01

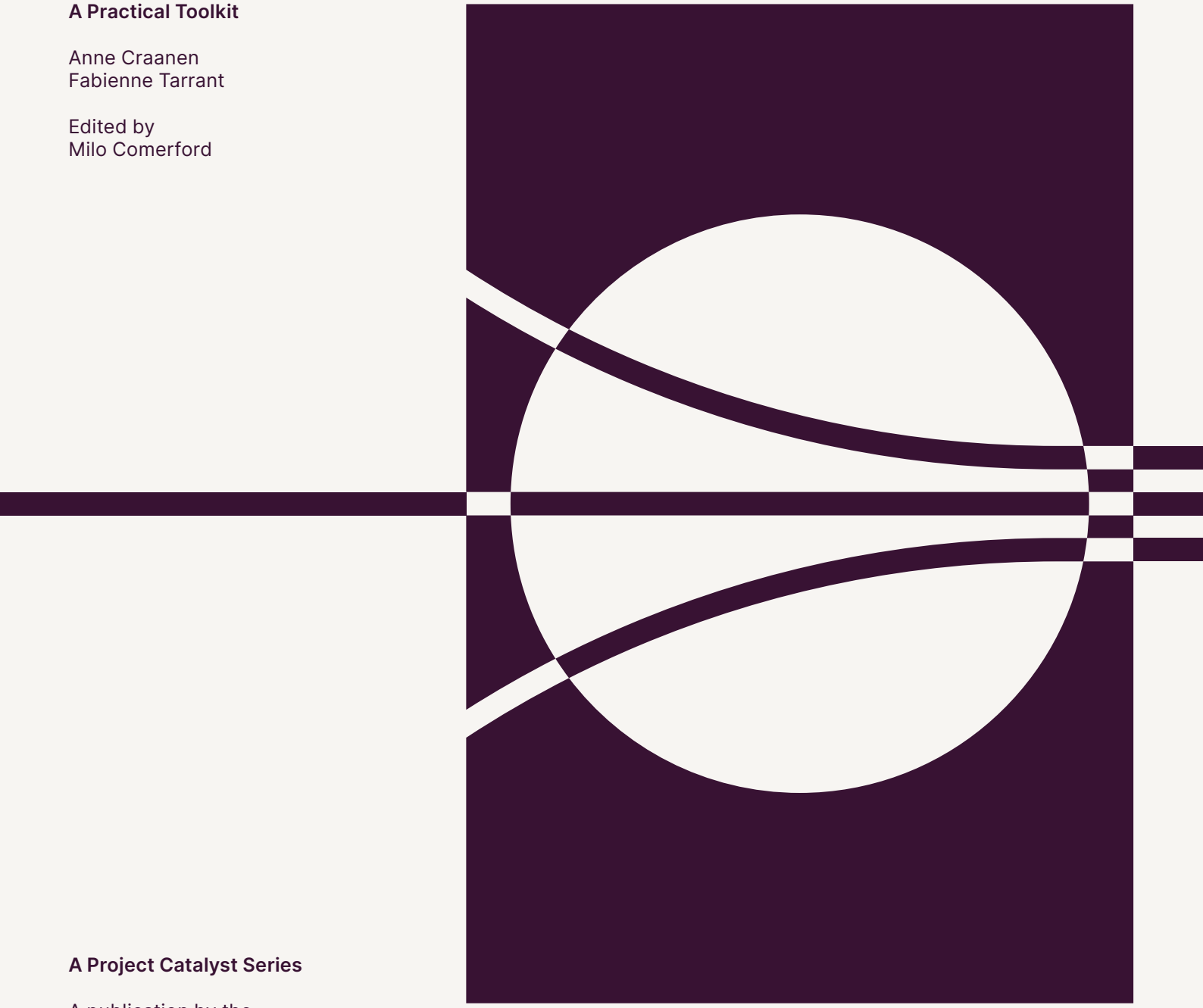
Addressing the Intersection of Misogyny, Targeted Hate and Violent Extremism

April 2026

A Practical Toolkit

Anne Craanen
Fabienne Tarrant

Edited by
Milo Comerford



A Project Catalyst Series

A publication by the Institute for Strategic Dialogue (ISD), produced as part of Project Catalyst led by the Christchurch Call Foundation.

ISD | Institute for Strategic Dialogue

CHRISTCHURCH CALL

A Practical Toolkit

Addressing the intersection of misogyny, targeted hate and violent extremism

Content Warning

This toolkit addresses sensitive and potentially distressing topics, including misogyny, targeted hate, violent extremism, sexual violence, rape, and sextortion. While every effort has been made to present information responsibly and respectfully, some materials may be upsetting for certain individuals.

Executive Summary

In this section

The issues of technology-facilitated gender-based violence (TFGBV), targeted hate, and violent extremism are often addressed as separate phenomena, despite their clear and growing overlap. This can challenge joined-up, targeted and effective efforts to these interconnected harms, including determining appropriate legal and policy responses.

This toolkit has been developed to support policymakers, regulators, practitioners, researchers, civil society - including victim and survivors' organizations - and technology platforms whose work interacts with TFGBV, targeted hate and/or violent extremism.

By mapping a broad spectrum of harms relating to online misogyny against diverse avenues for policy, legal and practitioner responses, the toolkit supports more coherent, rights-respecting, and coordinated whole-of-society responses to these overlapping challenges. Rooted in a public health-based approach to violence prevention, the toolkit focuses on opportunities for early intervention, boosting protective factors, and mainstreaming gender-transformative approaches that address harmful norms and support healthier masculinities.

Approach

At the core of the toolkit is a **Harms Taxonomy** that provides a practical granular framework for classifying harms associated with TFGBV, targeted hate, and violent extremism, which are framed as part of a continuum. Based on best practice classifications from the TFGBV sector, the taxonomy is rooted in five overarching categories of harm, which are mapped against their intersection with extremist and hate-fueled violence:

Harms	Online Harassment Online Impersonation Intimate Image Abuse Sexual Extortion Account Access Control

While all can cause serious harm, the analysis identifies online harassment, sexual extortion, and online impersonation as the TFGBV categories most likely to intersect with violent extremism. This includes through online harassment (including when this constitutes identity-based threats of violence), sexual extortion (such as through inciting self-harm rooted in supremacist beliefs), or the use of online impersonation to bring about gender-based harm (including human trafficking or terrorist recruitment). The taxonomy outlines concrete indicators relating to perpetrators, intent, and targets of violence, which need to be considered together in assessments of whether cases of TFGBV also constitute targeted hate or violent extremist activity. This toolkit is accompanied by a Definitional Annex, providing TFGBV harm definitions, alongside additional resources to support implementation of the toolkit.

Methodology

The toolkit's methodology is rooted in a comprehensive review of academic and policy literature, a synthesis of 20 existing harms taxonomies including more than 200 different harm types, and systematic analysis of where these TFGBV-related harms overlap with targeted hate and violent extremism. It builds on a substantial body of work examining the intersections between TFGBV, targeted hate, and violent extremism. This includes foundational contributions of feminist scholars, as well as the longstanding expertise of practitioner organizations, including women's and LGBTQI+ organizations, prevention practitioners, and support experts, who have led responses to gender-based harms for decades. The toolkit applies a gendered and intersectional lens, recognizing overlapping harms and the disproportionate impacts on women and LGBTQI+ people, while recognizing impacts on men and boys.

Application

The toolkit can serve as a practical tool for informing response efforts across a broad range of sectors, including:

Government and legal actors (including policymakers, regulators and law enforcement), to understand the connections between these types of violence, set clear thresholds for aligning effort, enabling proportionate and consistent legal responses, identify warning signs of escalation, and ensure responses to TFGBV, targeted hate, and violent extremism are rooted in fundamental rights.

The knowledge and research sector (such as academia and civil society researchers), to strengthen the evidence base by generating research in a more systematized and comparative manner, mapping trajectories of harm across different categories, systematically informing evidence-based policy, and improving accountability for government and platform responses.

The prevention and response sector (including prevention practitioners, women's and LGBTQI+ organizations, TFGBV and survivor support organizations), to center survivor safety and prevention by identifying overlapping harms and risk signals, supporting survivor-centered responses, applying relevant legal levers, and coordinating efforts with the wider ecosystem of actors focusing on the intersection of misogyny and violent extremism.

Platforms and industry bodies, to recognize and respond to the full spectrum of online misogynistic harms across different policy and enforcement areas, by designing policies that reflect the intersection of TFGBV, targeted hate, and violent extremism, improving content classification, moderation, and safety-by-design measures across the often siloed areas of gender-based violence, hate speech, and violent extremism.

Legal Frameworks

A systematic review was conducted of relevant regulatory frameworks in Canada, Kenya, and Jordan (the focus jurisdictions of Project Catalyst), to assess how policy and regulation apply across the harms identified in the taxonomy. This analysis identifies and assesses legal levers available when responding to different parts of the continuum of gender-based harm:

Canada has a comprehensive criminal law framework covering all TFGBV super-types primarily through the Criminal Code. Gender identity, expression, and sexual orientation are protected under human rights law, and terrorist propaganda is criminalized. However, gaps remain, including the absence of a standalone TFGBV or online safety framework and uneven coverage of specific sub-harms such as doxxing, leaving some gendered online harms inadequately addressed.

Jordan has strengthened its legal response to online harms through the Cybercrime Law No.17 of 2023, which explicitly criminalizes several TFGBV-related behaviors including impersonation, sexual extortion, and account access control. While targeted hate and violent extremism are addressed through constitutional and counter-terrorism provisions, gender is not consistently protected as a hate characteristic, and human rights organizations have raised concerns.[1] Legal frameworks criminalize same-sex sexual activity and lack protections for LGBTQI+.

Kenya addresses many TFGBV harms through a combination of the Penal Code and the Computer Misuse and Cybercrimes Act, covering online harassment, intimate image abuse, impersonation, sexual extortion, and account access control. The Constitution prohibits sex-based discrimination, and ethnicity-based hate speech and terrorist content are criminalized under cohesion and counter-terrorism laws. The Penal Code contains provisions that criminalize same-sex sexual activity and lack protections for LGBTQI+ individuals. While much of the legal framework was not originally designed for digital harms, Kenya has made meaningful progress toward digitalization of regulation and provides a relatively flexible basis for addressing gendered online harms.

How to Use This Toolkit

This toolkit is designed to be used as an action-oriented modular resource. Readers can use the different elements of the toolkit flexibly depending on their sector, use-case and specific harm they are addressing. In this way, the toolkit can help local authorities, regulators, or practitioners determine when a harm is best addressed through survivor support, public health interventions, platform action, or law enforcement involvement, reducing duplication and gaps in response.

1 Amnesty International: Jordan: New Cybercrimes Law Stifling Freedom of Expression One Year On. https://www.amnesty.org/en/latest/news/2024/08/jordan-new-cybercrimes-law-stifling-freedom-of-expression-one-year-on/

Below we summarize the key elements of the toolkit and their practical application:

Chapter 1: Understanding the varied ways that TFGBV intersects with violent extremism, including how misogyny can serve as a standalone violent extremist ideology, a core component of other supremacist ideologies, as well as a key risk factor and warning sign of violent extremism.

Chapter 2: Breaking down the concrete behaviors, tactics, and impacts associated with TFGBV and its overlap with targeted hate and violent extremism. This section provides a shared set of definitions and indicators to guide more targeted, proportionate, and coordinated responses across a spectrum of harmful activity.

SUPPORT RESOURCES

Resource 1: Practical questions to consider when analyzing TFGBV and its potential relationship to violent extremism

Resource 2: Example table for practically assessing thresholds of TFGBV, targeted hate and violent extremism in a given case

Chapter 3: Practical considerations for the broad range of sectoral responses to this spectrum of harms, including legal or regulatory responses; platform enforcement or safety-by-design; prevention and interventions; as well as research, monitoring and policy advocacy.

Chapter 4: Understanding the legal dimensions of this spectrum of harm areas across three Project Catalyst pilot countries (Canada, Kenya and Jordan), as well as instructive policy best practice from other international contexts.

Accompanying Definitional Annex: To be read in conjunction with the toolkit, providing further definitions and foundational literature, including existing TFGBV taxonomies, and relevant legal and policy frameworks.

1

State of Play: Misogyny and Violent Extremism

In this section

Misogyny is widely understood both as an attitude and a system of power. As an attitude, it involves hostility, resentment, or prejudice toward women; as a system, it functions to enforce patriarchal dominance and sustain gender inequality. Misogynistic and anti-LGBTQI+ attitudes, including anti-trans targeted hate, are rooted in binary, patriarchal constructions of femininity and masculinity, and in the presumed hierarchy that privileges masculinity. Research has shown that misogyny operates along a continuum, ranging from normalized sexism to explicit advocacy of violence, and plays a central role in shaping patterns of harm across both private and public spheres. It is also important to highlight that whereas online misogyny and TFGBV are often used interchangeably, for the purposes of this toolkit misogyny may both precede, as well as constitute a specific form of TFGBV. In this context, misogyny has a multifaceted relationship with extremism, defined by JM Berger as hostile action rooted in the inherently supremacist belief that "an in-group's success or survival can never be separated from the need for hostile action against an out-group. The hostile action must be part of the in-group's definition of success."

Intersections of Misogyny and Violent Extremism

1. Misogyny as a Form of Extremism

A growing body of research indicates that misogyny can constitute a form of extremism in its own right, often referred to as male supremacism. Where patriarchy operates as the ideological system prescribing gendered norms and hierarchies, misogyny functions as both the attitude — hatred or deep-seated prejudice toward women — and the system that polices those norms, to ensure that women and marginalized gender identities conform. In this framing, violence is justified through ideological narratives that portray women as threats, resources to be controlled, or enemies deserving punishment. Analysis of attacks linked to incel[2] ideology and other misogynistic belief systems show that, in some cases, such violence meets core criteria associated with violent extremism, including clear ideological motivation and the use of violence to intimidate or coerce broader audiences. Feminist literature has long challenged the tendency to treat misogynistic violence solely as hate crime or an individual pathology and instead situate it within the wider landscape of extremist harm. Literature also reveals gaps in research on other misogynistic communities, and often frames incel violence as the sole form of misogynistic extremist violence.

