Definitional Annex

In this section

This Annex is meant to be read in conjunction with the toolkit and provides further definitions and context on the TFGBV super-types of harm. The Annex also collates foundational literature, existing TFGBV taxonomies, relevant legal and policy frameworks, and jurisdictional harms landscape literature to support implementation and situate the taxonomy within broader research, policy, regulatory, and practice contexts.

Glossary

Purpose

Definitions of TFGBV harms vary widely across organizations, sectors, and jurisdictions, and often emphasize different elements of behavior, intent, or impact. For this reason, the glossary presents multiple definitions for each super-type of harm, rather than a single consolidated definition. This approach highlights key areas of convergence and divergence, surfaces definitional gaps, and supports more nuanced, context-aware application of the taxonomy across policy, regulatory, legal, platform, and prevention settings.

Definitions of harm super-types

The TFGBV harms super types include online harassment, online impersonation, account access control, intimate image abuse (IIA), and sexual extortion.

Synonyms and Variants

Cyberbullying
Online abuse
Digital harassment
Cyber harassment
Online sexual harassment
Harassment/spamming
Networked harassment
Cross-platform harassment

Definition(s)

United Nations Population Fund, UNFPA: "Online harassment is the use of technology to repeatedly contact, annoy, threaten or scare another person. Online harassment is an ongoing behavior over time rather than an isolated incident. Online harassment can be perpetrated by a single individual or mobs of individuals (mobbing), usually networks of male perpetrators who target women and minorities. When online harassment is perpetrated on the basis of the survivor's gender, sexuality or sexual orientation it constitutes a form of TFGBV".

Humane Intelligence: "Online harassment is an umbrella term that encompasses a wide range of behaviors via technology intended to silence or intimidate a target. It often includes repeated hostile messages, direct threats of violence, and offensive or abusive comments (including expression of sexism, racism, xenophobia, homophobia, transphobia or ableist prejudices). It may include coordinated pile-on attacks or sustained harassment campaigns by formal groups or informal groups intended to overwhelm the target".

Centre for International Governance Innovation, CIGI: "Harassment encompasses a variety of unwanted digital communication. It can involve a brief incident, such as a single targeted racist or sexist comment, or a long-term organized attack."

Sub harms definitions

Doxxing: Defined by UNFPA as "Gendered form of online harassment that consists of non-consensual disclosure of personal information involving the public release of an individual's private, personal, sensitive information, such as home and email addresses, phone numbers, employer and family member's contact information, or photos of their children and the school they attend with the purpose of locating and causing physical harm."

Cyberstalking: Defined by UNFPA as “Severe form of cyberobsessional pursuit, motivated by relational control or destruction, that consists of the use of technology to repeatedly stalk and monitor someone’s activities and behaviors in real-time or historically and that causes the survivor to feel fear”.

Inappropriate content: Humane Intelligence notes that “this abuse manifests when perpetrators intentionally share graphic violence, pornography, self-harm content, or other disturbing material with targets to cause psychological distress, desensitize them to abuse, or create trauma responses. Common tactics include sending unsolicited violent imagery, sharing content depicting sexual violence to normalize abuse, or exposing vulnerable individuals to content that triggers existing trauma. The harm occurs when individuals encounter this content without adequate preparation or when it's used to isolate, manipulate, or groom vulnerable individuals. Perpetrators may share such content directly with targets or create environments where targets are likely to encounter it.”

Flaming: Defined by UNFPA as the “posting or sending offensive messages over the Internet. These messages, called “flames”, may be posted within online discussion forums or newsgroups, or sent via email or instant messaging programs. The most common area where flaming takes place is online discussion forums”.

Dogpiling or mobbing: Also called cybermobbing or networked harassment, mobbing or dogpiling are defined by UNFPA as ”organized, coordinated and systematic attacks by a group of people against particular individuals or issues, such as by groups that target feminists or people who post about racial equality issues online. Outrage or shame mobs are a form of mob justice focused on publicly exposing, humiliating and punishing a target, often for expressing opinions on politically charged topics or ideas the outrage mob disagrees with and/or has taken out of context in order to promote a particular agenda.”

