“As UN Women reports, 73% of women have been victims of some form of online violence, prompting 9 in 10 to reduce their online engagement

Gender dimensions and youth engagement in cybersecurity

by **Avnita Singh**

Cybersecurity has become the arena where our rights, economies, and identities are increasingly defended or lost. Yet, women and youth, two of the most important actors in shaping this domain, remain underrepresented in decision-making and overrepresented among victims of online threats. According to the International Information System Security Certification Consortium (ISC)[1] women constitute only 24% of the global cybersecurity workforce, while the most digitally active generation — those under 30 — is often sidelined from influential policy roles. This article investigates the gendered dynamics of cyber victimisation, the institutional barriers to career access, and the dual reality of youth engagement — vibrant with creativity yet persistently at risk. Drawing on case studies from Africa, Asia, Europe, and Latin America, the analysis highlights how technology-facilitated gender-based violence (TFGBV) and online radicalisation exploit existing inequalities. It addresses policy shortcomings and outlines pragmatic steps, ranging from gender conscious national cyber policies to inclusive, youth-driven global cooperation platforms. Put simply, excluding half of the population and the most dynamic young minds weakens cybersecurity preparedness.

Introduction

In 2024 alone, the world recorded over 493 million ransomware attacks, a 42% increase from the previous year.[2] Beneath these statistics lie real human impacts, which are far more evenly distributed. Women and girls face higher risks of online harassment, while youth often lack institutional support to engage meaningfully in cyber governance.

> **“A security system that excludes its own innovators is neither complete nor resilient.”**

[1] International Information System Security Certification Consortium (ISC), Cybersecurity Workforce Study, 2023

[2] SonicWall Cyber Threat Report, 2024.

Gendered threats and impact

The evidence is clear:

- **Online abuse:** As UN Women reports, 73% of women[3] have been victims of some form of online violence, prompting 9 in 10 to reduce their online engagement.
- **Deepfake exploitation:** More than 96% of all deepfake content[4] online consist of non-consensual content targeting women.
- **Economic exclusion:** The global gender pay gap in cybersecurity is 16%[5], increasing to more than 25% in lower-income regions.

Ethnicity, socioeconomic status, and disability intersect to amplify these threats, worsening their impacts and further reducing reporting.

Workforce representation and barriers

While the global cybersecurity workforce reached 5.5 million in 2023,[6] women's representation remains limited to approximately one-quarter. Even in the regions with strong Science, Technology, Engineering and Mathematics (STEM) pipelines, women are often confined to lower-paying, less influential roles. Barriers include:

- **Stereotypes:** Perceptions of cybersecurity as a male-centric profession discourage early educational engagement, narrowing future talent pipelines.
- **Networking gaps:** In cybersecurity, women are 28% less likely to have access to professional mentorship.
- **Retention challenges:**

> **"An ISC[7] survey found that 45% of women in the cybersecurity field are considering leaving their jobs within five years due to hostile work environments."**

The gender and generational dimensions of cybersecurity

The gender and generational dimensions of cybersecurity should not be understood in isolation, as they intersect in ways that compound both vulnerability and exclusion. This intersection is particularly evident in the experiences of young women and girls, who are among the most active users of digital technologies while also being disproportionately exposed to online harms such as technology-facilitated gender-based violence (TFGBV), cyber harassment, and non-consensual digital exploitation.

These vulnerabilities are shaped by broader structural inequalities, including disparities in access to education, digital literacy, and economic opportunities. Young women often face barriers to entering cybersecurity education and professional pathways due to persistent gender stereotypes, limited mentorship opportunities, and restricted access to professional networks. As a result, their

3 UN Women, Online and ICT-facilitated Violence Against Women and Girls. 2021.
4 Sensity AI, The State of Deepfakes, 2023
5 Frost & Sullivan, Women in Cybersecurity, 2022
6 International Information System Security Certification Consortium (ISC), Cybersecurity Workforce Study, 2023.
7 *Ibid.*

representation remains limited not only in the workforce but also in decision-making processes within cybersecurity governance.

At the same time, their lived experiences in navigating digital platforms provide them with valuable insights into emerging risks and online behavioural patterns. This positions them as important contributors to cybersecurity innovation and policy development.

Recognizing this overlap is essential. Without an integrated approach that considers both gender and age, cybersecurity policies risk overlooking those who are both most affected by cyber threats and best placed to contribute to their prevention.

Youth: creative innovators in the digital sphere

Youth, defined here as individuals aged 15–29, form over 50% of the online global population. Their contributions are tangible:

- University-led cyber clubs in **Kenya** have developed phishing detection tools adopted by local banks.
- Youth activists have developed WhatsApp-based misinformation scanning systems during elections in **Brazil.**
- In **India,** young trainers have organized coding bootcamps and delivered cyber hygiene education to more than 80,000 rural women.[8]

[8] International Telecommunication Union, Digital Skills Development Initiatives Report, 2023.

These cases demonstrate that when given access to tools, resources, and a platform, youth can address policy gaps and technological demands more swiftly than many institutional actors.

The dark side of digital youth engagement

> **"Yet, the same skills that make youth innovative and creative also make them vulnerable to exploitation."**

- **Cybercrime recruitment:** Europol has observed a surge in "script kiddie" recruitment, with criminal networks enticing teenagers into paid hacking activities.
- **Extremist content dissemination:** A report by the UN Counter-Terrorism Committee shows that since 2020, there has been a 300% rise in youth-targeted extremist propaganda online.
- **Mental health:** Studies indicate that excessive online exposure results in higher rates of anxiety and depression, especially when combined with cyberbullying.

Recommendations

1. **Mainstreaming gender equity:** Ensure the inclusion of gender impact assessments in every national cybersecurity policy.
2. **Youth policy inclusion:** Create national and regional youth councils focused on cybersecurity.
3. **Capacity building:** Fund targeted technical training for women and youth in underserved regions, ensuring direct transition into sustainable employment.
4. **Digital literacy:** Embed comprehensive cyber hygiene and digital rights literacy into secondary school curricula nationwide.
5. **Accountability structures:** Mandate the publication of abuse and incident reports disaggregated by gender and age across all digital platforms.

Policy Context

> **"Existing international measures offer clear entry points for gender-sensitive cyber governance."**

The Budapest Convention on Cybercrime and its Protocols can be extended to include explicit gender-responsive implementation measures. The African Union's Convention on Cybersecurity and Personal Data Protection emphasizes the need for comprehensive capacity-building initiatives. Similarly, the UN General Assembly's Open-Ended Working Group (OEWG) on information and communication technologies (ICTs) has acknowledged the importance of multi-stakeholder engagement, integrating both youth and gender perspectives — in the development of cyber standards.

Conclusion

The international cybersecurity community cannot remain a conversation among the same constrained demographic. Women and youth are not "diversity of viewpoints"— they are critical to shaping security in an interconnected world. Excluding them weakens both the resilience and the legitimacy of our cyber policies.

About the Author

Avnita Singh is a freelance writer focusing on issues related to women, social inequality, and gender bias. Her work examines the challenges emerging within contemporary youth culture in relation to digital spaces and evolving social dynamics. She mainly produces content that explores these intersections, with an emphasis on awareness, critical analysis, and social impact.