2 Involuntary celibates (incels) are men who believe that they are not able to have an intimate relationship to which they are entitled. Incels believe that they are excluded from this "sexual market" due to factors including their appearance, height, race or mental health (with a focus on appearance as the primary factor).

2. Misogyny Underpinning Other Forms of Extremism

Beyond operating as a distinct ideology, misogyny also functions as a core component underpinning multiple forms of extremism. Research demonstrates that violent misogyny is present across far-right, far-left, and jihadist movements, where it reinforces hierarchies, legitimizes violence, and facilitates recruitment. Misogynistic narratives often intersect with anti-LGBTQI+ hate, antisemitism, and conspiracy theories, enabling the circulation and reinforcement of extremist ideas across ideological boundaries. Studies of far-right ecosystems in particular show how misogynistic online spaces can act as gateways into broader extremist networks and as connective tissue linking transnational communities.

3. Misogyny as a Risk Factor

Recent empirical research has examined misogyny as a risk factor for multiple forms of violence, including violent extremism. Survey-based studies show that misogynistic attitudes are associated with increased support for violent extremist attitudes, greater willingness to engage in interpersonal violence, and higher tolerance for violence against women. These relationships are shaped by factors such as hypermasculinity, entitlement, perceived threats to male identity, and revenge-oriented thinking. This evidence highlights how misogyny contributes to pathways into violence across both private and public domains and underscores its relevance for prevention and early intervention efforts.

4. Misogyny as a Warning Sign

Research has also highlighted misogyny as a warning sign of broader violent behavior. Analyses of terrorist perpetrators' histories show that many had prior records of domestic violence or other forms of expressed misogyny, often categorized as "private violence." Rather than representing a shift from private to public violence, subsequent attacks are better understood as a continuation of violence. Treating these forms of violence as separate risks minimizes the seriousness of violence against women and obscures critical warning signs that could support earlier intervention and violence prevention.

IMPACT ON BOYS AND YOUNG MEN

While women, girls, and LGBTQI+ communities are disproportionately harmed by misogyny and TFGBV, these dynamics also impact boys and young men. Patriarchal norms and rigid gender expectations constrict emotional development, stigmatize help-seeking, and normalize unhealthy relationships, contributing to anxiety, isolation, and silence around experiences of abuse. Boys who internalize these norms may struggle to recognize or disclose harm, including exposure to child sexual abuse material. Misogynistic online subcultures can exploit these vulnerabilities, functioning as entry points into broader extremist ecosystems where grievance-based masculinity is weaponized toward wider ideological commitments. At the same time, digital cultures that valorize aggression and sexual entitlement can serve as entry points into broader extremist ecosystems, making early engagement with boys and young men a critical prevention lever. Addressing misogyny's root causes therefore requires interventions that dismantle patriarchal systems while creating space for alternative narratives of masculinity centered on care, empathy, and help-seeking.[3] It is imperative that this is done through engaging men and boys, rather than excluding them or solely address them as perpetrators of gender-based violence. More information on how to engage men and boys in countering gender-based violence, and how ISD is working with Movember to tackle this, can be found here.

The key foundational principles on the following page stem from the above literature and practical insights from experience working at the intersection between misogyny, targeted hate, and violent extremism.

Whereas this toolkit is focused specifically on TFGBV, misogyny, and the intersection with targeted hate and violent extremism, we highlight instances where men and boys are affected.

This Toolkit uses the Project Catalyst definitions for Tech-Facilitated Gender-Based Violence (TFGBV), Targeted Hate & Violence and Violent Extremism, which differ from ISD's definitions.

DEFINITIONAL CRITERIA[4]

Tech-Facilitated Gender-Based Violence (TFGBV)	Acts of gender-based harm committed, enabled, or exacerbated by digital technologies. In other words, tech facilitated or online GBV encompasses "any act that is carried out via information communication technologies or other digital tools, which results in (or is likely to result in) physical, sexual, psychological, social, political, or economic harm, or other infringements of rights and freedoms".[5]
Targeted Hate & Violence (TH&V)	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 characteristic[6] 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.
Violent Extremism (VE)	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.

3 ISD, Digital Policy Lab: Policy Brief: Fostering Healthy Masculinities: Building Resilience Against Online Misogyny. https://www.isdglobal.org/publication/fostering-healthy-masculinities-building-resilience-against-online-misogyny/

4 Definitions from Project Catalyst: Lamphere-Englund (2025), Christchurch Call Foundation

5 UN Women's Expert Group Meeting Report for this shared definition across experts: https://www.unwomen.org/en/digital-library/publications/2023/03/expert-group-meeting-report-technology-facilitated-violence-against-women

6 These include ethnicity, religion, nationality, country of origin, gender (including gender assigned at birth and identity), sexual orientation and identity (including straight/heterosexual, lesbian, gay, trans, queer, and any other formulations), and political affiliation.

CONTINUUM OF HARMS

Misogyny gives rise to a wide continuum of harms. It is therefore essential to recognize that extremist violence is one manifestation of gender-based violence, rather than an inherently more "severe" or exceptional one. All forms of violence linked to (online) misogyny have significant and varied impacts on victim-survivors[7], their communities, and broader culture. While this project focuses specifically on the intersection of misogyny and extremism, we situate these harms alongside other forms of violence commonly framed as private (such as rape, femicide, sexual abuse, and intimate partner violence) and public (such as school shootings, and terrorism). Rather than ranking these harms, we place them on a shared continuum. Overarchingly, this continuum produces effects that extend beyond individual harm. By systematically excluding women and LGBTQI+ people from digital and public spaces, it undermines equal participation in social, political, and democratic life.

THE COMPLEX RELATIONSHIP BETWEEN MISOGYNY AND EXTREMISM

We understand the relationship between misogyny and extremism in four interconnected ways: as a form of extremism in its own right (including violence motivated by male-supremacist ideology); as a core component that underpins and reinforces other extremist movements; as a risk factor that increases vulnerability to adopting more extreme beliefs; and as a warning sign that may signal progression toward different forms of violence, including violence against women and girls and broader public-oriented attacks. This framing underpins how we analyze misogyny throughout the toolkit and directly informs both the harms taxonomy and the project's broader methodological approach.

PUBLIC HEALTH APPROACH OVER SECURITIZATION

We recognize concerns that framing misogyny or gender-based violence primarily through the lens of extremism risks over-securitizing the issue and narrowing it to a national security problem, rather than recognizing it as an everyday societal reality. This toolkit therefore centers a public health approach to prevention, focused on strengthening protective factors and addressing risk factors before harm manifests. This includes upstream, community-rooted engagement and education that positively engages men and boys; targeted interventions for individuals at heightened risk of harmful misogynistic involvement; and disengagement pathways for those already involved. By situating misogyny within a broader prevention agenda spanning gender-based violence, extremism, and wider violence-prevention efforts, this approach prioritizes early, coordinated, and evidence-based intervention.

GENDER-TRANSFORMATIVE APPROACH

Addressing misogyny and related forms of violence requires more than mitigating harm; it requires challenging the underlying gender norms, power structures, and inequalities that enable them. A gender-transformative approach seeks to actively question and reshape harmful constructions of masculinity and femininity, promote gender equality, and support healthier, more inclusive identities and relationships. Throughout this toolkit, we emphasize interventions that do not simply respond to individual incidents, but work to shift the social, cultural, and structural conditions that sustain misogyny, gender-based violence, and extremist mobilization.

MISOGYNY AND ANTI-LGBTQI+ TARGETED HATE

Misogynistic and anti-LGBTQI+ attitudes, including anti-trans targeted hate, are rooted in patriarchal constructions of gender and in hierarchies that privilege masculinity. Non-binary and trans identities challenge these hierarchies and are therefore frequently targeted with gender-based harms, hate, and violence. While women and LGBTQI+ communities are disproportionately affected, we also recognize that men and boys experience harm through rigid gender norms that shape expectations of masculinity, with implications for wellbeing, relationships, and vulnerability to harmful behaviors such as self-harm or violence. Importantly, LGBTQI+ individuals can also help misogynistic or exclusionary attitudes within and across communities, including by individuals who may themselves experience marginalization.

OVERLAP OF HARMS

While the harms taxonomy identifies distinct categories—such as online harassment or intimate image abuse—in practice, these harms frequently overlap. For example, coordinated harassment campaigns may also involve doxxing, impersonation, or the circulation of intimate images. In applying the taxonomy, we therefore identify individual harm types while explicitly recognizing where and how they intersect. This approach reflects the lived reality of victim-survivors and supports more accurate assessment, documentation, and response.

7 We use the term victims-survivors throughout this document to point to individuals who have experienced trauma, abuse, or crime, notably for the purposes of this document, from gender-based violence. The term survivor is sometimes preferred to empower individuals, whereas victims underscores the continued impact the violence had on a person. Given that this is a personal preference, we use the term victim-survivor. It is important to note that not all victims survive gender-based violence. Source: Sexual Assault Kit Initiative. Victim or Survivor: Terminology from Investigation Through Prosecution. RTI International. Sakitta.

2

The Harms Taxonomy

Understanding the continuum of tech-facilitated gender-based violence to violent extremism

In this section

This toolkit is rooted in ISD's Harms Taxonomy, developed to help stakeholders understand how online misogyny manifests across a spectrum of harms, TFGBV, targeted hate, and, in some cases, violent extremism. Rather than treating violent extremism as exceptional or separate, the taxonomy reflects a continuum of gender-based harm. Furthermore, we recognize that misogyny is inherently political and it can be difficult to therefore discern political or ideological motive that may mean it crosses over with violent extremism.

Intended to support prevention, enforcement, and intervention without ranking harms or privileging one form of violence over another, the taxonomy offers a structured way to:

- Identify common forms of TFGBV and the tactics used to carry them out
- Understand when harms may also meet thresholds for targeted hate or violent extremism, depending on context
- Support consistent classification of harmful behavior across policy, regulatory, enforcement, and platform settings
- Identify gaps where current legal, policy, or platform responses fall short

Rooted in best practice from the TFGBV sector - including Humane Intelligence's framework for analyzing harm through the lenses of harm types, perpetrators, intent, target, including on a community and societal level - the taxonomy focuses on the relationship of violent extremism to five main 'TFGBV super-types'.

Harm Super-Types	Online Harassment Online Impersonation Intimate Image Abuse (IIA) Sexual Extortion Account Access Control

This toolkit distinguishes between overarching categories of harm and more specific sub-harms. These sub-harms may also operate as tactics and be weaponized for super-types of harms identified; however, they are also inherently harmful. This includes harm that is reputational, economic, psychological, and physical in nature. This approach aligns with other established harm-based frameworks, which classify such practices according to their effects rather than solely their instrumental use.

Overarchingly, this continuum produces effects that extend beyond individual harm. By systematically excluding women and LGBTQI+ people from digital and public spaces, it undermines equal participation in social, political, and democratic life. In this way, TFGBV can advance misogynistic or male-supremacist goals by reinforcing gender hierarchies, normalizing intimidation, and weakening democratic norms rooted in equality and inclusion.

Indicators for Assessing When TFGBV Intersects with Violent Extremism

The table below sets out key indicators that help assess when and how TFGBV may intersect with violent extremism. It provides practical guidance for identifying the specific conditions under which gender-based harms may also meet violent extremism thresholds, based on what perpetrators are involved, why the harm is being carried out, and who or what is being targeted. Taken together, these indicators help practitioners consider patterns of coordination, ideological motivation, and targeting that may signal extremist mobilization.

Importantly, the indicators are context-dependent and should be applied holistically rather than as a checklist. Their purpose is to support informed judgment, proportional responses, and early prevention—helping to distinguish between TFGBV as a standalone harm, TFGBV that also constitutes targeted hate, and TFGBV that is violent extremist in nature.

Our analysis highlights **three TFGBV harms that most clearly intersect with violent extremism**:

- **Online Harassment**: Including hate speech, incitement, and threats of violence, which are tactics commonly used in violent extremism.
- **Sexual Extortion**: Which can involve coercion linked to supremacist beliefs or the funding of extremist activities through exploitation.
- **Online Impersonation**: This can include impersonation to advance supremacist beliefs or violent extremist agendas including human trafficking or terrorist recruitment.

Account Access Control and **Intimate Image Abuse** are less directly connected to violent extremism but may serve as tools within broader extremist strategies. The degree of intersection with violent extremism depends on perpetrator intent, such as whether perpetrators hold extremist beliefs or seek to use these tactics for ideological purposes.