Slut-shaming: Defined by UNFPA as ”a form of gender-based bullying often targeting teenage girls and LGBTQIA+ people, that consists of criticizing if they do not conform to social expectations regarding behavior, appearance and sexuality, often rooted in gender norms. Slut-shaming, stalking, the use of non-consensual photography and sexual surveillance frequently overlap, amplifying impact on targets.”

(Gendered or sexist) hate speech: Defined by UNFPA as ”any kind of communication in speech, writing or behavior, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in this case, based on their sex, gender, sexual orientation or gender identity. Gendered and sexist online hate speech reinforces systemic sexism while dehumanizing and encouraging violence against women and girls and LGBTQIA+ people”.

Cross-platform harassment: Defined by UNFPA as “coordinated and deliberately deployed harassment against a target, by a single harasser or a group of harassers, across multiple online spaces, social media and communication platforms, taking advantage of the fact that most platforms only moderate content on their own sites”.

Astroturfing: Defined by UNFPA as “Dissemination or amplification of content (including abuse) that appears to arise organically at the grass-roots level and spread, but is actually coordinated (often using multiple fake accounts) by an individual, interest group, political party or organization”.

Zoom-bombing: Defined by UNFPA as ”when people join online meetings or gatherings in order to post racist, sexist, pornopgraphic or antisemitic content to shock or disturb viewers in order to disturb viewers, it is a form of networked harassment.

Intimate Image Abuse (IIA)

Synonyms and Variants

Non-consensual explicit imagery (NCEI)
Non-consensual intimate image sharing (NCIIS)
Non-consensual intimate image abuse (NCII)
Image-based sexual abuse (IBSA) Online sexual harassment
Non-consensual image abuse
Image-based abuse
Non-consensual distribution of intimate images (NDII)
Revenge porn *(misnomer)*
Non-consensual pornography *(misnomer)*

Definition(s)

Humane Intelligence: "Intimate image abuse (IIA), formerly (and mistakenly) termed "revenge porn", involves the producing, reproducing and/or sharing of intimate images or videos without the depicted person's consent. The shift away from the older moniker emphasizes that the root of the issue isn't solely spiteful ex-partners seeking retaliation, but comprises a serious violation of privacy and consent. IIA is a persistent challenge for platforms that permit explicit content: distinguishing between consensual and non-consensual material is not always possible from content alone. Additionally, sexual content that may have been consensually recorded can be later shared non-consensually, further challenging an already fraught dilemma".

United Nations Population Fund, UNFPA: "Image-based abuse: use of images to coerce, threaten, harass, objectify or abuse. Deepfakes, non-consensual sexual imagery created using AI tools, are a form of image-based abuse".

Chayn & End Cyber Abuse: "Image-based abuse includes all forms of non-consensual taking, creating, altering, or sharing of (including threats to share) intimate images or videos. While this is generally understood as referring to sexual or nude images, we define ‘intimate images’ as any image which shows someone as they would not normally be seen in public. For example, for someone who usually wears a headscarf or other form of religious garb, a photograph of them without it would constitute an intimate image. Image-based abuse is often referred to as ‘revenge porn’, but this term is generally rejected as such material should not be viewed as porn nor revenge and the term obscures the complexity of the issue".

Centre for International Governance Innovation, CIGI: "The non-consensual distribution of intimate images, which is often problematically described as revenge porn, occurs when a person’s sexual images are shared with a wider than intended audience without the subject’s consent”.

European Institute for Gender Equality, EIGE: "Non-consensual intimate image (NCII) abuse against women and girls involves the distribution through ICT means or the threat of distribution through ICT means of intimate, private and/or manipulated images/videos of a woman or girl without the consent of the subject. Images/videos can be obtained non-consensually, manipulated non-consensually, or obtained consensually but distributed non-consensually. Common motivations include sexualizing the victim, inflicting harm on the victim, or negatively affecting the life of the victim".

Sub harms definitions

Non-consensual pornography or “revenge porn” (misnomer): Humane Intelligence refers to “revenge porn” as a “misnomer”, while Chayn and End Cyber Abuse’s Taxonomy note, “Image-based abuse is often referred to as ‘revenge porn’, but this term is generally rejected as such material should not be viewed as porn nor revenge and the term obscures the complexity of the issue”.

