United Nations
Interregional Crime and Justice
Research Institute

THE DIGITAL FRONTLINE:

Emerging Evidence on Technology-Facilitated Gender-Based Violence in Fragile and Conflict Settings

THE DIGITAL FRONTLINE:

Emerging Evidence on Technology-Facilitated Gender-Based Violence in Fragile and Conflict Settings

DISCLAIMER

This initiative was carried out with the support of the Directorate General for Political and Security Affairs of the Ministry of Foreign Affairs and International Cooperation of Italy. The opinions expressed in this publication are those of the authors and do not necessarily reflect the positions of the Ministry of Foreign Affairs and International Cooperation.

The opinions, findings, conclusions, and recommendations expressed in this publication are solely those of the authors and do not necessarily reflect the views or positions of the United Nations, UNICRI, or any other national, regional, or international entity involved.

The designations used and the presentation of material in this publication do not imply any opinion on the part of the United Nations Secretariat or UNICRI regarding the legal status of any country, territory, city, or area, or its authorities, nor regarding the delimitation of its frontiers or boundaries. Mention of specific institutions, or companies does not constitute an endorsement or recommendation by the United Nations Secretariat or UNICRI over others of a similar nature.

Tel: + 39 011-6537 111 / Fax: + 39 011-6313 368

Website: www.unicri.org

E-mail: unicri.publicinfo@un.org

Table of contents

Abbreviations and acronyms

AI	Artificial Intelligence
APC	Association for Progressive Communications
ASEAN	Association of Southeast Asian Nations
CSOs	Civil Society OrganizationsGBV Gender-Based Violence
ICTs	Information and Communication TechnologiesNAP National Action Plan
OSCE	Organization for Security and Co-operation in Europe
RSF	Rapid Support Forces
SDGs	Sustainable Development Goals
TFGBV	Technology-Facilitated Gender-Based Violence
UN	United NationsUNFPA United Nations Population Fund
UN Women	United Nations Entity for Gender Equality and the Empowerment of Women
VAWG	Violence Against Women and Girls
WHRD	Women Human Rights Defender(s)
WIM	Women in Media
WPS	Women, Peace and Security

Executive summary

Technology-facilitated gender-based violence (TFGBV) occurs in both peaceful and conflict-affected settings. To date, most research has focused on the manifestations of TFGBV across contexts, without systematically analysing how it may differ in environments marked by fragility, tension, and instability. This report focuses on the specific emerging patterns and impacts of TFGBV in fragile and conflict-affected settings, recognizing that both its manifestations and its consequences may differ significantly in these contexts. It explores how women operating across peace and security sectors are targeted, and how TFGBV can be used not only as a form of violence, but also as a strategy to undermine participation, destabilize governance, and contribute to broader conflict dynamics.

To analyse these patterns, the report draws on a global desk review of existing research, which remains largely qualitative and often based on testimonies. This is complemented by case studies from Sudan and Ukraine, supported by key informant interviews with experts and practitioners. Through this combined approach, the report identifies how TFGBV is embedded within broader systems of gender inequality, power relations, and insecurity. The analysis is further framed within the Women, Peace and Security agenda, which provides the normative framework for addressing the specific forms of violence and exclusion affecting women in conflict settings.

Findings confirm that fragile and conflict-affected settings create particularly conducive environments for the escalation of TFGBV. Weak institutional protection, heightened polarization, the proliferation of armed actors, and the erosion of social cohesion create conditions in which digital tools are used strategically to intimidate, monitor, discredit, and silence women. In these contexts, online violence often translates into offline harm, including threats, surveillance, reputational damage, and physical violence. The online environment has become a space where violence manifests through misogynistic narratives, targeted harassment, coordinated attacks, and disinformation campaigns. The report identifies several groups that are particularly exposed:

Women in armed and security roles, targeted through gendered disinformation and harassment aimed at undermining both their credibility and the institutions they represent.

Women journalists, especially those reporting on conflict, governance, and human rights, who face threats, smear campaigns, and coordinated online abuse.

Women politicians and public figures, subjected to gendered attacks designed to delegitimize their leadership and discourage their political participation.

Women human rights defenders and civil society actors, targeted through surveillance, harassment, and disinformation to restrict civic space and silence dissent.

Across these groups, TFGBV takes multiple forms. These include doxxing, where personal information is exposed to facilitate harassment, retaliation, or even arrest; coordinated harassment campaigns aimed at publicly discrediting women; and image-based abuse, including AI-generated manipulation of images or videos, used to damage reputations, trigger social backlash, or incite violence.

A cross-case analysis of Sudan and Ukraine highlights several common patterns in fragile and conflict settings. First, gender norms and stereotypes act as key drivers of TFGBV, with women targeted for transgressing expected social roles. Second, visibility and engagement on politically sensitive topics increase exposure to digital violence. Third, there is a strong continuum between online and offline harm, with digital attacks often translating into real-world risks. Finally, TFGBV is not only reactive but increasingly strategic, used to shape narratives, undermine institutions, and restrict women's participation in public life.

TFGBV has multidimensional consequences, which extend beyond individual harm. These include psychological distress and trauma; self-censorship and withdrawal from digital and public spaces; reduced participation in political, peacebuilding, and security processes; and erosion of trust in institutions and social cohesion. In already fragile contexts, these impacts are cumulative and systemic. They contribute to the shrinking of civic space, undermine inclusive governance, and weaken the implementation of the WPS agenda. By shaping who can safely participate in public life, TFGBV directly affects peace processes, decision-making, and recovery efforts.

In this sense, TFGBV in fragile and conflict-affected settings should be understood not only as a gender issue, but also as a **peace and security concern**. When used to silence women in leadership, security, and peacebuilding roles, digital violence contributes to instability, fuels polarization, and undermines inclusive peace processes.

Ultimately, addressing TFGBV is essential not only to protect women's rights, but also to ensure meaningful participation, strengthen governance, and support peacebuilding efforts in fragile and conflict-affected contexts.

CHAPTER 01

Introduction

The impact of conflict, violence, and insecurity on women and girls has long been examined within the United Nations. The UN Security Council first formally recognized these interlinkages in 2000 with the adoption of its landmark Resolution 1325 on Women, Peace and Security (WPS). It is structured around four core pillars: participation, protection, prevention, and relief and recovery, which guide efforts to ensure women's full, equal, and meaningful involvement in all aspects of peace and security. This resolution, together with the nine subsequent resolutions that followed, constitutes the normative framework to address the distinct ways in which women and girls are affected by conflict and to promote their participation in peace and security, conflict prevention, crisis response, and post-conflict recovery and peacebuilding.

Over time, new threats to peace and security have emerged, alongside new spaces in which violence is perpetrated. The rapid expansion of information and communication technologies and the widespread use of digital platforms have reshaped the forms of interaction, participation, and information-sharing across societies, influencing public and political life both in stable environments and in fragile and conflict-affected settings. This research focuses on the latter, and examines how, in this evolving landscape, technology-facilitated violence, including technology-facilitated gender-based violence, is embedded within broader conflict dynamics, reflecting the evolving nature of security threats in the digital age.

Fragile and conflict-affected settings provide particularly conducive environments for the manifestation and amplification of TFGBV. In such contexts, the proliferation of violence, the deterioration of living conditions, weak institutional protection, and heightened political and social

polarization create conditions in which digital technologies can amplify grievances, hostility, and resentment, as well as be directly used to intimidate, monitor, and target individuals. Women politically exposed and/or engaged in activism, peacebuilding, security and journalism are particularly exposed, as their visibility intersects with both gendered norms and conflict dynamics. TFGBV targets individuals based on gender, as well as profession, affiliation, religion, ethnicity, and other characteristics, through online hate speech, online harassment and cyberattacks intended to intimidate, discredit, foster exclusion, and ultimately silence affected individuals.

The WPS agenda addresses many of these dynamics as they manifest offline, such as gender-based violence in conflict, restrictions on women's participation in decision-making processes related to peace and security, and broader forms of exclusion. However, its core resolutions do not explicitly address the digital manifestations of these challenges. Recognition of these dimensions has instead evolved more gradually, with the United Nations Secretary-General's annual reports on WPS increasingly acknowledging the implications of digital technologies.[1] For instance, the 2024 report underscored that digital threats, including disinformation, online harassment, and algorithmic bias, disproportionately affect women in political, peacebuilding, and human rights roles, and called for stronger integration of gender perspectives into digital governance and protection mechanisms.[2] The 2025 report further noted that the military applications of new and emerging technologies, as well as the expansion of conflict into domains such as cyberspace and outer space, are creating new challenges for the implementation of the WPS agenda. It also highlighted the growing prevalence of technology-facilitated threats and attacks against women human rights defenders, peacebuilders, and women in politics.[3] However, National Action Plans (NAPs), which remain the main operational instruments of the WPS agenda, have addressed digital threats only to a limited extent. Existing research indicates that 19 out of 109 National Action Plans adopted worldwide (around 17 per cent) refer to issues such as digital security, cybersecurity, cybercrime, or the disproportionate impact of online harms on women.[4,5]

Overall, these developments point to growing attention to the role of digital spaces in shaping women's participation in peace and security, including the risks posed by digital violence in conflict-affected contexts. Women engaged in security, public life, peacebuilding, media, and advocacy are exposed to these dynamics and research is increasingly exploring and collecting data to better understand the manifestations and impacts of TFGBV. However, quantitative data remain limited and tend to focus primarily on civilians, activists, journalists, and women human rights defenders. While this study also examines the manifestations of TFGBV against these groups, it places particular emphasis on the effects of digital violence perpetrated against women operating in armed and security roles, an area that remains underexplored in both research and policy discussions. Building on an initial phase of global-level desk research, the analysis is further grounded in two conflict-affected contexts, Ukraine and Sudan, which provide insight into how these dynamics manifest in practice.

1 For a detailed analysis of how cybersecurity issues and technology-facilitated gender-based violence have been integrated into the WPS agenda and broader UN processes, it is recommended to consult existing research such as *System Update: Towards a Women, Peace and Cybersecurity Agenda* by the United Nations Institute for Disarmament Research (2021). This paper examines how cyber-related issues are being incorporated across key policy instruments, including WPS National Action Plans, United Nations Security Council resolutions on WPS, reports of the Security Council Informal Expert Group on WPS, and the Secretary-General's annual reports on WPS.

2 United Nations. (2024). *Report of the Secretary General on Women and Peace and Security* (S/2024/671).

3 United Nations. (2025). *Report* of *the Secretary General on Women and Peace and Security* (S/2025/556).

4 UN Women, *Women, Peace and Digital (In)Security in South-East Asia: Reflections on Diverse Experiences in the Digital Sphere*, Research Brief, 2024.

5 *Some good practices exist.* At the regional level, the Association of Southeast Asian Nations has integrated cybersecurity into its WPS agenda through the 2022 Regional Plan of Action on WPS. At the national level, the Philippines stands out as a leading example, becoming the first country in Southeast Asia to explicitly incorporate cybersecurity into its National Action Plan on WPS (2023–2033). At the subnational level, the Bangsamoro Autonomous Region of Muslim Mindanao (BARMM) has also integrated cybersecurity into its 2023–2028 Regional Action Plan on WPS.

CHAPTER 02

Research objectives and methodology

2.1 Research objective

The objective of this research is to support the implementation of the Women, Peace, and Security agenda by providing an analysis of the forms of digital violence targeting women engaged in peace and security efforts in conflict-affected settings, with a view to better integrating technology-facilitated violence into WPS frameworks and responses. Specifically, the study aims to:

- Identify the forms of online violence targeting women operating in conflict contexts, including women in armed and security roles, women's human rights defenders, and leaders.
- Assess the impact of such violence on women's participation in peace and security processes.
- Examine the broader implications of technology-facilitated gender-based violence for the implementation of the Women, Peace, and Security agenda.

2.2 Methodology

This research adopts a qualitative mixed-methods approach, combining a desk review with two country case studies to strengthen the evidence base and ensure practical relevance.

The desk review draws on academic literature, publications from the United Nations and non-governmental organizations, media articles, expert analyses, and official documents from international organizations and governments. This phase supported the mapping of how technology-facilitated gender-based violence manifests across women operating in conflict contexts, including women in armed and security roles, women's human rights defenders, and leaders in conflict settings. The research further incorporates qualitative insights from two case studies: Ukraine and Sudan. Ukraine provides a relevant context to examine digital violence targeting women in armed and security roles, as well as those engaged in civil society and peacebuilding, where women play an increasingly visible role. Sudan, in turn, offers important insights into the experiences of women human rights defenders, journalists, and activists working on peace and gender equality, who are frequently exposed to targeted online harassment and threats.

