

Potential Cyber Threats Related to Gender Disinformation

Karyna Horiainova
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
karyna.horiainova@nure.ua

Amal Mersni
International University of Sarajevo
Sarajevo, Bosnia and Herzegovina
amersni@ius.edu.ba

Oleksandra Yeremenko
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
oleksandra.yeremenko@nure.ua

Roman Kapusta
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
roman.kapusta@nure.ua

Abstract

Digital technology has both positive and negative effects. It amplifies opportunities for expression, participation, and information sharing but also multiplies online risks and threats. Gendered disinformation is not a new phenomenon, but it has gained momentum due to new technologies and social media. This study examines the issue of gendered disinformation in digital media, specifically the intentional spread of false information aimed at women to undermine their societal roles. The study recommends improving digital literacy, developing detection technologies, promoting cross-sector collaborations, and supporting victims. It emphasizes the need for a collective approach that respects all gender identities to address this urgent social and technological issue and promote a more equitable digital environment.

CCS Concepts: • **Social and professional topics** → *User characteristics*; Gender; • **Security and privacy**;

Keywords: Gender disinformation, Online security, Cybersecurity Awareness

1 Introduction

Today, many different media outlets deliberately contribute to the aggravation and incitement of people to internal conflicts against the background of gender inequality. The main tool for heightening such conflicts is the use of disinformation, which serves not only as a provocative means of focusing attention on the peculiarities of gender differences in the population but also as a developed environment for a potential cybercriminal who can use the created conflict for his or her own malicious purposes. The widespread use of social media has prompted society to focus not only on the problem of information integrity and accessibility but also on the moral damage to women and girls who inadvertently fall for disinformation campaigns. Against the backdrop of

ongoing gender conflict, cybercriminals use a variety of attack methods for their own benefit or to defend the interests of the political sector. Usually, they use social engineering methods and phishing attack vectors.

2 Understanding the Gender Dimensions of Disinformation

Defining gendered disinformation is challenging due to the presence of multiple, nuanced definitions. At its core, gendered disinformation involves the spread of false or misleading information specifically targeting women in prominent public roles, such as political leaders, journalists, and activists. This form of disinformation leverages societal stereotypes and misogyny to damage the public image of women's achievements and discourage them from seeking leadership positions [1, 3].

The connection between gendered disinformation and gender-based violence arises from the same context where people encounter online gender-based violence, highlighting an overlap between the two phenomena (Fig. 1). The use of gendered disinformation in cyber-attacks is a complex issue (see Fig. 2). Sophisticated tactics such as manipulated media, sexualized disinformation, threats, and the misuse of personal information through digital platforms are employed to undermine the credibility of women and instill fear, which can affect their professional and personal lives [3, 5].

Research suggests that there is a gender disparity in the commission of cybercrimes, with men more frequently engaging in activities such as hacking and gender-based offenses, including the deployment of spyware against partners and the distribution of non-consensual sexual content online. However, it is important to note that this observation pertains specifically to cybercrimes linked to gendered disinformation and not all cybercrimes universally [3].

The development of artificial intelligence (AI) is transforming cyber-attacks, especially in the dissemination of gendered disinformation. AI's capacity to automate the creation and spreading of false information increases the complexity of cyber-attacks, enabling more accurate targeting

that exploits gender-related weaknesses. Deepfake videos, AI-generated text, and content recommendation algorithms have led to a faster spread of disinformation and hate speech online. This phenomenon disproportionately affects women, journalists, and politicians. Without updated policies and effective tools, false or harmful content could worsen gender disparities in political engagement, privacy, national security, and civil rights globally [2, 5].

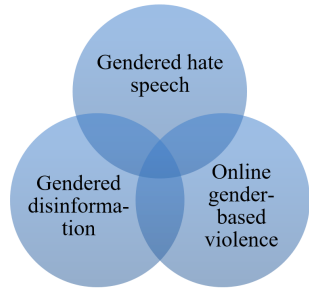


Figure 1. Relationship to gender-based violence and hate speech [4].