Voyeuristic recording (creepshots, upskirting, downblousing): Defined by UNFPA that ”these forms of IBA and sexual surveillance involve taking non-consensual photos or videos of survivors, mainly women and girls, in public places such as stores, public bathrooms, locker rooms, classrooms or the street; but also in their own apartments. They may entail taking images up a person’s dress or skirt (upskirting), taking a sexually suggestive picture of a woman without her noticing (creepshot) or surveilling or surreptitiously observing with the use of technological tools, and in some cases recording, another person in what would generally be regarded as a private place (digital voyeurism).”

Unsolicited sexual content, cyberflashing: Defined by UNFPA as a ”form of image-based abuse whereby a person sends an unsolicited image of their genitals or sexually explicit materials to another person without their consent. Also referred to as “dick pics”, cyberflashing is a form of unsolicited pornography which refers more widely to “sending unsolicited pornography, violent rape porn gifs or photographs in which a target’s photograph has been sexualized”.

Documenting/broadcasting sexual assault: Documenting or broadcasting sexual assault (rape videos) is defined by UNFPA as ”recording and/or disseminating images of sexual assault on social media, via text or on websites. This is an additional form of sexual violence against the victim-survivor.220 These videos may be subsequently used to shame or extort survivors, or are sold as non-consensual porn”.

Deceptive synthetic media: Defined by Humane Intelligence as "images, videos, or audio that has been altered or entirely created using artificial intelligence or other digital software to falsely depict real individuals, often with the goals to deceive, harass, or exploit targets. The creation of such deceptive synthetic media is done without the consent or knowledge of the individuals in question.”

Online Impersonation

Synonyms and Variants

Fake profile impersonation
Profile spoofing
Digital identity fraud
Catfishing
Social media account cloning
Email/messaging impersonation
Deepfake impersonation
Identity theft

Definition(s)

Humane Intelligence: "The unauthorized use of another person's identity or likeness on digital platforms to deceive, manipulate, or harm them or others...The use of a target's online identity or persona for personal gain or to harass, threaten, or smear their target”.

Chayn & End Cyber Abuse: "Impersonation is when a perpetrator uses technology to pretend to be someone else. Typically, a perpetrator creates fake social media accounts using the name and image of the person they are impersonating. They may use these accounts to share content or send messages that are harmful to the person in question, such as sending obscene or offensive messages to their personal or professional contacts".

United Nations Population Fund, UNFPA: "Impersonation is the process of stealing someone's identity so as to threaten or intimidate, as well as to discredit or damage a user's reputation".

UN Women & WHO Joint Programme: "Creation of a hoax social media account, often using the target's name and/or photo, to post offensive or inflammatory statements to defame, discredit, or instigate further abuse. A harasser can also impersonate someone the target knows in order to cause harm".

Social Development Direct: "Is the use of digital technology to assume the identity of a person or someone else to access private information, exploit, embarrass, discredit, or shame them, contact or mislead them, or create fraudulent documents. Gendered examples include creating fake social media accounts and websites to groom and recruit girls and women into sex trafficking, and romantic scams where women are scammed out of money".

Sub harms definitions

Catfishing: Defined by UNFPA as "Internet scam where the abuser pretends to be someone they are not, by creating false online identities in social media – often using other people's photos and developing extensive fake life stories and experiences, jobs and friends – with the objective of seducing another person or making them believe they are in an online relationship and use this as a means to ask for money, gifts or intimate images".

Sexual Extortion

Synonyms and Variants

Sextortion
Sexual blackmail
Intimate image extortion

Definition(s)

Humane Intelligence: "Extortion that either uses the release of intimate data as the threat and/or that extorts sexual favors from the target".

Equality Now: "Online sexual coercion and extortion refers to sexual exploitation and abuse when the means of coercion is abuse of power through threats or sharing sexual images or information online. Online sexual coercion and extortion can result in CSAM, live-streaming of sexual abuse, image-based sexual abuse, and online sex trafficking".

Centre for International Governance Innovation, CIGI: "Occurs when an individual has, or claims to have, a sexual image of another person and uses it to coerce a person into doing something they do not want to do. By threatening to release the image unless the other person does as they are asked, the person claiming to have the images is able to obtain additional sexual images, unwanted sexual activity, the continuation of a romantic relationship, engagement in human

trafficking, money or other things from the victim-survivor".

