women and girls with robust and well-enforced legislation. For this, they need to develop their knowledge and understanding of the nature of cybercrimes, including the different ways in which they target and affect women/girls and men/boys.⁴ Parliamentarians can also ensure that a comprehensive approach to cybercrime prevention is in place in their country, and that prevention efforts consider the fact that women and girls are particularly likely to be targeted by, and fall victim to, certain types of cybercrimes.⁵

The guiding questions for the debate will include the following:

- In what ways do cyberattacks and cybercrimes target and affect women/girls and men/boys differently?
- How can laws and policies better address cyberattacks and cybercrimes against women and girls?
- What are the good practices in preventing cybercrimes against women and girls?
- How can parliaments and parliamentarians promote the role of women in the fight against cyberattacks and cybercrimes, including female researchers working on cyber defence systems?

³ <https://impactotic.co/en/Why-are-women-more-victims-of-cybercrime-than-men%3F/>.

⁴ <https://www.coe.int/en/web/international-conference-women-cybercrime>.

⁵ Ibid.