INDICATORS FOR ASSESSING WHEN TFGBV INTERSECTS WITH VIOLENT EXTREMISM

INDICATOR	VIOLENT EXTREMISM INDICATION
Perpetrator[8]	• Male-supremacist networks, including violent subsets of manosphere -affiliated communities.[9] • Male supremacist lone actors. • Ideological violent extremist groups and organizations, including far-right, far-left, and Islamist networks. • Individual violent extremist actors connected to more loosely organized online extremist networks or communities. • Hybridized violent extremist actors with a nexus to state-linked threats. • Accelerationist or nihilistic violent online subcultures and networks, including Com network and related communities (e.g. 764, True Crime Community, No Lives Matter, Maniac Murder Cult).
Intent	• To promote, reinforce, or enforce male supremacist dominance and violent male-supremacist or misogynistic extremist ideology, asserting male superiority and the subjugation of women, trans, and non-binary people; including the legitimization of exclusion, submission, and gender-based violence. • To silence, punish, intimidate, or coerce women and LGBTQI+ individuals and communities, restricting their participation, visibility, or leadership in civic, political, and democratic spaces. • To deter or suppress activism, public engagement, or collective action by women, feminist movements, and LGBTQI+ communities through harassment, intimidation, or reputational harm. • To advance violent male-supremacist or misogynistic extremist objectives by strengthening, normalizing, and operationalizing extremist beliefs within online or offline communities. • To discredit, undermine, or infiltrate gender-equality movements, including feminist organizations and LGBTQI+ advocacy, through harassment, disinformation, surveillance, or coordinated disruption. • To facilitate grooming, recruitment, exploitation, or trafficking of women, girls, or minors for extremist purposes, including sexual exploitation or material support for violent activity. • To recruit, groom, or funnel individuals into exploitation or trafficking ecosystems, consolidating extremist power and cohesion. • To generate material, financial, or logistical support for violent activity. • To impersonate women, LGBTQI+ individuals, authority figures, or trusted community members in order to deceive, radicalize, recruit, exploit, or manipulate targets for extremist gain. • To justify or incite violence, reinforce extremist worldviews, or entrench ideological narratives. • To enforce ideological conformity and in-group control within extremist communities, including through humiliation, coercion, sexual extortion, or other gender-based abuses. • To intimidate targets, manipulate information environments, or facilitate ideologically motivated violence, including through coordinated harassment or communication interference.
Target	• Groups framed as symbolic or ideological enemies; women and LGBTQI+ individuals and the trans community, including feminists, gender-equality advocates, and public figures; individuals targeted on the basis of protected characteristics, including gender and sexuality. • Women and LGBTQI+ individuals in public, political, civic, or professional roles (e.g. journalists, politicians, judges, activists); feminist, LGBTQI+, or gender-equality organizations; health care workers, women's care and abortion providers, or those providing gender-affirming care for trans communities, communities framed as ideological opponents of male-supremacist or other extremist worldviews. • Minors[10], women and LGBTQI+ public figures, including journalists and activists; individuals targeted through deceptive or fabricated relationships; populations framed as symbolic enemies or mobilized through gendered narratives to intimidate, threaten, or justify mass violence. • Broader populations, where account compromise or identity manipulation is used to intimidate targets, distort public discourse, or enable mobilization toward ideologically motivated violence.

8 In all super-types, behavior can be perpetrated by the individuals mentioned, but also through inauthentic means such as coordinated action using bots or bot networks. Beyond individual actors, research also highlights a close relationship between TFGBV and broader harms: misogynistic behavior that begins online may escalate to offline violence in both private and public spheres. Studies find that those who commit acts of targeted violence frequently have prior histories of domestic violence, misogynistic behavior, or both — a dynamic documented, for example, in a 2023 US Secret Service report on the public security threat posed by such individuals (Institute for Strategic Dialogue. (2023). Misogynistic pathways to radicalisation: Recommended measures for platforms to assess and mitigate online gender-based violence. https://www.isdglobal.org/wp-content/uploads/2023/09/Misogynistic-Pathways-to-Radicalisation-Recommended-Measures-for-Platforms-to-Assess-and-Mitigate-Online-Gender-Based-Violence.pdf). This continuum from online to offline harm is also reflected in who perpetrates TFGBV more broadly: it is overwhelmingly carried out by individuals known to victim-survivors, most often current or former intimate partners. While this toolkit focuses on the intersection of TFGBV and extremism — where that dynamic may be less prevalent — it nevertheless acknowledges and reflects this wider context.

9 The Manosphere is a loosely connected network online that cannot be branded as extremist in its entirety. It is important to consider parts of the network as potential perpetrators, but it is reliant on other factors, such as violent and ideological intent, to consider a part of this network as relevant to violent extremism.

10 Sexual extortion also often targets adolescent boys.

Violent Extremism Indicators Per Harm Type

The tables below set out the same key indicators that help assess when and how TFGBV may intersect with violent extremism, broken down by super-harm type. This provides further detail on how online harassment, intimate image abuse, online impersonation, sexual extortion, and account access control can cross over with targeted hate and violent extremism, which also provides the grounding for the legal analysis below.

Key to this is Project Catalyst's definition of violent extremism, constituting activity which:[11]

1	2	3
Promotes ideological, political, or religious aims;	Advocates for or uses violence to realize those aims; and	Tolerates, supports, actively calls for, or directly uses violence against civilians or critical civilian infrastructure.

11 Full Project Catalyst definitions are outlined in the accompanying Annex.

12-15 Full definitions can be found in the accompanying Annex.

ONLINE HARASSMENT

VIOLENT EXTREMISM INDICATION

Harmful activity that advances violent male-supremacist or other ideologically extremist objectives, including through:

- The use of online harassment tactics—such as doxxing, targeted harassment, cyberstalking, and coordinated abuse—to intimidate, coerce, or silence individuals in ways that facilitate, enable, or promote violent extremist aims. This includes harassment intended to punish ideological dissent, force targets out of public life, or create enabling conditions for offline violence.
- Online harassment used to advocate for, justify, or operationalize violence in service of male-supremacist or other extremist ideologies, including targeting individuals based on gender, gender identity, sexual orientation, gender expression, sex characteristics, or non-adherence to prescribed gender roles or norms. Such harassment may function to normalize violent action, pressure others toward ideologically motivated violence, or punish perceived ideological enemies.
- Tolerance, endorsement, or explicit calls for violence against civilians or critical public infrastructure, where online harassment operates as a mobilization mechanism, signaling practice, or precursor to violent extremist activity.

TACTICS, BEHAVIORS & SUB-HARMS[12]

Doxxing, cyberstalking, inappropriate content, flaming, trolling, dogpiling or mobbing, body-shaming, slut-shaming, (gendered, sexist, homophobic or transphobic) hate speech, coordinated attacks, networked harassment, smear campaigns, cross-platform harassment, astroturfing, and zoom-bombing.

Case Study: Doxxing of Female Politician

In 2022, a Dutch anti-Covid conspiracy theorist doxxed a female Dutch Politician, Sigrid Kaag, by putting her address online. Following this, a person with a torch showed up outside her house and she was placed under additional security. Whereas it is unclear whether the doxxed address directly led to the man showing up with a torch, Sigrid Kaag faced the most online harassment out of any Dutch politician, and upon leaving Dutch politics, mentioned how the online hatred she faced was one of the reasons why she left politics. In the EU 2024/1385 Directive on Combating Violence Against Women and Domestic Abuse, doxxing is now criminalized as online harassment, allowing improved legal recourse to be taken.

INTIMATE IMAGE ABUSE (IIA)

VIOLENT EXTREMISM INDICATION

Intimate Image Abuse (IIA) meets the threshold of violent extremism only in a limited set of cases where it is deployed with explicit male-supremacist ideological intent and is directly linked to the advocacy, facilitation, or justification of violence. This includes:

- The dissemination of intimate images alongside explicit male-supremacist advocacy of violence, where IIA is used to dehumanize, threaten, or coerce targets as part of an ideological project that promotes or legitimizes violent action against women or LGBTQI+ people on the basis of gender.
- The targeting of women in central civic or democratic roles—such as politicians, journalists, or judges—through IIA intended to intimidate, silence, or remove them from public participation, where such attacks undermine democratic processes or civic institutions, for example through creating false sexualized narratives, and thereby constitute harm to critical civilian infrastructure in service of violent extremist objectives.

TACTICS, BEHAVIORS & SUB-HARMS[13]

Technology facilitated sexual violence and a particular form, so-called "revenge porn", deepfake sexual media, voyeuristic recording (creepshots, upskirting, down-blousing), producing, reproducing, or sharing unsolicited sexual content, cyberflashing, image-based sexual abuse, and documenting/broadcasting sexual assault.

Case Study: Far-Right Deepfakes Targeting of Taylor Swift

Taylor Swift is one of the most targeted celebrities from non-consensual deepfakes. A subset of this targeting has seen far-right extremist ecosystems frequently weaponizing sexualized imagery. Open-source investigations by ISD show that Taylor Swift is regularly targeted in far-right online spaces through pornographic and degrading depictions, including sexualized images showing her alongside extremist figures such as Adolf Hitler. These practices illustrate how TFGBV is used as a tactic within broader extremist propaganda and mobilization efforts.

ONLINE IMPERSONATION

VIOLENT EXTREMISM INDICATION

Violence that advances violent male-supremacist or other ideologically extremist objectives, including through:

- The use of online impersonation as a recruitment or radicalization tactic, including impersonating women, LGBTQI+ individuals, or trusted community figures to lure individuals into extremist networks, legitimize violent narratives, or facilitate pathways toward mass violence.
- The use of impersonation to enable, facilitate, or directly support violence against civilians or critical civilian infrastructure, including impersonating women or LGBTQI+ politicians, activists, or public figures to delegitimize them, incite violence, or undermine their political or civic participation in service of extremist goals.
- The use of impersonation to recruit, groom, or coerce women, girls, or LGBTQI+ individuals into sexual exploitation or trafficking as part of extremist activity, including to generate material support for violent movements or to facilitate sexual slavery within terrorist organizations.

TACTICS, BEHAVIORS & SUB-HARMS[14]

Catfishing, fake profiles, profile spoofing, identity and image theft, social media cloning, email/messaging impersonation, and deepfake impersonation.

Case Study: Impersonation for Recruitment

Coordinated impersonation campaigns use fake or "victim-authored" accounts to recruit or groom women into trafficking or extremist networks, gamify dehumanizing impersonation, and incite mob harassment or violence to silence women and public figures. Human and sex trafficking is also used to fundraise extremist activity, such as ISIS' use of trafficking-based coercion to recruit young Western women. Recruiters relied on impersonation of women, romantic manipulation, pressure to share intimate communications, and threats of shame or exposure to control victims. Upon arrival, the women were forced into marriages and sexual exploitation.

SEXUAL EXTORTION

VIOLENT EXTREMISM INDICATION

Violence that advances violent male-supremacist or other ideologically extremist objectives, including through:

- The use of sexual extortion as a coercive tactic to advance extremist ideology, including demanding sexual acts, images, or compliance under threat of exposure, where such threats are explicitly linked to male-supremacist or far-right narratives that justify domination or violence.
- The use of sexual extortion within recruitment or radicalization pathways, particularly in online ecosystems where far-right and male-supremacist communities overlap, employing coercion and sexualized control to draw individuals deeper into violent extremist networks.
- Operation within extremist communities that tolerate, endorse, or advocate sexualized violence against minors, women, or LGBTQI+ individuals, where sexual extortion reinforces violent ideological aims and contributes to broader patterns of advocating or perpetrating violence against civilians on the basis of gender, gender identity, sexual orientation, gender expression, sex characteristics, or non-adherence to prescribed gender roles or norms.

TACTICS, BEHAVIORS & SUB-HARMS[15]

Sexual blackmail, online sexual coercion and extortion, grooming, online sex trafficking, live-streaming sexual exploitation, coercion using hacked data, exploitation and trafficking.

Case Study: 764

764 emerged in 2021 from the "Com Network," an online community that focused on swatting while also engaging in sextortion and online Child Sexual Abuse Material (CSAM) distribution.[16] 764 is a network of online groups that engage in sextortion and the glorification of violence - using coerced Child Sexual Abuse Material (CSAM) to extort primarily minor victims, and leveraging it to force acts of violence or self-harm. They have also engaged in extensive swatting, harassment and intimidation campaigns to silence their victims. From 2020-2025, over 200 individuals were arrested in 28 different countries for sextortion, CSAM possession or violence linked to the network.

ACCOUNT ACCESS CONTROL

VIOLENT EXTREMISM INDICATION

Violence that advances violent male-supremacist or other ideologically extremist objectives, including through:

- The use of hacked or compromised accounts to conduct, enable, or amplify extremist harms, such as targeted harassment, doxxing, or impersonation, where account takeover functions as a mechanism for disseminating male-supremacist incitement or threats of violence against women, LGBTQI+ individuals, or other civilians.
- The compromising of accounts to escalate, legitimize, or normalize calls for sexual violence, femicide, or political violence, particularly where targets are women in public or civic roles (e.g. politicians, journalists), and the intent is to silence, intimidate, or undermine democratic participation in line with extremist objectives.
- The exploitation of system or account access to facilitate physical harm or operational support, including the disclosure of real-world locations, security vulnerabilities, or sensitive personal or organizational information, including women's health care and abortion providers, fertility clinics, and gender affirming care for trans communities, thereby enabling or accelerating ideologically motivated violence.

TACTICS, BEHAVIORS & SUB-HARMS

Hacking, password theft, account lockout, denial of service (DoS), internet-of-things (IoT) abuse, spyware and surveillance, tracking, privacy violations, doxxing, outing gender identity and/or sexual orientation, cyberstalking via devices.

Case Study: Targeted Hacking and Cyberattacks

Planned Parenthood reported a large-scale distributed denial-of-service (DDoS) attack that temporarily knocked its websites offline and forced redirection of traffic to alternative channels. The incident was framed as politically motivated harassment in the context of heightened anti-abortion activism. The operational effect was to deny access to time-sensitive health information and overwhelm digital infrastructure at a moment of peak public attention.

16 For more information, please see ISD's 764 explainer: https://www.isdglobal.org/isd-explainer/764/.

Impact Types

When TFGBV intersects with targeted hate or violent extremism, the resulting psychological and physical impacts share common features but differ in scale, coordination, and intent. While TFGBV already produces significant community and societal harms, its convergence with targeted hate or violent extremism systematizes and amplifies these effects, often through coordinated, ideologically driven campaigns. In these contexts, impacts extend beyond individual victims to produce broader societal consequences, including a chilling effect on public discourse, democratic engagement, and freedom of expression. The mass scale and ideological nature of these harms intensify their capacity to negatively reshape online and offline civic spaces. These dynamics extend beyond online spaces, discouraging women from public life, leadership, and civic participation, including standing for office or engaging in journalism and advocacy.

TFGBV functions not only as a distinct source of harm but as a deliberate operational and ideological tool utilized by violent extremists.