Organization of American States, OAS: "This form of violence can have various manifestations, such as sexual attacks organized or planned through ICTs or sexual violence following the online publication of the victim's personal data leading to their location (doxing); It can also occur when a perpetrator befriends a person online to get to know them and then sexually abuse them (as can occur with dating apps), or when a perpetrator forces a person to engage in sexual relations under the threat of publishing intimate or sexual information about them (sextortion)".

Sub harms definitions

Grooming: Defined by UNFPA as Specific type of technology-facilitated sexual experience by which children and young people are contacted through social media or other digital platforms with the purpose of sexually assaulting them. Online grooming consists of setting up an online abusive relationship with a child, in order to bring the child into sexual abuse or child-trafficking situations.

Account Access Control

Synonyms and Variants

Hacking

Definition(s)

Humane Intelligence: "Gaining access to someone's digital accounts without permission or exploiting access to someone's accounts to monitor, control, or harm them"..."Once inside, perpetrators can use that access for a number of forms of abuse, such as cyberstalking (read private messages, monitor activity, etc), to restrict a target's access to their own or shared accounts, services, and data, (changing settings, locking victims out by changing passwords, etc) or impersonate them, often as part of a broader pattern of digital abuse".

Organization of American States, OAS: "They consist of intentional acts to censor and harm women's organizations, including attacks on their channels of expression, such as accessing them without consent or hacking internet sites, social networks, or email accounts to undermine their operation; getting the organization's profile or social networks taken offline by using community standards to denounce content that the platform considers sensitive; denial of service (DoS) attacks, domain use restrictions or domain theft, and internet blackouts during a meeting or protest".

United Nations Population Fund, UNFPA: "Use of technology to gain illegal or unauthorized access to systems or resources to acquire personal information, alter or modify information, slander and denigrate the survivor, and / or exert violence against women's organizations".

Social Development Direct: "Can be perpetrated through the misuse of technology, including monitoring someone's activities on social media, and stalking and surveillance through tracking someone's location through existing software on their digital devices or through installing stalkerware. Stalking and monitoring is often repeated and can be an extension of IPV. In addition to stalking and monitoring through phones and personal digital devices, perpetrators can use other technologies, including the internet of things, such as smart home devices and drones to monitor and control women".

Tecnologia & Derechos Humanos, TEDIC: "Unauthorized attacks to gain access

to another person's accounts or devices. This may involve the unauthorized collection of information, as well as the blocking or deactivation of the victim's account; or the use of the hacked account to engage in behaviors that cause discredit or damage to the reputation of the account holder".

The Centre for Research & Education on Violence Against Women & Children, Learning Network: "Using technology to gain illegal or unauthorized access to systems or resources for the purpose of acquiring personal information, altering or modifying information, or slandering and denigrating the victim and/or VAW organizations".

Project Catalyst Definitions

Project Catalyst relies on a set of core definitions, that are crucial for analyzing when and if TFGBV meets targeted hate and violent extremism. We therefore define these here:

Definitions

Targeted Hate & Violence: targeted hate and violence, including subtypes of gender-based hate:

1. Actively dehumanizes other people by seeking to elevate the position of members in one group while diminishing that of non-members based on a particular protected characteristic1 of those people;

2. Advocates for or uses violence to realize that dehumanization; and,

3. Tolerates, supports, actively calls for, or directly uses violence against civilians or critical civilian infrastructure. (Lamphere-Englund & Thompson, 2024).

Violent Extremism (VE): violent extremism is defined as a type of mobilization which:

1. Promotes ideological, political, or religious aims;

2. Advocates for or uses violence to realize those aims; and

3. Tolerates, supports, actively calls for, or directly uses violence against civilians or critical civilian infrastructure. (Lamphere-Englund & Thompson, 2024).

Terrorism:

1. The perpetration of a criminal act (such as murder, kidnapping, hostage-taking, arson, and so on), or threatening such an act;

2. The intent to spread fear among the population (which would generally entail the creation of public danger) or directly or indirectly coerce a national or international authority to take some action, or to refrain from taking it.

