

GENDER BASED CYBER VIOLENCE AND HARASSMENT

Nino Gergidze

Revised by: Professor Manana Khachidze

Abstract

In our digitally interconnected world, the rapid evolution of technology has brought numerous benefits alongside challenges, particularly for women who are disproportionately affected by online violence. This abstract explores the various forms of gender-based cyber violence, including doxing, hate speech, cyber-stalking, cyber-flashing, and revenge porn. It highlights the severe consequences of such violence, which range from psychological distress to economic and social repercussions, exacerbating existing inequalities and discrimination. The presentation emphasizes the importance of legal frameworks like the Istanbul and Budapest Conventions, advocating for enhanced prosecution measures and international cooperation to combat these crimes effectively. By addressing online violence comprehensively, we aim to create safer digital spaces where all individuals, regardless of gender, can freely participate without fear of harassment or discrimination.

Introduction

In our era of digital advancement, technology profoundly shapes our daily lives, offering tremendous benefits but also exposing us to significant challenges. Amidst this progress, the persistent shadow of patriarchal norms amplifies the severity of issues and violence faced by women. Online violence, often trivialized as mere words on the internet, represents a critical form of gender-based violence that demands greater attention and action. Research from the World Health Organization reveals that one in three women globally will experience violence in their lifetime, with one in ten women encountering cyber violence by age 15. Motivated by these alarming statistics, this presentation seeks to shed light on the pervasive issue of gender-based cyber violence and advocate for meaningful solutions.

Forms of Gender-based Violence

Women face various forms of online harassment, including:

- **Doxing:** Publishing someone’s personal information online with malicious intent.
- **Hate speech:** Verbal or written attacks using discriminatory language based on religion, ethnicity, nationality, race, color, descent, gender, or other identifying factors. Online hate speech often includes sexualization, objectification, body-shaming, degrading comments, and rape threats, frequently originating from incel communities.
- **Cyber-Stalking:** Methodical and persistent electronic or digital stalking that involves repeated incidents, undermining the victim’s sense of safety.
- **Cyber-flashing:** Sending unsolicited sexual images via social media, messaging apps, or other digital means.
- **Revenge porn:** Posting intimate or sexual images or videos online without consent, typically following a breakup.

First Student Conference: “Gender Dimension of CyberSecurity”

The most prevalent forms of reported violence include misinformation and defamation (67%), cyber harassment (66%), hate speech (65%), impersonation (63%), hacking and stalking (63%), astroturfing (58%), video and image-based abuse (57%), doxing (55%), violent threats (52%), and unwanted sexually explicit content (43%).

Consequences

The consequences and harms of various forms of online violence are distinctly gendered, exacerbated by structural inequality, discrimination, and patriarchy. Women and girls subjected to online violence often face further victimization through harmful gender stereotypes, contravening international human rights norms. The internet has evolved into a platform where diverse forms of violence against women and girls manifest, including pornography, sexist games, and breaches of privacy. Women engaging in public discourse online are particularly vulnerable to harassment, exemplified by instances like anonymous campaigns advocating for the gang rape of women human rights defenders, accompanied by racist abuse on platforms like Wikipedia. Female ICT users have publicly decried sexist attacks. Research highlights that women human rights defenders challenging patriarchal norms are especially susceptible to online violence.

Online acts of gender-based violence against women and girls encompass threats that lead to psychological, physical, sexual, or economic harm. These acts inflict significant psychological distress due to their scale and repeated occurrence, resulting in depression, anxiety, fear, and in severe cases, suicidal tendencies among victims and survivors.

What Can We Do?

Cyber-attacks and violence against women often receive inadequate attention. To effect change, states must address cyberviolence with the same urgency as other forms of violence against women, utilizing all available tools. Failure to act jeopardizes online freedom of expression. Conversely, tackling online gender-based violence within the existing international human rights framework can safeguard the internet as an open, safe, and free platform for exchanging ideas.