Below we list some of the specific impacts particularly associated with violent extremist weaponization of TFGBV and online misogyny:

Normalization	Recruitment	Direct Incitement
Normalization of ideological gender-based violence within extremist belief systems and narratives	Recruitment and mobilization of supporters through gender-based grievances and misogynistic or male-supremacist framing	Direct incitement to violence against targeted individuals or groups, including the justification or facilitation of terrorist or mass-casualty attacks
Strategic Use of Fear	**Systematic Suppression**	**Dissemination**
Strategic use of fear, intimidation, and coercion to exert control over individuals, communities, or public spaces	Systematic suppression of civic and democratic participation through coordinated, ideologically driven harassment and intimidation campaigns	Amplified dissemination of extremist misogynistic ideologies as core organizing principles within violent extremist movements
Rationalizing		
Rationalization of gender-based violence as politically or ideologically justified, transforming individual acts of harm into collective, movement-oriented violence		

Support Resources

Guiding questions for analyzing TFGBV and its potential relationship to violent extremism

The following two resources are complementary to help readers implement the taxonomy. The first resource poses guided questions to help identify four main questions and proposes various answers that may indicate a greater likelihood of when TFGBV harms overlap with targeted hate and violent extremism. The second resource is more of an in-depth assessment tool that gradually takes readers through the thought process when using the taxonomy to help assess where gendered harms fall on the spectrum, and when they may be at risk of crossing over into targeted hate and violent extremism.

Questions to consider when analyzing TFGBV and its potential relationship to violent extremism

THIS CHECKLIST can help clarify which sector and actor is best placed to address different aspects of the intersection between misogyny, TFGBV, and violent extremism. For example, a municipality may struggle to conceptualize its role in responding to misogyny as a factor in pathways toward violence. By using the checklist, local authorities can better identify where they are able to intervene directly, and where responsibility may more appropriately sit with other actors, such as health, social, or prevention services, supporting a more coordinated and proportionate response.

STEP 1: IDENTIFY THE BEHAVIOR AND TACTICS

Questions	Considerations can include:
☐ What behaviors, tactics, or sub-harms are present? (One or more may apply)	• Distribution of non-consensual intimate images (NCII) • Online harassment, including doxxing • Hacking or account compromise • Cyberstalking

STEP 2: IDENTIFY THE HARM AND TFGBV SUPER-TYPE(S)

Questions	Considerations can include:
☐ Which TFGBV super-type(s) does the harm fall under? (Multiple categories may apply, as harms can overlap or occur simultaneously)	• Online harassment • Intimate Image Abuse (IIA) • Online impersonation • Sexual extortion • Account access control

STEP 3: ASSESS KEY CONTEXTUAL DIMENSIONS

Questions	Considerations can include:
☐ Who are the perpetrators? ☐ Who are the targets? ☐ What is the apparent intent? ☐ What form(s) of violence are present? ☐ Are there additional contextual signals?	• Individual actors • Organized or networked actors • Women or LGBTQI+ individuals • Public figures (e.g. politicians, journalists) • Feminist or gender-equality advocates • Silencing, punishment, or intimidation • Political exclusion or removal from public life • Ideological enforcement or mobilization • Psychological harm • Threats or incitement • Facilitation or justification of physical violence • Prior extremist or misogynistic rhetoric • Coordinated harassment • Links to male-supremacist or extremist networks

STEP 4: THRESHOLDING ANALYSIS

Questions	Thresholding considerations should consider the combined interaction of:
☐ Does the case meet the criteria for: Targeted Hate and Violence? Violent Extremism?	• Perpetrator identity and networked behavior[17] • Ideological intent • Targeting patterns • Use of TFGBV as a tool to advance broader violent aims

17 It is important to note that TFGBV is overwhelmingly perpetrated by individuals known to victim-survivors, most often current or former intimate partners. While this toolkit focuses on the intersection of TFGBV and extremism — where such dynamics may be less prevalent — it nevertheless acknowledges and reflects this broader context.

Case application table: Non-consensual intimate image abuse (NCII) of a political figure

THIS RESOURCE BELOW is intended to provide a practical use-case to detail how key actors, such as regulators, or prevention practitioners, can assess whether a specific case constitutes TFGBV and also meets thresholds for targeted hate or violent extremism. It provides guiding questions that help stakeholders make this assessment, and how such questions may be considered using the taxonomy.

How to use this table	Example
The case classification table below functions in two stages: Steps 1–6 provides structured questions focused on what happened (behavior), who it affected (targets), and the surrounding context (intent, coordination, violence signals), helping to establish whether the case meets the threshold for TFGBV. Steps 7–9 assess whether the case also meets additional criteria for Targeted Hate & Violence or Violent Extremism.	An individual distributes non-consensual intimate image abuse (NCII) of a female political figure and has a history of justifying violence against women and advocating for their exclusion from politics.

STEP 1: BEHAVIOR

Question to answer	What to record in practice	→ Applied to the sample NCII case	Threshold indicators	Indicative classification
What is the online activity?	Identify the specific actions taken and any enabling tactics used.	Distribution of NCII as the primary harm. Possible co-occurring tactics could include: doxxing, cyberstalking, hacking/ account compromise, coordinated harassment.	Evidence of account compromise, net-worked distribution, threats, cross-plat-form coordination, or doxxing could entail threshold.	Establishes the basis for classification.

STEP 2: TFGBV HARM TYPE

Question to answer	What to record in practice	→ Applied to the sample NCII case	Threshold indicators	Indicative classification
Which TFGBV harm category does this fit?	Map the behavior to the rel-evant TFGBV super-type(s). More than one category may apply.	Intimate Image Abuse (IIA) is the primary harm. This commonly co-occurs with online harassment. Account access control applies only where the intimate images were obtained through hacking or account compromise.	Co-occurrence across multiple super-types (e.g. IIA combined with harassment and/or account compromise) may indicate more systematic patterns of harm.	TFGBV threshold is met (at minimum through presence of intimate image abuse).

STEP 3: TARGET(S)

Question to answer	What to record in practice	→ Applied to the sample NCII case	Threshold indicators	Indicative classification
Who is targeted?	Identify who is being targeted and why the target profile is relevant. Is the target one person, or multiple people, and if so, is this based on a commonali-ty such as women in office, gender, gender identity, gender expression, sexual orientation, sex character-istics, or lack of adherence to societal norms around gender roles?	A political figure, which carries civic and democratic relevance. If the individual is a woman or LGBTQI+ person—or is framed as such—the targeting is gendered and identity-linked.	The target is a woman or LGBTQI+ public figure; the individual is framed as a symbolic or ideological enemy; or the harm is intended to silence, intimidate, or remove the target from public life.	Points toward potential targeted hate or violent extremism classification.

STEP 4: PERPETRATOR(S)[18]

Question to answer	What to record in practice	Applied to the sample NCII case	Threshold indicators	Indicative classification
Who is acting, is it organized?	Identify the type of actor involved and whether the activity appears individual or networked.	Individual actor in this case. Important to understand if they are connected to violent male-supremacist / extremist communities or engaged in other coordinated campaigns.	Evidence of organized or networked actors, involvement of violent extremist communities, amplification by ideological ecosystems, or indicators of hybrid influence operations.	Helps distinguish TFGBV from coordinated targeted hate/ violent extremism patterns.

STEP 5: INTENT

Question to answer	What to record in practice	Applied to the sample NCII case	Threshold indicators	Indicative classification
What is the apparent purpose of the behavior?	Assess intent using available contextual information, including past behavior, statements, or patterns.	The perpetrator may have a documented history of justifying violence against women and advocating for their exclusion from politics, however for this harm to occur it does not have to be repeated. The online activity itself may already signal an intent focused on political silencing and exclusion.	Explicit male-supremacist ideological framing; calls to remove women from civic or political life; intent to punish perceived ideological dissent or efforts to mobilize supporters around exclusionary narratives.	Points toward targeted hate and violence; may indicate violent extremism.

STEP 6: VIOLENCE

Question to answer	What to record in practice	Applied to the sample NCII case	Threshold indicators	Indicative classification
Is violence threatened, endorsed, or encouraged?	Identify whether violence is explicitly or implicitly advocated, endorsed, or facilitated.	The case implicitly or explicitly calls for violence, on the basis of gender, gender identity, sexual orientation, or based on being a perceived enemy (like feminists). Previous posting behavior may help to assess intent.	Explicit threats; incitement to violence; praise or endorsement of violent acts; calls for rape, femicide or mass-violence; or operational steps that enable offline harm (e.g. doxxing real-world locations)	Critical for determining whether targeted hate or violent extremism thresholds are met.

STEP 7: TARGETED HATE & VIOLENCE THRESHOLD

Question to answer	What to record in practice	Applied to the sample NCII case	Threshold indicators	Indicative classification
Does this meet the criteria for targeted hate and violence (TH&V)?	Apply TH&V definitional criteria to the facts of the case.	The case may meet the TH&V threshold where all three criteria are present: 1. identity-based dehumanization (targeting women, LGBTQI+), 2. advocacy or endorsement of violence, and 3. tolerance of, support for, or calls for violence against civilians.	Clear gender-based dehumanization combined with explicit endorsement or advocacy of violence, where targeting is framed as legitimate "punishment," exclusion, or removal from public life.	TFGBV + TH&V where all three criteria are satisfied.

18 It is important to note that TFGBV is overwhelmingly perpetrated by individuals known to victim-survivors, most often current or former intimate partners. While this toolkit focuses on the intersection of TFGBV and extremism — where such dynamics may be less prevalent — it nevertheless acknowledges and reflects this broader context.

STEP 8: VIOLENT EXTREMISM THRESHOLD

Question to answer	What to record in practice	→	Applied to the sample NCII case	Threshold indicators	Indicative classification
Does this meet the criteria for violent extremism (VE)?	Apply violent extremism definitional criteria to the facts of the case.		The case may meet the VE threshold where all three criteria are present: 1. a clear ideological or political aim (e.g. a male-supremacist project to exclude women from civic or political life); 2. advocacy, justification, or facilitation of violence to realize that aim; and 3. tolerance of, support for, or calls for violence against civilians or critical civilian infrastructure.	Explicit extremist ideology; explicit advocacy or endorsement of violence linked to ideological aims; evidence of networked mobilization or recruitment; or attacks intended to undermine democratic participation or civic institutions.	TFGBV + VE only where all violent extremism criteria are clearly met.

STEP 9: OUTCOME STATEMENT

Question to answer	What to record in practice	→	Applied to the sample NCII case	Threshold indicators	Indicative classification
What is the appropriate classification?	Provide a conclusion based on the evidence assessed in the preceding steps.		TFGBV is clearly established (Intimate Image Abuse). Targeted hate and violence are likely where rhetoric is identity-based and supports or endorses violence. Violent extremism is possible but is dependent on meeting TH&V, and the available evidence.	Classification depends on the combined interaction of intent, ideology, violence, perpetrator, and coordination, rather than any single factor in isolation.	Final classification is determined by the evidence collected and assessed across Steps 3–8.

THE ABOVE EXAMPLE might be of particular use to civil society practitioners, such as survivor-focused organizations. This may help them assess when IIA is illegal based on its content in a particular jurisdiction (for example in the UK, and recent proposals in Canada). However, it may also inform survivors about whether their case also meets the threshold of targeted hate. This may lead to additional legal charges based on relevant legislation protecting sexual orientation, or gender identity. This could further support accountability and the removal of the material.

3

Applying the Taxonomy Across Sectors

In this section

The toolkit can serve as a practical tool for informing response efforts across a broad range of sectors. This section outlines practical considerations for the broad range of sectoral responses to this spectrum of harms, including legal or regulatory responses; platform enforcement or safety-by-design; prevention and interventions; as well as research, monitoring and policy advocacy.

3Ⓐ

Government, Regulation & Legal

Actors across government, regulation, and law shape the legal, regulatory and protective environments in which responses to TFGBV, targeted hate and violence, and violent extremism operate. Responses in this sector must be grounded in the protection of fundamental rights, including freedom of expression, bodily autonomy, and the political participation and self-determination of women and marginalized communities.

They can use the taxonomy to support consistent, rights-respecting interpretation and decision-making across policy, regulation, and enforcement, particularly where gendered harms cut across multiple legal and institutional frameworks.

Policymakers

The intersection of TFGBV, misogyny, targeted hate, and violent extremism involves many different government departments, with responsibility spanning justice, gender equality, online safety, counter-extremism, health, education, and public safety. This requires joined-up policy development and reduces fragmented responses, as well as to understand misogyny and TFGBV across its full spectrum, rather than treating these harms only at their most extreme or isolated manifestations.

Policymakers can use the taxonomy to:

- Apply shared definitions that link TFGBV, hate crime, and violent extremism in a coherent way.
- Recognize misogyny as:
  - a standalone form of gender-based harm,
  - a driver of targeted hate, and
  - in some cases, a form of violent male-supremacist extremism.
- Identify gaps in existing legislation, including where intimate image abuse, online impersonation, account access control, or hate crime and political violence statutes lack a gendered perspective.
- Clarify roles and responsibilities across government portfolios, including where harms require prevention, regulation, or enforcement responses.
- Design coordinated responses between health, justice, digital and security ministries, including targeted support for women and LGBTQI+ public figures using the taxonomy's target categories.

The table below is designed as a practical decision-support tool for policymakers. It provides a structured set of questions showing how the taxonomy could be used to assess real-world challenges, policy gaps and systemic risks related to TFGBV, targeted hate and violent extremism.

GUIDING QUESTIONS FOR POLICYMAKERS

A. Classify the Harm	B. Identify Legal / Policy Thresholds	C. Evaluate Systemic / Contextual Risks
For example, are women/ LGBTQI+ public figures being politically targeted?	Are existing laws adequate for intimate image abuse, deepfakes, impersonation, hate speech? Are gendered political harms recognized in hate crime or VE statutes? Does misogyny or TFGBV meet the threshold for extremism in policy frameworks?	Is misogyny acting as an extremist ideology or recruitment driver? Are attacks part of organized political silencing of women/ LGBTQI+ people? Are extremist or male-supremacist networks mobilizing online?
D. Assess Threshold Potential	**E. Determine Response / Enforcement Actions**	**F. Cross-Sector / Multi-Agency Coordination**
Does TFGBV also constitute targeted hate or VE under the taxonomy's thresholds? Are specific user groups at elevated risk (politicians, journalists)?	Update or introduce legislation (deepfake, impersonation, political harassment). Recognize misogyny as extremism or a hate crime where appropriate.	Coordinate across gender, justice, digital, education, health, and security ministries. Support holistic national strategies on GBV, online safety, hate crime, and violent extremism.