3 Countermeasures to Protect Against Gender Disinformation in Cyberspace

To navigate the challenge of protecting oneself from gender disinformation online, it is crucial to adopt several effective strategies [1, 6].

One should question and verify the information encountered on the internet and not accept everything seen or read at face value. This is particularly important for headlines, images, or videos that might be fabricated. Seeking out trustworthy and independent sources, such as fact-checking websites, is advisable to ascertain the accuracy of any questionable claims. Furthermore, it is essential to be well-informed about gender issues and human rights in the realm of technology. Understanding gender equality, diversity, and justice in the digital environment is beneficial. Supporting groups and organizations dedicated to improving conditions for women and other gender minorities in technology is commendable.

It is also vital to express support for victims of gender-based misinformation and cyberbullying. It is important to avoid spreading false information or making derogatory comments about gender online. If you witness targeted harassment (Fig. 2), it is crucial to speak out against it and defend the rights and dignity of those involved. To ensure your online safety, it is recommended that you report any inappropriate content or behavior to the relevant website or authorities.

Securing one's online presence is also of significant importance. Utilizing strong passwords, encryption, and antivirus software to safeguard devices and personal information from unauthorized access is advisable. Caution should be exercised when sharing personal details, such as names, addresses, or

photos, with individuals who have not been deemed trustworthy or on suspicious websites. Additionally, thoughtful consideration should be given to the content one posts or shares online and the individuals one communicates with.

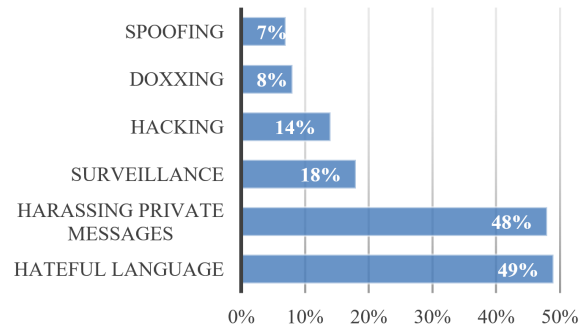


Figure 2. Women journalists' online threat experience [5].

4 Conclusion

Preventing gender-based disinformation in cyberspace requires a critical approach to information perception, literacy, and education on gender issues. Effective measures should also include supporting victims, raising awareness, and promoting solidarity within the online community. In addition, it is important to apply technical security measures to protect personal privacy and avoid danger from cybercriminals. Therefore, combating gender-based disinformation on the Internet requires a comprehensive approach that combines technical, educational, and social measures to ensure the safety and freedom of all users in the digital space.

References

- [1] Countering DISINFO. 2021. *Understanding the Gender Dimensions of Disinformation: 1. Gender Considerations in Counter-Disinformation Programming*. Retrieved February 10, 2024 from <https://counteringdisinformation.org/topics/gender/1-gender-considerations-counter-disinformation-programming>
- [2] Disinformation and Deepfakes: Countering Gender-Based Online Harassment. 2023. <https://www.csis.org/events/disinformation-and-deepfakes-countering-gender-based-online-harassment>. Retrieved February 10, 2024 from <http://www.ctan.org/pkg/acmart>
- [3] EU Disinfo Lab. 2021. *Gender-Based Disinformation: Advancing Our Understanding and Response*. Retrieved February 10, 2024 from <https://www.disinfo.eu/publications/gender-based-disinformation-advancing-our-understanding-and-response/>
- [4] UN Digital Library. [n.d.]. *Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms*. Retrieved February 10, 2024 from <https://documents.un.org/doc/undoc/gen/n23/233/65/pdf/n2323365.pdf?token=X5Bf3XCNtQVva4QbsA&fe=true>
- [5] UNESCO. 2021. *The Chilling: Global trends in online violence against women journalists*. Retrieved February 10, 2024 from <https://unesdoc.unesco.org/ark:/48223/pf0000377223>
- [6] UNESCO. 2023. *How to combat hate speech and gendered disinformation online?* Retrieved February 10, 2024 from <http://www.ctan.org/pkg/acmart>