Policies and Measures

In addition to the Lanzarote Convention on sexual abuse and exploitation against children and the Budapest Convention on cybercrime, the landmark Istanbul Convention is the Council of Europe's comprehensive framework for preventing and combating violence against women and domestic violence. It mandates States Parties to outlaw psychological violence, stalking, and sexual harassment, and calls for preventive measures in education. The convention encourages private companies and media outlets to adopt self-regulatory standards to curb verbal abuse of women.

Prosecution

Under the Istanbul Convention, perpetrators of cyberviolence against women must be prosecuted and sanctioned. To effectively combat this form of violence, it should be criminalized and not go unpunished. Accessible and secure online mechanisms are essential for women to report abuse, seek protection, and have harmful content removed. Law enforcement agencies need enhanced training to investigate and prosecute cyberviolence more effectively.

On October 1, 2023, the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (CETS 210) entered into force for the European Union, marking the EU's accession as the 38th Party to the Convention.

First Student Conference: “Gender Dimension of CyberSecurity”

As the most extensive legally binding human rights treaty addressing all forms of violence against women and domestic violence, the Istanbul Convention is particularly relevant in combating online and technology-facilitated violence against women.

Furthermore, the Istanbul Convention and the Budapest Convention complement each other synergistically: the Istanbul Convention addresses the gender-based nature of violence against women, while the Budapest Convention facilitates procedural powers and international cooperation in cybercrime investigations involving electronic evidence. These connections were explored in studies such as the T-CY Cyberviolence mapping study and "Protecting Women and Girls from Violence in the Digital Age," commissioned by the Council of Europe's Violence Against Women Division.

Impact on Women

Research indicates significant impacts on women's participation in social media:

- 80% limited their social media activity, refraining from expressing opinions on specific topics.
- A quarter restricted their social media usage, maintaining only professional or activist-related accounts.
- 40% engaged in self-censorship, avoiding discussing relevant topics in their professional fields.
- One-third changed jobs due to online harassment.
- A quarter faced dismissal or non-renewal of contracts, with half fearing job loss.
- 80% feared for their physical safety and lives, prompting actions from withdrawal to reducing their social media presence.

Conclusion

Gender-based cyber violence and harassment pose significant challenges in our digitally interconnected world, where technological advancements intersect with persistent inequalities and vulnerabilities for women. This article has explored various forms of online violence—from doxing to revenge porn—and their profound impacts on victims, ranging from psychological distress to economic and social repercussions.

The consequences of gender-based cyber violence are deeply rooted in structural inequality, discrimination, and patriarchal norms, exacerbating the marginalization of women in digital spaces. Victims often face not only immediate psychological harm but also long-term effects on their personal and professional lives, including fear for their safety and restricted participation in online and offline communities.

Effective response strategies require comprehensive legal frameworks and robust policy measures that recognize the gendered nature of online violence. The Istanbul Convention and the Budapest Convention provide crucial frameworks for preventing and combating these crimes, calling for legal protections, enhanced law enforcement capabilities, and international cooperation to ensure accountability and justice.

To address these challenges effectively, stakeholders must prioritize digital literacy, promote online safety initiatives, and support victims in reporting and recovering from cyber violence. Empowering women to navigate digital spaces safely and equitably is essential for fostering inclusive and resilient online communities.

By advocating for systemic changes and collective action, we can create a future where the internet is a secure and empowering platform for all individuals, free from gender-based violence and discrimination.

First Student Conference: “Gender Dimension of CyberSecurity”

Upholding human rights principles and promoting gender equality in digital environments are critical steps toward achieving this vision.

References:

1. Gender-based violence in EU: https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en
2. https://eige.europa.eu/publications-resources/publications/combating-cyber-violence-against-women-and-girls?language_content_entity=en
3. Un-women: <https://www.unwomen.org/en/what-we-do/ending-violence-against-women/faqs/tech-facilitated-gender-based-violence>
4. Council of Europe: <https://www.coe.int/en/web/cybercrime/the-budapest-convention>