Online Safety Regulators

Regulatory remits vary across jurisdictions. Some authorities only oversee large social media platforms, while others cover a wider range of services, including smaller platforms, pornography sites, dating apps, gaming platforms, and decentralized or emerging services. The following takeaways are intended to be applicable across these different regulatory models. By clarifying how misogynistic harms may also fall within hate speech or violent extremism frameworks, it highlights additional legal and regulatory levers beyond TFGBV-specific provisions and supports more proportionate and targeted enforcement decisions.

Regulators can use the taxonomy to:

- Clarify which laws apply across TFGBV, hate speech / targeted hate, and violent extremism for different types of content and behavior and use them to hold platforms to account.
- Shape regulatory guidance for platforms, including duties of care, safety-by-design measures and risk-mitigation requirements.
- Identify legislative gaps where harms are not yet covered. For example, Ofcom's VAWG guidance commits to evaluating gaps in the Online Safety Act based on an assessment of a platform's efficacy in responding to gender-based harms.
- Inform transparency reporting categories so that TFGBV, targeted hate and VE-relevant content can be tracked and responded to more accurately.
- Map the online misogyny and TFGBV threat landscape and identify which harms meet regulatory thresholds for enforcement.

This table is designed to support regulatory assessment, oversight, and enforcement in cases involving TFGBV, targeted hate, and violent extremism.

GUIDING QUESTIONS FOR REGULATORS

A. Classify the Harm	B. Identify Legal / Policy Thresholds	C. Evaluate Systemic / Contextual Risks
Did the platform correctly classify TFGBV, hate, or VE? Was the case triaged as "harassment" when hate speech/ VE criteria apply? Are multiple harm categories present?	Which legal frameworks apply (TFGBV, hate speech, VE)? Does the content meet statutory definitions for hate or violent extremist material? Are there gaps in legislation that limit enforcement?	Are platforms failing systematically (slow gendered hate speech removal)? Are victim-survivors provided resources if harm is identified or reported? Are coordinated inauthentic networks driving this hate speech?
D. Assess Threshold Potential	**E. Determine Response / Enforcement Actions**	**F. Cross-Sector / Multi-Agency Coordination**
Does the case require escalation to national security regulators? Is cross-platform coordination present? Should platforms treat the actor under extremist-content rules?	Issue corrective notices or penalties for misclassification. Require stronger platform detection systems and safety-by-design features. Mandate accurate transparency reporting (e.g., VE-relevant cases).	Collaborate with policymakers to close legislative gaps. Consult civil society and researchers on emerging harms. Coordinate with law enforcement on extremist or illegal activity.

Law Enforcement

Law enforcement support risk assessment, investigation, referral, and prosecution, particularly where misogyny or engaging in TFGBV may function as a warning sign or pathway toward continued, other forms of violence. This requires an additional understanding of behaviors, intent, and perpetrator profiles, and strengthen investigations and prosecutions by clarifying when ideological motivation is present and how it relates to the harms under investigation.

Law enforcement also support violence prevention by helping recognize when misogyny, TFGBV and gender-based violence may act as a warning sign or risk factor

for other forms of violence, including violent extremism. Where TFGBV is reported, law enforcement should ensure investigations are linked to appropriate survivor support services, helping to mainstream those referral pathways and ensuring survivors are directed to relevant resources alongside any criminal or investigative process.

Murad Code provides a voluntary, internationally grounded set of minimum standards for the safe, ethical, and survivor-centered gathering and use of survivor information in the context of documentation, investigation, and prosecution.

Sexual Extortion

Sexual extortion may involve nihilistic or accelerationist online violent subcultures and networks, including Com/764 and related communities (e.g. 764, No Lives Matter, Maniac Murder Cult).

Law enforcement can use the taxonomy to:

- Apply legal frameworks consistently and deliver proportionate, evidence-led enforcement. This supports clearer distinctions between harmful, hateful, and criminal behaviors, helping address current inconsistencies in enforcing offences related to misogyny and abuse targeting women and LGBTQI+ people. This will require appropriate training, checks and balances to ensure effective legal responses, and improved evidence on the changing online threat landscape.
- Understand the steps between engaging in misogynistic spaces, targeting women and LGBTQI+ people, and involvement in extremist activity, enabling clearer identification of when behavior crosses legal thresholds.
- Distinguish harmful, hateful, criminal and extremist behaviors, and identify indicators of hate crime and violent extremist motivation, ensuring that cases are pursued under the correct legal powers.
- Interpret relevant context (perpetrator history, coordination, target identity, use of violence, ideological framing) when assessing risk and support more accurate legal classification of offences.
- Analyze a suspect's online networks and trajectory, and decide when to refer cases to cybercrime, hate crime, GBV or counter-extremism/national security units, ensuring they are placed within the right teams to apply the appropriate legal tools.
- Support prosecutions by evidencing ideological motivation and consider the additional risk, such as politicians or journalists

3Ⓑ

Civil Society & Research

Across the civil society and research sectors, the taxonomy offers a common framework for analyzing and documenting gendered online harms. For researchers, the taxonomy supports rigorous study design and data collection that allows them to inform evidence-based policy; for civil society, it strengthens documentation, reporting, and advocacy. Across both groups, the taxonomy can improve coordination with policymakers, regulators, and platforms by offering a common language for understanding and responding to gendered online harms.

Researchers and academia

Researchers and academia require a shared analytical and conceptual framework for studying TFGBV, misogyny, targeted hate, and violent extremism. This includes methodological consistency, comparability across contexts, and stronger evidence-building on the relationships between identity-based hate and violent extremist ideologies.

Researchers and academia can use the taxonomy to:

- Develop coding frameworks for qualitative, quantitative, and computational studies using consistent harm categories.
- Build annotated datasets for NLP models, detection tools, and network analysis grounded in the specific harms outlined in the taxonomy. Project Catalyst Consortium partner Meedan are demonstrating this through their use of the Harms Taxonomy for annotation guidelines for their classifiers.
- Identify patterns of misogyny, targeted hate, and VE using shared definitions and thresholds.
- Compare harms across jurisdictions or platforms using standardized terminology.
- Generate evidence to inform wider multi-stakeholder work, such as policy development, regulatory guidance, and civil society interventions.

Civil society organizations

Civil society plays a critical intermediary role between affected communities, platforms, regulators, and policymakers. They require support to document, escalate, advocate, and coordinate, recognizing that responsibility for addressing these harms should not rest with civil society alone.

Civil society can use the taxonomy to:

- Identify risk profiles or indicators of targeted hate or violent extremism affecting specific communities, for example that they represent or engage closely with.
- Train activists, journalists, and community groups using an accessible and evidence-based harms framework.
- Escalate incidents to platforms or regulators using clearly granular harm labels.
- Submit structured evidence to policymakers or law enforcement, highlighting where current frameworks fail to capture TFGBV, targeted hate, or VE and use the taxonomy to advocate for legal and policy reforms addressing gaps in protection against gendered online harms.
- Draw on the shared vocabulary to hold governments and regulators accountable for proportionate content moderation, ensuring that enforcement distinguishes between TFGBV, targeted hate, and VE in ways that protect fundamental rights, including freedom of expression.
- Inform targeted online interventions aimed at shifting the center of gravity of communities subject to misogynistic normative shifts.

GUIDING QUESTIONS FOR CIVIL SOCIETY

A. Identify the Harm

Which TFGBV super type is involved (harassment, IIA, impersonation, sexual extortion, account access control)?

Is the target a woman, LGBTQI+ person, feminist, journalist, activist, or organization?

Are multiple harm types occurring simultaneously?

B. Apply Thresholding

Does the case meet TFGBV criteria under the taxonomy?

Is there evidence of ideological motivation and advocacy or justification of violence?

Does the case span beyond TFGBV (e.g. regulator or law enforcement)?

C. Identify Patterns & Context

Are similar harms affecting multiple individuals or groups?

Is harassment coordinated, networked, or cross-platform?

Are attacks timed around civic, political, or advocacy moments?

Are women/LGBTQI+ communities framed as ideological enemies?

D. Documentation & Evidence

Is evidence recorded using harm labels?

Are screenshots, URLs, timestamps, and escalation records preserved?

Is survivor consent and safety prioritized?

Is documentation suitable for platform, regulator, or LE escalation?

E. Escalation & Advocacy Actions

Escalate cases to platforms using taxonomy terminology.

Submit structured evidence to regulators or policymakers.

Highlight gaps in legal or policy protections (e.g. impersonation).

Support strategic advocacy or complaints processes.

F. Community Support & Training

Train activists, journalists, and community members using the taxonomy.

Build shared understanding of TFGBV, targeted hate, and VE distinctions.

Support community resilience and safe reporting practices.

Frontline & Prevention Practitioners

Practitioners in prevention, safeguarding, and community-based roles design and deliver prevention interventions, support victims and survivors, document harms, advocate for systemic change, and strengthen community resilience. This crucial sector can use the taxonomy to interpret harms through a gendered and intersectional lens, understand the community-level consequences of TFGBV, targeted hate, and violent extremism, and develop consistent language for training, advocacy, and casework. By clarifying how misogyny appears as a risk factor, a warning sign, and at times a form of extremism in itself, the taxonomy can support early intervention, safer referral pathways, and more effective prevention programs.

Violence prevention practitioners

Violence prevention experts including social workers, psychologists, public health professionals, and school-based practitioners work to identify early behavioral indicators, map pathways between TFGBV, hate, and violent extremism, and design upstream interventions grounded in a public health approach. By distinguishing between systemic forms of TFGBV and more targeted or violent extremist manifestations, practitioners would be supported in determining whether prevention efforts should be primary (addressing broad social norms and reducing population-level risk), secondary (targeting individuals showing early signs of harmful engagement), or tertiary (responding to high-risk behavior or imminent harm).

Violence prevention practitioners can use the taxonomy to:

- Identify early-stage engagement with harmful online spaces (e.g. Manosphere forums, incel communities, 764/ nihilistic groups) to guide secondary prevention responses.
- Recognize behavioral signals such as violent misogynistic rhetoric, hostility, coercion, and dehumanizing language – helping determine when risk is escalating from secondary towards tertiary prevention needs.
- Map risk trajectories and determine when to escalate concerns or refer to relevant support or safeguarding services.
- Design youth, school-based, or community programs on healthy masculinities, gender equality, digital literacy, and critical thinking, forming part of primary prevention to tackle the spectrum of harms associated with TFGBV.

This table is designed to support early identification, risk assessment, and prevention decision-making in cases involving TFGBV, targeted hate, and pathways toward violent extremism.

GUIDING QUESTIONS FOR VIOLENCE PREVENTION PRACTITIONERS

A. Identify the Harm	B. Identify Early-Stage Risk Indicators	C. Identify Motivations
Which super type is involved (harassment? IIA? impersonation?) Is the target a woman/LGBTQI+ individual? Is the behavior sexually exploitative, coercive, or humiliating?	Hostile or dehumanizing attitudes toward women/LGBTQI+ groups. Interest in misogynistic or male-supremacist online spaces. Sharing extremist or violent memes, videos, or narratives Reclaiming NCII or threats as “deserved” or “punishment.” Fixation on gender-based power, dominance, or entitlement.	Silencing or punishing behavior? Justification for violence? Identity-based hostility?

D. Assess Threshold Potential	E. Community-Level Considerations
Are there explicit threats? Is the individual connecting with extremist communities? Is violence being justified as necessary or deserved? Is harassment targeting women in civic/political roles?	Are similar harms affecting multiple individuals? Are online communities coordinating harassment? Does the behavior reflect broader misogynistic norms?

Women's, LGBTQI+, & TFGBV organizations

Organizations working with women, LGBTQI+ people, and other targeted groups are often at the forefront when tackling misogyny and TFGBV and advocating for meaningful policy and legal change. Systematized terminology for documenting gendered, sexualized, and identity-based harms may support them in doing so.

Organizations in this sector can use the taxonomy to:

- Classify and record digital harms using consistent terminology that reflects the spectrum of abuse.
- Identify when survivors are targeted because of identity, activism, or public roles.
- Recognize risk indicators for targeted hate or violent extremism to increase avenues for legal escalation.
- Highlight community-wide harms such as fear, withdrawal from public participation, and normalization of violence.
- Strengthen advocacy for legal reform, improved platform responses, and broader public protection.

Survivor support services

Survivor support services are often leading gender-based violence prevention efforts and involved in tertiary prevention in a public health model. When reporting harm to platforms, law enforcement, and regulators, clearer language for survivor support services may support structured case documentation and advocacy.

Survivor support services can use the taxonomy to:

- Support survivors by clearly classifying harms across TFGBV and targeted hate, with the option to identify potential VE-relevant elements when they arise.
- Understand the different forms of TFGBV more granularly - and specifically different forms of 'violence' which is understood in a distinct way across these harms - helping practitioners identify how online and offline harms interact within broader patterns of abuse.
- Identify when harm may amount to hate crime or involve elements of targeted or ideological punishment.
- Document cases in a structured, comparable way for legal, regulatory, or advocacy purposes.
- Provide survivors with precise terminology for platform complaints, legal proceedings, and referral processes.
- Escalate cases to platforms, regulators, or law enforcement using accurate harm labels.
- Advocate for legal and policy reform around hate crime, extremist misogyny, and online safety frameworks.