In addition, 13 key informant interviews were conducted with representatives of governments, international organizations, including the Organization for Security and Co-operation in Europe (OSCE) and the African Union, and experts in the fields of gender equality, gender-based violence, Women, Peace and Security, and TFGBV, with specific country expertise in Sudan and Ukraine. The chapter with the case studies draws on these interviews and includes direct quotations from participants.

2.3 Data gaps and research limitations

While the research provides an overview of how digital technologies are interlinked with the implementation of the WPS agenda, particular attention is given to how TFGBV manifests, how it affects women's participation in peace and security processes, and which measures can be adopted to prevent and respond to these risks.

Several data gaps and methodological limitations must be acknowledged. Collecting data in conflict-affected contexts such as Ukraine and Sudan presents significant challenges, particularly due to the reliance on primarily online consultations and the sensitivity of the topic. Secondly, although the research analyses the forms of TFGBV across multiple target groups in conflict settings, there is limited publicly available information on the experiences of women serving in armed and security roles. Existing literature often focuses on internal institutional challenges and gender dynamics within security and military institutions, with less attention to digital harassment and online attacks targeting women in these roles. As a result, incidents of technology-facilitated violence affecting these groups may be insufficiently documented.

Overall, the research is based on desk review and qualitative analysis of testimonies and anecdotal evidence, which does not allow for statistically representative findings. These limitations should be considered when interpreting the findings of this study and should provide a basis to underscore the need for further research, as well as for improved data collection on technology-facilitated gender-based violence in peace and security contexts.

CHAPTER 03

Defining Technology-Facilitated Gender-Based Violence

3.1 Definitions

Violence against women in digital environments has emerged as a growing area of concern and has been increasingly recognized and analysed over the past decade. Today, approximately *four in five people globally own a mobile phone (82 per cent of the world's population aged 10 and over),*[6] with smartphones accounting for the majority of these devices and enabling Internet connectivity for approximately 6 billion users worldwide[7]. As a result, digital spaces have become embedded in everyday life, blurring the boundaries between online and offline environments. Information and communication technologies (ICTs) have transformed how individuals communicate, access information, and participate in social, political, and professional life. At the same time, these technologies have created new avenues for violence and abuse, generating digital environments in which violence can be both perpetrated and amplified.

6 International Telecommunication Union, *Facts and Figures 2025*, Global mobile phone ownership estimates.

7 International Telecommunication Union, Global Connectivity Report 2025.

While technology-facilitated violence affects all individuals, some forms of violence, as well as the language, the type of threats and hate speech employed, demonstrate how such abuse is rooted in *gender norms*. GBV encompasses a number of harms perpetrated via digital technologies on the basis of the gender of an individual, often evolving in different and new forms alongside technological development. It is not an isolated phenomenon, but rather part of a broader social context of gender discrimination against women and girls. TFGBV reinforces and exacerbates structural gender inequalities,[8] influencing who is targeted, the forms the abuse takes (e.g. sexual threats, misogynistic commentary, and gender-based hate speech) and the actors perpetrating it. Perpetrators can range from individuals, family members, and members of the public to organized networks, political actors, and, in some contexts, State or non-State armed groups, often operating through coordinated troll groups, bot-driven campaigns and other organized online activities. These dynamics may be shaped by misogynistic attitudes, ideological agendas, and existing power structures.

Digital tools expand the arena in which violence can occur, increasing the *speed, reach and scalability* of abuse, often with the *anonymity* of perpetrators, producing a "snowball effect" as others join the attacks. Victims may experience a heightened sense of vulnerability and exposure, as the persistence and visibility of online attacks can make it difficult to escape or protect oneself. In this context, digital violence can also act as a *"powerful mechanism for silencing women's voices and policing their visibility in public life."*[9]

Gender-based hate speech, online threats of offline violence, doxxing, non-consensual sharing of images, AI-generated image abuse and manipulated content, and coordinated harassment campaigns involving trolls are among the forms of TFGBV employed to silence, intimidate, or discredit women in digital spaces. A variety of technological devices and services facilitate these forms of violence, including smartphones, computers, tablets, cameras, and geolocation systems, as well as social media platforms (e.g. Facebook, X, TikTok, Instagram), instant messaging applications (such as Telegram), editing applications and softwares, AI tools, email services, content-sharing platforms, and online discussion forums.

These phenomena are described using different terminology across policy, legal, and academic contexts, including online violence against women, cyber-violence, ICT-related violence, and technology-facilitated gender-based violence. While definitions may vary, they broadly refer to forms of gender-based violence that are enabled, mediated, or amplified by digital technologies. In 2018, in a report on online violence against women and girls from a human rights perspective, the United Nations Special Rapporteur on Violence Against Women defined such abuse as "any act of gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately."[10]

More recently, in 2022, *UN Women* convened an expert group to develop a shared definition of *technology-facilitated gender-based violence*. The group then defined TFGBV as "Any act that is committed, assisted, aggravated or amplified by the use of information and communication technologies or digital tools that results in or is likely to result in physical, sexual, psychological, social, political or economic harm, or other infringements of rights and freedoms on the basis of gender." [11]

8 UN Women, *Strategy: Preventing and Eliminating Technology-Facilitated Violence Against Women and Girls*, 2025.

9 International IDEA, Violence Against Women in the Digital Space: A Growing Threat to Democracy, 2025.

10 OHCHR, *Report of the Special Rapporteur on Violence Against Women, Its Causes and Consequences on Online Violence Against Women and Girls from a Human Rights Perspective,* 2018, A/HRC/8/47 para 23.

11 UN Women, *Expert Group Meeting Report on Technology-Facilitated Violence Against Women,* 2023.

3.2 Typologies

TFGBV evolves rapidly, as do digital technologies. Identifying and categorizing these forms of technology-facilitated gender-based violence not only supports analytical clarity but also contributes to their recognition within global policy debates, legislative frameworks and responses related to digital governance and security. The list below provides a non-exhaustive overview of key categories and forms of technology-facilitated gender-based violence. These categories are not always clearly delineated. Different forms of TFGBV may overlap and reinforce one another; for instance, disinformation campaigns may intersect with image-based abuse, threats and cyberbullying. The typologies presented below should therefore be understood as dynamic, evolving, and often interconnected.

 **Hate speech**	Any type of communication, in speech, writing, or behaviour, that attacks or uses pejorative or discriminatory language toward a person or a group based on identity, such as religion, ethnicity, nationality, race, colour, descent, gender, or other identity factors.[12]
 **Cyberbullying**	A form of online harassment involving the constant and intentional infliction of damage through digital technologies to undermine a target's self-esteem.[13]
 **Cyber-facilitated trafficking in persons**	The use of digital platforms to move persons across borders for sexual or labour exploitation, including to facilitate recruitment, exploitation and exertion of control and pressure over victims.[14]
 **Cyber harassment**	Cyber harassment involves the intentional use of ICTs to humiliate, harass, attack, threaten, alarm, offend, or insult a person. Unlike cyberstalking, in which there is a pattern of threatening behaviour, a single incident is sufficient to constitute cyber harassment, although the practice may also involve more than one incident.[15]
 **Cybermob**	Large group of online attackers who threaten, insult and verbally abuse a target, often in an organized and coordinated manner.[16]
 **Cyberstalking**	Persistent, unwanted and/or threatening surveillance, contact or pursuit conducted through technological means. Cyberstalking may turn to offline stalking and vice versa.[17]
 **Cyber sexual harassment**	Sending sexual content without permission, threatening with sex acts in private online spaces, such as over email, text, or on social media, and taking and/or sharing sexual pictures or videos of a person without permission.[18]

12 UN Women, Women, Peace and Digital (In)Security in South-East Asia, 2024.

13 *Ibid*.

14 *Ibid*.

15 United Nations Office on Drugs and Crime (UNODC). *Cyberstalking and Cyberharassment.*

16 *Ibid*.

17 United Nations Population Fund, The Virtual Is Real: Background on TechnologyFacilitated Violence Against Women and Girls.

18 UN Women, Normalized No More: An Evidence-Based Guide to Measuring Sexual Harassment, 2026.

Disinformation	False information deliberately created and spread to harm a person, social group, organization, or country.[19] [20] The false information is deliberately disseminated to deceive people.
Doxxing	Posting sensitive personal information, including full names, home and work addresses, telephone numbers, email addresses, family names, and financial or employment details, without permission.[21] The term derives from "dropping docs" and refers to the unauthorized extraction and publication of personal information as a form of intimidation or to enable harassment in the "real world". In some cases, this information has been posted on pornographic sites alongside false advertisements offering sexual services.[22]
Gendered disinformation	The term "gendered disinformation" can be used to describe information activities (creating, sharing, disseminating false content) which: ▸ Attacks or undermines people on the basis of their gender. ▸ Weaponizes gendered narratives to promote political, social or economic objectives.[23] Gendered disinformation has multiple aims: portraying women as weak, incompetent and sexualized objects, incapable of leadership; driving women and gender nonconforming persons out of public spaces and places of power; and silencing those who do not comply with gender norms. Gendered disinformation attacks not only individuals but also their collective struggles by seeking to delegitimize feminism and gender rights. The overall objective is to undermine human rights, gender equality, sustainable development and democracy. Gendered disinformation combines three defining characteristics of online disinformation – falsity, malign intent and coordination.[24]
Hacking	The misuse of devices like computers, smartphones, tablets, and networks to cause damage to or corrupt systems, gather information on users, steal data and documents, or disrupt data-related activity.[25] It is a tactic that can be used to facilitate harassment and intimidation in cases of technology-facilitated gender-based violence.
Identity theft and impersonation	Creating a fake profile, sharing false personal information, or assuming someone's identity with the intent to damage their reputation or threaten their safety. It undermines a person's credibility and can have serious social, professional, and security consequences.[26]

19 Wardle, Claire; Derakhshan, Hossein, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, Council of Europe, Aug. 2018, 2nd revised edition.

20 Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training, 2018.

21 United Nations Population Fund, *The Virtual Is Real: Background on Technology-Facilitated Violence Against Women and Girls.*

22 Organization of American States (OAS) Cybersecurity Program of the Inter-American Committee against Terrorism (CICTE) and Inter-American Commission of Women (CIM), *Online Gender-Based Violence Against Women and Girls: A Guide to Basic Concepts, Digital Safety Tools, and Response Strategies.*

23 Internet Governance Forum, Best Practice Forum on Gender and Digital Rights.

24 UN Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, A/HRC/53/25, 7 August 2023.

25 Fortinet, What Is Hacking?

26 Organization of American States (OAS) Cybersecurity Program of the Inter-American Committee against Terrorism (CICTE) and Inter-American Commission of Women (CIM), *Online Gender-Based Violence Against Women and Girls: A Guide to Basic Concepts, Digital Safety Tools, and Response Strategies*.

 **Image-Based Abuse**	The use of imagery to objectify, exploit, humiliate or harass a person. Examples include non-consensual sharing of intimate imagery.[27] It involves the taking, sharing or threatening to share sexually explicit images without consent, including AI-generated sexual imagery. Image-based abuse is an alarming manifestation of AI-driven harm. Advances in generative AI have lowered the barriers to producing hyper-realistic deepfake images and videos. A study conducted in 2023 estimated that 98% of all deepfake content online is non-consensual and pornographic, and that 99% of those depicted are women. This form of abuse combines sexual violence, reputational harm, and psychological trauma, often with long-lasting consequences for victims' personal and professional lives.[28]
 **Misinformation**	Misinformation is incorrect or misleading information. In contrast to disinformation, misinformation is not necessarily created or shared to create harm and the individual who shares it may not even be aware it is false.[29]
 **Sextortion**	A type of electronic blackmail, the demand for money, sexual acts, or additional explicit images in exchange for not exposing intimate images or private information.[30]
 **Shallowfake**	A manipulated image often created using basic and widely accessible editing software, such as placing one person's face onto another person's body. In contrast, more realistic and sophisticated manipulations (referred to as deepfakes) are generated with machine learning techniques.[31]
 **Trolling**	Deliberately provoking or upsetting individuals or groups online by posting inflammatory, irrelevant, or controversial messages.[32]

27 United Nations Population Fund, The Virtual is Real: Background on TechnologyFacilitated Violence Against Women and Girls.

28 Security Hero, State of Deepfakes: Realities, Threats, and Impact, 2023.

29 UN Women, *Glossary: Gender and Technology.*

30 United Nations Population Fund, *The Virtual Is Real: Background on Technology-Facilitated Violence Against Women and Girls.*

31 *Ibid.*

32 *Ibid.*

CHAPTER 04

TFGBV in conflict settings: evidence and patterns

4.1 How conflict exacerbates TFGBV

There is emerging evidence, based on country-specific analyses, that technology-facilitated gender-based violence risks intensify in conflict settings.