Additional Resources & Further Reading

This section collates additional resources referenced throughout the toolkit, as well as related materials that may support implementation. The resources include foundational literature and principles underpinning this toolkit, existing TFGBV taxonomies, relevant legal and policy frameworks, as well as the landscape of TFGBV harms in Kenya, Canada and Jordan. Together, they support readers in situating the taxonomy within broader research, policy, regulatory, and practice contexts.

Literature

These resources provide further context on the theoretical foundations, harms landscape, and prevention approaches referenced throughout the toolkit.

TFGBV, Misogyny, Gender, and Violent Extremism

- Jankowicz, N., Gomez-O'Keefe, I., Hoffman, L., & Vidal Becker, A. It's Everyone's Problem: Mainstreaming Responses to Technology-Facilitated Gender-Based Violence.
- Liz Kelly, "The continuum of sexual violence." Women, violence and social control. London: Palgrave Macmillan UK, 1987. 46-60.
- Bettina Rottweiler, Caitlin Clemmow & Paul Gill, 'A Common Psychology of Male Violence? Assessing the Effects of Misogyny on Intentions to Engage in Violent Extremism, Interpersonal Violence and Support for Violence against Women, Terrorism and Political Violence', DOI: 10.1080/09546553.2023.2292723.
- Alexandra Phelan, Jessica White, Claudia Wallner, James Paterson. Misogyny, Hostile Beliefs and the Transmission of Extremism: A Comparison of the Far-Right in the UK and Australia.
- Joshua M. Roose, Joana Cook, Supreme Men, Subjected Women: Gender Inequality and Violence in Jihadist, Far Right and Male Supremacist Ideologies.
- Cynthia Miller-Idriss, How Misogyny Fuels Violent Extremism.
- Cynthia Miller-Idriss, Man Up: The New Misogyny and the Rise of Violent Extremism.
- O'Hanlon R, Altice FL, Lee RK, LaViolette J, Mark G, Papakyriakopoulos O, Saha K, De Choudhury M, Kumar N. Misogynistic Extremism: A Scoping Review. Trauma Violence Abuse. 2024 Apr;25(2):1219-1234. doi: 10.1177/15248380231176062.
- Vink, D., Abbas, T., Veilleux-Lepage, Y., & McNeil-Willson, R. "Because They Are Women in a Man's World": A Critical Discourse Analysis of Incel Violent Extremists and the Stories They Tell. Terrorism and Political Violence, 36(6), 723–739.
- Gentry, C. E. Misogynistic terrorism: it has always been here. Critical Studies on Terrorism, 15(1), 209–224.
- Hoffman, B, Ware, J & Shapiro, E, 'Assessing the threat of incel violence', Studies in Conflict and Terrorism, vol. 43, no. 7, pp. 565-587.
- Down Girl: The Logic of Misogyny, Kate Manne.
- Caitlin Clemmow, Bettina Rottweiler, Elizabeth Pearson, Paul Gill, Public or private violence? Understanding the overlap between intimate partner abuse and susceptibility to violent extremism.

- Lone wolf terrorism through a gendered lens: men turning violent or violent men behaving violently? Jude McCulloch, Sandra Walklate, JaneMaree Maher, Kate Fitz-Gibbon, Jasmine McGowan.
- Pablo Castillo Díaz and Nahla Valji, SYMBIOSIS OF MISOGYNY AND VIOLENT EXTREMISM.
- ISD Explainer: The Manosphere. Institute for Strategic Dialogue (ISD).
- "764." ISD Global Explainers, Institute for Strategic Dialogue (ISD).
- Paula-Charlotte Matlach and Charlotte Drath, The 'cost of doing politics'? Gendered abuse and digital platforms' role in undermining democracy, Institute for Strategic Dialogue (ISD).
- Paula-Charlotte Matlach, Charlotte Drath, Allison Castillo, Martin Degeling Content, Crushing Comments: Gendered Harassment During the 2024 EU Parliament Elections on TikTok. Institute for Strategic Dialogue (ISD).