3C Platforms & Industry

Tech platforms, including trust and safety teams, product teams, as well as multistakeholder industry coalitions, play a central role in detecting, enforcing, and mitigating online harms. Tech platforms need clear, consistent frameworks to distinguish between gender-based abuse, targeted hate, and violent extremism in order to guide policy development, moderation decisions, detection models, and product design. Greater clarity on how misogynistic behavior moves from harassment to targeted hate or violent extremism supports more accurate classification and triage, more coherent cross-policy enforcement, and stronger coordination with regulators and civil society partners.

Tech platforms can use the taxonomy to:

- Develop and adjust platform policies to reflect the versatile nature of misogyny and TFGBV, ensuring harms are assessed across all relevant policy areas (examples including hate speech, violent extremism and terrorism or dangerous organizations and individuals lists, threats, violence and harm, harassment and bullying, and sexual abuse).
- Apply taxonomy-based thresholds to guide moderation workflows, including case triage and escalation across harassment, hate, and extremism teams.
- Apply the taxonomy to bridge traditionally siloed harm categories — such as gendered harassment and violent extremism — by foregrounding the ways these harms intersect and reinforce one another. This provides a practical framework for hybrid harm responses.
- Enhance reporting mechanisms by mapping taxonomy categories to user reporting flows (e.g., online harassment, hate, impersonation, VE-related harms).
- Translate taxonomy harms into detection signals, classifier training data, and risk-modeling inputs.
- Identify contextual indicators such as targeting of women or LGBTQI+ public figures, coordinated networked abuse, or cross-platform mobilization.
- Incorporate taxonomy categories into safety-by-design approaches to reduce coordinated gendered harms (e.g., doxxing, impersonation, deepfakes).
- Improve cross-platform coordination by using shared harm definitions and recognizing multi-platform patterns of abuse.
- Strengthen transparency reporting by classifying harms consistently across TFGBV, hate, and violent extremism. This should be accompanied by improved data access for researchers in order for TFGBV to be more adequately measured on platforms, as well as be better held to account when it comes to content moderation and human rights, including over-removal and subsequent consequences for freedom of expression.
- Recognize male-supremacist extremism and gendered hate mobilization as enforceable categories under existing policy frameworks, such as hate speech, violent extremism or dangerous organizations and individuals.

This table is designed to support consistent, context-aware decision-making by platforms when assessing, moderating, and responding to cases involving TFGBV, targeted hate, and violent extremism.

GUIDING QUESTIONS FOR PLATFORMS

A. Identify the Harm	B. Check for Contextual Signals	C. Threshold Assessment
Is the behavior harassment, impersonation, intimate image abuse, sexual extortion, or account compromise? Is the behavior sexualized or gender-related? Is a public figure user targeted?	Is the target a woman or LGBTQI+ person? Is the harassment coordinated or networked? Does the perpetrator reference male-supremacist or anti-LGBTQI+ narratives? Are there offline safety risks (doxing, threats, stalking)?	How does this case fall across TFGBV, TH&V, and VE criteria?
D. Enforcement Questions	**E. Systemic Risk Assessment**	**F. Required Actions**
Are there gaps in existing policies? Does this require policy review? Should evidence be preserved for law enforcement?	Is the case part of a broader pattern or community-wide attack? Are cross-platform networks or extremist communities involved? Is this targeting a protected group in a way that indicates structural or ongoing abuse?	Apply account actions (warnings, suspensions, removals). Take appropriate content moderation action. Hash and block future re-uploads. Notify or support targeted user. Escalate to threat intelligence, extremism, or specialized review teams. Strengthen detection models where gaps are identified.

4

Legal Dimensions and Best Practices

Legal and policy frameworks and best practice in responding to the spectrum of harms

In this section

This legal analysis translates the harms taxonomy into practical guidance on applying existing laws and policy frameworks to misogyny across a continuum of violence from TFGBV to targeted hate and violent extremism. With a focus on Project Catalyst priority geographies - Canada, Jordan, and Kenya - this section outlines how different legal systems recognize, categorize and respond to these harms, as well as where approaches might be falling short.

To support practical application, this section also draws on best practice from the European Union and the United Kingdom, illustrating how different jurisdictions have sought to respond to similar harms through online safety regulation, platform accountability measures, and victim-centered legal reforms. These are intended to provide examples of different policy approaches, rather than to hold up any single model as a gold standard.

Summary of Relevant Legislation and Application to the Continuum of Harm

The following table summarizes the legality of the main harm types in the jurisdictions of focus, namely Canada, Jordan, and Kenya.

HARM TYPES	CANADA	JORDAN	KENYA
Online Harassment	Captured in Criminal Code. However, not all sub-harms, for example doxxing is not an offence in itself.	Whereas online harassment is not explicitly mentioned, some sub-harms - such as doxxing – may be covered by Cybercrime Law No.17 of 2023, and Personal Data Protection Law.	Captured in Penal Code and The Computer Misuse and Cybercrimes Act (CMCA).
Intimate Image Abuse	Non-consensual intimate image abuse (NCII) and voyeurism in the Criminal Code, and strengthened in the proposed Protecting Victims Act (PVA).	Cybercrime Law No.17 and when in a family context, the Domestic Violence Law (2017).	The Penal Code and The Computer Misuse and Cybercrimes Act (CMCA).
Online Impersonation	Included as identity fraud in the Criminal Code.	Cybercrime Law No.17 of 2023, and the Personal Data Protection Law.	Penal Code and The Computer Misuse and Cybercrimes Act (CMCA)
Sexual Extortion	Included in the criminal code, with mentions in specific NCII offences. Proposed Online Harms Bill likely to further address this.	Explicitly mentioned in the Cybercrime Law No.17 of 2023, as well as applies to the Penal Code.	Included in Penal Code and The Computer Misuse and Cybercrimes Act (CMCA).
Account Access Control	Captured under criminal code.	Explicitly cited in the Cybercrime Law No.17 of 2023.	Included in Penal Code and The Computer Misuse and Cybercrimes Act (CMCA).
(Gender-Based) Targeted Hate	Gender identity and expression, and sexual orientation, captured in Canadian Human Rights Act (1985).	Race, language, and religion protected in the National Constitution. Gender equality is mentioned in the Labor Law.	Discrimination against marginalized and vulnerable groups and sex-based discrimination is prohibited in the Constitution. Ethnicity-based hate speech, The National Cohesion and Integration Act.
Violent Extremist / Terrorist Content	Terrorist propaganda captured under the Criminal Code, Anti-Terrorism Act, and proposed Online Harms Bill.	Rooted in Anti-Terrorism Act 2006.	Prevention of Terrorism Act, 2012 focused on incitement, promotion, and radicalization, also Computer Misuse and Cybercrimes Act, 2018.

The following section contains a detailed description of relevant legislation and policy frameworks in the focus jurisdictions, providing more context to the summary table above.

Canada Legal Frameworks

OVERVIEW

Research shows that women and girls disproportionately experience the most severe forms of intimate partner violence and sexual violence. Women are more likely to be killed by an intimate partner than by any other type of perpetrator in Canada.

In Canada, 95% of frontline workers reported working with a survivor who disclosed experiencing TFGBV. Harassment, threats, and tracking are the most common forms of violence.

In 2018, women were also more likely than men to report having experienced unwanted behaviors online that were sexual in nature, such as receiving unwanted sexually suggestive or explicit images or messages, or being pressured to send, share or post sexually suggestive or explicit images or messages.

Canada has two key frameworks when it comes to addressing gender-based violence: Canada's Strategy to Prevent and Address Gender-Based Violence (2017) and the National Action Plan to End Gender-Based Violence (2022). The latter seeks to engage all people in Canada in challenging the social norms, attitudes and behaviors that contribute to GBV, as well as the socio-economic factors that underpin it. It also recognizes the need for culturally appropriate and accessible protection services, and for improvements in the health, socio-economic and justice outcomes of those affected by GBV. These aims have led to significant investment in initiatives designed to address GBV and TFGBV.

However, as in many other jurisdictions, there is currently no legislation in Canada specifically targeting tech-facilitated GBV. Instead, such cases are typically prosecuted under the Criminal Code (1985)[19], which has undergone relevant amendments in recent years. These revisions increasingly recognize how certain offences disproportionately affect specific genders and reflect the growing cyber dimension of criminal activity.

TFGBV encompasses a wide range of behaviors, which can broadly be divided into two categories covered by the Criminal Code: harassment (including stalking, spying and threats) and image-based abuse (including voyeurism, the non-consensual distribution of intimate images and other forms of image exploitation). The Criminal Code also provides legal recourse for individuals seeking to bring cases of defamation, which may in some instances be related to TFGBV.

In December 2025, the Government of Canada announced the introduction of the **Protecting Victims Act**, to reform the Criminal Code. This legislation proposes to classify murders driven by hate or that occur alongside controlling or coercive behavior of an intimate partner, sexual violence or exploitation as first-degree murder. The proposed legislation would criminalize coercive control to facilitate intervention before intimate partner violence turns lethal.[20] It would also strengthen the prohibition on distribution of non-consensual sexual deepfakes, increase penalties for the distribution of intimate images without consent, and prohibit threats to distribute such images. It proposes to increase penalties for sexual crimes, including voyeurism, sexual assault, indecent exposure, non-consensual distribution of intimate images (including sexual deepfakes), and obtaining sexual services from a child. This proposed legislation would strengthen the illegality of the harms included in the continuum of violence outlined in this toolkit.

19 Consolidated in 1985 with the last update occurring in 2025.

20 Abuse often escalates through patterns of control long before physical violence occurs. A new offence would target patterns of coercive or controlling behavior, giving the justice system the tools to intervene before violence escalates.

PROVINCIAL "ANTI-SLAPP' LEGISLATION

However, Provincial "anti-SLAPP" (Strategic Lawsuits Against Public Participation) legislation exists in British Columbia, Ontario, and Québec. British Columbia's legislation is called the **Protection of Public Participation Act** (PPPA) (2019) while Ontario has its own equivalent legislation intended to protect citizens from lawsuits designed to silence speech on matters of public importance. Whereas such laws clearly have an important use case, such measures may inadvertently limit access to defamation proceedings, potentially contributing to a chilling effect for those targeted by (TF)GBV.

Beyond the **Criminal Code**, Canadians may seek redress under the C**anadian Human Rights Act** (1985), which includes gender identity and expression among its prohibited grounds of discrimination, thereby encompassing TFGBV-related cases.

Further protections are provided under more specific laws, such as the Act to amend the Criminal Code and the **Judges Act** (2023), which ensures that judges receive education and training on domestic violence and coercive control in intimate and family relationships. This legislation enhances the options available to TFGBV victims when perpetrators are intimate partners.

Similarly, the Act to amend the Divorce Act, the Family Orders and Agreements Enforcement Assistance Act and the Garnishment, Attachment and Pension Diversion Act (2019) acknowledges that women are more likely than men to experience gender-based violence, including sexual assault and intimate partner violence. It also recognizes that Indigenous women and gender-diverse individuals, such as transgender, queer and gender non-conforming people, are disproportionately affected by family violence. The legislation explicitly frames family violence as a form of violence against women and a manifestation of systemic gender-based discrimination, incorporating gender-sensitive language and recognizing the impact of intersecting identities on women's experiences of violence.

The Canadian Labour Code (2018), the Parliamentary Employment and Staff Relations Act and the Budget Implementation Act (2017) have collectively strengthened the framework for preventing harassment and violence, including sexual harassment and sexual violence, in the workplace. Consequently, these statutes may be invoked where TFGBV arises in employment contexts.

Recent amendments to An Act to amend certain Acts and to make certain consequential amendments (firearms) (2023) have further bolstered protections for victims of domestic and intimate partner violence, including the introduction of "red flag" laws addressing the role of firearms in GBV situations. While not specifically directed at TFGBV, these provisions may nonetheless apply in relevant cases.

Finally, the proposed Online Harms Act, intended to amend the Criminal Code, the Canadian Human Rights Act (2017) and other related statutes, sought to regulate online platforms and tackle various forms of harmful digital content. The proposed Online Harms Act, Bill C-63, follows two earlier failed attempts at online-harms legislation—Bill C-36, introduced in 2021 but scrapped amid public pushback and an election call, and a subsequent effort that stalled after extensive 2022–23 consultations and did not advance before the last election—before finally being tabled as the new Online Harms Act in February 2024.

EXAMPLE

In 2018 Alek Minassian murdered 10 people in Toronto, eight of which were women. Before his attack, Minassian posted to Facebook stating his allegiance to the incel rebellion and Elliot Rodger, the perpetrator of the Isla Vista attack in California in 2014. This attack was not prosecuted as terrorism and has been labeled as "isolated incident". Following this, another attack in Toronto inspired by Alek Minassian on a massage parlour in 2020, was deemed an act of terror inspired by the incel movement. This marks the first instance in which an incel-inspired attack was deemed an Act of terror globally.

In Canada, the Anti-Terrorism Act (ATA) (2001) provided amendments to various Canadian statutes, including the **Criminal Code and the Security of Information Act**. The amendments were designed, among others, to define "terrorist activity"; create a process for listing an entity that, upon listing, becomes defined as a terrorist group; create new terrorism offences; and to create stronger laws against hate crimes and propaganda. A terrorist designation listing provides an indicator for service providers to remove an entity's online presence on social media and other associated online platforms. **The Criminal Code** defines terrorism as an act committed "in whole or in part for a political, religious or ideological purpose, objective or cause" with the intention of intimidating the public "...with regard to its security, including its economic security, or compelling a person, a government or a domestic or an international organization to do or to refrain from doing any act."

The 2018 National Strategy on Countering Radicalization to Violence summarizes Canada's approach to countering terrorism and violent extremism, while Canada's 2019 Digital Charter outlines Canada's approach to internet technologies and the online space, in which the 9th principle addresses the issue of violent extremism and notes that the online space should be "free from hate and violent extremism."

PRACTICAL USE-CASE

This legal analysis can help survivors, advocates, and support services identify overlapping legal pathways when responding to online harassment. For example, in Canada, sustained online harassment directed at women may fall under criminal law provisions. Where that harassment also includes racialized abuse, additional protections related to discrimination or hate-based targeting may apply. Similarly, when women who are members of LGBTIQ+ communities are targeted through harassment referencing sexual orientation, gender identity, or expression, relevant human rights frameworks may also be engaged.