TFGBV in conflict-affected contexts is exacerbated by the proliferation of violence, the deterioration of living conditions across many levels, including education, employment, and safety, and the weakening of institutions such as the judiciary, defence, and law enforcement. Political instability further intensifies the targeting of specific groups, including women leaders, journalists, and human rights defenders, who are often subjected to online harassment, disinformation campaigns, and digital threats.

At the same time, misogynistic attitudes and restrictive gender norms remain among the underlying drivers of TFGBV, making women who occupy visible, public, or leadership roles a target, as they challenge socially prescribed expectations. The forms of abuse they experience are also emblematic and reflective of these dynamics: attacks frequently focus on women's appearance, sexuality, while their bodies are judged, weaponized, and used as tools of discrediting and control, particularly during periods of political tension, backlash, and war.

In fragile and conflict-affected settings, the dangerousness of TFGBV may increase, as it can

more easily translate into real and immediate risks. Practices such as doxxing, digital harassment, or image-based abuse can quickly turn into offline violence. Doxxing can expose women to arrest, physical violence, or retaliation. Gendered disinformation campaigns can harm not only individuals but also entire groups of women within specific professions, while also contributing to polarization and weakening social cohesion, as illustrated later in the case of Ukraine. Image-based abuse, including AI-generated manipulation of photos or videos, can have severe consequences, for instance, when religious or cultural pretexts (e.g. removing the hijab from photos of women's rights defenders in Sudan, or manipulating the content of what female journalists say) are used to justify hostility or incite violence against women. TFGBV can therefore be deployed as a tactic by different actors, including armed groups, foreign actors, and political stakeholders, undermining efforts toward stability, democratic governance, and peace. When women in political, peacebuilding, civil society, public and media roles are silenced, withdraw from public life, or are forced to relocate, the effects extend beyond the individual level and become broader governance issues.

A cautious analysis of existing quantitative data allows for some observations regarding the prevalence of technology-facilitated gender-based violence and its potential interconnections with broader structural and conflict factors. Available evidence suggests that the prevalence and intensity of online violence against women vary across regions. Data from the Economist Intelligence Unit, for instance, indicate higher reported levels of online abuse in parts of Africa and the Middle East.[33] While the study does not explicitly establish a causal relationship with fragility or conflict, the regions reporting higher levels of online abuse include several fragile and conflict-affected contexts and tend to score lower on gender equality and Women, Peace and Security indicators. Although these findings do not allow for definitive conclusions, they point to a potential interconnection between structural gender inequalities, insecurity, and increased exposure to digital violence.

This data does not provide disaggregated information on women targeted by TFGBV by profession. However, other qualitative reports offer greater insight into the specific forms of TFGBV affecting women operating professionally in peace and security roles. For instance, a briefing note by the organization ACAPS highlights that in Yemen, a survey conducted by an online youth platform found that, among people with access to the Internet, about 69% of women had experienced some form of online violence, compared with 32% of men.[34] The same report notes that women in public roles, including politicians, activists, journalists, civil society representatives, are at heightened risk of TFGBV, including defamation, blackmail, and hacking, often aimed at discouraging their participation in public life. Engagement in peacebuilding activities may further expose women to such risks. The report documents disinformation campaigns attempting to associate Yemeni women involved in civil society and peacebuilding with foreign actors allegedly seeking to "ruin" the country. [35] Similarly, in northwest Syria, analysis by ACAPS and UNFPA indicates a sharp increase in TFGBV during periods of acute crisis and political instability.[36]

Although data are scarce, the topic is increasingly discussed. During the *first UNFPA-led Inaugural Symposium on Technology-Facilitated Gender-Based Violence,* held online in November 2025, stakeholders from sub-Saharan Africa discussed and showcased how online violence escalates during periods of political tension, conflict and elections. Again, women politicians, journalists, and activists were reported to face online hate speech, ethnic harassment, and coordinated disinformation campaigns. The dis-

33 The Economist Intelligence Unit, *Measuring the Prevalence of Online Violence Against Women,* 2021.

34 ACAPS. Yemen, Shedding Light on TechnologyFacilitated GenderBased Violence, 2024.

35 *Ibid.*

36 ACAPS and UNFPA, Technology-Facilitated Gender-Based Violence in Syria, 2025.

cussions also emphasized that while most of the current focus remains on how TFGBV manifests and how it is widespread through social media, new complex and less visible forms of violence are emerging. These include the use of spyware and surveillance technologies[37] to monitor, track, and target women human rights defenders, thereby facilitating intimidation and, in some cases, offline harm.[38] Similarly, emerging technologies such as artificial intelligence enable the production of deepfakes and the large-scale dissemination of gendered disinformation.

The United Nations Secretary-General Reports on conflict-related violence against women do recognize online Violence Against Women and Girls (VAWG) as an emerging form of harm. For instance, the 2024 report of the United Nations Secretary-General highlighted cases in Myanmar, Afghanistan, Libya, Yemen, and Ethiopia, all conflict-affected countries, where women were subjected to TFGBV. In Myanmar women associated with the resistance movement faced targeted online harassment, including the circulation of sexually explicit images, sexualized and discriminatory rhetoric that incited physical violence. In Afghanistan and Ethiopia organizations supporting human rights and women human rights defenders were targeted through online harassment, and intimidation. In Libya sexual assaults were filmed and shared online; in one instance, this occurred after the victim had publicly denounced an armed group on social media. In Yemen, online violence narrowed the operating space for women engaged in politics or civil society organizations.[39] The 2025 report similarly documents the continued use of online threats and hate speech targeting women active in public life, particularly in contexts such as Afghanistan and Syria.[40]

4.2 Who is targeted

As highlighted in the previous section, in fragile and conflict settings, some of the power dynamics and practices of gender inequality are mirrored online as well.

While TFGBV affects women and girls as civilians, in conflict settings, it is pertinent to broaden the perspective to women operating in security, public, and visible roles, who are not only exposed but also attacked, silenced, and targeted online through hate speech, harassment, and defamation that replicate patterns of violence they already face offline. This is not incidental. Specific forms of violence, and their consequences, are directed at these particular groups to maximize impact, silence participation, and undermine stability, social cohesion, and peace processes. The following groups emerge as particularly exposed within the framework of the Women, Peace and Security agenda:

- **Women engaged in armed and security roles:** While most conflict-related violence, including TFGBV affects activists and civilians, there are documented instances in which female military personnel, combatants, or women affiliated with armed forces have been targeted or abused. Digital threats, including disinformation campaigns and online harassment, can undermine their security, damage their professional reputation, and discourage both participation and recruitment into security sectors. Women in these roles are frequently targeted not only because of their gender, but also because they challenge deeply entrenched norms regarding who is expected to occupy military and security positions. As a result, attacks often combine gendered narratives with political or military objectives, portraying women as unfit, immoral, or as symbols of institutional weakness.

37 Association for Progressive Communications (APC), *From Context to Collective Action: Outcomes of Africa's First Symposium on Technology-Facilitated GenderBased Violence*, 2026.

38 Front Line Defenders and Access Now, *Unsafe Anywhere: Women Human Rights Defenders Speak Out About Pegasus Attacks,* 2022.

39 United Nations Security Council, *Conflict-Related Sexual Violence: Report of the Secretary-General*, S/2024/292, 2024.

40 United Nations Security Council, Conflict-Related Sexual Violence: Report of the Secretary-General, S/2025/259, 2025.

For instance, in Myanmar, following the *2021 military coup*, research conducted by *Myanmar Witness*, a project of the *Centre for Information Resilience*, analysed approximately *1.6 million Telegram posts* and identified widespread politically motivated online abuse targeting women. The report documented, among other patterns, online violence targeting women supporting the *National Unity Government*, and participating in armed resistance groups such as in the *People's Defence Forces (PDF)*. Some of the recurring narratives portrayed women associated with the PDF as *morally corrupt*, engaging in illegal or promiscuous behaviour. Other narratives depicted them as *sexual "prey"* for male members and leaders of the groups and organisations. Online attacks were often expressed through coded slang and sexually suggestive language, normalizing and trivializing sexual abuse, including rape. *Doxxing* was also frequently used and personal information such as home addresses, photographs, and other identifying details were shared online, leading to offline violence and arrests.[41]

- **Journalists:** Women journalists and media workers are particularly vulnerable to TFGBV, facing digital harassment, doxxing, and gendered disinformation, particularly when reporting on issues related to the rule of law, corruption, human rights, or gender issues. They also face higher risks of deepfake attacks and smear campaigns, aimed at damaging their credibility and professional standing, further discouraging engagement in investigative reporting.[42]

  In conflict-affected and fragile settings, these dynamics may intensify. Women journalists covering war and political issues are at heightened risk of targeted and gendered forms of online violence. The report *Digital Violence: Syrian Women Journalists and Human Rights Defenders* documents a few individual testimonies of female journalists who were targeted online in connection with their reporting on armed groups and areas liberated from ISIS.[43] According to other studies, in Mexico, female reporters covering political violence and organized crime are persistently subjected to cyber threats, which often escalate into physical violence.[44] These examples suggest that reporting on politically sensitive issues can increase exposure to digital violence.

  One landmark 2021 study examining how online abuse is used to silence, intimidate, and push women journalists out of public life is UNESCO's The Chilling: Global Trends in Online Violence Against Women Journalists.[45] The study draws on surveys of 901 women journalists from about 125 countries, 173 in-depth interviews, and two bigdata case studies assessing over 2.5 million posts on Facebook and Twitter directed at two prominent women journalists, Carole Cadwalladr and Nobel Peace Prize laureate Maria Ressa. One of its central findings is that around 73–75% of the women journalists surveyed have experienced some form of online violence in the course of their work, including harassment, threats of physical and sexual violence, and smear campaigns fuelled by disinformation.

  The case of Nobel Peace Prize laureate Maria Ressa in the Philippines shows how online harassment, including death threats, rape threats, and disinformation campaigns, is

41 Centre for Information Resilience, Digital Battlefields: Online Abuse and Gendered Harms in Conflict Contexts, 2024.

42 Derechos Digitales, Response to the Call for Inputs on Technology-Facilitated Gender-Based Violence and Its Impact on Women and Girls, submitted to the Office of the United Nations High Commissioner for Human Rights (OHCHR), 2025.

43 Syrian Female Journalists Network (SFJN), Digital Violence: Syrian Women Journalists and Human Rights Defenders in the Digital Space: *Risks and Threats*, 2018.

44 Derechos Digitales, *Response to the Call for Inputs on Technology-Facilitated Gender-Based Violence and Its Impact on Women and Girls*, submitted to the Office of the United Nations High Commissioner for Human Rights (OHCHR), 2025.

45 UNESCO, *The Chilling: Global Trends in Online Violence Against Women Journalists*, 2021. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000377223.

used to intimidate journalists reporting on politically sensitive issues.

"Death threats. Rape threats. Doxxing. Racist, sexist, and misogynistic abuse. In text, image, and memes. These are just some of the features of the online violence that Maria Ressa, the Filipino-American journalist who founded the Manila-based news site Rappler, has faced daily since the Philippines' 2016 election. She said that none of her experiences in the field prepared her for the massive and destructive campaign of gendered online abuse, threats, and harassment directed at her. At one point, in response to an investigative series on state-linked disinformation, she recorded receiving more than 90 hate messages an hour on Facebook." [46]

- **Politicians, public figures and decision-makers:** Female politicians are frequently targeted by online threats, online harassment, fake stories, humiliating or sexually charged images, including photomontages, amplified by trolls and bots.[47] Gendered attacks often aim at framing them as untrustworthy, unintelligent, emotional/angry/crazy, or based on stereotypes,[48] using physical appearance, or gendered narratives to portray women as unfit for leadership, discouraging women's political participation.