Sexual Exploitation, Sextortion, and Gendered Harms

- Karlsson, J., & Corneteg, N. "Then 'she' took a screenshot and it all began": A report on financial sextortion of children, with particular focus on the vulnerability of boys. ECPAT Sweden.
- Technical document of the Global Manifesto. Global Alliance for the Protection of Boys from Sexual Violence.
- Nordin, T., et al. A scoping review of masculinity norms and their interplay with loneliness and social connectedness among men in Western societies. American Journal of Men's Health, 18(6).

Trafficking, Recruitment, and Gender-Based Exploitation in Extremism

- Binetti, Ashley. A New Frontier: Human Trafficking and ISIS's Recruitment of Women from the West. Washington, DC: Georgetown Institute for Women, Peace and Security, 2015.

Prevention and Risk Frameworks

- Reimer, Jordan, Public Health Approach to Prevention. Institute for Strategic Dialogue (ISD).
- Sara Bundtzen, Misogynistic Pathways to Radicalisation: Recommended Measures for Platforms to Assess and Mitigate Online Gender-Based Violence. Institute for Strategic Dialogue (ISD).
- Zoe Manzi, Helena Schwertheim, Fabienne Tarrant, Sid Venkataramakrishnan, Carolin von Bredow, Fostering Healthy Masculinities: Building Resilience Against Online Misogyny, Institute for Strategic Dialogue (ISD).
- Omar Salem, "Searching for Safer, Healthier Digital Spaces," Search for Common Ground (April 2024).
- Search for Common Ground, A Social Network Assessment of Influencers and Communication Channels.
- Search for Common Ground, Envisioning a Path Forward Building an Evidence Base for the Sudanese National Strategy to Prevent, Counter & Transform Violent Extremism.
- Search for Common Ground, MEET ME AT THE MASKANE: A Mapping of Influencers, Networks, and Communication Channels in Kenya and

Tanzania.

Taxonomies, Frameworks, and Mappings of THGBV

These resources informed the development of the Harms Taxonomy and include TFGBV taxonomies and frameworks; conceptual and analytical guides; glossaries and terminology resources; mapping and landscape analysis; and practical guides. These resources also provide further detail on the individual, community, and societal impacts of TFGBV.

Table 1: Taxonomies, classifications, and frameworks consulted for our Harms Taxonomy

Organization	*Date*	*Taxonomy / Framework / Classification (hyperlinked)*
The United Nations Population Fund (UNFPA) Taxonomy	**2025**	• An Infographic Guide to Technology-facilitated Gender-based Violence
Humane Intelligence Taxonomy	**2025**	• Tech-Facilitated Gender-Based Violence
World Wide Web Foundation & Women's Rights Online Framework	**2024**	• From theory to practice: Building and testing a framework for definitions of online gender-based violence and other terms • Database: Airtable document that centralizes the mapped terminologies and manifestations
Chayn & End Cyber Abuse Taxonomy	**2022**	• Taxonomy of Tech Abuse • Orbits: a global field guide to advance intersectional, survivor-centred and trauma-informed interventions to TGBV
Association for Progressive Communications (APC) **Taxonomy**	**2017**	• Online gender-based violence: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences o *citing Internet Governance Forum (IGF) 2015: Best Practice Forum (BPF) on Online Abuse and Gender-Based Violence Against Women*
The United Nations Population Fund (UNFPA) **Framework**	**2021**	• Technology-facilitated Gender-based Violence: Making All Spaces Safe
The United Nations	n.d.	• Technology-Facilitated Gender-Based

Population Fund (UNFPA) Glossary		Violence: A Growing Threat
Centre for International Governance Innovation (CIGI) Mapping	**2020**	• Technology-Facilitated Gender-Based Violence: An Overview
Social Development Direct **Mapping**	**2023**	• Global Partnership TFGBV Preliminary Landscape Analysis
The Centre for Research & Education on Violence Against Women & Children, Learning Network Taxonomy	**2013**	• Technology-Related Violence Against Women
Equality Now **Framework**	n.d.	• Tech-facilitated gender-based violence (TFGBV)
UN Women & WHO Joint Programme **Mapping**	**2023**	• Technology-Facilitated Violence Against Women: Taking Stock of Evidence and Data Collection
European Institute for Gender Equality (EIGE) Glossary	**2022**	• Cyber Violence against Women and Girls Key Terms and Concepts
Luchadoras Mapping	2024	• LA VIOLENCIA EN LÍNEA CONTRA LAS MUJERES EN MÉXICO
Organization of American States (OAS) **Framework**	**2021**	• Online gender-based violence against women and girls: Guide of basic concepts
CyberSafe Project Mapping	**2020**	• Cyber Violence Against Women & Girls Report
ICRW - International Center for Research on Women **Framework**	**2019**	• TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE: WHAT IS IT, AND HOW DO WE MEASURE IT
TEDIC - Tecnologia	**2024**	• Tipos de violencia de género facilitada