Highlighting how gendered harms intersect with race, sexuality, and other protected characteristics, can support more informed reporting, referral, and advocacy decisions. It helps ensure that the full context of harm is recognized, rather than directing survivors toward a single legal pathway that may not adequately capture their experience.

Jordan Legal Frameworks

OVERVIEW

Jordanian female journalists face threats such as extortion, doxxing, and harassment that often spill over into offline spaces. According to reports nearly 40% of women in the Arab States have experienced some form of violence, although the actual numbers are likely much higher. In the Arab States, a regional study found that 60% of female internet users in the region have been exposed to online violence in the past year.

Jordan's legal framework is increasingly regulating harmful online behavior in ways that impact both TFGBV and the prevention of violent extremism. The Cybercrime Law No. 17 of 2023 serves as the central instrument linking both. Its provisions regarding unauthorized access, impersonation, fabricated content, reputational harm, non-consensual sharing or manipulation of images, and the facilitation of sexual exploitation directly address these forms of gendered digital abuse. In addition, the Personal Data Protection Law may also be used, with implications for online impersonation or doxxing.

Several of these offences, particularly those related to misinformation, incitement, and false accounts, are routinely employed to monitor and restrict extremist propaganda, online recruitment, and coordinated disinformation that can support radicalization. While not specifically drafted for counter-terrorism purposes, this law provides practical tools to regulate online spaces where both TFGBV and extremist activities can occur.

Other previous statutes complement this framework. The Penal Code (1960) criminalizes sexual violence, grooming, defamation, and intrusion into private spaces, with provisions that now extend into digital contexts relevant to TFGBV. These offences may also intersect with some extremist behavior, as terrorist groups may utilize coercion, reputational threats, or sexual exploitation to recruit, intimidate, or control individuals.

The Anti-Human Trafficking Law (2009) enhances protections where online grooming or cross-border exploitation is linked to organized networks, some of which may overlap with violent extremism.

Additionally, confidentiality protections in the Telecommunications Law (1995) and procedural safeguards in the Protection from Domestic Violence Protection Law (2017) help address digital abuse within intimate relationships.

The Anti-Terrorism Law (2006)[21] remains Jordan's primary counterterrorism law, addressing online incitement, recruitment, and financing. Although it does not specifically address gender, extremist propaganda and online harassment weaponizing gendered narratives or targeting women activists and community leaders, may be relevant here.

21 Amended 2014; latest updates ongoing.

Thus, TFGBV and online extremism often coexist within the same digital ecosystems, and their underlying behaviors (coercion, manipulation, intimidation, and reputational harm) are regulated by overlapping legal provisions.

However, the laws have received some criticism regarding freedom of expression and how these laws may be misused. For example, Amnesty International, argue that Jordan's 2023 Cybercrime Law No. 17 features vague and overly broad terms such as "spreading fake news", "provoking strife", "threatening societal peace", and "online assassination of character", may enable the authorities to criminalize peaceful dissent and criticism.

In practice, Amnesty International points out that this law has led to the prosecution of numerous individuals, including journalists and activists, for voicing pro-Palestine views, criticizing government policies, or advocating for peaceful protests. Documented instances reveal that many individuals have been arrested without warrants or clear charges, interrogated without legal representation, and subjected to intimidation. Critics argue that this has resulted in a shrinking civic space and a pervasive climate of self-censorship, where many are reluctant to express their opinions online.[22]

22 Amnesty International: Jordan: New Cybercrimes Law Stifling Freedom of Expression One Year On. https://www.amnesty.org/en/latest/news/2024/08/jordan-new-cybercrimes-law-stifling-freedom-of-expression-one-year-on/

Kenya Legal Frameworks

OVERVIEW

In Kenya, Research by the National Crime Research Centre (NCRC) demonstrates a high prevalence of cyber harassment, publication of false information, unauthorised access (such as hacking), child pornography and wrongful distribution of obscene or intimate images. The Office of the Director of Public Prosecutions (ODPP) indicated that the most prevalent forms of TFGBV are online child sexual exploitation and abuse, cyber-bullying, non-consensual sharing of intimate images, cyber-stalking/harassment and hate speech. Women politicians have faced unprecedented levels of violence, harassment, intimidation, and backlash both online and offline apparently designed to discourage them from seeking office.[23] The threat of online arguments turning into offline violence is particularly concerning in Kenya, as the country experiences a high rate of femicides annually.

23 The Kenyan 2022 elections included violence against women as they campaigned for positions or showed support for candidates, where women suffered harassment, intimidation, backlash, and violence both offline and online. https://pollicy.org/wp-content/uploads/2023/05/Byte_Bullies_report.pdf?

While Kenya does not have specific TFGBV legislation, its legal frameworks are grounded in constitutional protections and statutes that can be applied to such harms. There are multiple Kenyan laws that address gender-based violence, though for the most part, online gender-based violence is not specifically addressed. The Constitution of Kenya (2010) provides the foundation which guarantees dignity, equality, freedom from discrimination, and access to justice and fair trial for all individuals. The Constitution specifically mandates protection for marginalized and vulnerable groups and sex-based discrimination is prohibited. The state bears a constitutional obligation to enact legislation that redresses historical disadvantages suffered by marginalized groups, including women.

REGIONAL AND GLOBAL TREATIES

Kenya's framework is further grounded in obligations under regional and global treaties including the International Covenant on Civil and Political Rights, the African Charter on Human and People's Rights, the Convention on the Rights of the Child, and the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), which enshrines freedom from discrimination; abolishment of discriminatory customs, practices and law; elimination of prejudices and stereotypes; suppression of trafficking, exploitation and prostitution; and equality before the law. In 2024, Kenya joined African jurisdictions adopting Digital and Social Media Guidelines by the Association of African Election Authorities. Kenya also signed the 2023 International Statement to Remove Online Child Sexual Abuse materials and adopted the African Union Child Online Safety and Empowerment Policy in 2024. In 2025, the Communications Authority of Kenya's (CA) Industry Guidelines for Child Online Protection and Safety entered into force, with a primary focus on safeguarding children's rights to access information and ensuring the safe use of ICT products. This includes that all ICT service providers align with local and international laws against CSAM.

The Penal Code (1930) contains general criminal provisions applicable to TFGBV cases, including prohibitions against incitement to violence, threats, intimidation, negligent acts that cause harm to another person, extortion. Because these provisions are expressed broadly, they can apply to incitement, threats, intimidation, and harm carried out online. This includes cyber-harassment, cyber-bullying, doxxing, non-consensual sharing of intimate images

and sexual extortion. Article 181 prohibits circulation of obscene media. These could apply to acts of online GBV, but the Penal Code does not explicitly state this nor is it clear the extent to which these offences apply online. It is important to note that Penal Code 162 criminalizes same-sex sexual activity and lacks protections for LGBTQI+ individuals.

The Sexual Offences Act (2006) prohibits sexual harassment, exploitation, and assault. Although it primarily addresses offline conduct and does not expressly regulate offences committed online, certain acts that constitute TFGBV crimes can nonetheless be inferred from its provisions.

Computer Misuse and Cybercrimes (2018) acts as the primary legislation addressing computer-systems related offences. The Act criminalizes unauthorized access[24], false publications[25], production, possession and dealing in child pornography and CSAM, cyber harassment, and wrongful distribution of obscene or intimate images.[26] However, critical gaps exist and terms like "obscene" and "intimate" remain undefined for the Penal Code and CMCA, leaving interpretation to case-by-case judicial determination. In November 2025, amendments to the Act expanded the National Computer and Cybercrimes Coordination Committee's authority to restrict access to websites containing prohibited content, including child exploitation material, terrorism content, and extreme religious practices. The amendments also broadened cyber harassment provisions to include conduct likely to cause suicide and extended phishing definitions to cover fraudulent calls.

Complementary laws provide additional potential avenues to address different forms of TFGBV. Additional protections can take place through the Data Protection Act (2019)[27], which outlaws non-consensual sharing of personal information applicable to image-based sexual abuse; the Children Act[28], which aims to protect minors from obscene materials and sexual exploitation; the Victim Protection Act (2014)[29]; the Employment Act (2008)[30]; the Protection Against Domestic Violence Act (2015)[31]; the Persons with Disabilities Act[32] and the Prohibition of Female Genital Mutilation Act.[33]

The National Cohesion and Integration Act (2008) penalizes hate speech, however, it exclusively focuses on ethnicity-based hate speech and does not include a focus on gender. The National Cohesion and Integration Bill (No. 74 of 2023) currently under consideration in the National Assembly, aims to address online hate speech, ethnic contempt, and digital disinformation. However, enforcement challenges exist, including requirements for complete video evidence and difficulties establishing source and provenance.

The Prevention of Terrorism Act (POTA) is Kenya's primary counter-terrorism framework, addressing radicalization, collection of information, publication of offending material, and prohibition from broadcasting. The Act[34] criminalizes acts supporting, promoting, or facilitating terrorism, including sharing terrorist content and images. The POTA does not define "terrorism", however, section 2 defines a "terrorist act".[35]

CIVIL SOCIETY CONCERNS

Civil society organizations have raised significant concerns about both the gaps in the legal framework and its misuse. This is enabled by vague definitions and expanding certain powers, as noted by Human Rights Watch that the 2025 CMCA amendments threaten online expression by expanding government powers that could suppress dissent and restrict online speech.

24 Sections 14 and 15 can be relied on where doxxing, cyber-surveillance, cyber-stalking and non-consensual sharing of intimate images are undertaken by accessing a survivor's computer and personal information or data therein, while Section 16 can be relied upon when the offensive act is undertaken by intercepting the survivors' computer and transmitting data therefrom. https://www.kictanet.or.ke/mdocs-posts/existing-legal-framework-in-kenya-addressing-technology-facilitated-gender-based-violence-a-report/

25 Section 22 of the CMCA prohibits publication of false, misleading or fictitious data that advocates hatred on the basis of, among others, sex or that maligns a person's reputation. Section 22 can be used to prosecute online defamation and cyber-bullying, while Section 23 can be used to prosecute online defamation, non-consensual sharing of intimate images and cyber-bullying and artificial-intelligence image-based sexual abuse. https://www.kictanet.or.ke/mdocs-posts/existing-legal-framework-in-kenya-addressing-technology-facilitated-gender-based-violence-a-report/

26 The CMCA empowers a criminal court to, upon conviction, award compensation to be paid by the convicted offender, recognizing the irreparable harm that is caused to survivors by TFGBV offences under the CMCA (including wrongful distribution of obscene or intimate images) especially where images, videos or information are widely circulated to third parties, courts are increasingly invoking Section 43 of the CMCA to award compensation to survivors. For example, in Republic v Kalmoi Shale Ahmed, the High Court of Kenya at Garissa, upon convicting the accused person for the offence of wrongful distribution of obscene or intimate images contrary to Section 37 of the CMCA, ordered him to compensate the victim KES 500,000 "for the pain and suffering and the damage to her dignity." https://www.kictanet.or.ke/understanding-technology-facilitated-gender-based-violence-tfgbv-in-kenya-legal-gaps-harmful-language-and-the-path-forward/?

27 This Act regulates the processing of personal data, and provides for the rights of data subjects, and the duties of data controllers and processors. It outlaws non-consensual sharing of personal information and can be extrapolated to address OGBV such as non-consensual distribution of intimate images. https://www.kictanet.or.ke/?mdocs-file=48843

28 The Act shields children against obscene materials and sexual exploitation, prostitution, incitement or pressure to engage in sexual behavior. https://www.kictanet.or.ke/?mdocs-file=48843

29 This Act protects victims of abuse of authority and criminality through protection of vulnerable victims. It defines injury as physical harm, emotional suffering, trauma, or pregnancy brought on by sexual assault. https://www.kictanet.or.ke/?mdocs-file=48843

30 This Act regulates employment and among other things, prohibits sexual harassment in the workplace. https://www.kictanet.or.ke/?mdocs-file=48843. The Employment Act protects workers from sexual harassment in the workplace, including online harassment, cyber-stalking, or digital threats from colleagues or supervisors. Employers must create a safe work environment, which includes addressing digital misconduct on work platforms (emails, messaging apps, virtual meetings).

31 The Act provides for protection from violence in domestic spaces. It defines violence to include defilement, maltreatment, and sexual violence

Implementation for the legislative frameworks that apply to TFGBV face significant systemic challenges. A general lack of public awareness about TFGBV laws and available legal remedies leads to low reporting rates, while the vague and ambiguous definitions of legal provisions makes it difficult for survivors, policymakers, and judicial officers to identify, report, investigate, or prosecute crimes effectively.

EXAMPLE

Although Kenya does not have specific a law that explicitly defines doxxing, existing laws prohibit it.

The Constitution protects the right to privacy and limits freedom of expression when it infringes on others' rights or reputations. The Computer Misuse and Cybercrimes Act criminalizes behaviors such as cyber harassment, identity theft, and impersonation, which can apply to doxxing-related conduct. The Data Protection Act also regulates the handling of personal data, indirectly addressing doxxing by restricting how personal information may be collected, used, or shared.

during marriage. https://www.kictanet.or.ke/?mdocs-file=48843

32 Protects individuals with disabilities from online exploitation or discrimination, who may be more vulnerable in digital spaces. Ensures accessible reporting mechanisms for victims of digital violence. Holds offenders accountable for using technology to target people based on their disability.