  According to a study conducted by the Inter-Parliamentary Union on sexism, harassment, and violence against women in parliaments in the AsiaPacific region, 60% of the women parliamentarians surveyed have been the target of hate speech, disinformation, image-based abuse, or doxing online.[49] For women in public life, these threats pose particular risks, with a cumulative "snowball effect" that can undermine their professional and private lives. Artificial intelligence and other digital tools can also be used to monitor online activity, map social networks, and fabricate images or messages that can damage reputations, weaken professional standing, and incite harassment. In conflict-affected and fragile contexts, the digital sphere becomes another front line of struggle.[50]

  For instance, evidence from Yemen shows how online violence against women politicians is embedded within broader conflict dynamics. Reports indicate that Yemeni female politicians have been systematically targeted through coordinated digital campaigns using bots, fake accounts, and manipulated content. These attacks often focus on their private lives, circulating personal photos or fabricating images, including through emerging technologies such as deepfakes, with the aim of discrediting and silencing them. Such campaigns are part of wider strategies of intimidation, polarization, and control, whereby conflict actors, groups and/or networks use digital tools to wage reputational and psychological warfare against women in public life.[51]

- **Women human rights defenders, women's rights organizations:** Online harassment, coordinated disinformation campaigns and threats also target individuals advocating for gender equality and women's rights, to delegitimize their work, undermine their credibility, and restrict their participation, as well as affect social cohesion and disrupt peacebuilding efforts. While activists are targeted with defamation, smear campaigns and online and offline hate speech, the attacks against women human rights

46 *Ibid.*

47 Lucina Di Meco, *Online Threats to Women in Politics: The Shaping of Narratives and Implications for Democracy*, UN Women Expert Group Meeting paper (EGM/CSW/65), 2020.

48 *Ibid.*

49 InterParliamentary Union, *Sexism, Harassment and Violence Against Women in Parliaments in the AsiaPacific Region: Online GenderBased Violence and Beyond*, 2025.

50 The Stimson Center, The Impact of Artificial Intelligence on Violence Against Women and Girls, 2026.

51 Qantara.de, Yemen's Other War: Female Politicians Targeted on Social Media, 2022.

defenders typically target their personal behaviour, moral conduct or sex lives. Another example of how digital technologies can reinforce attacks against women human rights defenders (WHRD), is the deployment of advanced surveillance technologies, such as spyware. These tools enable the covert extraction of personal data and monitoring of communications, without the knowledge or consent of the individual targeted. Pegasus spyware, for example, has been central to numerous investigations[52] due to its surveillance capabilities, enabling covert access to messages, calls, microphones, cameras, and data stored on devices without requiring users to download or click on files or malicious links. Between 2016 and 2018, the spyware was used to target an estimated *50,000 individuals*, including activists and high-profile public figures. Although sex-disaggregated data are not publicly available, civil society organisations and human rights defenders have underscored the gendered implications of such surveillance. The use of spyware can disproportionately affect women by heightening exposure to harassment, reputational attacks, intimidation, and psychological pressure, thereby contributing to self-censorship and reduced participation in public and political life.[53,54]

4.3 Consequences

Technology-facilitated gender-based violence generates a wide range of consequences that often extend beyond digital spaces. In conflict and fragile settings, women in armed and security roles, as well as politicians, journalists, and women human rights defenders, may cope by self-censoring, withdrawing from online platforms, or reducing their engagement in digital spaces, offline spaces and public debate due to fear and sustained harassment. These dynamics affect their participation in public and political life, undermining democratic processes[55] but also lead to economic harm, psychological distress, and reputational damage, while weakening trust in institutions.

52 The "Pegasus investigations" refer to a series of inquiries into the use of Pegasus spyware developed by the NSO Group, including the 2021 *Pegasus Project* led by Forbidden Stories and Amnesty International, the European Parliament's PEGA Committee (2022–2023), and subsequent national investigations.

53 Access Now, Pegasus Targets Women Activists, 2021.

54 Amnesty International & Forbidden Stories, Pegasus Project, 2021.

55 UN Women, Placing Gender Equality at the Heart of the Global Digital Compact: Taking Forward the Recommendations of the Sixty-Seventh Session of the Commission on the Status of Women. 2024.

In conflict settings, digital violence may further translate into offline harm, including surveillance, intimidation, and physical threats. The examples below illustrate how these online abuses can translate into tangible, real-world consequences:

Online abuse	Offline consequences
Economic harm	Loss of employment or abandonment of professional and income-generating activities due to online harassment, threats, or reputational attacks, either as a voluntary response or as a forced consequence of sustained abuse. In fragile and conflict-affected contexts, where economic opportunities are already limited, women often bear an increased burden of care due to displacement, isolation, or the absence of male family members who may have been more directly involved in the conflict. At the same time, social protection systems are frequently weak or disrupted. In such conditions, the impacts of TFGBV can further exacerbate economic vulnerability, and the loss of income may increase dependency on family or community structures, heighten exposure to further forms of violence, and limit women's ability to relocate, seek protection, or continue their professional activities safely.[56]
Erosion of trust in institutions	Failure to hold perpetrators accountable erodes trust in judicial and institutional systems, signalling that technology-facilitated harms are tolerated or unpunished. In fragile and conflict-affected settings, where institutional legitimacy may already be weakened, this can deepen distrust in both State and non-State actors and institutions, undermine the rule of law, and discourage reporting of abuses.[57] [58]
Psychological distress	Experiences of TFGBV can cause depression, anxiety, stress, and fear, as well as self-harm. In conflict settings, where individuals may already be exposed to trauma, displacement, or insecurity, these impacts can be cumulative, intensifying existing vulnerabilities and affecting both personal well-being and the ability to remain engaged in professional or public roles.
Reduced participation in public and political life	TFGBV discourages women from speaking up, participating in decision-making processes, or engaging in mediation, negotiations, public or security roles. In fragile settings, this can directly affect peace processes, governance, and recovery efforts, as women's exclusion reduces the diversity of perspectives and weakens inclusive decision-making, ultimately undermining WPS commitments.[59] In addition, these dynamics can have longer-term "pipeline" effects by discouraging women from entering or remaining in these sectors, thereby limiting future participation and leadership across peace, security, and governance institutions.

56 Geetha, R., The Impact of Online Harassment on Women's Societal Development, International Journal of English Literature and Social Sciences, 9(6), 2024.

57 UN Women, The Dark Side of Digitalization: Technology-Facilitated Violence against Women in Eastern Europe and Central Asia, 2024.

58 UN Women, Model Framework for Legislation on Technology-Facilitated Violence Against Women and Girls, 2025.

59 Georgetown Institute for Women, Peace and Security. Technology-Facilitated Gender-Based Violence: Policy Brief, 2024.

Online abuse	Offline consequences
Self-censorship and reduced online presence	Women may withdraw from digital spaces to avoid targeting, thereby reducing their ability to communicate, mobilize, and access information. Research indicates that 28% of women subjected to technology-facilitated violence deliberately reduced their online presence and self-censored for fear of privacy or safety violations.[60] [61] In conflict contexts, where digital platforms may represent one of the few remaining spaces for participation and advocacy, this withdrawal can further isolate women, diminish their visibility, and reduce attention to the issues they have contributed to raising awareness of.
Technology-Facilitated Physical Violence	Digital threats may translate into offline harm, including through doxxing, surveillance, or tracking.[62] In fragile settings, this link is especially acute, as exposure of personal information can lead to arrest, retaliation, or physical violence, as documented in contexts such as Myanmar.
Reputational and social harm	Disinformation, gendered narratives and image-based abuse may damage women's credibility, expose them to stigma, or lead to exclusion from communities, professional networks, as well as from roles in negotiations, debates, and leadership positions.[63] In contexts where social cohesion is already fragile, such attacks can deepen divisions and reinforce gender-based discrimination.
Surveillance and security risks	The use of spyware and other surveillance tools by State or non-State actors increases risks of retaliation, arrest, or violence, especially for activists, journalists and WHRDs.[64] These practices can be embedded within broader systems of control and repression, further constraining civic space and limiting women's ability to operate safely.

Across these dimensions, the impacts of TFGBV are not only individual but also cumulative and systemic. They affect entire sectors by discouraging participation, limiting diversity, and weakening the overall environment in which women operate. At the same time, they erode trust in institutions, weaken social cohesion, and constrain inclusive governance processes. Over time, these dynamics shape who can participate, whose voices are heard, and how decisions are made, with direct implications for the implementation of the Women, Peace and Security agenda and the sustainability of peacebuilding and recovery efforts.

4.4 Digital tools shaping the four pillars of the WPS agenda

The analysis above shows that digital technologies increasingly shape the activities, risks, and opportunities experienced by women operating in peace and security contexts, including security actors, peacebuilders, and women human rights defenders. Both the opportunities created by digitalization and the harms associated with technology-facilitated gender-based violence can be understood through the four pillars of the Women, Peace and Security agenda. As a conceptual framework, this research draws on the model developed by Dr. Agnieszka Fal-Dutra

60 The Economist Intelligence Unit, Measuring the Prevalence of Online Violence Against Women, 2021.

61 UNESCO, The Chilling: Global Trends in Online Violence Against Women Journalists, Paris, UNESCO, 2021.

62 Centre for Information Resilience. *Digital Battlefields: Online Abuse and Gendered Harms in Conflict Contexts*. 2024.

63 UN Women, The Dark Side of Digitalization: Technology-Facilitated Violence Against Women in Eastern Europe and Central Asia, 2024.

64 Front Line Defenders and Access Now, *Unsafe Anywhere: Women Human Rights Defenders Speak Out About Pegasus Attacks,* 2022.

Santos and Dr. Outi Donovan,[65] which identifies three main ways in which digitalization is framed within WPS discussions:

- **Digitalization as an instrument**: understood as a set of tools that enable or facilitate activities such as reporting violations and improving monitoring mechanisms.

- **Digitalization as a source of empowerment**: frames technology as a pathway to enhance women's access to opportunities, participation, and decision-making processes.

- **Digitalization as a threat**: focuses on the insecurities generated by technological advancement at both individual and state levels, including technology-facilitated gender-based violence.[66]

This framework provides a useful lens to understand how digital technologies intersect with each of the four WPS pillars. Across prevention, protection, participation, and relief and recovery, digital tools can function as enablers and as sources of risk. For instance, they can support conflict prevention and the monitoring of gender-based violence, enhance protection mechanisms, facilitate women's participation in decision-making processes, and contribute to recovery efforts. At the same time, they can be used to spread disinformation, enable surveillance, reinforce gender inequalities, and perpetrate violence against women.

Across all four pillars, digitalization therefore shapes both the implementation of the WPS agenda and the lived experiences of those it seeks to support. The following table summarizes some of the main opportunities and risks associated with digital technologies under each pillar.

65 FalDutra Santos, A., & Donovan, O. (2025). *Between Contested Narratives and Transformative Actions: Digitalization Discourse, Policy, and Practice in the Women, Peace and Security Agenda*. International Feminist Journal of Politics, 27(2), 250–269.

66 *Ibid*.

	Opportunities	Risks
Participation	▸ Online platforms can enable women's engagement in political, civic, and peace processes. ▸ Online platforms can provide access to virtual training and capacity-building opportunities. ▸ Digital networks can strengthen advocacy, coordination, and knowledge sharing. ▸ Digital technologies can support women's participation in digital governance and technology-driven fields, including data analytics, AI, and emerging defence technologies. ▸ Digital technologies can enable greater involvement of women in armed roles, including in specialised units such as cybersecurity or drone-related teams, contributing to operational and strategic functions.	▸ TFGBV can discourage women from maintaining an online presence and reduce their participation in digital and public spaces. ▸ Algorithmic bias can reduce visibility, representation, and access to opportunities. ▸ Digital exclusion can limit participation due to lack of connectivity, digital literacy, or resources. ▸ The weaponization of digital technologies, including surveillance and censorship, can create additional security risks and barriers to participation.
Protection	▸ Mobile applications and early-warning systems can support women at risk, including through digital reporting of threats and violations. ▸ Digital tools can enable the reporting and documentation of gender-based violence at local, regional, or national levels. ▸ Digital monitoring and surveillance technologies can support protection efforts in conflict settings (e.g. alert systems, safe corridors).	▸ Digital surveillance tools, such as spyware, can target women activists, journalists, and human rights defenders. ▸ Data breaches and doxxing can expose sensitive personal and location information. ▸ The misuse of AI and digital technologies can enable profiling, tracking, and restrictions on freedom of movement.
Prevention	▸ AI and data analytics can support the detection and prevention of sexual violence and exploitation. ▸ Early-warning systems can help anticipate conflict-related risks, tensions, and escalation. ▸ Digital platforms can support awareness-raising and prevention campaigns.	▸ Disinformation campaigns can disrupt social cohesion and peace efforts. ▸ Online harassment can be used to intimidate or silence women. ▸ Digital technologies can reinforce gender stereotypes and discriminatory narratives.
Relief and recovery	▸ Digital cash transfers, e-services, and online humanitarian assistance can support women survivors. ▸ Telemedicine and e-health services can improve access to gender-sensitive healthcare. ▸ Online psychosocial support and remote counselling can assist individuals affected by conflict. ▸ Digital platforms can support skills development and livelihood restoration.	▸ Lack of access to technology can exclude women from recovery programmes and services. ▸ Privacy risks can arise from the storage of sensitive personal and health data. ▸ Cybersecurity threats can disrupt aid delivery, communication systems, and access to services.