& Derechos Humanos Framework		por la tecnología
Gender-Based Violence Area of Responsibility (UNFPA)	**2023**	• Learning Brief 1: Technology-facilitated gender-based violence in humanitarian contexts
CHAYN Guide	**2025**	• DIY Online Safety Guide

TGBV Harms Landscapes and Legal Frameworks: Kenya, Jordan, Canada

The below resources include additional resources that inform the Toolkit's legal analysis, specifically its application to the overlap between TFGBV, targeted hate, and violent extremism.

Kenya

- David Indeje, Existing Legal Framework in Kenya Addressing Technology-Facilitated Gender-Based Violence. A Report, KICTANet.
- Byte Bullies: A report on Online Violence Against Women in the 2022 Kenya General Election, Pollicy.Caroline Kimeu, As social media grows in Kenya, so does the disturbing and toxic 'manosphere'.
- Femicide cases in Kenya fuel urgent calls for action to end violence against women, UN Women.
- Unmasking The Trolls: Research on Online Gender-Based Violence in Kenya, KICTANet.
- Fighting Violence Against Women Online: A Comparative Analysis of Legal Frameworks In Ethiopia, Kenya, Senegal, South Africa, and Uganda, Chioma Nwaodike and Nerissa Naidoo.
- DPA Digital Digest: Kenya [2025 Edition], Digital Policy Alert.
- Kenya: Communications Authority's industry guidelines for child online protection and safety in Kenya enter into force, Digital Policy Alert.
- Kenya: Computer Misuse and Cybercrimes (Amendment) Act, 2025 including content moderation regulation enters into force. Digital Policy Alert.
- Kenya: Human Rights and Criminal Justice System Responses to Terrorism. UNODC.
- BRIEFING PAPER: DOXING, DIGITAL ABUSE AND THE LAW, Equality Now.
- Kenya: New Cybercrime Amendments Threaten Online Expression: Authorities Should Repeal Provisions that Undermine Free Speech, Human Rights Watch.

Canada

- What to Know About Tech-Facilitated Gender Based Violence in Canada, Tech Safety Canada.
- Legal Remedies for Technology-Facilitated Gender-Based Violence Toolkit, Tech Safety Canada.
- Facts, stats and WAGE's impact: Gender-based violence, Government of Canada.
- Fact Sheet: Technology-facilitated gender-based violence, Government of Canada
- Mapping policy responses to technology facilitated gender-based violence in the G7 countries: OECD Public Governance Policy Papers, OECD.
- Breaking the Cycle of Gender-based Violence: TRANSLATING EVIDENCE INTO ACTION FOR VICTIM/SURVIVOR-CENTRED GOVERNANCE. OECD.
- Canada overhauls Criminal Code to protect victims and keep kids safe from predators. Department of Justice Canada.
- Who Designates Terrorism? The Need for Legal Clarity to Moderate Terrorist Content Online. Tech Against Terrorism.
- Tech Policy Press, An Overview of Canada's Online Harms Act, Mandy Lau.
- How anti-SLAPP laws work in Canada: And how the case of Steven Galloway points to their limits. CANADALAND.
- THE ONLINE REGULATION SERIES 2021 | CANADA (Update). Tech Against Terrorism.

Jordan

- The Impact of Technology- Facilitated Gender-Based Violence (TFGBV) on Survivors in Jordan, KVINFO.
- Fatima Mohammad Alkhadire, The Technology Facilitated gender Based Violence Legislative Mapping Paper, Jordan Open Source Association (JOSA).
- Jordan: New Cybercrimes Law stifling freedom of expression one year on, Amnesty International.