32 The Act aims to protect people from having their mental or bodily integrity violated through female genital mutilation (FGM) by prohibiting the practice.https://www.kictanet.or.ke/?mdocs-file=48843

34 The Prevention of Terrorism Act (Cap. 59B).

35 Section 2 defines a "terrorist act" as an act or threat of actions - a) which - i. involves the use of violence against a person; ii. endangers the life of a person, other than the person committing the action; iii. creates a serious risk to the health or safety of the public or a section of the public; iv. results in serious damage to property; v. involves the use of firearms or explosives; vi. involves the release of any dangerous, hazardous, toxic or radioactive substance or microbial or other biological agent or toxin into the environment; vii. interferes with an electronic system resulting in the disruption of the provision of communication, financial, transport or other essential services; viii. interferes or disrupts the provision of essential or emergency services; ix. prejudices national security or public safety; and b) which is carried out with the aim of - i. intimidating or causing fear amongst members of the public or a section of the public; or ii. intimidating or compelling the government or international organization to do or refrain from any act; or iii. destabilizing the religious, political, constitutional, economic or social institutions of a country, or an international organization. Provided that an act which disrupts any services and is committed in pursuance to a protest, demonstration or stoppage of work shall be deemed not to be a terrorist act within the meaning of this definition so long as the act is not intended to result in any harm referred to in paragraph (a) (i) to (iv)." (https://www.unodc.org/documents/terrorism/Publications/Kenya%20HR%20manual/Kenya_Manual_e-book.pdf)

4Ⓓ Approaches from Elsewhere: The European Union and the United Kingdom

The European Union's Directive (EU) 2024/1385 on combating violence against women and domestic violence represents a significant step forward in addressing technology-facilitated gender-based violence (TFGBV). Unlike many jurisdictions where digital gender-based-harms are addressed indirectly or through fragmented provisions, the Directive establishes a dedicated, gender-specific legal framework that explicitly recognizes the cyber environment as a central site of violence against women and girls.

Alongside this, the Directive can be used in conjunction with the Digital Services Act, which establishes binding obligations on online platforms to assess and mitigate systemic risks, including illegal content and gender-based harms, while strengthening transparency, user redress, and regulatory oversight. It provides a risk-based framework that complements criminal law by addressing how platform design and amplification can contribute to harms such as TFGBV, targeted hate, and extremist content.

Alongside Directive (EU) 2024/1385, the EU Terrorist Content Online (TCO) Regulation, in force since June 2021, is a key legal framework to consider where misogyny or TFGBV intersects with terrorist or extremist content. The TCO applies to hosting service providers that operate in or target EU Member States and requires the rapid removal of content that meets EU definitions of terrorism, as set out in the EU Combating Terrorism Directive.

Importantly, the TCO can apply to gendered extremist content, including misogynistic material, where it promotes, glorifies, or supports terrorist violence or actors. This means that certain forms of misogynistic propaganda, incel-related violence, or praise for attackers may fall within terrorism frameworks, even where they are also understood as TFGBV or hate-based harm.

APPLYING EU LAW AT THE INTERSECTION OF MISOGYNY AND VIOLENT EXTREMISM

In the EU, content that glorifies or promotes attackers such as Elliot Rodger—including manifestos, videos, memes, or praise framing his actions as justified or inspirational—may constitute terrorist content under the TCO Regulation. While such material is often discussed primarily in terms of online misogyny or TFGBV, its ideological framing, advocacy of violence, and potential to inspire further attacks can trigger terrorism-related obligations for platforms, including rapid removal and reporting.

In the UK the Online Safety Act (OSA) provides the core framework governing platform responsibilities. Its legally binding duties focus on illegal content and on protecting children, both of which capture many forms of TFGBV in practice. Ofcom is the regulator responsible for implementing and enforcing these duties, including through guidance and supervision. Recent Ofcom work on harms affecting women and girls has also emphasized systemic measures (e.g., recommender systems and coordinated abuse), though parts of the approach have been framed as guidance rather than automatically binding rules. However, they have also indicated that they will push for amendments to the OSA if they find platforms do not uphold these obligations in 2027.

A CASE-STUDY FROM THE UNITED KINGDOM ON MULTI-STAKEHOLDER COLLABORATION

The UK Online Safety Regulator, Ofcom, has set out new Guidance for tech platforms to take improved action against online harms targeting women and girls, including cyber-harassment, intimate image abuse, and stalking. Whereas the Guidance is voluntary, Ofcom has committed to making formal recommendations to the government on where the Online Safety Act (OSA), the UK's online regulation, may need to be strengthened if platforms fail to take foundational steps to ensure their systems do not promote misogynistic content. This shows how regulators might work with policymakers to close legislative gaps when it comes to countering online misogyny and various forms of TFGBV.

APPLYING UK LAW AT THE INTERSECTION OF TFGBV AND VIOLENT EXTREMISM

The Maniac Murder Cult (MMC) illustrates why analyzing TFGBV through a continuum-of-harms lens is essential for determining when gender-based online abuse can also be applied to terrorism and extremist legal frameworks.

MMC is a transnational, predominantly online white supremacist neo-Nazi network that the UK government proscribed in July 2025 on the basis that it commits and promotes acts of terrorism. Importantly for this toolkit, MMC has also been documented using sexual extortion as part of its operational tactics. These behaviors may initially appear as TFGBV, such as coercion, exploitation, or image-based abuse, but when examined through the taxonomy's indicators of perpetrator, intent, and targets, they can also meet the threshold for terrorism-related activity.

Applying the harms taxonomy makes it possible to distinguish when sexual extortion constitutes TFGBV alone, and when it also forms part of a terrorist ecosystem. In such cases, content may fall within the scope of terrorism offences and be treated as illegal terrorist content under the Online Safety Act, triggering stronger platform obligations and potential criminal enforcement.

This example shows the potential value of the toolkit: enabling actors such as law enforcement to move beyond surface-level categorization of harms and instead apply a context-specific, evidence-based analysis. By examining who is responsible, why the harm is being carried out, and how it is being used, practitioners can determine which legal and regulatory frameworks apply and ensure responses are both effective and proportionate.

4Ⓔ Best-Practice Considerations for Regulating the Spectrum of Gendered Online Harms

Drawing on the comparative legal analysis across Canada, Kenya, Jordan, and selected best-practice examples from the EU and UK, three cross-cutting considerations emerge for policy responses to TFGBV, targeted hate, and their intersection with violent extremism. These criteria are not intended as prescriptive models, but as practical considerations for policymakers assessing whether existing legal frameworks are fit for purpose.

The Harms Taxonomy and this Toolkit has focused on the continuum of TFGBV, targeted hate, and violent extremism. Through our stakeholder mapping and legal frameworks analysis across Canada, Jordan, and Kenya, we recognize that a multi-stakeholder, whole-of-government, and cross-regulatory approach is needed. This means using the right legislative frameworks for the right harms — whether TFGBV alone, TFGBV at its intersection with targeted hate, or TFGBV at its intersection with violent extremism — and drawing on GBV legislation, cyber safety and cybercrime frameworks, and counter-terrorism frameworks as appropriate. A key lesson from the jurisdictions reviewed is that where these harms are placed legislatively shapes how they are understood, resourced, and responded to. The most effective approaches combine these frameworks in a layered way, and this informs the policy principles set out below.

1. Gender-Responsive and Intersectional Legal Framing

Across the focus jurisdictions, there is growing recognition that women and girls are disproportionately targeted by gender-based abuse, including TFGBV. However, this recognition is not consistently reflected across criminal and cybercrime laws, particularly for harm types such as account access control and online impersonation, which are often treated as gender-neutral technical offences despite their gendered use and impact.

The EU Directive 2024/1385 represents a notable advancement by explicitly naming violence against women and girls in the cyber context and by criminalizing specific forms of online abuse, including cyber harassment and non-consensual intimate imagery. At the same time, the Directive has faced criticism for not fully addressing harms targeting LGBTQI+ communities, highlighting the limits of a women-only framing in capturing the full spectrum of gendered harm.

In the UK, while there is no standalone TFGBV statute, Ofcom's Violence Against Women and Girls guidance under the Online Safety Act adopts a more expansive understanding of gendered harm. It explicitly recognizes the distinct impacts of online abuse on women and girls, while also acknowledging the harms experienced by men and boys, particularly through exposure to misogynistic content. This approach offers a useful model for integrating gender awareness into regulatory practice without rigidly categorizing harms by victim group alone.

BEST-PRACTICE INSIGHT

Legal and regulatory frameworks are most effective when they explicitly recognize the gendered and intersectional nature of online harms, while remaining flexible enough to capture how the same harm types affect different groups in different ways. Legal and regulatory frameworks are also most effective when they take a survivor-centered approach.

2. Digitalization of Legislation

A second key distinction concerns whether legal frameworks are meaningfully adapted to the digital environment. Jordan and Kenya both have dedicated cybercrime legislation, which provides clearer pathways for addressing online harms in principle. However, limited enforcement and uneven application raise questions about operational capacity and the translation of law into practice.

Canada, by contrast, largely relies on extending existing criminal offences into the online sphere through the Criminal Code. While this approach has enabled the prosecution of cyber harassment, intimate image abuse, and related harms, it lacks a comprehensive, standalone framework for online safety and TFGBV, potentially limiting coherence and preventative action.

When it comes to terrorist and extremist content, all jurisdictions prohibit such material, but the legal thresholds differ significantly. Kenya places emphasis on radicalization and incitement, while Jordan applies broader definitions that might capture a wider range of online expression. The EU Terrorist Content Online Regulation (TCO) and the UK Online Safety Act (OSA) stand out for explicitly addressing the online dissemination of terrorist content, introducing clear procedural obligations for platforms and enabling faster removal mechanisms.

BEST-PRACTICE INSIGHT

Explicitly digitalized legal frameworks—particularly those that combine criminal law with platform regulation—provide clearer thresholds, stronger enforcement tools, and greater consistency in responding to online harms, including when TFGBV intersects with extremist activity.

3. Human Rights, Proportionality, and Risk of Over-Enforcement

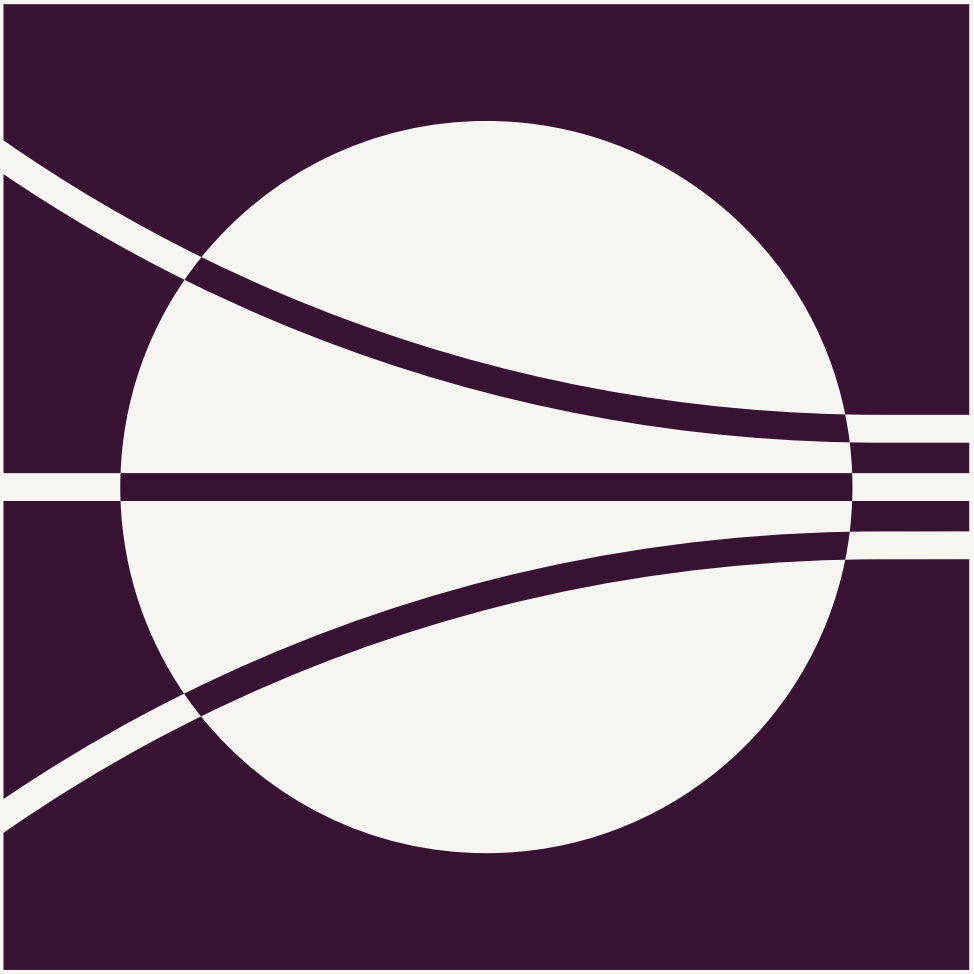
All jurisdictions examined above face ongoing challenges in balancing harm prevention with the protection of fundamental rights. In Jordan and Kenya, civil society organizations have raised concerns about broad or vague legal definitions—particularly around terrorism or morality—which risk being applied in ways that undermine freedom of expression and disproportionately affect marginalized groups.

At the same time, EU and UK online safety frameworks have also attracted criticism, particularly during their drafting phases, over the risk of over-removal of lawful content and the potentially chilling effect on political speech and minority voices. Canada has faced similar debates around hate speech regulation and freedom of expression, despite having less comprehensive online safety regulation. However, the DSA and OSA also has protections - a) via systemic risks to fundamental rights, and b) more directly, the various provisions around transparency (e.g. platform responses with a justification for takedowns) and the requirement to allow for appeals.

These tensions underscore the importance of proportionality, contextual assessment, and safeguards against misuse. The harms taxonomy in this toolkit is designed to support this balance by helping decision-makers distinguish between harmful but lawful content, illegal activity, and material that warrants escalation under hate crime or counter-terrorism frameworks.

BEST-PRACTICE INSIGHT

Rights-respecting regulation requires clear thresholds, contextual analysis, and procedural safeguards to prevent over-enforcement, while still enabling timely intervention where harms escalate or become coordinated and ideologically driven.



Amman | Berlin | London | Paris |
Toronto | Washington DC

ISD | Institute for Strategic Dialogue

CHRISTCHURCH CALL