CHAPTER 05

Case studies

To explore in more detail how TFGBV manifests in conflict settings, and intersects with conflict dynamics and political participation, the research focused on selected examples from Ukraine and Sudan. In Ukraine, women have assumed increasingly visible roles in security, civil society, and international advocacy since the 2022 full-scale invasion, making the country a relevant context for examining how online harassment, disinformation, and gendered digital attacks are used to undermine women's credibility and participation. Sudan, similarly, offers important insights due to the central role women played in the 2019 revolution and ongoing pro-democracy activism, while also facing significant online intimidation and abuse aimed at silencing their voices.

Given the scope of the consultations conducted, this chapter provides insights into the experiences and testimonies of women operating in peace and security spaces, and how their work, or the work of their organizations, has been affected by TFGBV, alongside anecdotal examples and expert observations[67]. The case studies do not attempt to be "representative" nor to provide systematic comparisons, but rather to make observations on how TFGBV manifests in conflict contexts and reflect on the potential implications for the implementation of the WPS agenda.

67 The chapter draws on interviews conducted by UNICRI and includes direct quotations from participants, reproduced with minimal editing to preserve their original meaning and authenticity.

5.1 Ukraine

"Everyone who is active in digital spaces and working for a democratic and peaceful Ukraine is at risk."

From a WPS perspective, Ukraine has inspired reflections in several ways. Firstly, it provides an opportunity to examine the implementation of the WPS agenda within the context of an ongoing war, as Ukraine updated its National Action Plan (NAP) on WPS in 2022,[68] while the country was in active military conflict.[69] A new NAP is underway, demonstrating a strong commitment to ensuring that it addresses key issues faced during the war. According to some interviewees, the upcoming plan might mark a pivotal advancement by explicitly addressing technology-facilitated gender-based violence, an emerging threat absent from the previous plan.

Secondly, Ukraine has inspired many by "redefining" the role of women in wartime and showcasing grassroots resilience. Ukrainian women have mobilized as soldiers, volunteers, and community leaders. Today, more than 75,000 women serve in Ukraine's Armed Forces, marking a 20 per cent increase since 2022, with an increasing number of women attaining officer ranks as well.[70] More than 5,500 are deployed directly on the front line, according to Ukraine's Ministry of Defence. In the current war, technology is also reshaping women's roles in combat, with thousands of women deployed as drone pilots and front-line technicians. Hence, drone piloting is becoming one of the military's most prominent combat roles among female recruits.[71]

In parallel, many civil society organizations have been created to advocate for peace. Many women-led organizations work on gender equality, democracy, security and peace, implement national projects that advocate for women's rights and social cohesion and promote women's meaningful participation in reconciliation processes, recovery efforts, including through digital platforms.

Over the years, as women's roles in the conflict have expanded, various forms of TFGBV have emerged, targeting women engaged in peacebuilding, democracy, gender equality and security-related efforts, as well as gendered disinformation campaigns directed at women in security and armed roles.

"Bot farms and coordinated online attacks target women in sensitive positions across several contexts, including military, political, and public debates. Some campaigns specifically target women connected to the military sphere."

68 Ukraine, Cabinet of Ministers. *National Action Plan on United Nations Security Council Resolution 1325 on Women, Peace and Security until 2025.*

69 Merja E. Kähkönen, *Transformative Peace for Women in Ukraine? Implementing the WPS Agenda in a War*, *International Affairs, vol. 101, no. 6, 2025.*

70 "Жінки в ЗСУ: "Бажання служити сприймають за примху" [Women in the Armed Forces: "The Desire to Serve Is Perceived as a Whim"]," DW, October 9, 2023.

71 Forbes, David Hambling, A Woman's Place Is in the Drone War: How Technology Changes Attitudes, 25 March 2026.

TFGBV against women in the armed forces

Historically, in Ukraine, women have traditionally been underrepresented in military institutions, reflecting broader social norms and institutional barriers that limited their participation primarily to non-combat and caregiving functions. However, as seen in the previous paragraph, women have challenged these norms and entered the armed forces in large numbers since the full-scale invasion. Despite this shift, they continue to face discrimination even where formal equality exists and access to combat roles has expanded. These dynamics create barriers at different levels, with reports sharing that women are often *passed over for frontline positions*, discouraged from certain roles, or required to prove themselves more than their male counterparts. *"Soft discrimination" persists through assumptions that women should be protected or excluded from combat* and female commanders may face resistance from their superiors and subordinates alike. There is a dual perception. On one hand, military personnel are currently held in high regard, as the ongoing conflict has elevated their status, making it ***"a social and political marker."*** On the other hand, deeply rooted gender norms take time to change. Since women remain underrepresented in the military, this can reinforce perceptions that men's roles and experiences are more valued, and that women should adapt accordingly.

"Although Ukraine has made progress through legal amendments, access to military academies, and the possibility for women to take officer positions the reality remains challenging. Any attempt to protect women's rights in the armed forces can immediately become grounds for online harassment and bullying. This creates additional pressure on women who want to be vocal, often leading to burnout and exhaustion."

Female soldiers and veterans experience multiple forms of online abuse. **Sexist and misogynistic trolling** is one, with women targeted with sexist comments accused of abandoning their "womanly" roles and portrayed as promiscuous or "unnatural." **Offline and online harassment**, is another form of GBV and TFGBV women are subjected to, affecting them both offline and online: ***"There have also been changes regarding women in the army, which have shifted perceptions of women's roles. However, sexual harassment remains high."***

"There is also a perception among some men that women should not fully realize their potential. Many women want to take on combat roles, and they should have the choice to do so, but male perceptions within the military about what women should or should not do remain a barrier."

"Discrimination within the armed forces? Short answer: absolutely yes. Women in the armed forces face challenges of inequality derived from the patriarchal structure of the armed forces - even though Ukraine has made huge progress, and they amended the law to allow women to be educated in military academies and work in senior positions. But still, attempts to protect women's rights are often attacked online."

Another pervasive form of TFGBV is **online gendered disinformation campaigns** against women in the military, which are targeted and orchestrated efforts to harass, discredit, and silence female service members, frequently utilized as a form of hybrid warfare to undermine national security and cohesion.

The Ukrainian armed forces have been the target of coordinated online disinformation campaigns, particularly since the beginning of the full-scale invasion. Women in the military are often targeted as part of broader disinformation campaigns that reinforce stereotypes, that ridicule and mock them and that uses sexualized narratives to undermine public trust in both the armed forces and in women's military capacities. Such narratives are amplified online and through coordinated bot networks.[72]

72 Detector Media, How Propaganda Attempts to Discredit Ukrainian Women, August 30, 2023.

According to interviewees, these disinformation efforts by Russian actors generate false narratives at an alarming scale, with two primary objectives. The first is to undermine the image of the Ukrainian army by implying that female units are sent to the front because of a shortage of men, framing women soldiers as proof of national weakness or desperation. The second is to silence women in security roles, military personnel and police officers, thereby disincentivizing women from joining the army. As the role of women in the military remains a polarized topic in Ukraine, such narratives exploit societal divisions, enabling disinformation to spread more rapidly and deepen polarization.

"In the military sphere, the gender dimension is part of a broader anti-Ukrainian disinformation campaign directed against the armed forces as a whole. These narratives aim to discourage women from joining the military by suggesting that they should remain in more 'traditional' social or family roles instead."

Disinformation campaigns often circulate on social media, such as Telegram, with the intention to generate panic, confusion and fear. For instance, disinformation narratives circulating on Telegram channels claimed the alleged mobilization of pregnant women, based on a misrepresentation of an official Ukrainian Ministry of Defence initiative concerning the development of military uniforms adapted for pregnant servicewomen.

"Ukraine's armed forces launched a small project to design special uniforms for pregnant servicewomen. However, this initiative was picked up by propaganda, which falsely claimed that "they are even recruiting pregnant women to join the armed forces."

"Since the beginning of the full-scale invasion, we have experienced a lot of influence from bots producing negative narratives against women in the armed forces. One of the narratives promoted is that Ukraine is recruiting women because it is running out of men."

Fake images, videos, and AI- deepfakes are emerging forms of violence being used to disseminate misleading images and videos, **portraying female soldiers as unfit or abused**, and portraying Ukrainian "female battalions" as deserting or being subjected to mass sexual violence.[73] [74] The goal is to seed panic around mobilization of women in the military and generate a feeling of "shame", using sexist stereotypes, sexualized attacks, and misleading narratives to delegitimize women serving in the armed forces.

As reported by interviewees, for women in armed and security roles, these forms of harassment, disinformation, and targeted attacks can generate stress and anxiety, and it does impact on women's participation in the armed forces. In fact, while gendered disinformation does not appear (according to consultations) to significantly affect women currently serving in the armed forces, it may discourage potential recruits from joining and pursuing a career in the military.

"Other narratives portray women as ineffective in combat roles, or spread sexist stereotypes, such as referring to women as "field wives." These narratives are sexist and derogatory."

According to one interviewee, alongside female servicemembers, disinformation also targets the **families of military personnel** and described them as one of the most sensitive groups in society. This specific group is targeted with the aim to turn family members against state authorities and military leadership, provoke strong emotional reactions, generate distrust, resentment, and unrest within military communities. Within this group, wives, mothers, and daughters become the primary targets and are particularly vulnerable to online manipulation, pressure, and targeted disinformation campaigns as they may lack access to professional networks and protec-

73 *Ibid.*

74 Global Center on Cooperative Security and RUSI, The Impact of Gendered Narratives in the Conflict in Ukraine, 2023.

tive tools to identify the attacks and take a distance from them. These activities can be classified as political disinformation, using psychological pressure as part of broader foreign information manipulation and interference efforts, and deliberately targeting family networks to provoke emotional responses against military authorities and institutions, thereby weakening social cohesion and public support for the military.

TFGBV against activists, leaders, journalists and women's rights defenders

TFGBV and gendered disinformation also target individuals and groups working in civil society and political spheres. Consultations revealed specific forms of TFGBV perpetrated against women working in sensitive professional fields, such as peacebuilders, leaders, and journalists. Attacks include the leaking of personal information, the exposure of past activities, and attacks that undermine reputation and safety. Such practices are often part of broader power dynamics and structural pressures, sometimes linked to political competition aimed at silencing women and excluding them from opportunities to build expertise, experience, and resilience.

"During Women's March on 8 March, there were both online and offline attacks. Videos were manipulated, edited, taken out of context, and shared online. This caused distress, and some people were deeply affected."

In addition, some online narratives seek to discredit efforts to promote women's rights and leadership, portraying them as non-essential in times of conflict and arguing that attention and resources should instead be directed exclusively toward military priorities.

"Even without commenting, if you work on gender equality, you can still be attacked. People say that resources are being spent on unimportant issues and should instead go to the frontline rather than to WPS or gender initiatives. Because of this, I have reduced my presence on social media, and many people are deeply affected by this."

Women leaders, politicians, and those who aspire to political roles are often attacked, harassed online, or victims of misinformation and doxxing, especially when they become more active and vocal or when they express unpopular positions. Support structures exist, even if they are getting weaker due to lack of funding. One interviewee working specifically on this topic shared that some Ukrainian women's media platforms provided support to women leaders experiencing misogyny and harassment on social media, creating support networks through advocacy. These platforms play an important role in helping women share their experiences and in turn supporting other women to continue their engagement and not withdraw from public life. However, she informed that in February 2025, when USAID funding was cut, two or three media platforms that supported women in leadership positions in local government and politics were forced to close.

"They need to know that they are not alone, and that they can use their voice to support others. It is important to speak out, share experiences, and not remain silent. Media can play a key role by amplifying these stories and highlighting such cases."

Women in the **media** are also key targets of TFGBV. The experiences of Ukrainian women journalists have been widely documented, including in reports produced by Women in Media (WIM) Ukraine, which provide in-depth analysis of these patterns. Women journalists, particularly those covering the war, politics, or corruption, are frequently targeted with coordinated online harassment, threats, and gendered disinformation. WIM documents cases in which women journalists have been subjected to online abuse following the publication of war-related content. For instance, some female journalists experienced a wave of harassment across multiple social media platforms, including threats of sexual violence and the dissemination of their personal data, after reporting on military-related issues.

The attacks were further amplified through Telegram channels and other digital platforms to intimidate and silence them.[75]

Similarly, **civil society organizations** are also a target, especially those engaged in equality, peace and security, the rights of refugees and internally displaced persons in conflict settings. These issues are frequently the underlying trigger for online attacks, particularly when they are perceived as controversial by certain groups. Many CSOs leaders are aware of subjects that might increase online tensions, and as a coping strategy they limit their exposure or avoid debating about certain issues online.

