FACTSHEET

UNIDIR

Tech-Facilitated Gender-Based Violence:
Implications for International Peace and Security

What is Technology-Facilitated Gender-Based Violence (TFGBV)?

Although there is no legal or universally agreed definition, UN Women defines TFGBV as; *"an act, that is committed, assisted, aggravated or amplified by the use of Information and Communications Technologies (ICTs) or other digital tools, that results in or is likely to result in physical, sexual, psychological, social, political or economic harm or other infringement of rights and freedoms."*

TFGBV can take on many different forms, below are some examples.

Cyber harassment

Persistent unwanted online monitoring, publishing of private or personal information (doxxing), trolling, or contact causing fear (e.g. humiliation or threats).

38%

of women around the world have reported experiencing online violence, based on a study covering 51 countries. More than half of the women knew their perpetrator.

7/10

women experienced online violence, including doxxing, according to a survey conducted with 640 women human rights defenders, activists and journalists, across 119 countries.

Image-Based Sexual Abuse (IBSA)

Generation and non-consensual sharing of intimate images, including manipulation of intimate images through generative AI (e.g. deepfake intimate images) that can be used for harassment, blackmail or extortion.

1/5

respondents reported an experience of IBSA, in a survey conducted with 16,000 participants across 10 countries. Rates were higher among LGBTQ+ and younger respondents.

98%

of deepfakes are pornographic in nature, and 99% targeted women, according to a study analyzing over 95,000 deepfake videos across 85 online platforms and 100 websites.

Tech- facilitated trafficking in persons

Use of digital platforms to recruit, transfer, harbor, or receive people through threats, force, coercion, fraud, or deception for sexual abuse.

A study with Ukrainian refugees in **Germany**, **Poland** and **Switzerland** showed that they face high risks of sexual exploitation, including forms facilitated through websites and social media platforms used to recruit and exploit victims.

UN investigations have documented that ISIL used digital platforms to facilitate trafficking in persons from **Iraq** to **Syria**, with women and girls disproportionately targeted for sexual slavery and exploitation.

Misinformation / disinformation

Gendered false narratives, including language that expresses prejudice, contempt or deeply ingrained stereotypes against women which can be used to incite violence, discrimination or hatred based on gender.

In some armed conflicts, such as **Ethiopia** and **Myanmar**, social media platforms and algorithms have amplified and accelerated the spread of harmful rhetoric and hate speech contributing to incitement to ethnic-based and gender-based violence, including systematic rape and other forms of sexual violence.

FACTSHEET

UNIDIR

Why is TFGBV relevant to international peace and security?

- Threats to individual and collective safety have direct implications for international peace and security, especially in cyberspace, where online violence transcends borders and can generate transnational security risks.
- There is a documented continuum between online and offline harm, as TFGBV frequently escalates into physical violence, including violence facilitated by conventional weapons.
- Gendered misinformation, disinformation, and online hate speech can directly or indirectly intensify conflict-related sexual violence (CRSV) and other forms of gender-based violence.
- While everybody can be at risk of TFGBV, data show that adolescent girls and boys are at very high risk, considering their exposure to technology and social media.
- Growing evidence has linked online misogyny to pathways into violent extremism, with individuals/groups displaying misogynistic abuse and threats online more likely to engage in, or support, violent extremist ideologies.
- TFGBV is a significant threat to the Women, Peace and Security (WPS) agenda because it not only inflicts direct harm to women and girls but also suppresses their participation in civic, political, and peacebuilding processes.
- In a study with women human rights defenders, activists and journalists four in ten women reported experiencing offline attacks connected to digital abuse.
- A survey of 901 journalists in 125 countries found that TFGBV led 30% to self-censor on social media and 20% to withdraw from online interaction.

Areas for action

Combating TFGBV, as with all forms of gender-based violence (GBV), requires a multi-pronged response coupled with resource allocation and political will. Actions should prioritize survivors' needs, agency, and safety, and guarantee access to trauma-informed services, justice, and protection.

UN and Multilateral Organizations

- Include TFGBV in early warning systems for conflict and conflict-related sexual violence.
- Investigate TFGBV through UN mechanisms and ensure accountability, remedies, and support for victims.
- Hold multistakeholder dialogues to prevent TFGBV and reduce risks throughout the technology life cycle.

Industry

- Establish, review, monitor, and evaluate platform-specific TFGBV reporting mechanisms.
- Create systems for content moderation, cyber harassment prevention, and removal of users engaging in TFGBV, including cooperation with law enforcement where appropriate.
- Ensure AI-based tools and algorithms do not amplify biased or harmful gendered content.
- Institutionalise gender-responsive threat modeling and gender-sensitive standards when designing systems based on new technologies.

National Governments and Civil Society

- Support research and disaggregated data collection on TFGBV to better understand the problem.
- Adopt national laws that contextually address different forms of TFGBV with tailored measures.
- Raise awareness and build capacity on digital safety, online risks, and TFGBV.
- Create reporting systems and programmes that support TFGBV victims, considering age, gender, and particular circumstances.
- Address TFGBV in national cybersecurity policies and Women, Peace and Security National Action Plans.
- Mainstream gender considerations in the 11 Norms of Responsible State Behaviour in Cyberspace.
- Address TFGBV in discussions on existing and potential threats in the UN Global Mechanism on ICT Security.
- Share national best practices to address TFGBV in national ICT security policies and legal frameworks.