One trend that emerged during the consultations is that **often women active in online spaces do not always recognize TFGBV or fully grasp its severity.** At the same time, they may not be aware that they are engaging in forms of self-censorship, reducing their online presence and activism to manage the psychological burden and protect their mental health. Some do acknowledge the need to implement safeguarding policies and invest in digital literacy and security training, and to strengthen protection from online harassment and to maximize the potential of technology to connect women, build supportive communities, and support networks.

"I use social media only if the communication manager asks me, if not, for lack of time and engagement, I avoid it. But another reason why I quit social media is that I don't have time to reply to all the comments, and it affects my mental health. Before the full-scale invasion, I was more active online."

"Before, I had the energy to comment and reply. But there was always a lot of negativity, and now I don't feel able to invest time in this, I need to protect my mental well-being."

Platforms and channels of dissemination

Multiple digital platforms are used for the dissemination of these narratives. According to experts interviewed, the primary platform is **Telegram**, widely used for information consumption due to its easy accessibility and the proliferation of anonymous channels. Telegram, without providing any editorial oversight or compliance with journalistic standards, facilitates the manipulation of emotions and narratives, including the spread of false information. A study by Detector Media confirms this trend, noting that due to the absence of content moderation, Telegram has become a primary platform for coordinated disinformation. The analysis found that much of this content includes narratives expressing disdain for Ukrainian women, including mocking female refugees and women serving in the military.[76]

"It is very easy to manipulate emotions here, to spread fake stories and provocations without compliance with editorial requirements. It is easy to access and easy to use."

A second important platform is reported to be **Viber**, a messaging platform widely used for communication at the local and micro-community level (e.g. residential buildings, schools, and neighbourhood groups). At this level, disinformation often takes the form of rumours, which can then be amplified through Viber groups, contributing to the broader spread of disinformation campaigns.

TikTok, through its short-video format, enables the rapid and emotional framing of information and is used primarily by the youth. For older audiences, **YouTube** remains influential, where narratives related to anti-military messaging or pseudo-peace campaigns can circulate, often attempting to influence family perceptions and attitudes toward women in the military.

75 Women in Media Ukraine, *Monitåf Gender-Based Violence Against Women Journalists in Ukraine* (various reports, 2022–2024).

76 Detector Media, *How Propaganda Attempts to Discredit Ukrainian Women*, 30 August 2023.

5.2 Sudan

Over the past few years, the Internet has played an increasingly significant role in Sudanese political and social life, with internet penetration reaching approximately 42.4% in 2025.[77] In 2018, only about 29% of the population had access to the Internet, and just 7% were active social media users.[78] Since then, connectivity has expanded steadily, resulting in the current levels of internet access and social media engagement.

Social media played an important role during the 2019 revolution against Omar al-Bashir, when protesters and activists turned to digital platforms to communicate, mobilize demonstrations on the ground, and document human rights violations. Hashtags were widely used to raise awareness about the protests, many of which gained international attention.[79] The revolution brought together diverse groups and communities from across Sudan, with women and youth activists, leaders and journalists at the forefront. Women were estimated to constitute up to 70% of the protesters, contributing to widespread hopes for change and freedom.[80] Both online and offline media landscapes became active, with journalists, activists, and human rights defenders increasing their presence on social media and digital platforms.[81]

However, the optimism that followed the revolution gradually faded. Despite women being a driving force behind the 2019 uprising, their representation in the transitional government remained limited: only four women were appointed as ministers, and two held positions in the Sovereign Council. Beyond exclusion, women also faced targeted attacks. Women who joined the transitional government, along with other female activists, were subjected to waves of technology-facilitated gender-based violence.[82]

The increased mobilization of civil society has been accompanied by growing online abuse and public backlash. Since 2023, Sudan has descended into a protracted civil war between the Sudanese Armed Forces and the Rapid Support Forces, resulting in a severe humanitarian crisis and the collapse of civic space. In this context, digital platforms have become an additional terrain for violence. Both conflicting parties exploit social media platforms for disinformation, polarization, and intimidation. Platforms such as Facebook, WhatsApp, TikTok, and X have become tools for propaganda, surveillance, the spread of hate speech, and targeted harassment, particularly against women activists, journalists, and human rights defenders.[83,84,85]

"During the 2019 revolution, women were present in public spaces, and for the first time it felt like we were truly claiming and owning those spaces. However, after the revolution, there was a strong backlash against women. We witnessed a rise in online attacks, 'hon-

77 Data Reportal, *Digital 2025: Sudan*.

78 Data Reportal, *Digital 2018: Sudan*.

79 Al Jazeera, *"#Tasgut Bas: How Social Media Told the Story of Sudan's Uprising"*, 2019.

80 Harvard International Review, *The Women's Revolution: Female Activism in Sudan,* 2020.

81 Internews, *Sudanese Media Ecosystem,* 2025.

82 Hajar Karam, Hopes and Actions, *No Safe Space: The Global Reach of Online Gender-Based Violence, Sudan in Focus*, 2025.

83 Small Wars Journal, M. *Turner,* "Violent Non-State Actors and Generative AI in Warfare: The RSF and the Sudanese Civil War" *Small Wars Journal,* 2026.

84 Chr. Michelsen Institute (CMI), Samia al-Nagar, Liv Tønnesse, *From Emergency Response to Feminist Action: The Evolving Role of Women-Led Organizations in Sudan,* 2023.

85 Internews, Sudanese Media Ecosystem, 2025.

our' killings, and sexual harassment. Greater visibility for women was met with greater resistance. As women became more visible and vocal, violence escalated. Many continued to raise their voices, but they often paid a heavy price for doing so."

TFGBV in Sudan: patterns and interlinkages with conflict

Technology-facilitated gender-based violence is a growing concern in Sudan. Reported incidents include doxxing, cyberbullying, stalking, hate speech, blackmail, and intimidation.[86,87] Women are targeted not only because of their gender but also because of intersecting identities such as religion, ethnicity, profession and/or political affiliation. Being female in itself increases exposure to digital violence, with forms of abuse that differ in nature and intensity from those faced by male counterparts.[88] Exposure is intensified by patriarchal customs and a strong "blame culture", where stigma, fear and lack of trust in justice mechanisms discourages women from reporting abuse to family members or to the police.[89,90]

Consultations confirmed that restrictive gender norms limit women's freedom to express opinions publicly and online. As a result, women reportedly use online spaces but adopt coping strategies such as using pseudonyms or avoiding posting photos or sensitive content to reduce risks and protect their identity. One interviewee noted that women frequently continue to use digital platforms because they are among the few remaining spaces for expression and advocacy, even while knowing that these spaces expose them to heightened risks.

"When women cannot occupy public spaces safely, their digital presence becomes the next target."

"It happens at any level. Women are killed or harassed for going live on Facebook or posting pictures. There are even cases of women subjected to violence by family members due to their online activities."

TFGBV is also weaponized within Sudan's broader conflict dynamics. Armed groups use social media to terrorize communities, threaten activists, journalists and human rights defenders, and spread hate speech. In several cases, online incitement overlaps with, and exploits threats of, physical violence. In one widely circulated example, a female Rapid Support Forces fighter publicly called for soldiers to commit rape as a way of "purifying the bloodline,"[91] illustrating how digital incitement, misogyny, and conflict-related sexual violence can converge. This example is significant because it shows how online platforms are not merely reflecting violence offline but also contribute to normalizing and amplifying narratives that incite atrocities.

TFGBV against women human rights defenders

As in other contexts, the topics that women address online shape their exposure to TFGBV. Women who speak publicly about politics, human rights, gender equality, the war, or conflict-related abuses are primary targets of coordinated smear campaigns and digital violence.

"The main fear is that of surveillance and potential retaliation, especially as 'phone searches' are carried out. To avoid security risks, I am less vocal on social media. It is

86 Chr. Michelsen Institute (CMI), Samia al-Nagar, Liv Tønnesse, From Emergency Response to Feminist Action: The Evolving Role of Women-Led Organizations in Sudan, 2023.

87 *Global Voices Advox,* In Sudan, Women and Minorities Targeted by Online Harassment Lack Legal Protections, 2020.

88 Al-Sakkaf, Nadia. *Sudanese Women, Digital Revolution and Backlash*, SecDev Foundation, 2025.

89 *Ibid.*

90 UNICRI, Access to Justice in the Digital Age: Empowering Victims of Cybercrime in Africa, 2025.

91 Small Wars Journal, M. *Turner,* Violent Non-State Actors and Generative AI in Warfare: The RSF and the Sudanese Civil War, *Small Wars Journal,* 2026.

easier to use anonymous profiles if you are a woman in Sudan. Journalists mostly report from outside the country due to high risks, jail, disappearance, or violence. Online advocacy increases exposure to hate speech and threats. Digital threats easily translate into physical risks, especially in cases of doxxing."

Perpetrators include fundamentalist groups, political actors, government affiliates, and sometimes family members. The spectrum of risk ranges from online trolling and hacking to offline violence and retaliation. WHRDs, activists, and journalists play a vital role in documenting abuses and maintaining global attention on women's rights violations in Sudan. However, activism comes at a cost.[92] A key and unique study, *Sudanese Women, Digital Revolution and Backlash* by Dr. Nadia AlSakkaf, documents the extent of these risks. One activist recounted in this study:

"I published a post on Facebook about civil disobedience at the start of the revolution, and hell broke loose. I was arrested, my organization's activity was frozen, and its assets seized. My WhatsApp account was hacked, my photo deleted, and my contacts stolen from my phone and distributed in groups by an unknown person." [93]

Such examples show that online attacks often serve as gateways to physical suppression. Women activists have been targeted by politically motivated online smear campaigns involving fabricated images, false accusations, and rumours intended to discredit their work and reputation.[94] Image-based abuse is increasingly used against women activists and represents one of the most alarming manifestations of AI-driven harm, combining sexual violence, reputational attacks, and psychological trauma.[95] Women activists reported the manipulation of their images or voices to create false pornographic content and the circulation of these materials online. The more visible and active a woman is, the more organized the attacks may become.

"A few years ago, a group shared photos of me and my friends, several activists, including feminist and LGBTQ+ activists. They posted multiple pictures and added false captions. Today, it's even worse due to AI. In one case, an activist's voice was used in a pornographic video; in another, her face was inserted onto another body. You never really know who is behind these actions, it could be people from society, government security actors, or political groups."

These attacks often rely on sexual shame and reputation-based harm. Women described photoshopped images placing them in indecent positions, and rumours questioning their honour. Religion and culture are also weaponized to incite violence.

92 Chr. Michelsen Institute (CMI), Samia al-Nagar, Liv Tønnesse, From Emergency Response to Feminist Action: The Evolving Role of Women-Led Organizations in Sudan, 2023.

93 Al-Sakkaf, Nadia, Sudanese Women, Digital Revolution and Backlash, SecDev Foundation, 2025.

94 Chr. Michelsen Institute (CMI), Samia al-Nagar, Liv Tønnesse, From Emergency Response to Feminist Action: The Evolving Role of Women-Led Organizations in Sudan, 2023.

95 Stimson Center, *The Impact of Artificial Intelligence on Violence Against Women and Girls*, 2026.

"In 2016, an online platform failed to respond adequately to a serious threat. A Facebook page called "Sudaniat against Hijab" posted my picture without consent and falsely claimed that I was against the Hijab... In a context like Sudan, this is extremely dangerous, especially if religious fundamentalist groups see it, our lives can be at risk."[96]

The consequences can be immediate and severe.

"The impact was immediate. Some women stopped going to the office out of fear. We organised ourselves as a group and kept contacting Facebook. I compiled the information and sent a detailed file to Front Line Defenders, an organisation based in the Global North. They supported the case and engaged with Facebook, and eventually the page was taken down. We also tried to find out who was behind the page, but we were never given that information."

Yet, social media remains an important space for women and youth peer support, activism and advocacy, helping to spread awareness and amplify peace and security issues that otherwise receive limited attention. An interviewee emphasized that ***"youth use digital platforms to amplify voices and mobilize communities, yet this same visibility exposes them to hostility and targeted attacks. In other words, digital participation is simultaneously a source of empowerment and a source of risk."***

"In contexts such as Sudan, where civic space is limited and only a small number of activists can operate on the ground due to structural constraints, digital platforms play a crucial role in enabling participation, advocacy, and political engagement."

Despite these risks, Sudanese women have also developed forms of digital resistance. Before the 2023 conflict, a Facebook group called *Inboxat* (a tweak of the English word "inbox") was created to expose harassers by publishing inappropriate messages they had sent to women. Hashtags were also used to call out abuse and organize collective responses.[97]

What emerges is that online attacks are deeply embedded in broader systems of gender control and political repression. They are not isolated acts of online abuse, but part of wider strategies to silence dissent and punish women for their visibility.

Platforms and channels of dissemination

"Our life is increasingly online, including work, advocacy, and opportunities for writing and research. I use X and Facebook mainly for political engagement and activism."

"I use TikTok and Instagram primarily to stay up to date, but I am not very active on these platforms. I would describe myself mostly as a silent user. That said, online spaces are extremely important for movement-building."

Facebook is the most used social media platform in Sudan, with a dominant market share of approximately 77.57% as of 2026, while X, TikTok, and WhatsApp are also important for communication and news circulation, particularly during the conflict.[98,99]

96 Information about this case can also be found at: *Global Voices Advox,* In Sudan, Women and Minorities Targeted by Online Harassment Lack Legal Protections, 2020.

97 *Ibid.*

98 StatCounter Global Stats, *Social Media Stats in Sudan,* 2026.

99 Internews, Sudanese Media Ecosystem, 2025.

The consultations highlighted that several groups have tried to report fake posts, manipulated images, and abusive content to platform providers, but responses were often delayed or inadequate. Participants described cases in which women's photos were digitally manipulated, such as removing the hijab to trigger backlash, and circulated online. In some instances, despite being reported, such content was not removed by platforms. A frequently cited justification for inaction was the protection of "free speech". As a result, harmful content remains online, including manipulated images targeting women activists. This reflects a broader systemic lack of sensitivity to the cultural and security realities faced by women in conflict settings.

"What this shows is that platforms often do not understand the local context. For them, it may appear as free speech, but for us, it is a direct threat. When our pictures are stolen and used in this way, in a context where we could be harmed or even killed, this is not free speech."

"There is a lack of sensitivity and cultural understanding. Platforms are often slow to respond and fail to recognise that the risks women face, and the realities in different countries, are very different. The question remains: how can we better communicate to large tech companies that context matters, and that the needs and risks faced by women vary significantly across regions?"

5.3 Cross-case patterns

Despite the limitations of the consultations and the lack of comprehensive quantitative data on TFGBV against women operating in peace and security sectors in Sudan and Ukraine, the two case studies offer important insights into how technology-facilitated gender-based violence manifests in fragile and conflict settings. Several cross-cutting patterns emerge.

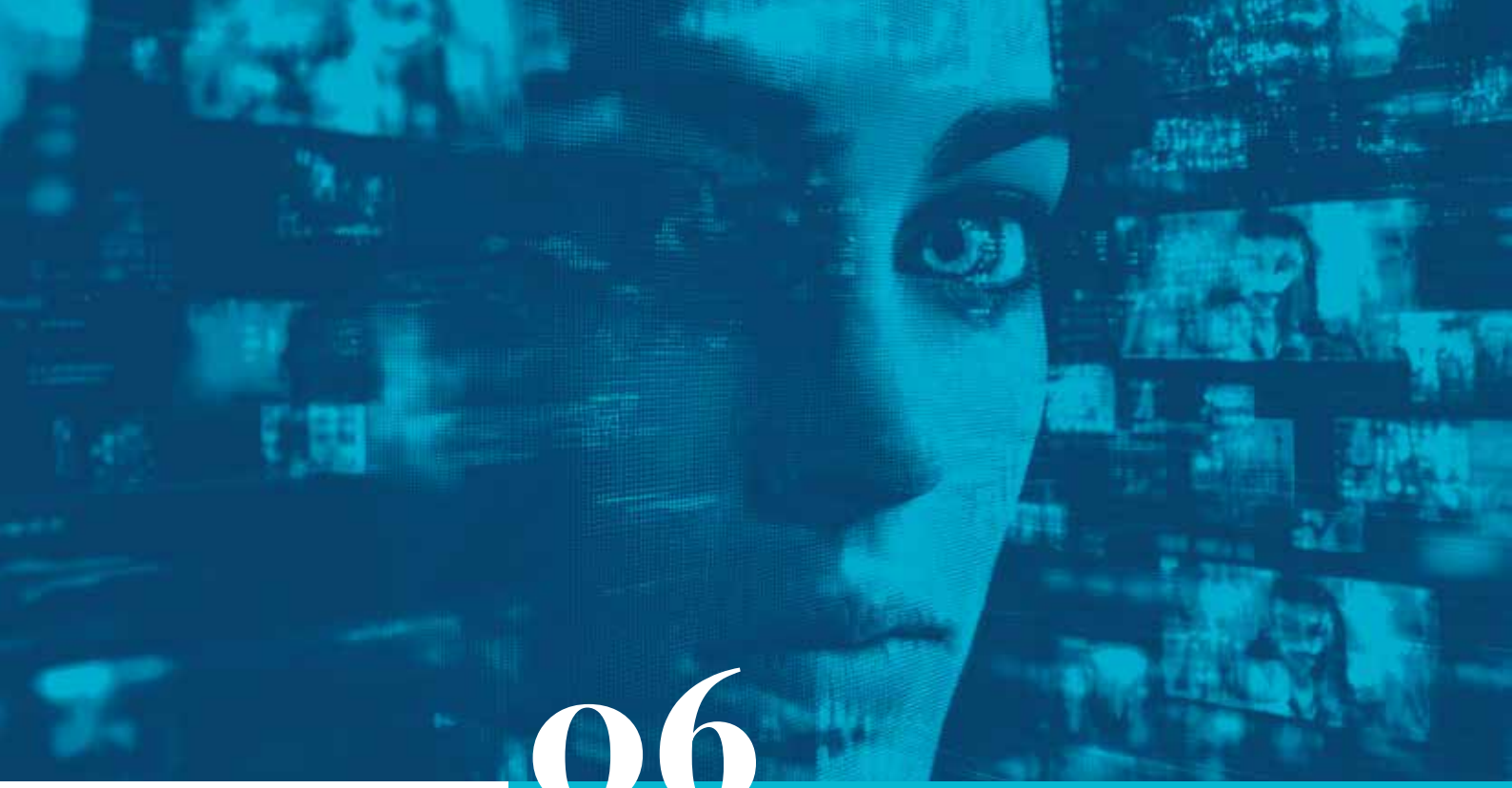
First, gender norms and stereotypes act as key drivers of TFGBV across both contexts. The persistence of restrictive gender norms and stereotypes regarding the roles women are expected to occupy remains a key barrier for women operating in security and public spaces, in Ukraine, in Sudan, and globally, particularly in the context of a broader backlash against women's rights and gender equality. In Ukraine, women's increasing presence in the armed forces and security sector has been actively weaponized through gendered disinformation campaigns and foreign disinformation manipulation efforts. These narratives reinforce the idea that women should remain in traditional, domestic roles and portray the presence of women in the armed forces as a sign of weakness of the Ukrainian army. In Sudan, women's visibility in public and political life, especially following the 2019 revolution, has similarly triggered backlash, with online and offline attacks used to punish women for transgressing the socially prescribed roles. Across both contexts, attacks frequently target women through narratives related to their appearance, sexuality, and morality as a means of discrediting, intimidating, and controlling them.

Second, the topics women engage with directly shape their exposure to violence. Women who speak out on politically sensitive issues, such as conflict, peacebuilding, human rights, gender equality are more likely to be targeted. In Ukraine, civil society actors noted that engagement on controversial or politically charged topics often results in increased online harassment and coordinated attacks. Similarly, in Sudan, women addressing issues related to governance, war, or rights violations face heightened risks, including smear campaigns, surveillance, and threats.

Third, there is a strong continuum between online and offline violence. TFGBV is not an isolated digital phenomenon but is deeply embedded within broader systems of violence and repression. Across both contexts, online abuse, including doxxing, disinformation, threats, and image-based violence, can translate into real-world consequences such as reputational harm, professional exclusion, harassment, arrest, or physical attacks. In Sudan in particular, this link is especially acute, with digital exposure sometimes leading directly to violence or retaliation. Perpetrators may include state and non-state actors, foreign actors, or individuals within communities, demonstrating that digital violence both reflects and amplifies existing conflict dynamics.

Finally, the impacts of TFGBV are severe, multidimensional, and cumulative. Across both contexts, exposure to online violence leads to significant psychological effects, including stress, anxiety, and trauma. Women human rights defenders, journalists, activists, and women in public-facing roles are highly aware of these risks, which often result in restrictive coping strategies. Self-censorship is widespread, with women limiting their participation in public discussions, avoiding sensitive topics, or disengaging from online spaces altogether. This can also lead to withdrawal from public and civic life, reducing participation in leadership, advocacy, and decision-making processes. At the same time, impacts manifest in context-specific ways. In Sudan, TFGBV is intertwined with systems of coercion, surveillance, and gendered repression, and online attacks can rapidly escalate into physical harm. In Ukraine, while psychological impacts are also significant, gendered disinformation campaigns particularly affect perceptions of women in the armed forces and may discourage potential recruits from joining. Disinformation targeting the families of military personnel can undermine trust in institutions and weaken social cohesion.

Across both contexts, TFGBV is not incidental but instrumental to silence, control, and exclude women with far-reaching implications for social cohesion, democratic participation, and peacebuilding.



CHAPTER 06

Conclusions and recommendations

6.1 Conclusions

This research demonstrates that different forms of technology-facilitated gender-based violence manifest in fragile and conflict settings. Several media sources, academic literature, and reports from international organizations and civil society have already documented and denounced the diverse forms of digital violence affecting women working in security, media, and peace advocacy roles. The case studies presented here further illustrate and confirm these findings.

TFGBV does not occur randomly but targets specific groups of women. The first target group analysed, although based on consultations held with Ukrainian stakeholders and limited available documentation, is women in armed and security forces. This group is targeted on two main grounds. First, they challenge traditional gender roles and social norms, disrupting expectations about the roles women are supposed to occupy. Second, their presence in the armed forces is instrumentalized to undermine the image of the military, portraying it as "weak" or diminished. These coordinated online attacks damage women's professional credibility and discourage their participation. The second target group, women leaders, civil society actors, journalists, and women's rights defenders in fragile and conflict settings, is also particularly exposed. They are targeted both because they challenge dominant narratives and because they denounce inequalities, abuses, and violations. Their visibility and public engagement make them strategic targets within broader political and conflict dynamics, where silencing their voices becomes a way to limit accountability and control public discourse.

As conflicts continue to spread across continents, and as violence and polarization increasingly permeate both online and offline spaces, this research shows that **TFGBV cannot be understood as an isolated phenomenon**. In fragile and conflict-affected contexts, conflict parties, individuals, and organized groups use digital platforms to destabilize, threaten, and inflict harm, targeting women as part of broader ideological struggles, power dynamics, and mechanisms of control.

These dynamics have **repercussions that extend beyond their impact on women and girls**. Technology-facilitated gender-based violence is not only a gender issue, but also a structural threat to **inclusive governance, human rights, and social cohesion.** When women in these roles are targeted, the messages they carry and the constituencies they represent are also undermined. In this sense, **TFGBV in fragile and conflict settings can also be understood as a peace and security concern,** as it contributes to instability, fuels polarization, and can be instrumentalized by conflict actors as part of broader strategies of intimidation, information manipulation, and control.

As a consequence, **the Women, Peace and Security agenda itself is weakened.** Designed to address the specific forms of violence affecting women and girls in conflict while promoting inclusive and lasting peace, it is directly challenged by the persistence and evolution of TFGBV. Addressing it is therefore not only a matter of protection, but also essential to ensuring meaningful participation and inclusive peace outcomes. Ultimately, TFGBV shapes who can participate, whose voices are heard, and what kind of peace is possible.

6.2 Recommendations

The following recommendations are directed at Member States, international organizations, civil society organizations, and digital platforms. While many of these recommendations may be challenging to implement in active conflict settings, several can and should be progressively adopted, even in fragile and insecure environments.

Strengthen the integration of digital dimensions within WPS

TFGBV has clear implications for the implementation of the Women, Peace and Security agenda. As highlighted in previous chapters, the use and abuse of digital technologies in general, and TFGBV in this context, play a role across all four pillars of the WPS agenda. Within each pillar, technology and digitalization can function as instruments and enablers of empowerment, but also as threats. In fragile and conflict settings, TFGBV should also be understood and addressed as a threat to peace and security, given its impact on participation, social cohesion, and stability. It is therefore important to strengthen efforts to address this issue. This can be done, for instance, by:

- Ensuring that statements delivered during WPS open debates, as well as National Action Plans, recognize both the opportunities and risks associated with digital technologies.
- Ensuring the inclusion of digital dimension, online evidence collection and concrete actions to address the impact of digital technologies and TFGBV on women's safety, freedoms, participation, and protection.

Promote multi-stakeholder efforts and dialogues

Strengthen coordination and planning of initiatives and dialogues involving Member States, civil society, technology platforms, and social media companies. These efforts should deepen understanding of how TFGBV manifests in conflict-affected contexts and ensure that gender dimensions are considered when addressing cyber threats in such settings. International, regional, and national-level awareness-raising initiatives should also be expanded.

Promote legal reforms

TFGBV is rapidly evolving in conflict settings, where digital technologies are increasingly weaponized. Legal frameworks often lag behind and fail to adequately protect women. It is recommended to:

- Introduce specific legal provisions that criminalize forms of digital violence, including image-based abuse, doxxing, and online harassment.
- Ensure that legal frameworks enable effective investigation and prosecution of TFGBV cases, including through the admissibility of digital evidence, and in contexts where perpetrators may include non-state armed actors or operate across jurisdictions.
- Establish safeguards to guarantee the privacy and protection of survivors, particularly in conflict contexts where reporting may expose victims to additional risks.
- Create safe and confidential reporting mechanisms to encourage women to come forward.

Strengthen digital platforms accountability

Digital platforms play a central role in addressing TFGBV, particularly in conflict settings where information ecosystems are polarized and manipulated and where disinformation, propaganda, and coordinated harassment are used as tools of intimidation and psychological warfare. Technology companies should:

- Strengthen content moderation systems and ensure the rapid removal of harmful and abusive content, particularly in high-risk contexts where such content may incite violence or lead to offline harm.
- Improve detection of coordinated campaigns, including bot-driven disinformation and gendered harassment, especially where these are linked to conflict actors, foreign information manipulation, or organized networks.
- Cooperate with national authorities, while respecting human rights standards where governance structures may be weak or fragmented, to address online abuse.
- Develop context- and culturally sensitive responses that account for the heightened risks faced by women in conflict environments, recognizing that content considered “low-risk” in one context may have severe consequences in another.
- Promote public–private partnerships aimed at strengthening effective prevention, response and accountability mechanisms related to TFGBV and the misuse of emerging technologies, such as AI, which can amplify gendered disinformation and abuse in conflict settings.

Strengthen training and capacity building

Capacity-building efforts are essential to address TFGBV in conflict settings. This includes:

- Training law enforcement and judicial actors to effectively investigate and prosecute digital violence.
- Enhancing cybersecurity awareness and digital safety skills for women, particularly those in high-risk roles such as journalists, activists, and members of the security sector, with specific attention to high-risk environments where digital threats may translate into physical harm
- Providing targeted training for civil society actors, journalists, women leaders, and relevant institutions on identifying and responding to disinformation campaigns, including gendered narratives.
- Establishing peer support structures and training for victims of TFGBV, as well as for family members who are also targeted.

Strengthen research and evidence

Further research is needed to better understand the nature, scale, and impact of TFGBV in conflict settings. In particular, more evidence is required on how digital violence affects women working in armed and security roles. This includes the collection of gender-disaggregated data, as well as analysis of:

- The type of online attacks against women in armed and security roles and their impacts.
- The role and effects of gendered disinformation campaigns, including those driven by foreign and conflict actors.
- Methods for collecting evidence of TFGBV in conflict settings.
- The implications of systematic online attacks against women human rights defenders, activists, leaders, and CSOs for democratic and inclusive governance.

Strengthen support structures

Strengthening support systems is critical in conflict contexts, where institutional protection may be limited. This includes:

- Expanding access to psychosocial, legal, and financial support for survivors of TFGBV.
- Supporting civil society organizations, women's rights organizations, and legal aid groups working on these issues.
- Encouraging visibility and solidarity mechanisms, whereby public exposure of cases can mobilize support networks and reduce isolation for survivors.

When cases are made visible, civil society actors can play a key role in advocating for justice, supporting victims, and countering harmful narratives.

Bibliography

- ACAPS. 2024. Yemen: Shedding Light on Technology-Facilitated Gender-Based Violence. https://www.acaps.org/fileadmin/Data_Product/Main_media/20240909_ACAPS_Middle_East_Hub__t echnology-facilitated_gender-based_violence_01.pdf.
- ACAPS and UNFPA. 2025. Technology-Facilitated Gender-Based Violence in Syria. https://www.acaps.org/fileadmin/Data_Product/Main_media/20250603_ACAPS_UNFPA_Syria_TFGBV.pdf.
- Al Jazeera, *#Tasgut Bas: How social media told the story of Sudan's uprising,* 2019.
- Al-Sakkaf, Nadia. 2025. Sudanese Women, Digital Revolution and Backlash. SecDev Foundation. https://secdev-foundation.org/wp-content/uploads/2025/06/Sudan-DVAW-2023-psychosocial-en.pdf.
- Amnesty International and Forbidden Stories. 2021. Pegasus Project. https://www.amnesty.org.uk/knowledge-hub/all-resources/pegasus-project-massive-data-leak-reveals-israeli-nso-groups-spyware-used-target.
- Association for Progressive Communications (APC). 2026. From Context to Collective Action. https://www.apc.org/en/blog/context-collective-action-outcomes-africas-first-symposium-technology-facilitated-gender-based.
- Association of Southeast Asian Nations. 2022. ASEAN Regional Plan of Action on Women, Peace and Security.
- Bangsamoro Autonomous Region. 2023. Regional Action Plan on Women, Peace and Security 2023–2028.
- BBC. 2022. "Ukraine's Women Soldiers." https://www.bbc.com/news/world-63491977.
- Centre for Information Resilience. 2024. Digital Battlefields. https://www.info-res.org/app/uploads/2024/11/Digital-Battlefields-FINAL.pdf.
- Chr. Michelsen Institute (CMI), Samia al-Nagar, and Liv Tønnessen. 2023. From Emergency Response to Feminist Action. https://www.cmi.no/publications/9830-from-emergency-response-to-feminist-action-the-evolving-role-of-women-led-organizations-in-sudan.
- DataReportal. 2025. Digital 2025: Sudan. https://datareportal.com/reports/digital-2025-sudan.
- Derechos Digitales, Response to the Call for Inputs on Technology-Facilitated Gender-Based Violence and its Impact on Women and Girls, submitted to the Office of the United Nations High Commissioner for Human Rights (OHCHR), 2025. Available at: https://www.derechosdigitales.org/wp-content/uploads/OHCHR-TFGBV-1.pdf.
- Deutsche Welle (DW). 2023. «Жінки в ЗСУ.» October 9. https://www.dw.com/uk/жінки-в-зсу-бажання-слузити-сприймають-за-примху/a-66995226.
- Detector Media. 2023. "Shell of Femininity with a Dark Core." August 30. https://en.detector.media/post/shell-of-femininity-with-a-dark-core-how-propaganda-attempts-to-discredit-ukrainian-women/.
- Economist Intelligence Unit. 2021. Measuring the Prevalence of Online Violence Against Women.

- European Parliament. 2026. EPRS Briefing: Women in Conflict Zones. https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/782670/EPRS_BRI(2026)782670_EN.pdf.
- Fal-Dutra Santos, Agnieszka, and Outi Donovan. 2025. "Between Contested Narratives." International Feminist Journal of Politics 27 (2): 425–453.
- Forbes. 2026. David Hambling, "A Woman's Place Is in the Drone War." March 25.
- Front Line Defenders and Access Now. 2022. Unsafe Anywhere. https://www.frontlinedefenders.org/sites/default/files/unsafe-anywhere-women-human-rights-defenders-speak-out-about-pegasus-attacks_en.pdf.
- Geetha, R. 2024. "The Impact of Online Harassment." International Journal of English Literature and Social Sciences 9 (6).
- Global Center on Cooperative Security and RUSI. 2023. The Impact of Gendered Narratives in Ukraine. https://www.globalcenter.org/wp-content/uploads/GCCS-RUSI-2023-PB-Impact-Gendered-Narratives-Conflict-Ukraine.pdf.
- Global Voices Advox. 2020. "In Sudan, Women Targeted by Online Harassment." https://advox.globalvoices.org/2020/10/04/in-sudan-women-and-minorities-targeted-by-online-harassment-lack-legal-protections/.
- Government of the Philippines. 2023. National Action Plan on Women, Peace and Security 2023–2033.
- Hajar Karam, Hopes and Actions, No Safe Space: The Global Reach of Online Gender-Based Violence, Sudan in Focus, 2025.
- Harvard International Review, The Women's Revolution: Female Activism in Sudan, 2020.
- Harvard Kennedy School Carr-Ryan Center. "Women, AI, and Digital War-Fighting." https://www.hks.harvard.edu/centers/carr-ryan/our-work/carr-ryan-commentary/women-ai-and-digital-war-fighting-invisible.
- Heinrich Böll Foundation. 2024. "Gender Misinformation and Rape Culture." https://ua.boell.org/en/2024/02/27/gender-misinformation-and-rape-culture.
- ICRC Blogs. 2024. "Online Violence, Real Life Impacts." https://blogs.icrc.org/law-and-policy/2024/01/04/online-violence-real-life-impacts-women-girls-humanitarian-settings/.
- Internews. 2025. Sudanese Media Ecosystem. https://internews.org/wp-content/uploads/2025/10/Internews-Sudan-media-mapping-2025-V2.0.pdf.
- International IDEA. 2025. "Violence Against Women in the Digital Space." https://www.idea.int/blog/violence-against-women-digital-space-growing-threat-democracy.
- Inter-Parliamentary Union (IPU). 2025. Sexism, Harassment and Violence against Women in Parliaments: Asia-Pacific. https://www.ipu.org/news/press-releases/2025-03/60-women-mps-asia-pacific-report-online-gender-based-violence.
- Internet Governance Forum. Best Practice Forum on Gender and Digital Rights.
- ITU. Facts and Figures.
- Kähkönen, Merja E. 2025. "Transformative Peace for Women in Ukraine?" International Affairs 101 (6). https://academic.oup.com/ia/article/101/6/2019/8315399.
- Smit, H. 2022. Learning Brief: Risks of Technology-Facilitated GBV. GBV AoR Helpdesk. https://gbvaor.net/node/1789.
- StatCounter Global Stats. 2026. Social Media Stats Sudan. https://gs.statcounter.com/social-media-stats/all/sudan.
- Stimson Center. 2026. Impact of AI on Violence Against Women. https://www.stimson.org/2026/the-impact-of-artificial-intelligence-on-violence-against-women-and-girls/.

- SUWRA. 2025. The Hell on Earth: Systemic Attacks in Sudan. https://drive.google.com/file/d/13DBZXoz-Rul02GseT875CA2x6ZEMjyEby/view.
- Syrian Female Journalists Network (SFJN), *Digital Violence: Syrian Women Journalists and Human Rights Defenders in the Digital Space: Risks and Threats*, 2018, available at: https://media.sfjn.org/wp-content/uploads/2018/01/Digital-Violence-Report_English.pdf.
- Texty.org.ua. "AI and TikTok: Journalists Turned into Fakes." https://texty.org.ua/projects/116307/cshtuchnyj-intelekt-i-tiktok-yak-vidomyx-zhurnalistok-peretvoryuyut-na-fejky/.
- Turner, M. 2026. "Violent Non-State Actors and Generative AI: RSF in Sudan." Small Wars Journal. https://smallwarsjournal.com/2026/02/11/generative-ai-sudan-civil-war/.
- UN Human Rights Council. 2018. Report of Special Rapporteur: Online Violence. A/HRC/38/47.
- UN Human Rights Council. 2023. Report of Special Rapporteur: Freedom of Expression. A/HRC/53/25.
- UN Security Council. Various. Reports S/2019/800; S/2020/946; S/2021/827; S/2022/740; S/2023/725; S/2025/556.
- UNFPA. n.d. The Virtual Is Real. https://www.unfpa.org/thevirtualisreal-background.
- UNICRI, *Access to Justice in the Digital Age: Empowering Victims of Cybercrime in Africa*, 2025. Available at: https://unicri.org/sites/default/files/2025-08/Cybercrime_Africa_web_0.pdf.
- UNIDIR. 2021. System Update: Women, Peace and Cybersecurity. https://unidir.org/files/2021-09/UNIDIR_System_Update.pdf.
- UNODC. Cyberstalking and Cyberharassment. https://www.unodc.org/cld/ar/education/tertiary/cybercrime/module-12/key-issues/cyberstalking-and-cyberharassment.html.
- UNESCO. 2021. The Chilling: Online Violence Against Women Journalists. https://unesdoc.unesco.org/ark:/48223/pf0000377223.
- Women in Media Ukraine, *Her Voice, Their Target: Gendered Online Violence Against Ukrainian Women Journalists*, 2025.